SEGURIDAD®
EN AMÉRICA

Cuidando al sector turístico

Especial:
Seguridad en eventos deportivos
Soluciones contra incendio

Reportaje: Blindaje automotriz

Año 24 / No.140
Septiembre - Octubre

www.seguridadenamerica.com.mx

ArmorCarTech

BLINDAJE AUTOMOTRIZ

Ingeniería en blindaje de autos

Autos de lujo

Traslado mercancía

Traslado de valores

Táctico para uso policiaco

Manejamos todos los niveles

Antiasalto | Antisecuestro | Antiatentado

Tel. 5525-6310-37

www.armorcartech.com

Info@armorcartech.com

SEGURIDAD EN AMÉRICA

Año 24 / No. 140 / Septiembre - Octubre / 2023

Portada:
M360

Síguenos por

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

Representante en Perú
Gladys Grace Andrich Muñoz
Director Gerente, Nexo Consultores Internacionales
(+52) 511-221-0445 / Cel. +51-9999-75218
nexo@terra.com.pe

Representante en Uruguay
Diego Escobal, DSE
VEA Consultores en Seguridad,
(+5892) 3553-341 / (+598) 9919-4768
descobal@veaconsultores.com.uy

Representante en Ecuador
José Echeverría, CPP
Soluciones de Seguridad Corporativa

Representante en Panamá
Jaime Owens, CPP
+507-6618-7790
jowens.cpp@gmail.com

Representante en Israel
Samuel Yecutieli
+972-52-530-4379
yecutieli@segured.com

Representante en Chile
Alfredo Iturriaga, CPP
Vicepresidente Ejecutivo,
RacoWind Consultores Ltda
Tel. +56-2-871-1488 / +56-9-9158-2071

Representante en Costa Rica
César Tapia Guzmán, CPP, PCI, PSP
Socio Fundador de COOPESEGURIDAD SCS de Costa Rica RL.
Tel. +506 7010-7101

Apoyando a:

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

EDITORIAL

A sólo 10 días de las elecciones presidenciales anticipadas, Ecuador sufrió la trágica pérdida de uno de los aspirantes al cargo, en un acto de violencia que conmocionó al país.

De acuerdo con la BBC, el 9 de agosto el ex diputado ecuatoriano Fernando Villavicencio fue asesinado a tiros tras finalizar un acto de campaña en Quito. Recibió una ráfaga de disparos hacia las 18:20 hora local, al salir del colegio Anderson de la capital y abordar en un vehículo aún rodeado de escoltas.

Su fallecimiento fue confirmado y la Fiscalía de Ecuador informó que uno de los sospechosos del ataque también murió, después de haber resultado herido en el cruce de balas.

Villavicencio aseguraba que Ecuador se había convertido en un "narcoestado", proponía restablecer la seguridad con las fuerzas armadas y la policía en las calles, y paralelamente emprender una lucha contra lo que denominaba la "mafia política".

"Hoy Ecuador está tomado por el narcotráfico y también la mafia albanesa. Es decir, queda claro para América Latina, lo mismo que en Colombia y en México, que no es posible que el crimen organizado se instale en una sociedad y la someta sin el contubernio y la connivencia del poder político", dijo en una entrevista ofrecida en mayo al medio CNN en Español.

El apoyo a Villavicencio estaba al alza y los últimos sondeos lo colocaban en segundo lugar en las preferencias de los ciudadanos.

¿QUIÉN FUE VILLAVICENCIO?

Nació el 11 de octubre de 1963 en Sevilla, en la provincia de Chimborazo. Desde adolescente se vinculó a organizaciones sociales indígenas y de trabajadores. Según la biografía de la página web de su campaña, en 1999 fue líder sindical de la Federación de Trabajadores Petroleros (Fetrapec).

Estudío Periodismo y Comunicación Social en la Universidad Cooperativa de Colombia. Como periodista de investigación, colaboró con varios medios de comunicación ecuatorianos e internacionales, y también escribió 10 libros.

El suyo es el primer asesinato de un candidato presidencial registrado en Ecuador, y se produjo menos de un mes después de que Agustín Intriago, el alcalde de Manta, una ciudad portuaria clave para el crimen organizado, fuera asesinado durante una aparición pública.

Estimado lector, como siempre lo invitamos a reflexionar sobre lo que acontece en Latinoamérica en materia de seguridad. ¿Usted considera que la ubicación geográfica de Ecuador y su economía dolarizada lo convierten en un paraíso natural para las redes extranjeras del crimen organizado?

Diseñamos e integramos soluciones tecnológicas personalizadas para fortalecer las estrategias de

SISSA
Monitoring Integral

SEGURIDAD EN TUS EVENTOS DEPORTIVOS

Videovigilancia **con analíticos (AI)**

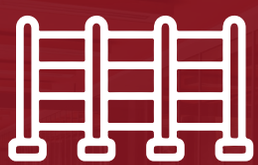
Control de acceso **peatonal y vehicular**

Sistemas de gestión **de identidad biométrica**

SOLUCIONES DE SEGURIDAD ELECTRÓNICA

Apertura y cierre de puertas **automatizado y remoto**

Alarma y detección de incendios



Seguridad **perimetral física**

CONTÁCTANOS

para obtener más información sobre los servicios de integración de **SISSA Monitoring Integral**

www.sissamx.com.mx

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 Israel Austria, ingeniero de Soluciones de Milestone Systems para América Latina, 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

Armando García Sánchez,

gerente de Consultoría en Timur Latinoamérica

¿Considera que antes de la militarización, la seguridad privada podría contribuir para combatir la inseguridad pública del país? Sí, no, ¿por qué?

Definitivamente. Hoy en día la seguridad privada ha cobrado relevancia, este sector ha alcanzado un nivel de profesionalización notable, que converge perfectamente con los últimos avances en tecnología, logrando con ello, ser un estupendo aliado para el sector de la seguridad pública, y pese a que en ocasiones su relación pudiera resultar un tanto compleja, no se puede negar el hecho de que ambos sectores pueden lograr una eficiente interacción y complementariedad para mantener un entorno seguro. Es importante destacar que, aunque la seguridad privada puede brindar un valioso apoyo, la seguridad pública sigue siendo la principal responsable de mantener la paz y el orden en una sociedad.

Considero que antes de pensar en la militarización del país, sería interesante seguir avanzando con la profesionalización y desarrollo de ambos sectores, capacitándolos adecuadamente, otorgándoles los recursos necesarios para el adecuado desarrollo de sus funciones, revisando y adecuando, o en su caso, implementando la legislación que permita operar y proteger a ambos sectores. La coordinación efectiva y la colaboración entre ambos son fundamentales para lograr un ambiente seguro y protegido para la sociedad antes de pensar en la posibilidad de usar la fuerza militar para lograrlo. ■

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.”

ESR EMPRESA SOCIALMENTE RESPONSABLE

COPARMEX® CIUDAD DE MÉXICO

AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C.

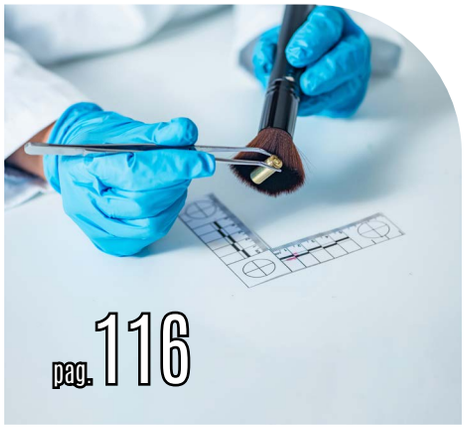
01 (55) 5639 1643 ó 5639 3574
contacto@protectio.com.mx
www.protectio.com.mx

ÍNDICE

Septiembre - Octubre 2023

ÍNDICE

Septiembre - Octubre 2023



TECNOLOGÍAS PARA LA SEGURIDAD DE EVENTOS DEPORTIVOS

Fotos: FreePick

MÉXICO

Eduardo Marcial García

La inversión en tecnología de seguridad adecuada y su integración con estrategias de seguridad integrales contribuye a crear entornos seguros y confiables para la realización de eventos públicos

Los lamentables hechos de violencia sucedidos en marzo de 2022 en el Estadio Corregidora de Querétaro, México, fueron determinantes y un parteaguas para que se considere la seguridad como un pilar fundamental en estadios y eventos masivos, ya que el impacto para en la seguridad de las personas e imagen puede ser catastrófico de no ser controlado el riesgo adecuadamente.

El FanID es una de las primeras medidas que adopta la Femexfut y la Liga MX después de estos hechos, esta medida de identificación biométrica del asistente a un evento deportivo fue implementada por primera vez en el mundial de Rusia del 2018 y se volvió una medida obligatoria para asistir a un partido de la Liga MX en México a partir de abril de este año.

A partir de ahora la seguridad en eventos deportivos se puede ver enormemente potencializada si los datos biométricos son complementados con tecnologías de apoyo a los esquemas de seguridad del evento, algunos de estos nuevos esquemas pueden ser:

CENSO DE BARRAS

Una gran parte de los actos de violencia en los estadios son iniciados por las llamadas barras o porras, a partir de la inclusión del FanID se puede mantener un censo obligatorio a las barras de cada equipo y se puede conocer con premeditación la cantidad de asistentes de las barras a un evento, con esto se puede calcular el riesgo de forma anticipada.

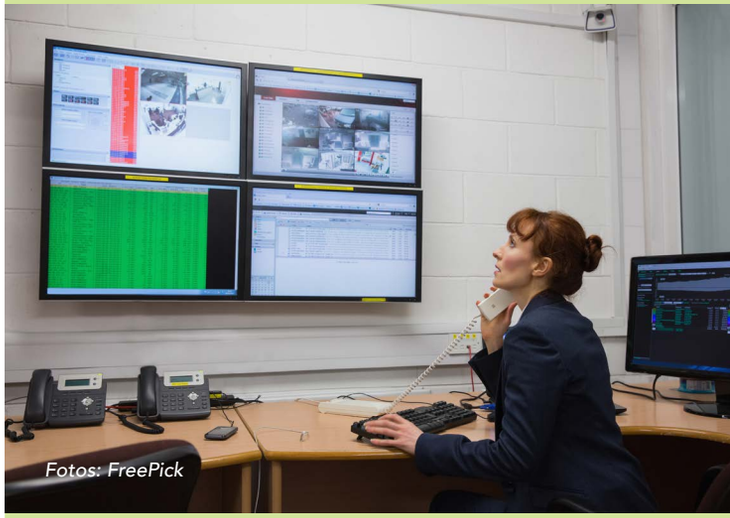
ANALÍTICA DE VIDEO MULTIOBJETIVO

Cuando se habla de analítica de video, es importante considerar el fin o alcance a la que va destinada esta tecnología, ya que no todas las tecnologías de analítica aplican en un entorno con diversas variables como lo es un evento deportivo.

Algunas de las características con las que debe contar una tecnología analítica para eventos son:

- **Algoritmo no cooperativo:** esta es una de las características fundamentales ya que un algoritmo común te pide ciertas condiciones ideales para el reconocimiento de personas, un algoritmo no cooperativo está diseñado para que la persona no esté dispuesta a ser reconocida, lo que permite su funcionamiento bajo condiciones adversas como ángulos e inclinaciones del rostro, uso de barba y bigote, uso de casco de motocicleta, uso de lentes obscuros, rostro parcialmente tapado o incluso el cambio de la edad de la persona.
- **Multiobjetivo:** debe contar con la capacidad de analítica de múltiples objetivos a la vez, en un evento deportivo será complicado realizar filas únicas, por lo que la inclusión de un algoritmo multiobjetivo será crucial para no entorpecer la operación de un evento.
- **Conteo y ocupación:** permite realizar no sólo un conteo de las personas que asisten a un evento, sino todo un control de la estadía y ocupación dentro de la justa deportiva, permitiendo contar con información valiosa en caso de una emergencia, incluso con fines mercadológicos.
- **Listas negras:** esta capacidad del sistema debe permitir la inclusión de listas de personas no autorizadas, de tal forma que si un asistente al evento es detectado realizando actos indebidos en un evento, éste sea adherido a una lista negra para en el siguiente evento no permitir su entrada, sin embargo, esta característica también puede ser utilizada para generar una lista gris donde permite conocer la cantidad exacta de asistentes de la porra o barra que ingresan al evento.
- **Listas blancas:** con esta función identificas a personal del que necesitas saber su ingreso, como un alto funcionario o un VIP.
- **Topología adaptable:** su implementación debe permitir diferentes escenarios de comunicación entre los distintos módulos que componen el sistema, esto permite que se pueda contar con una base central que sea actualizada en tiempo real y sistemas satélite en cada estadio, de tal forma que si un asistente al evento es detectado realizando actos indebidos en un evento éste sea adherido a una lista negra.
- **Análisis de características:** esta función permite identificar características clave de la persona, como edad, género y vestimenta, permitiendo realizar búsquedas rápidas por características cuando es requerido, como en la búsqueda de un menor o en una investigación, esto también aplica en un ámbito mercadológico para identificar por ejemplo, cuántas personas usan la playera de su equipo.
- **Identificación de emociones:** permite identificar el estado de ánimo de una o varias personas, conociendo estas emociones se pueden prever casos de riña o violencia, además de capitalizar la misma tecnología como un tema mercadológico para saber el estado de satisfacción de los asistentes.
- **Vinculación de objetivos:** determina el contacto o vínculo entre personas de forma gráfica, permitiendo conocer quién estuvo en contacto con quién, esto tiene varias aplicaciones, desde una posible investigación para determinar vínculos entre revendedores, hasta en la búsqueda de un niño perdido y determinar con quién tuvo contacto.

A partir de la inclusión del FanID se puede mantener un censo obligatorio a las barras de cada equipo y se puede conocer con premeditación la cantidad de asistentes de las barras a un evento, con esto se puede calcular el riesgo de forma anticipada



Fotos: FreePick

En el mundial de Sochi (Rusia) en 2018 se implementó una tecnología de reconocimiento facial masivo, que permitió el control de los eventos y logró disminuir los incidentes durante la duración del mundial

Fotos: FreePick


Fotos: FreePick

En el mundial de Sochi (Rusia) en 2018 se implementó una tecnología de reconocimiento facial masivo, que permitió el control de los eventos y logró disminuir los incidentes durante la duración del mundial, existieron casos de personas que fueron fichadas en los primeros partidos, posteriormente fueron identificados intentando ingresar en partidos posteriores y fue negado su ingreso.

DETECCIÓN DE ARMAS POR IA

Cuando hablamos de detección de armas automáticamente pensamos en la detección de metales, sin embargo, la tecnología de detección no ha sufrido innovaciones en muchos años, aún cuando ahora tenemos muchas armas fabricadas con polímeros.

Bajo el contexto anterior algunas empresas y sitios de gobierno comienzan a implementar tecnologías de detección apoyadas por IA, que identifican la masa y forma de un objeto alertando en caso de una posible arma, el uso de esta tecnología se está haciendo cada vez más común en escuelas, recintos de gobierno, parques de diversiones y estadios, todas estas tienen un factor en común, el flujo masivo de personas por sus controles de acceso.

CENTRAL DE SEGURIDAD DE EVENTO

El mejor complemento para la tecnología es una central de seguridad donde se tenga visión de las plataformas y comunicaciones del evento, algunas de las características que puede tener son:

- **Centralización:** esto permite al analista de monitoreo centrar sus esfuerzos en una misma plataforma.
- **Movilidad:** puede ser incluso una central móvil.
- **Funcionalidad:** su composición por funciones permite a sus analistas concentrase en su alcance determinado, es decir existe alguien que se encarga del monitoreo, alguien que atiende un incidente, etc.

CONCLUSIÓN

El uso de tecnologías e IA en eventos puede mejorar los esquemas de seguridad de éstos, además se pueden capitalizar en ámbitos diferentes al de la seguridad algunas de las funciones tecnológicas, como en el análisis de *data* con fines mercadológicos.

Además, es importante contemplarse que México se acerca a un mundial de futbol y deben considerarse esquemas más seguros buscando el bienestar de las personas que asisten a los eventos y cuidar la imagen de las organizaciones que están detrás de los equipos.

Estos esquemas de seguridad pueden ser tropicalizados para otras verticales como la seguridad escolar, donde el alto flujo diario incentiva su uso, además de que las escuelas, colegios y universidades también organizan justas deportivas que cuentan con una cantidad considerable de asistentes. ■

Eduardo Marcial García, CPP, gerente de Seguridad, Tecnología y Riesgos en Grupo Control Seguridad / Contech Secure Solutions. *Más sobre el autor:*

¡Paragon establece el estándar para el futuro!

Revolucionando la prevención de pérdidas.

La nueva función Ambiscan de Paragon le permite atrapar las armas que entran y previniendo el hurto de piezas valiosas de metal (herramientas, producto metálico, etc.).

ESCANEAR PARA MÁS INFORMACIÓN

PARAGON

Ambiscan

MADE IN THE USA

GARRETT

BLINDAJE AUTOMOTRIZ, ESTRATEGIA DE PROTECCIÓN PARA EJECUTIVOS DE EMPRESA

Los grupos empresariales, tanto los de capital externo como los nacionales, deben considerar en sus estrategias de seguridad el uso de unidades blindadas para sus niveles directivos

Fotos: FreePick

MÉXICO

José Luis Sánchez Gutiérrez

El blindaje automotriz es un sistema de protección para todas las personas que estén dentro del vehículo contra prácticamente cualquier ataque, viniendo balístico del exterior dependiendo del nivel de blindaje. Esa protección puede ser aplicada en todas las partes del habitáculo del automóvil para una máxima eficiencia.

Desde mi perspectiva, veo cuatro fases con las cuales se logra complementar la estrategia de seguridad de la empresa con el blindaje automotriz:

FASE 1: BENEFICIOS DEL BLINDAJE AUTOMOTRIZ EN LA PROTECCIÓN DE EJECUTIVOS DE EMPRESA

El blindaje automotriz aplicado a la protección de ejecutivos de empresa ofrece una serie de beneficios significativos. Estos beneficios incluyen:

- **Seguridad personal:** el blindaje automotriz proporciona un nivel adicional de protección para los ejecutivos mientras se desplazan, minimizando el riesgo de ser víctimas de ataques violentos o secuestros. Esto brinda tranquilidad tanto a los ejecutivos como a sus familias, permitiéndoles concentrarse en sus responsabilidades laborales sin preocupaciones excesivas por su seguridad personal.
- **Protección contra armas de fuego y explosiones:** el blindaje automotriz está diseñado para resistir impactos de balas y explosiones, lo que proporciona una barrera física de protección contra estos ataques. Esto es especialmente relevante en áreas donde los niveles de violencia armada son altos o en situaciones donde los ejecutivos pueden estar expuestos a amenazas específicas.
- **Reducción del riesgo de robo y asaltos:** los vehículos blindados son menos propensos a ser objetivo de robos o asaltos debido a su nivel de seguridad superior. Los delincuentes generalmente evitan vehículos blindados debido a las dificultades adicionales que representan para llevar a cabo sus actividades delictivas.
- **Privacidad y confidencialidad:** el blindaje automotriz también proporciona un entorno más seguro para las conversaciones y reuniones confidenciales dentro del vehículo. Los ejecutivos pueden sentirse más cómodos al discutir información sensible sabiendo que están protegidos de escuchas o vigilancia no autorizadas.

FASE 2: COSTOS ASOCIADOS AL BLINDAJE AUTOMOTRIZ

Es importante tener en cuenta que el blindaje automotriz es una inversión significativa y conlleva costos considerables. Algunos de los costos asociados al blindaje automotriz incluyen:

- **Costo inicial:** el proceso de blindaje de un vehículo implica modificaciones estructurales y la instalación de materiales de alta resistencia. Esto resulta en un costo inicial considerable que varía según

GSI
SEGURIDAD PRIVADA

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

Profesionales en Seguridad Privada

Oficiales de Seguridad

- *Oficiales de seguridad.*
- *Protección ejecutiva.*
- *Rastreo y monitoreo.*
- *Oficiales de seguridad armados.*
- *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 de prestadores de servicios Centro de Evaluación

Certificación del Sistema de Calidad DNV ISO 9001

AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C.

Empresas de GSI Grupo Seguridad Integral

BASC

el nivel de protección requerido y el tipo de vehículo a blindar.
- **Mantenimiento y reparaciones:** los vehículos blindados requieren un mantenimiento regular y especializado para asegurar su funcionalidad y durabilidad a lo largo del tiempo. Además, en caso de daños o reparaciones necesarias, los costos pueden ser más altos debido a la naturaleza especializada del blindaje.
- **Mayor consumo de combustible:** debido al aumento de peso del vehículo como resultado del blindaje, es común que se produzca un incremento en el consumo de combustible. Esto puede generar costos adicionales a largo plazo en términos de llenado de combustible.

FASE 3: DESVENTAJAS Y CONSIDERACIONES

A pesar de los beneficios mencionados, el blindaje automotriz también presenta algunas desventajas y consideraciones que deben tenerse en cuenta:

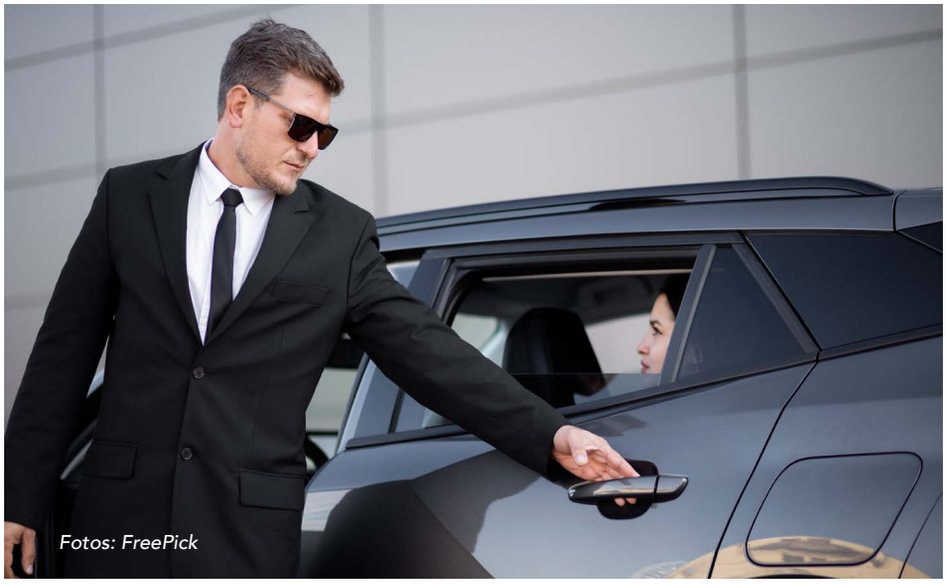
- **Peso adicional y limitaciones de rendimiento:** el blindaje automotriz aumenta significativamente el peso del vehículo, lo que puede afectar su rendimiento general, incluida la aceleración, la velocidad máxima y la maniobrabilidad. Es importante considerar estas limitaciones al elegir un vehículo blindado, ya que podría afectar la comodidad y la eficiencia de los desplazamientos.
- **Espacio interior reducido:** la instalación de materiales de blindaje puede reducir el espacio interior del vehículo, lo que puede afectar la comodidad de los ocupantes, especialmente en modelos más pequeños. Los ejecutivos y sus acompañantes pueden experimentar una sensación de confinamiento, lo cual puede ser un aspecto por considerar en términos de comodidad y necesidades personales.
- **Mantenimiento y reparaciones especializadas:** el blindaje automotriz requiere mantenimiento y reparaciones especializadas por parte de técnicos capacitados. Esto puede significar que se necesiten servicios y piezas específicas que pueden ser más costosos y difíciles de encontrar en comparación con los vehículos convencionales. Es fundamental contar con un proveedor confiable y experimentado para garantizar un mantenimiento adecuado y la disponibilidad de piezas de repuesto.

FASE 4: VALOR AGREGADO DEL BLINDAJE AUTOMOTRIZ

A pesar de las desventajas y costos asociados, el blindaje automotriz ofrece un valor agregado significativo para la protección de ejecutivos de empresa. Algunos aspectos destacados incluyen:

- **Diferenciación y prestigio:** el uso de vehículos blindados demuestra un compromiso serio por parte de la empresa en la seguridad y protección de sus ejecutivos. Esto puede aumentar la percepción de confianza y profesionalismo tanto entre los ejecutivos como entre sus colaboradores y socios comerciales.
- **Continuidad de las operaciones:** al proporcionar una capa adicional de seguridad, el blindaje automotriz garantiza la continuidad de las operaciones empresariales al proteger a los ejecutivos clave. Los desplazamientos seguros y sin incidentes permiten que los ejecutivos cumplan con sus responsabilidades y tomen decisiones importantes sin interrupciones.
- **Tranquilidad y bienestar:** la protección brindada por el blindaje automotriz reduce el estrés y la ansiedad tanto de los ejecutivos como de sus familias. Saber que se cuenta con una medida de seguridad efectiva aumenta el bienestar general y permite que los ejecutivos se centren en sus tareas sin distracciones ni preocupaciones excesivas.

Considero de manera final que el blindaje automotriz aplicado a la protección de ejecutivos de empresa ofrece una serie de beneficios importantes, como seguridad personal, protección contra armas de fuego y explosiones, reducción del riesgo de robo y asaltos, así como privacidad y confidencialidad. Sin embargo, es necesario tener en cuenta los costos asociados, las limitaciones de rendimiento y espacio interior, así como las consideraciones de mantenimiento y reparaciones. A pesar de estas desventajas, el valor agregado del blindaje automotriz incluye diferenciación y prestigio, continuidad de las operaciones y la tranquilidad y bienestar de los ejecutivos que se alinea a los objetivos de las empresas generando real valor humano y económico. ■



Fotos: FreePick

José Luis Sánchez Gutiérrez,
director de Seguridad Patrimonial en SMITHFIELD / Granjas Carroll de México (Industria Alimentaria).
Más sobre el autor:

ESPECIALISTAS EN

TRASLADOS VIP

Y PROTECCIÓN EJECUTIVA

NUESTROS SERVICIOS:

GRIPERS
ESPECIALISTAS EN
SEGURIDAD INTRAMUROS

AUDITORÍA Y
CONSULTORÍA

ANÁLISIS DE RIESGOS

ESTUDIOS
DE CONFIANZA

VIGILANCIA Y DETECCIÓN
DE VIGILANCIA Y CONTRAVIGILANCIA

CAPACITACIÓN EN
ARMAS DE FUEGO

grip®
global risk prevention

CONTÁCTANOS

55 1391 6570

comercial@grip.mx

SÍGUENOS EN REDES SOCIALES

www.grip.mx

¿DEBEMOS BLINDAR NUESTROS TRACTOCAMIONES?

Hay muchas opciones en el mercado, por ello se recomienda averiguar la antigüedad de la empresa blindadora, las certificaciones con las que cuenta, las normas con las que cumplen sus productos y de ser posible, conocer sus plantas de producción

MÉXICO

Cap. Eduardo Joel Espinoza Sosa

El hombre de negocios, Lawrence Bossidy, dijo: "Estoy convencido que nada de lo que hacemos es más importante que contratar y desarrollar personas. Y al final del día, apuestas por la gente, no por estrategias".

Por ello doy por sentado que es una afirmación que los colaboradores son el activo más valioso para las empresas. La vida de una persona que comparte su fuerza e intelecto para desarrollar cualquier acción dentro de una entidad socioeconómica simplemente es invaluable.

Como líderes de organizaciones es imperioso recordar que son los equipos de trabajo y las personas que aportan a la organización en su conjunto, las que provocan los cambios. Por ello, nuestros colaboradores deben ser atendidos, protegidos y procurados.

Cuando las personas se sienten bien, ofrecen lo mejor de sí mismos en sus empleos, confían en su empresa reduciendo la resistencia a los cambios de ritmo, roll, adaptación. La inversión en nuevas personas que pasan a formar parte de la organización es alta y más en sectores como el de autotransporte federal de carga.

Son muchos y diversos los factores que han colocado a este sector en una situación de crisis de inseguridad. Citando al artículo informativo titulado "Estadísticas de Robo de Carga en México durante 2022"[1]: "De acuerdo con el informe anual del Centro de Inteligencia para la Cadena de Suministro (SCIC) de Sensitech, en 2021 el hurto de mercancía reportó 19 mil 876 casos en territorio mexicano" […] "Según los informes de finales de año (2022), en el país se registraron más de 19 mil asaltos contra el transporte de carga, lo que quiere decir que las estrategias implementadas tanto por autoridades federales como por empresas transportistas, continúan fracasando y siendo insuficientes".

Ahora sabemos que más de la tercera parte de los asaltos reportados a tractocamiones en las diferentes carreteras del país han involucrado el uso de armas de fuego, es decir, se estima que anualmente aproximadamente en tres mil 800 casos, las armas han sido accionadas con consecuencias lamentables.

De acuerdo con los datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) y la FGR se refieren que, todos los días, un promedio de 36 transportistas fueron víctimas de la delincuencia en las carreteras del país, el año pasado.

PROCESOS A CONTEMPLAR

Aunado a este flagelo y derivado de la alta demanda, para las empresas aseguradoras es crucial determinar si la conducta del conductor contribuyó o no en el siniestro, las medidas de seguridad que la empresa transportista emplea para contribuir a la disminución de esta exposición y los mecanismos de reacción que se ofrecen. Aspectos que nos conducen a considerar sistemas efectivos de gestión de riesgo que contemplen los procesos de:

1) Selección de rutas principales y alternas.
2) Discriminación de horarios de traslado.
3) Gestión tecnológica que va desde el control remoto de la apertura de puertas hasta la parada total de motor, la geolocalización de la unidad y de la carga, como parte intrínseca de la trazabilidad de los productos.
4) Empleo de centros coordinadores de monitoreo fijos o móviles sobre las rutas.
5) Blindaje de los tractocamiones.

EL MEJOR ALIADO EN
SEGURIDAD Y MONITOREO
PARA TU NEGOCIO Y OPERACIONES

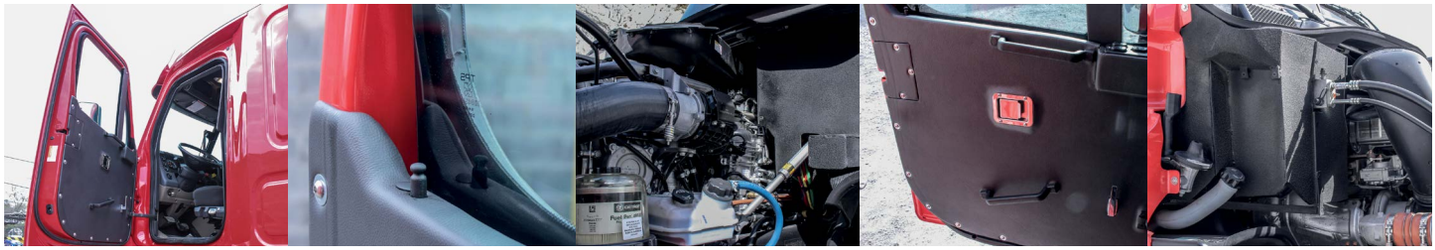
RASTREO MONITOREO VISÍTANOS SOS ALARMAS CCTV

www.skyangel.com.mx

(55) 5687 9011 Ext. 400-405
info@skyangel.com.mx

+1 (956) 568 3611
info@skyangelguard.us

/SkyangelGPS /company/SkyangelMx /SkyangelGPS



Este último punto representa una inversión que reduce el riesgo de pérdida total de un vehículo, lo que puede significar menores costos para las empresas, ya que además de proteger al Recurso Humano se protege también la carga y las aseguradoras pueden disminuir sustancialmente el precio de sus pólizas. El retorno de una inversión de esta magnitud es a mediano plazo pues el desempeño de los operadores se centra en apegarse al plan de viaje con la confianza de que, en caso de ser abordado por miembros de la delincuencia, no se tendrá que lamentar incidentes mortales.

TIPOS DE BLINDAJE PARA TRACTOCAMIONES

Habiendo estudiado los modos de operar y el tipo de armamento que habitualmente emplean los delincuentes en el robo a transporte de carga, la empresa blindadora TPS Armoring ha diseñado niveles de protección que evitan los secuestros y los atentados, con una protección que actúa en contra de diversos calibres de armas de fuego, desde .44 Magnum hasta 7.62 x 39 mm., cumpliendo con normativas mexicanas, americanas y europeas.

Por ejemplo, el Blindaje Nivel IV Plus - Antisecuestro tiene la finalidad de proteger durante un ataque cuyo objetivo sea sustraer a los ocupantes de la unidad de transporte de carga. Por su resistencia a impactos y explosivos, se considera al Nivel IV como un blindaje de 360° el cual cumple con las normativas NU 0108.01, NOM 142 SCFI 2000, CEN 1063 y BPAM BRV 2009.

Por otro lado, el Blindaje Nivel V Plus - Antiatentado se refiere a un blindaje total, con capacidad antisecuestro y con mayor robustez y resistencia a distintos tipos de municiones y explosivos. Cumple con las normativas UL 752, NU 0108.01, NOM 142 SCFI 2000, CEN 1063 y BPAM BRV 2009.

Para la instalación de estos niveles de protección en tractocamiones, la antigüedad de la unidad no tiene por qué ser una limitante, lo que se debe considerar es que la unidad de carga debe estar en buenas condiciones y que pueda soportar el peso del blindaje requerido sin comprometer el funcionamiento de la unidad.

Es importante tomar en cuenta que cuando se blinda un modelo que no es apropiado para recibir este tratamiento, el vehículo puede volverse incómodo, poco práctico y lento, ya que el blindaje agrega peso a la unidad, aproximadamente entre 600 y 900 kilogramos para el Nivel IV y entre mil y 1,500 kilogramos en el caso del Nivel V. Por ello te invito a que busques a un asesor calificado para que atienda el caso de manera muy particular y te recomiende la mejor opción.

FACTORES PARA TOMAR EN CUENTA

Al pensar en blindar un tractocamión en uso se consideran factores determinantes:

- El peso añadido es fundamental, pues los motores del pasado no tienen la misma potencia que los actuales.
- Los caballos de fuerza del motor determinan la resistencia de la unidad para moverse de forma ágil y sin limitaciones de seguridad para el conductor y sus acompañantes.
- El kilometraje da una idea del estado de la unidad en función del uso. Este aspecto puede variar dependiendo de si se dio un buen uso al vehículo y si éste recibió mantenimiento en tiempo y forma.

En suma, en uso o nuevo los tractocamiones tienen una opción de ser blindados equilibrando la relación funcionalidad-protección-potencia. Hay muchas opciones en el mercado, por ello te recomiendo averiguar la antigüedad de la empresa blindadora, las certificaciones con las que cuenta, las normas con las que cumplen sus productos y de ser posible, conocer sus plantas de producción.

En el caso de TPS Armoring, te esperamos en la Ciudad de Monterrey, Nuevo León, para que conozcas nuestros productos, procesos, materias primas y servicios. Así como en los Punto de venta y Centros de Servicio Mecánico Post Venta en las plazas de Ciudad de México, Guadalajara (Jalisco) y Cancún (Quintana Roo), para que conozcas nuestros productos terminados y los servicios especializados que se ofrecen.

Espero haber dejado elementos de juicio ante la retórica de si debes blindar tus tractocamiones. Protejamos a los colaboradores, a todos ellos quienes se han sumado voluntariamente a nuestros proyectos empresariales. Siempre somos más quienes encontramos de manera proactiva la solución a las vicisitudes que se presentan.

A tus órdenes. ■

Fotos: Cortesía TPS Armoring

Referencias:

1 https://www.safelinkmexico.com/estadisticas-de-robo-de-carga-en-mexico-durante-2022/

Cap. Eduardo Joel Espinoza Sosa, CPP, coordinador de Seguridad Patrimonial de TPS Armoring. *Más sobre el autor:*

DISTRIBUCIONES E IMPORTACIONES
DEL PEDREGAL , S.A. DE C.V.

Blindaje Arquitéctonico

JOYERÍAS

PANIC ROOMS

PUERTAS BLINDADAS

EMBAJADAS

Ventas de materiales

Balísticos Certificados

(55) 5216-0050

www.blindaje007.com

Blindaje@prodigy.net.mx
ReneRivera@Deipedregal.com

Columna de
Jaime A. Moncada

jam@ifsc.us

Es 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:

SEGURIDAD CONTRA INCENDIOS EN EDIFICIOS DE ALTA CONCURRENCIA

EUA

Los edificios de alta concurrencia, también llamados sitios de concurrencia masiva presentan problemas específicos de seguridad contra incendios como el movimiento físico y comportamiento de los ocupantes, capacidad de las salidas, y métodos apropiados de alertar y dirigir a los ocupantes en caso de una emergencia. Paralelamente a esto, los ocupantes de este tipo de edificaciones no están familiarizados con la localización de las salidas o cómo resguardarse en caso de un incendio. Muchas de estas ocupaciones presentan niveles de iluminación muy bajos como bares, iluminación que puede confundir como en discotecas, u operar en obscuridad casi total como teatros o cines.

Los sitios de alta concurrencia se definen como ocupaciones para reuniones públicas, donde se reúnen cientos de personas. Ejemplos de este tipo de ocupaciones son estadios, auditorios con asientos fijos o movibles, grandes salones de reunión, restaurantes, bares, bibliotecas, salas de conciertos, salas de exhibición, centros de convenciones, centros deportivos y terminales de pasajeros para transporte, entre otros. Generalmente cuando hay una densidad importante de ocupantes y el recinto tiene más de 50 personas, este recinto se evalúa como una ocupación de reunión pública. Si el recinto tiene menos de 50 personas, se evalúa como un uso auxiliar a otro tipo de ocupaciones.

Para ilustrar los riesgos específicos de los diferentes tipos de edificios con concurrencia masiva, me voy a centrar, de aquí en adelante, en la descripción de los riesgos y protecciones en un estadio. Es decir, debe quedar claro que los requerimientos de un estadio son muy diferentes a los que pueda requerir una discoteca, o una sala de cine o un aeropuerto.

Foto: Cortesía IFSC

En un concierto, por ejemplo, puede ser difícil discernir si existe un incendio, o identificar de dónde proviene el humo, o encontrar las vías de evacuación

Foto: Cortesía Jaime A. Moncada

Los estadios modernos no permiten la evacuación hacia la grama, limitando la posibilidad de una evacuación rápida a un sitio más seguro

RIESGOS CON EL NÚMERO DE OCUPANTES

El 24 de mayo de 1964 se enfrentaron en el Estadio Nacional de Lima, las selecciones de Perú y Argentina en la final clasificatoria para las Olimpiadas de Tokio. Aquel día la asistencia oficial fue de 47mil 197 espectadores, la capacidad máxima del estadio. Argentina ganaba uno a cero, cuando faltando dos minutos para el final del partido, Perú marcó el gol del empate. Sin embargo, el árbitro uruguayo Ángel Pazos anuló el gol. La decisión provocó una reacción en cadena que se inicia con aficionados enfurecidos invadiendo la cancha, peleas en las tribunas y la fatídica decisión de la policía de utilizar gases lacrimógenos contra los mismos aficionados en las tribunas. Esto desata una estampida hacia las vías de egreso que habían sido cerradas por la policía. El resultado fue 318 muertos y más de 500 heridos, la peor tragedia en un estadio de cualquier tipo en el mundo y otro desafortunado "récord mundial" para nuestra región.

El peor incendio en un estadio ocurrió 21 años más tarde, en el Estadio *Valley Parade* en Bradford, Inglaterra, un 11 de mayo de 1985. Esa tarde, mientras Bradford City empataba contra Lincoln City, dos equipos de la tercera división del futbol inglés, basura que durante años se había colectado debajo de las graderías del estadio, prendió fuego. Este incendio rápidamente enciende el techo de madera sobre estas graderías y en cuestión de pocos minutos todo un cos-

tado del estadio estaba incendiado. Afortunadamente la mayoría de los espectadores pudieron evacuar hacia la grama, pero por la rapidez del incendio, 56 personas perdieron la vida y 265 más quedaron heridas.

CÓDIGOS DE PREVENCIÓN DE INCENDIOS

Estos dos incidentes ilustran algunos de los objetivos principales en los códigos de seguridad contra incendios: evitar y/o controlar un incendio mientras que, paralelamente, se ofrezcan métodos seguros, eficientes y eficaces de evacuación. La seguridad contra incendios de un edificio o estructura se obtiene cuando éste se evalúa como un todo. No solamente es importante la definición de los sistemas contra incendios, ya sean éstos automáticos (por ejemplo, rociadores automáticos) o manuales (como, conexiones para mangueras), sino que se deben analizar simultáneamente con los medios de evacuación, la construcción y compartimentación del edificio, sus contenidos y terminados interiores, los métodos de alarma de incendios y notificación a los ocupantes, la iluminación interior, elevadores, señalización, sistemas de aire acondicionado y calefacción, entre muchos otros.

Los códigos modernos de incendios, como los de la NFPA, han desarrollado, para la mayoría de los riesgos, una metodología prescriptiva, donde los edificios y estructuras son evaluados desde el punto de vista de su uso u ocupación. Bajo este concepto, cada ocupación tiene requerimientos diferentes a otros tipos de ocupaciones. Es decir, los requerimientos de seguridad de un hospital son diferentes a los de un edificio de almacenamiento. Pero también, debido a la diferente arquitectura de cada edificio, el análisis normativo dará un resultado diferente para cada edificio, así sean de una misma ocupación. En los edificios de concurrencia masiva, reitero, el énfasis está en el movimiento eficaz de los ocupantes y en el control del incendio.

RETOS DE LA ARQUITECTURA MODERNA

Siguiendo con el ejemplo de un estadio, debemos entender que el diseño arquitectónico e ingenieril de estos edificios ha evolucionado, y de la misma manera han cambiado los retos para el ingeniero de protección contra incendios. Hoy día el estadio moderno es utilizado para una gran variedad de eventos, desde un partido de fútbol, hasta conciertos, mítines políticos, y conferencias religiosas, donde el campo deportivo está ocupado por espectadores incrementando la capacidad del recinto y modificando los planes de evacuación. La estructura puede ser también techada, introduciendo complicaciones durante la evacuación del humo en un incendio. El estadio moderno también incluye amplias áreas cubiertas como *suites* corporativas, restaurantes, bares, cocinas, tiendas, áreas VIP, cabinas de transmisión, palcos para la prensa, camerinos y oficinas que incluyen riesgos de incendios con cargas de fuego altas.

Estadio cubierto donde el manejo de la capa de humo en un incendio es esencial para permitir suficiente tiempo de evacuación

LA NORMATIVA DE LA NFPA

Como era de esperarse, esta normativa tiene extensos requerimientos para edificios de concurrencia masiva, los cuales se encuentran principalmente en la norma NFPA 101, Código de Seguridad Humana. Continuando con la referencia anterior del riesgo en un estadio, la principal diferencia en su diseño es si éste se ha clasificado como un "área de asientos protegida contra el humo" o no. Cuando existe un sistema de control de humo que mantenga la capa de humo 1.8 m encima de las vías de evacuación y las áreas cubiertas del estadio están protegidas con rociadores automáticos, entre otras protecciones, se permite que los factores de capacidad de las salidas sean menos restrictivos y las distancias a las vías de evacuación se puedan hacer más largas.

El concepto de "área de asientos protegida contra el humo", mejor conocida en inglés como '*smoke protected seating*', busca equiparar la seguridad de un estadio como si éste estuviera totalmente al aire libre. La evaluación del estadio se separa de las reglas prescriptivas típicas en las normas de la NFPA, y requiere la realización de una Evaluación de la Seguridad Humana, lo cual suena más sencillo de lo que es. Este reporte debe ser realizado por escrito, elaborado por profesionales competentes y con experiencia, y debe ser revisado anualmente con autorización de la autoridad competente local.

Las condiciones que deben considerarse en esta evaluación incluyen aproximadamente 80 factores diferentes. Debo mencionar, casi de manera anecdótica, que a diferencia de las regulaciones de la FIFA, NFPA 101 permite que el tiempo de flujo nominal durante la evacuación sea de 11 minutos en estructuras con más de 25 mil sillas.

El estadio moderno debe incluir también un análisis de ingeniería de protección contra incendios en la definición de la resistencia al fuego de la estructura. Dependiendo de los objetivos de protección, se puede diseñar el sistema de evacuación con lo que técnicamente se denomina como una "secuencia de alarma positiva", donde se permite una pre-alarma de hasta 180 segundos antes de que la señal de alarma general sea iniciada. Se requiere también que empleados estén presentes, alrededor del estadio, en suficiente cantidad y con conocimiento de los protocolos operacionales de control de multitudes, seguridad, sistemas de monitoreo y sistemas contra incendios.

Para concluir, un estadio es una edificación cada vez más compleja, y lo mismo se debe asumir en los otros tipos de edificios y estructuras con concurrencia masiva. Los problemas de seguridad humana y protección contra incendios apuntan a que los aspectos de diseño del estadio deben ser conjugados con la gestión del mismo. Los criterios establecidos por la NFPA no sólo sirven para la evaluación de edificios nuevos, sino para la reforma de edificios existentes. Sin embargo, los criterios de diseño son complejos y requieren la participación de profesionales experimentados, competentes y con experiencia previa. ■

INTEGRACIÓN DE SISTEMAS DE ALARMA Y DETECCIÓN DE INCENDIOS:

ELIMINA CUALQUIER AMENAZA DE SEGURIDAD

MÉXICO | Jamin Castillo Ocampo

Los sistemas de alarma y detección de incendios deben ser implementados e integrados a manos de especialistas en seguridad electrónica que cuenten con las credenciales y experiencia suficientes para garantizar un servicio de calidad

Sabemos que, como responsable de la seguridad de tu organización, siempre te encuentras en búsqueda de las mejores prácticas para garantizar la protección de tus equipos, personal e infraestructura.

Los sistemas de alarma y detección de incendios forman parte de aquellas tecnologías que te permitirán garantizar la seguridad de tu organización y, por ende, el cumplimiento de tus objetivos, ya que estos sistemas están diseñados para evitar cualquier situación de riesgo relacionada con el fuego y siniestros de consecuencias importantes tanto para tu personal como para la economía de tu organización.

Una vez que tu sistema de alarma y detección esté integrado en tu organización, es fundamental realizar las pruebas correspondientes para que, en caso de ser necesario, se realicen los ajustes pertinentes, y para asegurar la respuesta del sistema en el momento que éste deba activarse ante la detección de eventos

¿QUÉ ES UN SISTEMA DE ALARMA Y DETECCIÓN DE INCENDIO?

Un sistema de alarma y detección de incendios es un sistema de seguridad que detecta en tiempo real posibles amenazas de incendio, y alerta a los encargados de seguridad de manera oportuna para que puedan tomar las medidas pertinentes para mitigar inmediatamente cualquier situación de riesgo.

Los sistemas de alarma y detección de incendios están especialmente diseñados para detectar la presencia de humo y temperaturas de riesgo que puedan desencadenar conatos de incendio, además de que tienen la capacidad para detectar escapes de gas y otras tantas amenazas relacionadas con la seguridad de tu organización.

Además, si quieres tener una solución robusta, es posible integrar estos sistemas con otras tecnologías de seguridad y vincularlas a la central de monitoreo de tu organización o de las autoridades pertinentes (bomberos y policía).

En SISSA Monitoring Integral contamos con un equipo de expertos en sistemas de seguridad electrónica que pueden ayudarte a evaluar tus necesidades reales y, de esta manera, implementar e integrar el sistema de alarma y detección de incendios que mejor se adapte a las características de tu organización a fin de elevar sus niveles de seguridad

¿CÓMO INTEGRAR UN SISTEMA DE ALARMA Y DETECCIÓN DE INCENDIOS DE MANERA EXITOSA?

En teoría, ningún sistema de alarma y detección debería ser igual a otro, ya que su implementación depende directamente de las necesidades y características específicas de la organización.

No obstante, a continuación, te presentamos algunas recomendaciones que te pueden ser de utilidad al momento de implementar un sistema de alarma y detección de incendios.

- **Evalúa tus necesidades:** lo primero que debes hacer es evaluar la situación actual de tu organización mediante un análisis de riesgo, a fin de identificar tus necesidades reales en materia de seguridad.
- **Selecciona los dispositivos a implementar:** una vez identificadas tus necesidades reales, deberás investigar y evaluar las características de los sistemas de alarma y detección que existen en el mercado, incluyendo sensores, alarmas y otros dispositivos, con el objetivo de seleccionar el que mejor se adapte a tus requerimientos.
- **Contacta a un integrador de confianza:** además de que un integrador capacitado y experimentado te puede ayudar con los pasos anteriores, también se encargará de implementar tus sistemas de manera adecuada e integrarlos con los demás sistemas de seguridad de tu organización para crear una solución robusta y que no permita errores.
- **Realiza pruebas:** una vez que tu sistema de alarma y detección esté integrado en tu organización, es fundamental realizar las pruebas correspondientes para que, en caso de ser necesario, se realicen los ajustes pertinentes, y para asegurar la respuesta del sistema en el momento que éste deba activarse ante la detección de eventos.

INTEGRACIÓN DE SISTEMAS DE ALARMA Y DETECCIÓN DE INCENDIOS A MEDIDA

Como ya se adelantaba anteriormente, los sistemas de alarma y detección de incendios deben ser implementados e integrados a manos de especialistas en seguridad electrónica que cuenten con las credenciales y experiencia suficientes para garantizar un servicio de calidad que te permita cumplir con tus objetivos de seguridad para el beneficio de tu organización.

En SISSA Monitoring Integral contamos con un equipo de expertos en sistemas de seguridad electrónica que pueden ayudarte a evaluar tus necesidades reales y, de esta manera, implementar e integrar el sistema de alarma y detección de incendios que mejor se adapte a las características de tu organización a fin de elevar sus niveles de seguridad.

Además, podemos brindar a tus sistemas un servicio de mantenimiento preventivo y correctivo que permita su actualización y cuidado continuo para asegurar el correcto funcionamiento de todos sus elementos.

Nuestros servicios de integración están dirigidos tanto a grandes empresas como a pequeños negocios, sin importar su giro o sector al que pertenezcan. En SISSA sabemos que, más allá del tamaño de la organización, lo que realmente importa es la calidad del servicio que ofrecen.

Si te interesa obtener más información sobre nuestro servicio de integración de sistemas de alarma y detección de incendios, no dudes en contactarnos por cualquiera de nuestros canales de comunicación y con gusto te atenderemos. ■

Fotos: SISSA Monitoring Integral

Jamin Castillo Ocampo, director de Operaciones en SISSA Monitoring Integral. *Más sobre el autor:*

INGENIERÍA BÁSICA

DE SISTEMAS DE DETECCIÓN Y ALARMAS DE INCENDIOS

Requerimientos mínimos

VENEZUELA | **Carlos E. Guerrero**

El génesis de cualquier Ingeniera Básica, proyecto o diseño, en todas las disciplinas de la Ingeniería, pasa por un diseño y la protección contra incendios no es la excepción. Un buen diseño no sólo salva vidas, también ahorra dinero y hace más eficiente una instalación. Para el caso particular de los sistemas de detección y alarmas de incendios, que son los llamados a avisar y trabajar en la etapa incipiente del incendio (los rociadores funcionan cuando hay llamas en el sitio del incendio y la temperatura en el techo llega a la de activación), deben ser diseñados por especialistas en la materia, para que cumplan su cometido. Tema aparte son los sistemas de detección y alarmas de incendios que protegen riesgos especiales, tales como, paneles fotovoltaicos sobre techo y sensibles al agua (centros de datos, cuartos de control, comunicación, etc.).

El código NFPA 72 (Código Estadounidense de Alarmas de Incendios y Señalización), en su capítulo 7 (documentación) entre otros, indica expresa y claramente todos los documentos necesarios para cumplir con el diseño de un sistema de detección y alarmas de incendios. De algunos de los documentos requeridos y otros que recomiendo ampliamente, para realizar un diseño básico, versará este artículo (también se deben revisar y cumplir las leyes, códigos y normas locales aplicables, en esta materia).

A pesar que los diseños son realizados de forma "genérica" (sin nombrar marcas y modelos), se debe recomendar dispositivos con nombre y apellido que cumplan con los requisitos del diseño

INFORME DE DISEÑO

El primer documento es el informe de diseño (o resumen narrativo) escrito. El propósito de este documento es suministrar una clara y simple descripción del sistema y trabajo que se va a ejecutar.

Particularmente lo inicio con un listado de definiciones, que puede ser tan largo como complejo sea el sistema. Esto lo hago pensando en que no necesariamente todas las personas que leen este documento son conocedores de sistemas de protección contra incendios.

Recomiendo que este informe incluya análisis y descripción del riesgo a proteger, y los fundamentos, tales como: institución que hace el listamiento de los equipos, calificaciones del diseñador, requerimientos de los futuros instalador, programador del sistema y mantenedor. También incluyo información acerca del suministro de energía (primaria y secundaria), señales que se están supervisando y medios de desconexión de los dispositivos de notificación. De requerirse puertos IP, deben ser especificados en esta parte del informe para que el Departamento de IT lo tenga en cuenta.

También incluyo información de circuitos y vías (Clase de cableado) y el motivo o bajo cuya orden se está realizando el diseño.

DIAGRAMA DE MONTANTES

El segundo documento es el diagrama de montantes, que es un plano que muestra el recorrido de la tubería vertical por toda la instalación, disposición general del sistema en la sección transversal de la instalación, cantidad de montantes, tipo y cantidad de circuitos por montante, tipo y cantidad de dispositivos por circuito.

El tercer documento es el juego de planos, los cuales muestran la ubicación de todos los dispositivos (mejor usando NFPA 170: Estándar de Símbolos de Seguridad Contra el Fuego y Emergencia, capitulo 8), y que, junto al diagrama de montantes, son los documentos más importantes para el instalador. Estos deben incluir detalles típicos de instalación donde se muestre, entre otros datos, altura de instalación y espaciamiento, niveles de presión sonora mínimos que deben ser generados por los aparatos de notificación audible, potencia de ajuste de las cornetas, candelas a las que deben trabajar las luces estrobo, entre otros.

MATRIZ DE ENTRADA / SALIDA

El cuarto documento es la matriz de entrada / salida (o de causa y efecto).

1.38- Cable para incendios		
A- ESPECIFICACIONES		**B- IMAGEN (referencial)**
Marca / modelo	CENTELSA / FPL	
Certificacion	UL	
Cantidad de cables	2 (+ y -)	
Calibre	#14 (NAC y 24VDC)	
Material del cable	Cobre (alambre solido o cableado)	
Material del aislante	PVC	
Aislante retardante a la llama	Si	
Material de la cubierta	PVC	
Cubierta retardante a la llama	Si	
Autoextinguible	Si	
Temperatura del aislamiento	105°C	
Hilo de rasgado	Si	
C- DESCRIPCION, D- PROCEDIMIENTO DE INSTALACION y E- MATERIALES		
Este cable se debe instalar en tubería metalica o bandeja portable, en ambos casos sin compartir la tubería con señales de potencia y respetando el % de la seccion transversal de tubería para el llenado de conductores segun RETIE (2 conductores = 31%. Mas de 2 conductores = 40%)		
F- Unidad de medida:	Metro lineal	
G- Tolerancia para la aceptacion:	5%	
H- Ensayos a realizar:	Continuidad y aislamiento	
I- Equipos	sonda (20m) + escalera (1) + megger (1) + multimetro (1)	
J- Medida y forma de pago:	Visualmente. 50% de anticipo, 25% con el equipo en obra, restante 25% contra entrega del sistema 100% operativo	
K- No conformidad:	No aplica para instalaciones nuevas	

ESPECIFICACIONES TÉCNICAS

Como cuarto documento, yo incluyo las especificaciones técnicas (genéricas) de todos los dispositivos especificados en el diseño. Aquí incluyo, las especificaciones técnicas como tal (por ejemplo marca / modelo recomendado, tiempo de vida útil, agencia que debe listar, temperatura de operación, tensión de alimentación, intensidad, tensión de salida, cantidad de direcciones, entre otros), descripción, procedimiento de instalación, materiales (si aplica), unidad de medida, tolerancia para la aceptación (si aplica), pruebas a realizar, equipos necesitados para realizar las pruebas de recepción, forma de medición (para realizar cortes y al instalador), forma de pago recomendada (al instalador) y manejo / tolerancia de no conformidades.

INSTALACION #1

MATRIZ CAUSA & EFECTO

CEGURO S. A. S.

SALIDAS del sistema - DESCRIPCION

PANEL DE CONTROL (PISO 1)

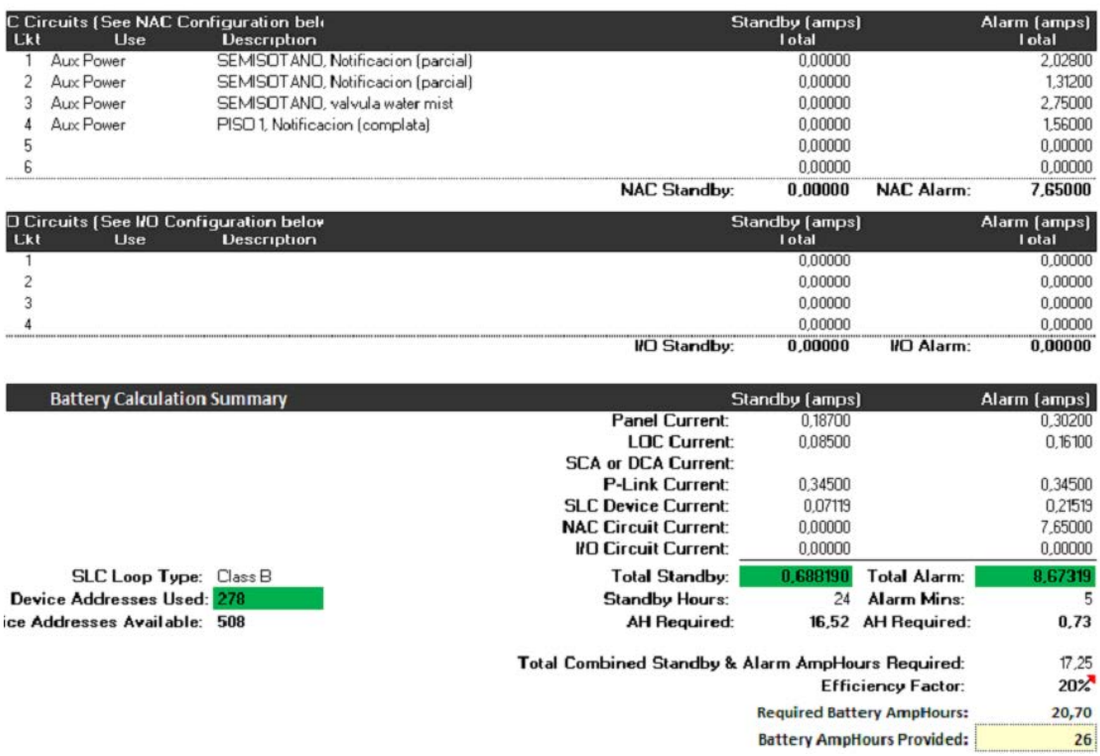
NOTIFICACION (modulo de control) / CONTROL (Ventilacion + talaqueras + Control

UBICACIÓN	ENTRADAS del sistema - DESCRIPCION	EJES	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	N	N	N
			Activar Indicador luminoso "Led" ROJO Cmdo de la Salida de ALARMA ("ALARM")	Accion Salida audible de ALARMA ("ALARM")	Activar Indicador luminoso "Led" AMBAR (simbolo de la Salida de SUPERVISION ("SUPERVISORY")	Activar las Salida audibles de SUPERVISION ("SUPERVISORY")	Activar Indicador luminoso "Led" AMBAR (simbolo de la Salida de PREALARMA ("PRE-ALARM")	Accion Salida audible de PREALARMA ("PRE-ALARM")	Activar Indicador luminoso "Led" ROJO de la Salida de PRE-DESCARGA ("PRE-RELEASE")	Accion Salida audible de PRE-DESCARGA ("PRE-RELEASE")	Activar Indicador luminoso "Led" ROJO de la Salida de DESCARGA (RELEASE)	Accion Salida audible de DESCARGA (RELEASE)	Activar Indicador luminoso "Led" VERDE de la Salida de FALLA ("FAULT")	Activar Indicador luminoso "Led" AMBAR de la Salida de avisos de PUESTA A TIERRA ("EARTH FAULT")	Notificacion Modulo de Control Piso 1	Notificacion Modulo de Control Piso 4 y 5	Modulo de Control Pisos 6, 7 y CUBIERTA	Valvula Water Mist - Sala de Computo, PISO 1	Valvula Water Mist - SIE - PISO 1	Valvula Water Mist - Sala de Computo, PISO 1
															Fuente Auxiliar #1 / NAC #1 (Panel de Control de Piso 1)	Fuente Auxiliar #2 / NAC #2 (Panel de Control de Piso 1)	Fuente Auxiliar #3 / NAC #3 (Panel de Control de Piso 1)	Fuente Auxiliar #4 / NAC #4 (Panel de Control de Piso 1)	Fuente Auxiliar #5 / NAC #5 (Panel de Control de Piso 1)	Fuente Auxiliar #1 / NAC #1 (Fuente de Piso 1)
			SENSOR DE HUMO TIPO PUNTUAL																	
PISOS 1 y 2	Sensor de Humo Activado	A	X	X											X	X	X	X	X	X
	Avería Sensor de Humo	B					X	X												
PISOS 3, 4 y 5	Sensor de Humo Activado	C	X	X												X				
	Avería Sensor de Humo	D					X	X												
PISOS 6, 7 y	Sensor de Humo Activado	E	X	X											X					

Este documento es importante para el usuario final y/o el interventor.

HOJAS TÉCNICAS

El quinto documento es el juego de hojas técnicas de todos los dispositivos especificados. A pesar que los diseños son realizados de forma "genérica" (sin nombrar marcas y modelos), se debe recomendar dispositivos con nombre y apellido que cumplan con los requisitos del diseño. De esta forma, el cliente, tiene al menos una rápida forma de solicitar y obtener presupuestos por el suministro de los dispositivos especificados en el diseño. Además, otros documentos del diseño como la memoria de cálculos eléctricos, son basadas en características obtenidas de estas hojas técnicas, de dispositivos específicos del mercado local. De cualquier forma, la oferta de fabricantes de los sistemas de detección y alarmas de incendios, permite que normalmente exista más de una marca que cumple con los requerimientos técnicos de la mayoría de los diseños. La diferencia puede estar en el costo de la inversión, características básicas, entre otras.



C Circuits (See NAC Configuration bel			Standby (amps)		Alarm (amps)
Ckt	Use	Description	Total		Total
1	Aux Power	SEMISOTANO, Notificacion (parcial)	0,00000		2,02800
2	Aux Power	SEMISOTANO, Notificacion (parcial)	0,00000		1,31200
3	Aux Power	SEMISOTANO, valvula water mist	0,00000		2,75000
4	Aux Power	PISO 1, Notificacion (complata)	0,00000		1,56000
5			0,00000		0,00000
6			0,00000		0,00000
		NAC Standby:	0,00000	NAC Alarm:	7,65000

D Circuits (See I/O Configuration below			Standby (amps)		Alarm (amps)
Ckt	Use	Description	Total		Total
1			0,00000		0,00000
2			0,00000		0,00000
3			0,00000		0,00000
4			0,00000		0,00000
		I/O Standby:	0,00000	I/O Alarm:	0,00000

Battery Calculation Summary	Standby (amps)		Alarm (amps)
Panel Current:	0,18700		0,30200
LOC Current:	0,08500		0,16100
SCA or DCA Current:			
P-Link Current:	0,34500		0,34500
SLC Device Current:	0,07119		0,21519
NAC Circuit Current:	0,00000		7,65000
I/O Circuit Current:	0,00000		0,00000
Total Standby:	0,688190	Total Alarm:	8,67319
Standby Hours:	24	Alarm Mins:	5
AH Required:	16,52	AH Required:	0,73

SLC Loop Type: Class B
Device Addresses Used: 278
ice Addresses Available: 508

Total Combined Standby & Alarm AmpHours Required: 17,25
Efficiency Factor: 20%
Required Battery AmpHours: 20,70
Battery AmpHours Provided: 26

NAC Circuit Configuration & Voltage Drop *CONSEJO SUPERIOR DE LA JUD 25/03/2022*

NAC 1 **MAX Circuit Current (amps): 3** **Source Voltage Used (VDC): 20,4**

Usage: Aux Power **Description:** SEMISOTANO, Notificacion (parcial)

Wire Type	Ohms/1000ft	Length 1-Way	Actual Ohms	Max Load (amps)	Volts @ EOL	Min Volts Req'd
#14 Stranded	3,26	300	1,956	2,028	16,43	16

Circuit Devices			Standby (amps)		Alarm (amps)	
Qty	Lookup Type	Description	Each	Total	Each	Total
11	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,858000
3	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,234000
3	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,234000
3	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,234000
2	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,156000
2	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,156000
2	Strobes	Potter SPKSTR-24WLP, 15cd	0,000000	0,000000	0,078000	0,156000
			Total Standby:	0,00000	**Total Alarm:**	2,02800

Con la memoria de cantidades y las especificaciones técnicas, el usuario final puede realizar análisis de costos e incluso, llamados a licitación

MEMORIAS DE CÁLCULOS ELÉCTRICOS

El sexto documento son las memorias de cálculos eléctricos, que incluye de baterías (para panel de control, fuentes de alimentación auxiliares remotas y amplificadores de audio) y caída de tensión de los dispositivos de notificación.

La mayoría de los grandes fabricantes de sistemas de detección y alarmas de incendios, tienen en su página web, calculadoras en hoja de Excel que permiten hacer estos cálculos de forma rápida, exacta y con la presentación adecuada para la entrega. Estas calculadoras se pueden descargar gratuitamente.

El cálculo de baterías es importante, porque suministra la carga eléctrica (Ah) que deben tener las dos baterías recargables de 12VDC, para que cumplan con el tiempo (*stand by* y alarma) requerido por NFPA 72. Este cálculo también suministra información si se necesitara especificar un gabinete independiente para guardar las baterías calculadas.

El cálculo de caída de tensión también es importante, porque asegura que todos los dispositivos de notificación, funcionan correctamente.

Para las cornetas del sistema de voz evacuación (cuando se especifique), se realizan cálculos de distancias máximas. Yo uso la siguiente ecuación (cortesía de POTTER):

$$Dm = \frac{Tp - Tm}{Iz} \times Cc$$

donde:

Dm = Distancia (m) máxima de 1 cable
Tp = Tensión (V) del amplificador
Tm = Tensión (V) mínima de la corneta
Iz = Intensidad (A) de la zona calculada.
Cc = Conductividad (S) del cable.

MEMORIA DE CANTIDADES

El séptimo documento es la Memoria de Cantidades. Este suministra un listado de las especificaciones técnicas de cada dispositivo, con sus respectivas cantidades. Este documento también incluye, cantidades de infraestructura y de cualquier otro elemento especificado en el diseño.

Con esta memoria de cantidades y las especificaciones técnicas, el usuario final puede realizar análisis de costos e incluso, llamados a licitación.

Este documento no es requerido por NFPA 72, pero a mí parecer, es un producto fundamental y necesario que ayuda a dimensionar el trabajo a realizar.

Por último, documentos adicionales (contratados) de soporte que justifiquen el diseño y ayuden a su implementación, como, por ejemplo: Normas de otras especialidades (diferentes a NFPA) que sean vinculantes, licencias / permisos de construcción o intervención, trámites a futuro, que serán necesarios (instalaciones que son patrimonio de la nación) realizar por la empresa instaladora, presupuesto aproximado, listado de consumibles (memoria de cantidades), listado mínimo de repuestos (memoria de cantidades), estudio de mercado y listado de accesorios eléctricos (memoria de cantidades). ■

Fotos: Cortesía Carlos E. Guerrero Roa

Carlos E. Guerrero Roa, gerente técnico en CEGURO, S. *A. S.*
Más sobre el autor:

SISSA
Monitoring Integral

DETECCIÓN Y SUPRESIÓN DE INCENDIOS

Detecta oportunamente conatos de incendio en tus instalaciones y suprímelos eficazmente con ayuda de nuestro servicio de integración a medida.

- **Detectores automáticos** de incendios
- **Paneles y centrales** de alarma
- **Dispositivos** de notificación
- **Detector de humo** por aspiración
- **Alarmas por** sonificación, voceo y sirenas
- **Cámaras de** detección de incendios y humo

CONOCE MÁS DE NOSOTROS

WWW.SISSAMX.COM

Contáctanos y descubre cómo podemos ayudarte a garantizar la seguridad del personal, activos y la operabilidad de tu organización a través de soluciones totalmente personalizadas.

CIBERSEGURIDAD EN VEHÍCULOS DE PROTECCIÓN EJECUTIVA

foto: freepik

VENEZUELA | **Adolfo M. Gelder**

De acuerdo con el Informe de Ciberseguridad Automotriz Global 2023, la industria automotriz se está expandiendo rápidamente hacia un vasto ecosistema de movilidad inteligente, introduciendo nuevos niveles de sofisticación cibernética y vectores de ataque

En el año 2005 ingresé a trabajar como instructor de tiro para el personal de seguridad (oficiales de seguridad y escoltas) de la mayor empresa de producción de alimentos de Venezuela, en el año 2007 ascendí a supervisor general de seguridad de dicha organización, recuerdo cuando en el año 2008 vino a Venezuela la princesa de Tailandia a entregar un premio a dicha corporación por la utilización del vetiver en la producción de algunos productos.

Allí fue cuando tuve mi primera experiencia en el estudio, planificación y ejecución de avanzadas móviles en la protección ejecutiva, los profesionales que están leyendo y que se dedican a esta rama de la seguridad sabrán que al realizar una avanzada de un punto A a un punto B, son muchísimas las variantes a evaluar, entre estas podría nombrar:

- Tránsito automotor.
- Vías terrestres.
- Puntos donde falla la señal de telefonía.
- Solicitar en el destino u hotel la identificación del personal que labora en dicha espacio: gerente nocturno, gerente diurno, entre otros.
- Buscar una habitación que esté al final del pasillo, que no tenga accesos por ventanas.

Son muchas variantes que les pudiera mencionar, pero de nada valdría porque éstas, a su vez, no son estrictas o fijas, ya que siempre variarán de acuerdo con el momento y circunstancia, lo interesante de todo esto es mantenerse siempre a la vanguardia y no tener estructuras de seguridad rígidas, ya que como dice Ivan Ivanovich en su libro *"Protección Ejecutiva en el siglo XXI: La Nueva Doctrina"*: "Tenemos que saber quiénes son, cómo saben quiénes somos, tenemos que saber dónde están, cómo saben dónde estamos, tenemos que seguirlos, cómo nos siguen a nosotros, tenemos que sorprenderlos, cómo nos quieren sorprender a nosotros".

Tomando en consideración este punto donde se les sugiere que debemos mantenernos a la vanguardia de las nuevas tendencias o doctrinas, el área tecnológica no escapa de esto, el personal de seguridad y protección ejecutiva debe estar alineado y conocer las tendencias de ciberseguridad para prestar un servicio acorde con los nuevos tiempos.

El año pasado recibí una llamada telefónica de un colega venezolano radicado en Perú, quien presta protección a una de las cantantes de reggaetón de moda, el cual tenía un inconveniente con su equipo de operadores de protección, ya que se había filtrado la información del lugar de estadía donde esta cantante estaría un fin de semana con su pareja, al filtrarse la información un cúmulo de fanáticos se acercaron a recibir en el aeropuerto a la cantante y el doble de personas estuvieron atentos al arribo de la misma en el hotel destino, ella molesta le reclamó a su equipo de seguridad, ya que sólo cinco personas conocían este itinerario.

Al realizar las técnicas correspondientes determiné que uno de estos escoltas, días previos al viaje, había ingresado a una página pornográfica utilizando su teléfono móvil celular descargando un *malware*, por el cual se filtró la información, evidentemente un cantante no es el tipo de objetivo que busquen asesinar, tal vez extorsionar cómo posiblemente fue esta la ocasión, y al no concretarse la misma fue expuesta la privacidad de la cantante.

En los primeros seis meses de este año, las predicciones se han hecho realidad, por ejemplo: los ataques y manipulaciones en la infraestructura EV, los ataques basados en API han aumentado drásticamente lo que permite a los adversarios expandir el impacto a una escala mayor de vehículos, incluso flotas enteras

Los distintos equipos de profesionales dedicados a la ciberseguridad tienen la tarea de enfrentar las amenazas que van más allá de los ataques directos contra los vehículos, apuntando a flotas, aplicaciones y servicios de movilidad e incluso a las estaciones de carga de vehículos eléctricos

Pongo esto como ejemplo para entrar en contexto sobre la seguridad informática y la seguridad de la información que debe tener un equipo de protección y más si hablamos sobre la ciberseguridad en los vehículos de protección ejecutiva, como bien saben ya los automóviles dejaron de ser vehículos con computadoras ahora son computadoras hechas vehículos.

COMPUTADORAS QUE SON VEHÍCULOS

Sólo tenga esto en consideración, si existe un altercado donde un atacante intenta detener el vehículo de un VIP mediante disparos a los neumáticos, estos van a resistir y continuar la marcha ya que cuentan con el dispositivo *Run Flat*, el cual no es más que un neumático macizo de caucho dentro del neumático convencional, si bien es cierto que la huida o marcha no será a gran velocidad nos sacará del apuro al continuar la marcha sin detenerse.

Pero en los vehículos modernos la situación cambia, ya que si este altercado ocurriera los sensores van a reconocer la falla y la computadora ordenará que el vehículo se detenga exponiendo totalmente al PMI y a la operación en sí, es por esto que conocer de ciberseguridad en los vehículos de protección ejecutiva es vital.

De acuerdo con el Informe de Ciberseguridad Automotriz Global 2023, la industria automotriz se está expandiendo rápidamente hacia un vasto ecosistema de movilidad inteligente, introduciendo nuevos niveles de sofisticación cibernética y vectores de ataque.

Dice este informe que los nuevos vectores de ataque redefinirán la ciberseguridad automotriz, ya que han transformado dicha industria en un ecosistema de movilidad inteligente más, sin embargo, con la transformación hay nuevos riesgos de seguridad informática que deben abordarse, como, por ejemplo, el aumento exponencial de los ataques cibernéticos tanto en su magnitud, frecuencia y sofisticación.

En los primeros seis meses de este año, las predicciones se han hecho realidad, por ejemplo: los ataques y manipulaciones en la infraestructura EV, los ataques basados en API han aumentado drásticamente lo que permite a los adversarios expandir el impacto a una escala mayor de vehículos, incluso flotas enteras.

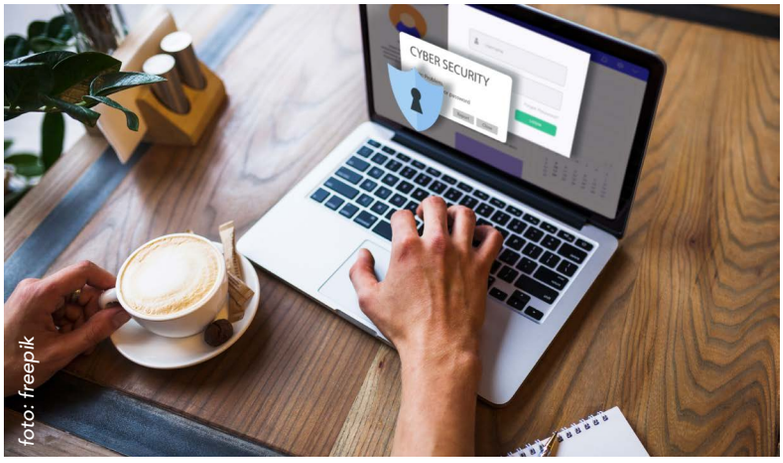


foto: freepik

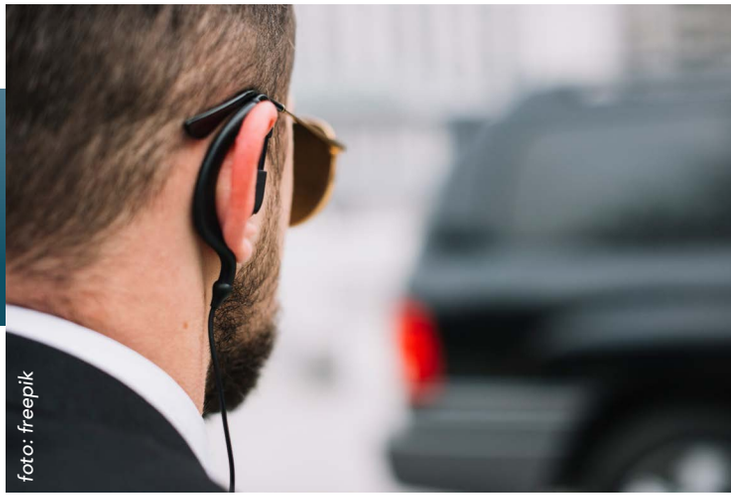


foto: freepik

Pero no todo es malo, ya que las empresas o instituciones han tomado en cuenta todas estas problemáticas y han comenzado a implementar y mejorar por medio de normativas para proteger los activos de movilidad inteligente y garantizar la confianza y seguridad de los conductores y operadores de protección ejecutiva.

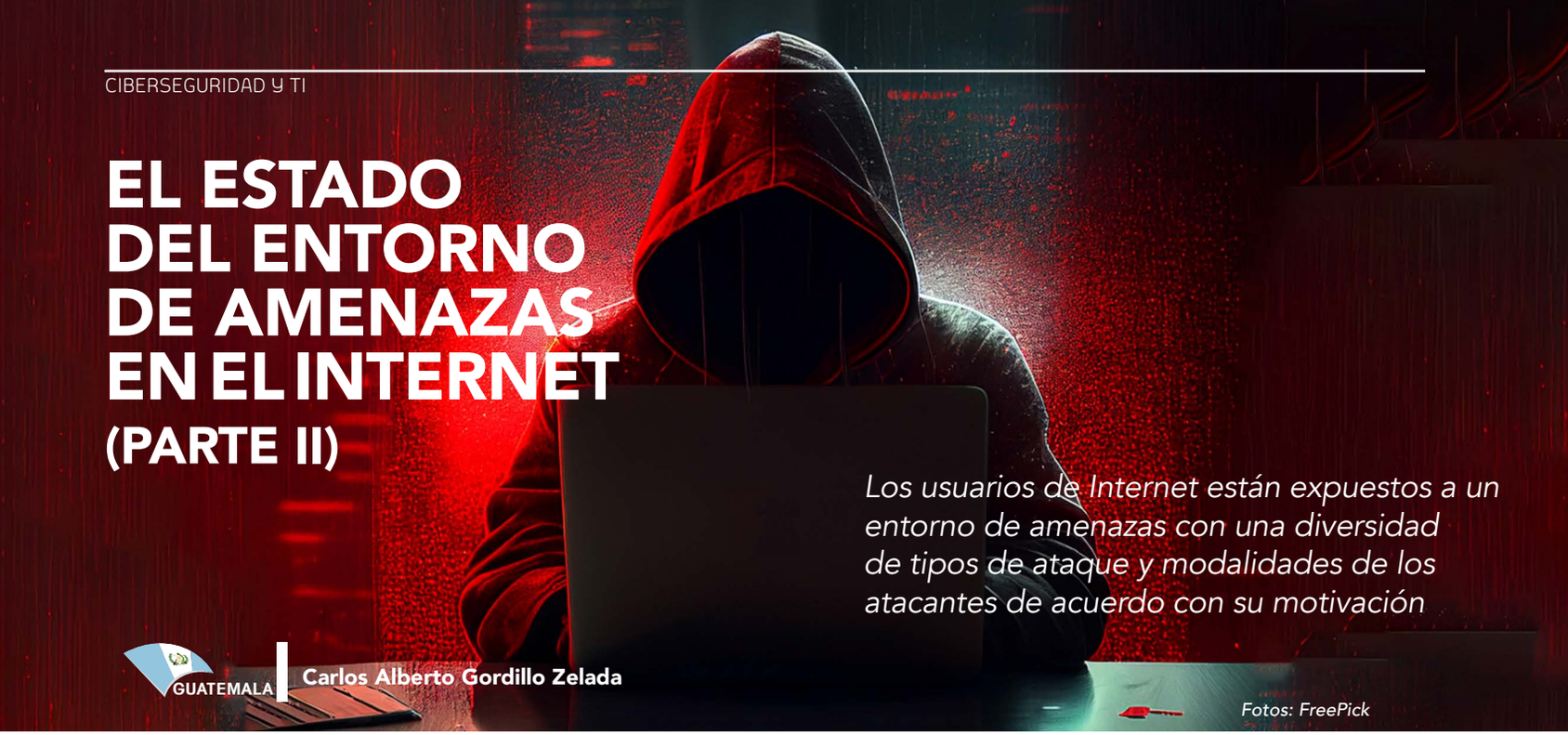
Existen normas como la ISO/SAE 21434, la UNECE WP.29 R155 y R156, esta última entró en vigor en el año 2021, presentó su primer hito en el año 2022 y en este año 2023 tuvo una de las mejores actualizaciones que ha recibido aplicándose a todos los tipos de vehículos nuevos. Los distintos equipos de profesionales dedicados a la ciberseguridad tienen la tarea de enfrentar las amenazas que van más allá de los ataques directos contra los vehículos, apuntando a flotas, aplicaciones y servicios de movilidad e incluso a las estaciones de carga de vehículos eléctricos, ya que éstos representan actualmente el 4% de los ataques o incidentes a EV lo cual sin duda seguirá en aumento durante este año.

Los profesionales de la ciberseguridad nos hemos dedicado a fortalecer las distintas ramas de la seguridad, pero también lo han hecho los ciberdelincuentes, por lo cual los operadores de protección ejecutiva deben permanecer cada vez más atentos y en constante capacitación para garantizar que se puedan cumplir los objetivos y servicios trazados.

A medida que los vectores de ataques crecen y se vuelven más complejos, la ciberseguridad de IT centrada en vehículos de protección ejecutiva se entrelaza cada vez más. ■

Adolfo M. Gelder, director del Proyecto Mente Táctica. *Más sobre el autor:*

EL ESTADO DEL ENTORNO DE AMENAZAS EN EL INTERNET (PARTE II)



Los usuarios de Internet están expuestos a un entorno de amenazas con una diversidad de tipos de ataque y modalidades de los atacantes de acuerdo con su motivación

GUATEMALA | **Carlos Alberto Gordillo Zelada**

Fotos: FreePick

TIPOS DE AMENAZAS EXISTENTES

Las amenazas por parte de las fuentes adversarias puede dar como resultado fraudes y robos; una amenaza interna puede provocar destrucción de *hardware* o instalaciones, implantar código malicioso, destruir datos o programas, borrar información, bloquear el sistema e incluso cambiar contraseñas y usuarios para mantener el acceso al sistema; mientras que los *hackers* maliciosos pueden realizar ataques en las redes, operar *bots* para controlarla, llevar a cabo actos criminales para apropiarse de dinero, así como servicios de inteligencia extranjera, *phishing*, actos terroristas, envío de *spam* o distribuir código malicioso o *software* espía.

ATAQUES (EXTERNOS)

Los ataques a las redes o hacia servidores objetivo pueden venir de atacantes utilizando la conexión a Internet, en ocasiones pueden venir de empleados o ex empleados, utilizando credenciales robadas o utilizando atributos que les fueron concedidos por sus responsabilidades en la organización. Estos atentados pueden realizarse con el propósito de fraude, obtener algún beneficio monetario o de apropiarse de propiedad intelectual de la organización.

En el X.800 y RFC 4949[1] se define la clasificación de los atentados a la seguridad, como activos y pasivos, en donde los ataques pasivos son de la naturaleza del monitoreo de la transmisión de datos, con el objetivo de obtener información que esté siendo transmitida, en donde pudieran estar nombres de usuario, contraseñas o cualquier otra información, con el simple hecho de revisar el contenido de los mensajes. El otro tipo de ataque pasivo es el análisis de tráfico, normalmente datos encriptados; y el objetivo es analizar la información que está siendo transmitida, con esto se pueden identificar patrones de comunicación, frecuencia y la longitud de los mensajes que están siendo intercambiados, esto para poder identificar la naturaleza de la información que está siendo transmitida. Estos últimos, son ataques bastante difíciles de detectar pues no existe ninguna alteración en los datos.

Los ataques activos involucran la modificación de los datos del mensaje capturado o la creación de mensajes falsos, y está subdividido en cuatro categorías:

- **Mascarada:** esto se presenta cuando un atacante se hace pasar por un usuario real en la comunicación entre dos interlocutores. Usualmente este tipo de atentado incluye una de las otras categorías de ataques activos.
- **Repetición:** este tipo de situación involucra la captura pasiva de cierta información o datos y posteriormente retransmitirlo para producir un efecto no autorizado.
- **Modificación del mensaje:** este ataque se hace a través de tomar una parte del mensaje legítimo y alterarlo, modificarlo para retrasarlo o reordenarlo, para producir un efecto no autorizado.
- **Denegación de servicio:** este ataque bloquea o inhibe el uso normal de un servicio de comunicaciones; este ataque debe tener un objetivo específico, con la intención de no permitir que se alcance el destino requerido, incluso logrando una interrupción de la red completa que quiere comunicarse al equipo afectado.

Los ataques activos presentan características opuestas a los ataques pasivos, ya que, aunque se pueden detectar, éstos son bastante difíciles de controlar, pues existe una variedad muy grande de *software*, potencial físico y vulnerabilidades de red. Siendo el propósito principal de la detección, la recuperación de una interrupción o de reducir los retrasos que éstos puedan provocar, tratando de que el efecto sea el menos dañino posible.

MALWARE (PROGRAMAS MALICIOSOS)[2]

Término utilizado para describir el *software* "malvado" o al *software* maligno, dentro del cual el más conocido es el virus de computadora, pero también existen otras variantes como *Trojan Horses*, el *spam* y otros tipos como los RATs (*Remote Access Trojans*).

- **Virus:** son programas donde ellos mismos se adjuntan a programas legítimos en la computadora de la víctima; para después infectar otros programas que son transferidos a otras computadoras y donde son ejecutados. Normalmente contaminan medios portátiles de almacenamiento y se transfieren a computadoras, cuando estos dispositivos son conectados.

- ***Worms:*** este tipo de programa actúa como virus y puede propagarse de muchas formas; saltando directamente de una computadora a otra, sin la intervención de un usuario en la computadora receptora. Este tipo de amenazas toman ventajas de vulnerabilidades o debilidades en el *software*, siendo propagados directamente al instalarse él mismo, en otra computadora; son altamente agresivos en su modo de esparcimiento.
- ***Payloads:*** cuando los virus y los *worms* son propagados, normalmente ellos ejecutan *payloads*, que son segmentos de código que ejecutan daño en el sistema infectado, pudiendo borrar archivos del disco duro, o instalando otro tipo de *malware*.
- ***Trojan horses:*** este tipo de programas se categoriza como un *malware* no-móvil, estos programas normalmente aparentan ser una cosa, tal como un juego o incluso una versión pirata de un programa comercial, pero que en realidad son *malware*, escondiéndose él mismo, borrando un archivo del sistema y toman el nombre del archivo borrado.
- ***Rootkits:*** estos programas son *trojan horses* reemplazando programas legítimos, capaces de ejecutar diferentes comandos al tomar el control de la cuenta primaria o administrador *(root, administrator,* etc.) utilizando esos privilegios para ocultarse y ejecutando un grupo de instrucciones para causar daño al sistema.

BOTS O BOTNETS

Un *bot* también conocido como *zombie*, es un dispositivo conectado a Internet (computadora o dispositivo móvil), que infecta con *malware* sin que el usuario esté conciente y es controlado remotamente por un atacante para realizar una actividad maliciosa. Un *botnet*, es un grupo de estos dispositivos que son coordinados por el atacante, en donde este tipo de redes típicamente expanden escaneando el ambiente conectado en línea y encontrando las vulnerabilidades en los dispositivos conectados pudiendo proveer poder computacional para aumentar la capacidad del atacante.

Los *botnets* son utilizados para varios propósitos dentro de los cuales están los ataques de denegación de servicio distribuidos (DDoS), propagación de *malware*, envío de *spam*, robar datos o manipular información, realizar campanas de fraude o realizar campanas masivas de publicaciones en redes sociales con el interés de manipular la opinión pública.

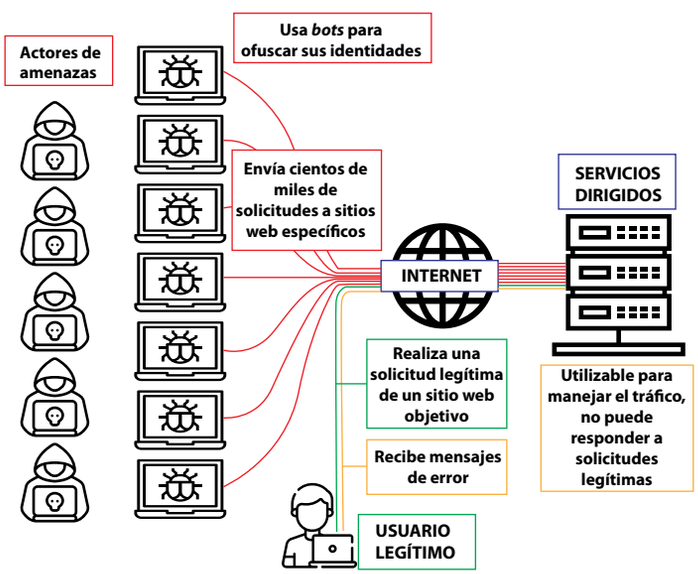


Fig 1. Forma en que opera una Denegación de Servicio Distribuida (DDos)[3]

MAN-IN-THE-MIDDLE

Esta es una técnica en la cual el atacante intercepta la comunicación entre dos dispositivos en la red, en donde uno podría ser la victima y le otro un servidor web, sin que la victima se de cuenta, dando la apariencia de que la víctima se esta comunicando con directamente y de forma segura con el servidor web. Durante éste, el atacante, monitorea la comunicación, cambia el enrutamiento del tráfico, altera la información, entrega el *malware* a la computadora de la víctima pudiendo accesar información personal de la víctima o cualquier otro tipo de información sensible que este dentro de la computadora afectada. Este tipo de ataque puede utilizar otras herramientas como *phishing, eavesdropping* u otras técnicas para poderlo lograr.

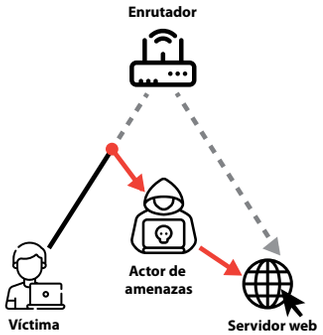


Fig.2. Forma en que opera un ataque Man-In-The-Middle[4]

PHISHING, SPOOFING, SPEAR-PHISHING Y WHALING

Este tipo de técnicas o métodos son utilizados por los atacantes y pueden hacerse pasar por organizaciones con credibilidad, con la intención de atraer a un gran número de receptores y lograr que les sean provistos, usuario y contraseñas, información bancaria u otro tipo de información personal. Este tipo de ataques son clasificados dentro de las técnicas de la ingeniería social actuando inicialmente con el envío de un correo electrónico utilizando el nombre de un origen confiable, mientras que el usuario se convierte en víctima cuando abre adjuntos maliciosos o da clic en enlaces que lo redirigen a sitios web.

El *spoofing* generalmente actúa enmascarando el sitio web, la dirección de correo de origen o el número telefónico con el de un sitio confiable, logrando que la víctima reciba el mensaje y engañándola para que le proporcione información personal, bancaria u otro tipo de información sensible dándole clic a algún enlace o adjunto malicioso infectando la computadora con algún *malware.*

El *spear-phishing* ocurre cuando el atacante envía un mensaje personalizado hacia su víctima, que en su mayoría, han utilizado alguna otra técnica de ingeniería social para mencionar detalles y son creíbles para la víctima como que un origen confiable. *Whaling* es un tipo de *spear-phishing* dirigido a ejecutivos *senior* o a otro tipo de receptores con alto perfil con privilegio de acceso y autorizaciones que pudieran utilizar para accesar a los sistemas de información al robar usuarios y contraseñas.

RANSOMWARE

El *ransomware* generalmente instala un *software malicioso* usando un *trojan horse* desplegado por *phishing* o visitando algún sitio web. Este tipo de ataque restringe el acceso a una computadora o algún dispositivo mediante la encriptación de la información contenida y cuyo atacante demanda un pago para liberar el secuestro del dispositivo, usualmente el pago debe ser realizado con una criptomoneda y de esta manera liberar el dispositivo. En algunas ocasiones este ataque también puede interrumpir el servicio de cierto servidor, amenazar con distribuir información confidencial o personal a menos que el rescate sea pagado.

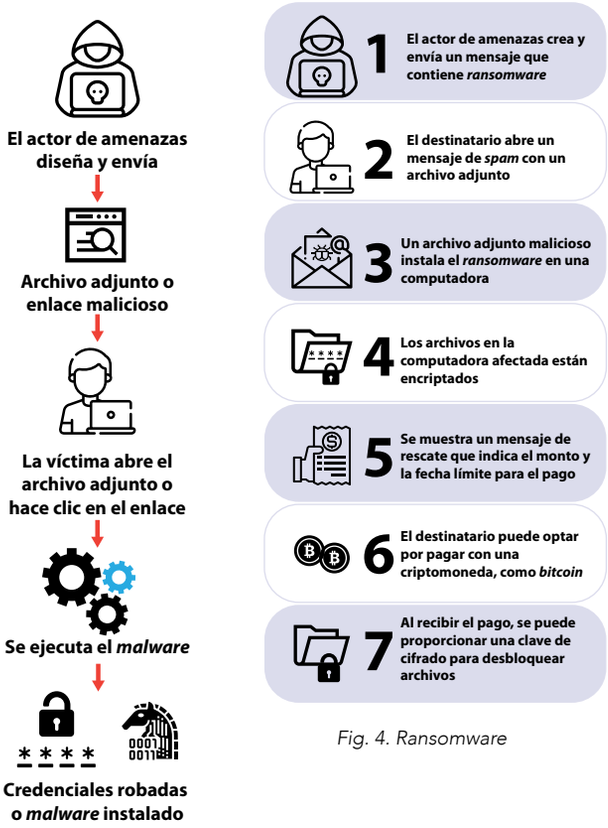


Fig. 4. Ransomware

Fig. 3. Phishing y spear-phishing

CONCLUSIÓN

La seguridad informática tiene como objetivo principal proteger la confidencialidad, la integridad y la disponibilidad de los sistemas de información, dicha protección de la información y de los sistemas incluye el acceso no autorizado, el uso, la interrupción, la modificación, la destrucción y la divulgación de los datos e información. Las organizaciones que actualmente utilizan como medio de comunicación el Internet, deben realizar esfuerzo para proteger ante un entorno de amenazas al estar conectado por este medio, y que en muchos casos pone en riesgo la reputación de la organización al ser víctima de un ataque, comprometiendo la información.

Es por ello, que para tener un ambiente protegido es necesario iniciar con la implementación de su política de seguridad, lo que dará un marco apropiado para que los procedimientos y estándares sean correctamente aplicados e incluso se mantenga una cultura de seguridad en la organización, la cual será de aplicación general para los empleados, proveedores y clientes.

Dentro del ambiente de seguridad integral se puede tener un entorno de amenazas controlado, esto incluye el conocimiento de las amenazas y los riesgos, su impacto en la organización, así como el establecimiento de procedimientos y planes de acción a seguir en el caso del descubrimiento de brechas de seguridad, identificación de vulnerabilidades, seguimiento de incidentes y documentación de los mismos, así como la publicación lecciones aprendidas en donde la administración de la seguridad es parte de la cultura organizacional, siendo los más importante, conocer el entorno de amenazas al que están expuestas las organizaciones, puesto que el conocer a nuestro enemigo, nos dará la posibilidad de estar preparados.

RECOMENDACIÓN

Dada la importancia del conocimiento del entorno de amenazas para mantener un sistema de seguridad integral, así también se hace necesaria la adopción e implementación de una política de seguridad de la información en la que se definen las directivas, las regulaciones, las reglas y las prácticas que se prescribirán por la administración de la organización con el objetivo de gestionar, proteger y distribuir información. Dentro de esta política se deben definir también los estándares, los procedimientos y las pautas para la organización a manera de contar con todas las herramientas necesarias. Dentro de los componentes básicos de la política deben estar: el propósito, el alcance, los roles y responsabilidades, y la definición del criterio de cumplimiento.

Es también importante el establecimiento de un proceso continuo de evaluaciones de riesgos en las que se pueden tener mediciones periódicas de los riesgos a los que está expuesta la organización en el entorno de amenazas en el Internet, de forma que se tenga un ciclo de evaluación, monitoreo y respuesta, para mantener un ambiente de control. ■

Referencias:

[1] *X.800 forma parte de la Unión Internacional de Telecomunicaciones, aprobada el 22 de marzo de 1991 en Ginebra y el RFC 449 describe el Internet Security Glossary, Versión 2.*

[2] *Fuente: Corporate Computer Security – 3rd Edition - Randall J. Boyle - Raymond R. Panko.*

[3] y [4] *Fuente: An Introduction to the Cyber Threat Environment - Canadian Centre for Cyber Security.*

- *Corporate Computer Security – 3rd Edition - Randall J. Boyle - Raymond R. Panko.*
- *An Introduction to the Cyber Threat Environment - Canadian Centre for Cyber Security.*
- *An Introduction to Information Security - NIST Special Publication 800-12 Revision 1 • Network Security Essentials – 6th Edition – William Stallings.*

Carlos Alberto Gordillo Zelada, Ingeniero en Electrónica y MSc Tecnologías de la Información con especialidad en Seguridad Informática. *Más sobre el autor:*

Protegemos lo **que más valoras.**

SOLUCIONES ESTRATÉGICAS
RE & MI
S.A. DE C.V.
SEGURIDAD PRIVADA

#EmpresaSegura

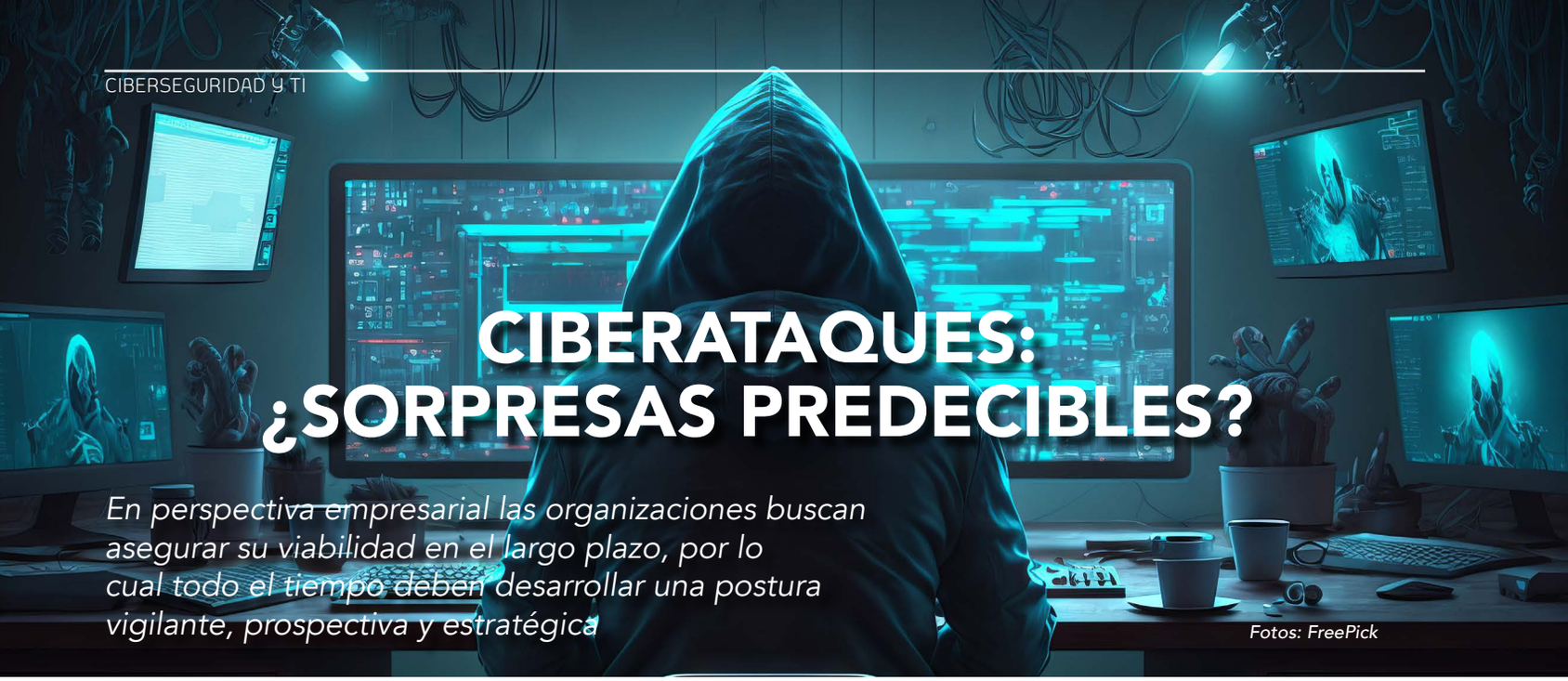
Seguridad inquebrantable

Tu confianza está respaldada por nuestra experiencia.

Eje Central Lázaro Cárdenas #555
Int. 303, Benito Juárez, CP 03020,
Ciudad de México.

www.remi.mx

Informes al teléfono:
55 72 58 92 26



CIBERATAQUES: ¿SORPRESAS PREDECIBLES?

En perspectiva empresarial las organizaciones buscan asegurar su viabilidad en el largo plazo, por lo cual todo el tiempo deben desarrollar una postura vigilante, prospectiva y estratégica

Fotos: FreePick

COLOMBIA

Jeimy Cano

Con el paso de los días se advierte cada vez más un mundo turbulento, incierto, novedoso, y ambiguo (Ramírez & Wilkinson, 2016), donde todos los esfuerzos por concretar una nueva estabilidad, implican necesariamente generar inestabilidades moderadas o extremas para alcanzar lo que podría llamarse un equilibrio dinámico, al que todo el mundo debe acostumbrarse, con la salvedad de que en algún momento llegará el "agotamiento" por adaptación propio de los cambios permanentes e inesperados.

En el mundo de los negocios, sin riesgos no se generan nuevas oportunidades, ni se concretan mejores utilidades. En este sentido, el gobierno y gestión de riesgos se convierte en un mantra natural de las organizaciones con el fin de alcanzar certezas y moverse con inciertos menores para concretar su agenda estratégica. Por tanto, comprender la esencia de lo que significa el riesgo impone un reto y una ruta conceptual y práctica para las organizaciones. Lo anterior se puede sintetizar en tres preguntas (Renn, 2008, p.12):

- ¿Qué son los resultados indeseables y quién determina qué significa indeseable?
- ¿Cómo podemos especificar, calificar o cuantificar las posibilidades de resultados indeseables?
- ¿Cómo agrupar las distintas clases de resultados indeseables en un concepto común que permita la comparación, el establecimiento de prioridades y la comunicación eficaz del riesgo?
- La respuesta a estas preguntas implica necesariamente tres juicios de valor (que deberán estar debidamente fundados) como son: (Renn, 2008, p.44)

La lista de criterios en función de los cuales debe juzgarse la aceptabilidad o tolerabilidad del riesgo, los equilibrios entre los criterios mencionados previamente, y las estrategias de resiliencia para hacer frente a las incertidumbres restantes.

Así las cosas, como se puede observar el riesgo más allá de ser una probabilidad que se calcula o concreta de forma cuantitativa, termina como una valoración conjunta e inteligente (debidamente documentada y retada) de aquellos que participan en el proceso, con el fin de situar y declarar un apetito de riesgo, que termina definiendo hasta dónde la organización es capaz de soportar el estrés de sus variables más importantes, sin activar sus umbrales de operación alternativos, para mantener sus planes y alcanzar sus objetivos claves.

En este entendido, la gobernanza del riesgo demanda identificar y comprender la compleja red de agentes, normas, convenciones, procesos y mecanismos que intervienen en la recogida, el análisis y la comunicación de la información pertinente sobre el riesgo, así como la toma de decisiones sobre su gestión (Renn, 2008), que no es otra cosa, que reconocer de forma sistémica el acoplamiento e interacción de cada uno elementos de esta red, con el fin de establecer los puntos más sensibles en este tejido de interconexiones donde un evento no esperado o no deseado puede concretar efectos dominó que puedan alcanzar la dinámica de toda la organización, sin capacidad de respuesta o amortiguamiento de sus efectos.

Considerando lo anterior, el riesgo de un ciberataque para una organización puede reescribirse siguiendo la definición de Luhmann (1990), como "la posibilidad de un daño futuro, superior a todos los costos razonables", que en últimas se traduce como la toma de decisiones corporativas sobre el apetito de riesgo de la empresa y su ventana de exposición frente sus amenazas conocidas, latentes y emergentes, que conlleven resultados indeseables que se pueden dar por la materialización de este tipo de eventos adversos.

En este sentido, los ciberataques se pueden catalogar como sorpresas predecibles, que son aquellas en las que: (Bazerman & Watkins, 2004)

- Los líderes permanecen ajenos a una amenaza o problema emergente.
- Los líderes reconocen la amenaza, pero no le dan la prioridad.
- Los líderes reconocen la amenaza, dan la prioridad, pero no responden eficazmente.

Lo anterior supone una baja madurez en la gobernanza y gestión del riesgo cibernético donde las prioridades y lecturas de este riesgo a nivel corporativo son disyuntas, creando una zona de inestabilidad

e incierto que tendrá como objetivo la dinámica de la organización y sus procesos, comprometiendo su promesa de valor y sobremanera, exponiendo a la empresa a consecuencias no previstas y no lineales, comoquiera que el riesgo cibernético es un riesgo sistémico, emergentes y disruptivo (Cano, 2023).

ASUMIR EL RETO EN LAS EMPRESAS

En perspectiva empresarial las organizaciones buscan asegurar su viabilidad en el largo plazo, por lo cual todo el tiempo deben desarrollar una postura vigilante, prospectiva y estratégica en donde hoy, el riesgo cibernético y el incremento de ciberataques, marcan una nueva ruta corporativa frente a las iniciativas digitales que apalancan la transformación digital de las compañías. Por tanto, se hace necesario que las compañías asuman el reto de conectar la dinámica empresarial con un aumento sostenido de la densidad digital donde los clientes demandan nuevas experiencias, novedosas y ajustadas con sus expectativas.

Así las cosas, al menos tres preguntas deberán estar sobre la mesa para movilizar los análisis y decisiones respecto a las iniciativas digitales de la empresa (Kaplan *et al*., 2015):

- ¿El negocio está informado sobre el incremento del nivel de exposición de la empresa con la nueva iniciativa? ¿Está ajustada con la declaración de apetito de riesgo de la compañía?
- ¿Cómo se diseñará esta iniciativa para generar la mejor experiencia en el cliente y el menor riesgo de pérdida (daño o inaccesibilidad) del servicio por un ciberataque?
- ¿El negocio conoce con claridad la dinámica y amenazas del ecosistema digital donde se enmarca la iniciativa que se quiere desarrollar?

Cuando la organización descuida o ignora los retos que impone el riesgo cibernético crea una serie de condiciones que habilitan la materialización de posibles ciberataques. Estas condiciones son:

- La organización falla en la caracterización de sus adversarios, alineado con sus objetivos de negocio.
- La organización no logra conectar las piezas de información de la inteligencia de amenazas, para analizarla y establecer sus impactos.
- La empresa no incentiva a los analistas o ejecutivos claves para adelantar prospectiva de los riesgos latentes y emergentes.
- La comunidad empresarial no preserva la memoria ni aprendizajes de ciberataques previos ni de sus estrategias para atenderlos.
- La organización no hace ejercicios ni simulaciones periódicas para retar su saber previo y así hacerse más resiliente en el futuro cercano.

En este contexto, los riesgos de negocio, atravesados por esta nueva realidad digital, deberán considerar al menos tres elementos para su comprensión (Kaplan *et al*., 2015):

- Un activo de información valioso (por ejemplo, información sanitaria personal, un proceso de fabricación de un nuevo producto).
- Un atacante (por ejemplo, ciberdelincuentes organizados, un actor patrocinado por el Estado, amenaza interna).
- Un impacto empresarial (por ejemplo, exposición normativa o legal, espionaje espionaje industrial), los cuales constituyen el marco de comprensión tradicional de los posibles alcances de los riesgos cibernéticos y sus posibles impactos, superando las posturas tradicionales de gestión de riesgos que por lo general terminan con apuestas de controles basados en un ejercicio de protección y aseguramiento, y no situado en las consecuencias que se pueden concretar por cuenta de la materialización de un ciberataque.

En consecuencia, una organización que comprende el nuevo escenario de riesgo cibernético en lectura de los riesgos de negocio (ahora enriquecidos y aumentados en el contexto digital), sabe que tarde o temprano tendrá un evento cibernético adverso y por lo tanto deberá adaptarse a las sorpresas, actuar con flexibilidad ante la inevitabilidad de la falla, implementar una postura de falla segura, monitorizar los potenciales efectos de borde y activar los umbrales de operación que le permitan mantener la operación a pesar de un ataque cibernético exitoso.

Concebir el gobierno y gestión de riesgos cibernéticos como un espacio más de aprendizaje y reto permanente del equipo ejecutivo, significa trasladar el foco de atención de los riesgos en sí mismos al desarrollo e implementación de estrategias frente a sus consecuencias. Significa replantearse los procesos de construcción y lectura de la realidad en red, donde participen los diferentes actores para crear y mantener conexiones mucho más estrechas entre el equipo de ciberseguridad y cada función empresarial crítica -desarrollo de productos, *marketing* y ventas, cadena de suministro, asuntos corporativos, RRHH y gestión de riesgos- con el fin de establecer los acuerdos de niveles de protección ajustados con el apetito de riesgo empresarial, la salvaguarda de los activos de información y el funcionamiento de los procesos empresariales clave, de forma eficiente y eficaz. ■

Referencias:

- *Bazerman, M. & Watkins, M. (2004) Predictable surprises. The disasters you should have seen coming and how to prevent them. Boston, MA. USA: Harvard Business School Press.*
- *Cano, J. (2023). Maturity Model for Boards of Directors in Cyber Risk Governance. A Conceptual and Practical Proposal. En: Rocha, Á., Fajardo-Toro, C.H., Riola, J.M. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies. Vol 328. 39–51. Springer, Singapore. https://doi.org/10.1007/978-981-19-7689-6_4*
- *Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. & Rezek, C. (2015). Beyond cybersecurity. Protecting your digital business. Hoboken, NJ. USA: John Wiley & Sons.*
- *Luhmann, N. (1990). Technology, environment and social risk: a systems perspective. Industrial Crisis Quarterly, 4(3), 223- 231. doi:10.1177/108602669000400305*
- *Ramírez, R. & Wilkinson, A. (2016). Strategic reframing. The Oxford Scenario Planning Approach. Oxford, UK. Oxford Press.*
- *Renn, O. (2008). Risk Governance. Coping with Uncertainty in a Complex World. London, UK.: EarthScan.*

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:

ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Estableciendo mejores prácticas para la ciberseguridad

Fotos: FreePick

COLOMBIA

Javier Nery Rojas Benjumea

Las normas que forman la serie ISO-27000 son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.

Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés, Information Security Management System (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos.

- **ISO 27000:** facilita las bases y lenguaje común para el resto de las normas de la serie.
- **ISO 27001:** especifica los requerimientos necesarios para implantar y gestionar un SGSI. Esta norma es certificable.
- **ISO 27002:** define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.
- **ISO 27003:** proporciona una guía para la implantación de forma correcta un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.
- **ISO 27004:** proporciona pautas orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI.
- **ISO 27005:** define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información orientado en cómo establecer la metodología a emplear.
- **ISO 27006:** establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001.
- **ISO 27007:** es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar implementaciones de la ISO/IEC-27001.
- **ISO 27008:** define cómo se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos.
- **ISO 27009:** complementa la norma 27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivo de hacer más eficaz su implantación.
- **ISO 27010:** indica cómo debe ser tratada la información cuando es compartida entre varias organizaciones, qué riesgos pueden aparecer y los controles que se deben emplear para mitigarlos, especialmente cuando están relacionados con la gestión de la seguridad en infraestructuras críticas.
- **ISO 27011:** establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando cómo implantar los controles de manera eficiente.
- **ISO 27013:** establece una guía para la integración de las normas 27001 (SGSI) y 20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.
- **ISO 27014:** establece principios para el gobierno de la seguridad de la información, para que las organizaciones puedan evaluar, monitorizar y comunicar las actividades relacionadas con la seguridad de la información.
- **ISO 27015:** facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros, tales como servicios bancarios o banca electrónica.
- **ISO 27016:** proporciona una guía para la toma de decisiones económicas vinculadas a la gestión de la seguridad de la información, como apoyo a la dirección de las organizaciones.
- **ISO 27017:** proporciona una guía de 37 controles específicos para los servicios Cloud, estos controles están basados en la norma 27002.
- **ISO 27018:** complementa a las normas 27001 y 27002 en la implantación de procedimientos y controles para proteger datos personales en aquellas organizaciones que proporcionan servicios en *Cloud* para terceros.

- **ISO 27019:** facilita una guía basada en la norma 27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI.

Como ya se indicó la ISO 27001 es un estándar para la seguridad de la información (*Information Technology – Security Techniques – Information Security Management Systems – Requirements*), aprobado y publicado como estándar internacional en octubre de 2005, por la International Organization for Standardization y por la International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según el conocido "Ciclo de Deming": denotado por las siglas PDCA – acrónimo de *Plan, Do, Check, Act* (Planificar, Hacer, Verificar, Actuar).

Es consistente con las mejores prácticas descritas en ISO 27002, anteriormente conocidas como ISO/IEC 17799, cuyo origen es la norma BS 7799-2:2002; desarrollada por la British Standards Institution (BSI), entidad de normalización británica.

LA VERSIÓN ACTUAL DE LA NORMA ES ISO-27001:2013

La norma se encuentra dividida en dos partes, la primera se compone de los siguientes puntos:

- **Objeto y campo de aplicación:** especifica la finalidad de la norma, su uso dentro de una organización y el modo de aplicación del estándar.
- **Referencias normativas:** recomendación de la consulta a documentos necesarios para la aplicación del estándar.
- **Términos y definiciones:** los términos y definiciones usados se basan en la norma ISO 27000.

Contexto de la organización: se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información (SGSI). Se debe determinar el alcance.

- Entendiendo la organización y su contexto.
- Entendiendo las necesidades y expectativas de los implicados.
- Determinando el campo de aplicación del SGSI.
- Sistema de gestión de la seguridad de la información.

Liderazgo: habla sobre la importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas y asignando a los empleados de la organización roles, responsabilidades y autoridades, asegurando así la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operatividad.

- Compromiso.
- Políticas.
- Roles organizativos, responsabilidad y autoridades.

Planificación: se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicionalmente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para lograr dichos objetivos.

- Acciones para abordar riesgos y oportunidades.
- Objetivos de la seguridad de la información y cómo conseguirlos.

Soporte: se trata sobre los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de las partes interesadas, la importancia sobre la comunicación en la organización. La importancia de la información documentada.

- Recursos.
- Competencias.
- Concienciación.
- Comunicación.
- Información / documentación.

Operación: el cómo se debe planificar, implementar y controlar los procesos de la operación, así como la valoración de los riesgos y su tratamiento.

- Planificación operacional.
- Evaluación de riesgos.
- Tratamiento de los riesgos.

Evaluación de desempeño: debido a la importancia del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), se debe realizar un seguimiento, una medición, un análisis, una evaluación, una auditoría interna y una revisión por la dirección del SGSI del sistema de gestión de la información, para asegurar su correcto funcionamiento.

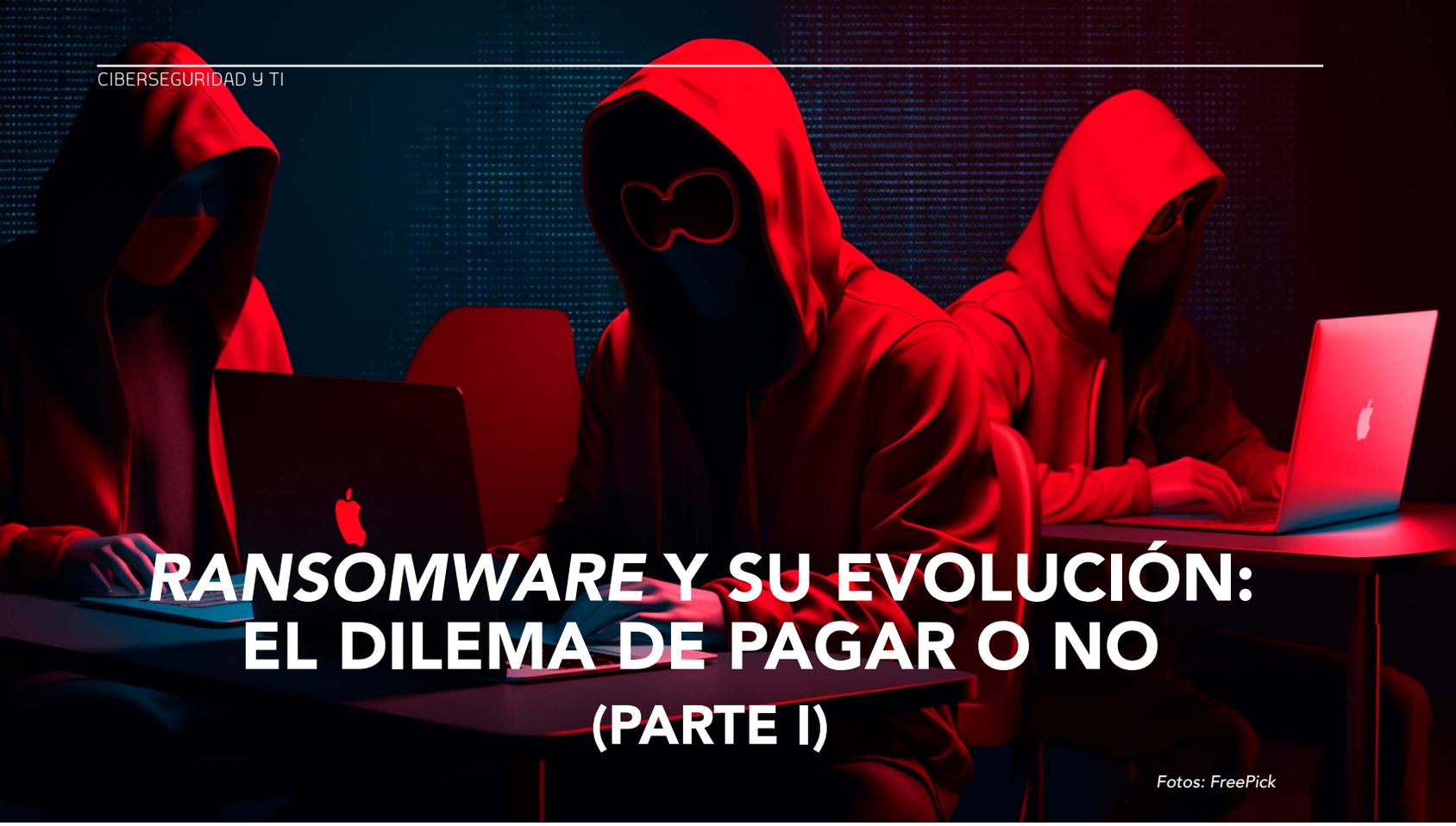
- Supervisión, medida, análisis y evaluación.
- Auditorías internas.
- Revisiones de la gestión.

Mejora: habla sobre el tratamiento de las no conformidades, las acciones correctivas y la mejora continua.

- Disconformidades y acciones correctivas.
- Mejora continua.

La segunda parte de la norma ISO-27001:2013, está conformada por el anexo A, el cual establece los objetivos de control y los controles de referencia. ■

Javier Nery Rojas Benjumea, MBA, CPP, *Board Certified in Security Management. Más sobre el autor:*



RANSOMWARE Y SU EVOLUCIÓN: EL DILEMA DE PAGAR O NO (PARTE I)

Fotos: FreePick

MÉXICO

Gigi Agassini

El ransomware ha estado por varias décadas y las primeras versiones surgieron a finales de los 80

El costo promedio de un ataque de *ransomware* es de 4.54 millones de dólares estadounidenses, sin incluir el pago de rescate que se efectúe para tratar de recuperar la información, según el reporte 2022, "Costo de una violación de datos" (Cost of Data Breach Report 2022), de IBM. En dicho reporte se menciona que, el once por ciento de las infracciones del estudio fueron ataques de *ransomware*, lo que significa un aumento desde 2021, cuando el 7.8% de las infracciones fueron *ransomware* para una tasa de crecimiento del 41%.

Particularmente en los últimos años se ha incrementado de manera sustancial los ataques de *ransomware* a diferentes compañías, sin importar su tamaño y/o giro y aunque existen varias preguntas alrededor de este vector de ataque la más común cuando eres víctima de éste es, ¿pagar o no pagar? Aunque no es nada sencilla la respuesta y depende de muchos otros factores de análisis para que tu organización pueda decidir qué es lo mejor para el negocio, comencemos revisando los básicos.

MALWARE

El *ransomware* es una forma de *malware* que cifra los archivos de la víctima, lo que permite al atacante exigir un "rescate" y que la víctima pueda "restaurar el acceso a su información" o datos, una vez realizado el pago del rescate solicitado, los costos pueden variar yendo desde cientos hasta miles de dólares pagaderos en criptomonedas, normalmente.

Malware, es la abreviatura de '*software malicioso*' (del inglés, *malicious software*), es un término genérico que se utiliza para describir cualquier tipo de *software* o programa diseñado para dañar, infiltrarse o realizar acciones no autorizadas en un sistema informático,

El ransomware es una forma de malware que cifra los archivos de la víctima, lo que permite al atacante exigir un "rescate" y que la víctima pueda "restaurar el acceso a su información" o datos, una vez realizado el pago del rescate solicitado, los costos pueden variar yendo desde cientos hasta miles de dólares en criptomonedas


Fotos: FreePick

dispositivo o red, sin el conocimiento o consentimiento del propietario o usuario.

El *malware* puede manifestarse de diferentes formas y llevar a cabo una variedad de actividades maliciosas, como robar información personal o confidencial, corromper archivos, bloquear el acceso a sistemas o dispositivos (*ransomware*), monitorear actividades del usuario, enviar *spam*, realizar ataques de denegación de servicio (DDoS) o instalar otros programas maliciosos. Existen diversos tipos de *malware* y entre los más comunes están:

- **Virus:** se adjunta a archivos ejecutables y se propaga al ejecutar dichos archivos.
- **Gusano *(Worm):*** se replica y se propaga a través de redes, aprovechando vulnerabilidades de seguridad.
- **Troyano *(Trojan):*** se presenta como un programa legítimo, pero en realidad, realiza acciones maliciosas en segundo plano.
- ***Ransomware*:** bloquea el acceso a archivos o sistemas y exige un rescate para restaurarlos.
- ***Spyware*:** monitorea y registra las actividades del usuario sin su conocimiento, con el fin de recopilar información personal.
- ***Adware:*** muestra publicidad no deseada, generalmente en forma de ventanas emergentes.
- ***Botnet:*** controla una red de dispositivos infectados para llevar a cabo ataques coordinados o distribuir *spam*.

Estos son sólo algunos ejemplos, pero el *malware* puede presentarse en muchas otras formas y variantes. La detección y prevención de *malware* son aspectos clave de la ciberseguridad, y se utilizan programas antivirus y otras herramientas de seguridad para proteger los sistemas contra estas amenazas.

SOFISTICACIÓN DEL *RANSOMWARE*

El *ransomware* ha estado por varias décadas y las primeras versiones surgieron a finales de los 80, el primer ataque conocido fue el troyano AIDS (también conocido como PC Cyborg) que en 1989 se lanzó a través de un disquete, se dirigía a los usuarios afirmando ser un *software* que podía proporcionar acceso a información relacionada con el SIDA. El rescate por víctima era de 189 dólares si querían restaurar el acceso a sus sistemas, el tipo de criptografía usado fue simétrica.

Con el tiempo el *ransomware* ha evolucionado y ha empleado algoritmos de encriptación mas sofisticados, explotando vulnerabilidades por la falta de actualización de sistemas y utilizando complejos métodos de distribución lo que ha permitido que este vector de ataque sea hoy, de los más peligrosos y usados por los criminales cibernéticos.

Estos son algunos de los vectores típicos de distribución de *ransomware* para infectar sistemas:

- **Correos electrónicos de *phishing*:** los atacantes envían correos electrónicos fraudulentos que contienen archivos adjuntos o enlaces maliciosos.
- ***Descargas maliciosas:*** los usuarios, sin saberlo, descargan archivos infectados de sitios web comprometidos o, a través de anuncios maliciosos.
- ***Kits de explotación*:** los ciberdelincuentes aprovechan las vulnerabilidades del *software* no actualizado o parchado para enviar "descargas de actualización" con *ransomware*.
- ***Compromiso del protocolo de escritorio remoto (RDP):*** los atacantes obtienen acceso no autorizado a los sistemas con credenciales RDP débiles o comprometidas.

Una vez que se descargan y abren (archivos, *links*), los delincuentes pueden hacerse cargo de la computadora de la víctima, especialmente si tienen herramientas de ingeniería social integradas que engañan a los usuarios para que permitan el acceso administrativo. Algunas otras formas más agresivas de *ransomware*, como NotPetya, aprovechan los agujeros de seguridad para infectar computadoras sin necesidad de engañar a los usuarios, lo que hace más compleja su detección.

Una vez que el *ransomware* se apodera del equipo de la víctima puede realizar diferentes acciones, desde borrar archivos, modificar información, pero por mucho la más común es cifrar algunos o todos los archivos de la víctima.

La infección no es evidente de inmediato para el usuario. El *malware* opera silenciosamente en segundo plano hasta que se implementa el sistema o el mecanismo de bloqueo de datos. Luego

Con el tiempo el ransomware ha evolucionado y ha empleado algoritmos de encriptación mas sofisticados, explotando vulnerabilidades por la falta de actualización de sistemas y utilizando complejos métodos de distribución lo que ha permitido que este vector de ataque sea hoy, de los mas peligrosos

Fotos: FreePick

aparece un cuadro de diálogo que le dice a la víctima que los datos han sido bloqueados y exige un rescate para desbloquearlos nuevamente. Para entonces, es demasiado tarde para guardar los datos a través de cualquier medida de seguridad.

ENCRIPTACIÓN DEL *RANSOMWARE*

A lo largo del tiempo, los desarrolladores de *ransomware* han evolucionado las técnicas de encriptación para hacerlos más sofisticados y difíciles de detectar. Estos son algunos ejemplos de las diferentes etapas de evolución en las encriptaciones de *ransomware*:

1) ***Ransomware* de cifrado simétrico:** los primeros *ransomware* utilizaban algoritmos de cifrado simétrico, como DES (*Data Encryption Standard*), para encriptar los archivos de la víctima. Estos algoritmos utilizan la misma clave para cifrar y descifrar los datos. Sin embargo, la debilidad de este enfoque es que, si se descubre la clave de cifrado, todos los archivos pueden ser descifrados sin pagar el rescate.
2) ***Ransomware* de cifrado asimétrico:** para superar la limitación de la clave compartida, los desarrolladores de *ransomware* adoptaron el cifrado asimétrico. Utilizan un par de claves, una clave pública para encriptar los archivos y una clave privada correspondiente para descifrarlos. La clave privada se mantiene en manos de los atacantes, lo que dificulta el descifrado sin pagar el rescate.
3) ***Ransomware* con comunicación encriptada:** los *ransomware* modernos comenzaron a utilizar comunicaciones encriptadas para proteger la comunicación entre el *ransomware* y el servidor de control. Esto dificulta el seguimiento de la actividad del *ransomware* y la identificación de los responsables.
4) ***Ransomware* con algoritmos de cifrado más fuertes:** a medida que los métodos de detección y descifrado de *ransomware* mejoraron, los atacantes comenzaron a utilizar algoritmos de cifrado más fuertes, como AES (Advanced Encryption Standard) con claves más largas. Esto dificulta aún más el descifrado de archivos sin la clave adecuada.
5) ***Ransomware* híbrido:** algunos *ransomware* utilizan una combinación de algoritmos de cifrado simétrico y asimétrico. Utilizan el cifrado simétrico para encriptar rápidamente los archivos de la víctima y, a continuación, utilizan el cifrado asimétrico para proteger la clave simétrica utilizada. Esto combina la velocidad del cifrado simétrico con la seguridad adicional del cifrado asimétrico.
6) ***Ransomware* de doble extorsión:** una evolución reciente es el *ransomware* de doble extorsión. Además de encriptar los archivos de la víctima, los atacantes también amenazan con filtrar datos confidenciales si no se paga el rescate. Esto agrega una capa adicional de presión para que las víctimas paguen.

Definir los tipos de *ransomware* es difícil, porque el concepto de *ransomware* ha evolucionado y las capacidades técnicas del *ransomware* son similares a las de otro *malware*. Hasta mediados de la década de 2010, el *ransomware* solía centrarse sólo en una o dos acciones, como el cifrado o el bloqueo. Esto facilitó la agrupación de *ransomware* en categorías simples como *Encryption Ransomware* o *Lock Screen Ransomware*.

Sin embargo, el *ransomware* ya no está vinculado a tales descripciones y su evolución ha hecho que categorías tan simples ya no sean suficientes para representarlo. Esto se complicó aún más por la falta de homogeneidad en la denominación del *ransomware* por parte de la industria de la ciberseguridad y la tradición de creer que los tipos eran mutuamente excluyentes. Hablar de *ransomware* en la actualidad no debe ser en términos de tipo, sino en términos de acciones que realizan y activos a los que apuntan.

¡Hasta la próxima! ■

Gigi Agassini, CPP, *International Security Consultant. Más sobre la autora:*

amesis MR

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

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.

- Comité de Relación con Autoridades
- Comité de Estadísticas del Sector
- Comité de Capacitación y Desarrollo
- Comité de Relaciones Públicas
- Comité de Tecnología e Innovación

NUESTROS SOCIOS

Tracking Systems de México S.A. de C.V. · sitel Seguridad Satelital · Holkan · skyguardian · skymeduza · ADS LOGIC TELEMATICS
SEGURIDAD 360 .com · SECUREWITNESS · INFO TRAX · TECNO LOGISTIK · GLOBAL MIT · RAINDE
ATLANTIDA · GEOTRACKING RASTREO SATELITAL · Tecno GPS · TTC · DUMAX · ISIS SEGURIDAD INTEGRAL
GEOTRUCKS · GRUPO ALFIL · SEC SOLUCIONES · RCU SISTEMAS · GPSMonitor RASTREO SATELITAL · GPS TRACKER MX Vamos contigo
MAGNI Tracking · TSNVISION TECHNOLOGY SECURITY VISION · BLC · SATECH

c.administrativa@amesis.org.mx
amesis.org.mx

COMUNÍCATE
55 3334 4707

LA INMINENTE TRANSFORMACIÓN DIGITAL EN SEGURIDAD

"La innovación es lo que distingue a un líder de los demás", Steve Jobs

Fotos: FreePick

MÉXICO

Diego Escobal

Esta de moda el término "transformación digital", como digitalización, era digital y muchos otros que tienen un significado similar, pero ¿qué es la trasformación digital en Seguridad?

Existen muchas definiciones en la web, pero para que sea entendible en términos de seguridad, es disminuir el uso del papel, los reportes a lápiz y llevarlos a un ambiente digital, ya sea en celulares, *tablets* o en computadoras, para obtener información centralizada, y hago referencia en todas las actividades, ya sea ventas, administración u operaciones.

No podemos negar que estamos en la 4ta revolución industrial. La revolución del Internet de las Cosas, la digitalización, automatismos digitales, los hábitos de consumo e innovación. Al igual que las revoluciones anteriores, las empresas que no logran el cambio y la adaptación al nuevo mundo, quedarán en el camino.

Vamos a preguntarle cómo le fue a Blockbuster, rechazando una propuesta de Netflix, o a las discográficas con Spotify, cómo les va a los taxistas con Uber, la preocupación de los hoteles con Airbnb, las telefonías con WhatsApp, los correos con el *e-mail*, las páginas amarillas con Google, la lista es interminable.

Ahora bien, hablemos de lo nuestro. ¿Qué pasa en Seguridad? ¿Qué pasa si decidimos no digitalizar la empresa o la gestión de seguridad de la empresa donde trabajo? No pasa absolutamente nada, seguirá igual que hasta el momento. Sólo que otras empresas o personas lo harán y ocuparán nuestro espacio.

"NO DIGITALIZAR MI EMPRESA NO ES MALO, LO MALO ES QUE OTRAS SÍ LO HARÁN"

Veamos entonces, cuáles serían los objetivos de la digitalización de las operaciones de Seguridad (no contemplemos los procesos de ventas y administrativos) y sobre todo, qué beneficio tiene para mi empresa. El hecho de no desaparecer con el tiempo, ya es un gran beneficio, pero básicamente, existen dos grandes objetivos: "hacer mejor las cosas, y dos, obtener beneficios económicos", pero vamos a describir algunos objetivos incluidos en esos dos.

- **Ofrezco seguridad, no guardias.** Los que hemos contratado servicios de guardias de seguridad, hemos recibidos muchas promesas de excelentes servicios, pero muy pocas empresas se preocupan realmente por la seguridad que necesitamos.

Fotos: FreePick

Algunas empresas de seguridad automáticamente se limitan sólo a dar un servicio de horas hombres. No ofrecen la oportunidad de analizar los riesgos, o mejorar mis procesos. Entiendo que así lo piden en adquisiciones, pero vale la pena intentarlo, dar un servicio mas allá que sólo la "materia prima".

- **Doy un servicio de seguridad, y entrego reportes con una plataforma digital de cómo se cumple el contrato.** Eso tampoco sucede a menudo. Muchas empresas de seguridad no ofrecen una herramienta digital que permita reportar las actividades y darle al responsable de Seguridad información valiosa.
- **Ventaja competitiva.** Evidentemente que si la empresa de seguridad ofrece reportes de informes de incidentes, registro de novedades, accesos en las casetas, supervisión efectiva y todos los reportes de cómo hacen las cosas, va a satisfacer las necesidades de información y estarán colaborando activamente con la gestión de los riesgos de los clientes. Cosa que otras empresas, no lo hacen.
- **Cumplimiento del contrato.** O llamado comúnmente "amarrar al cliente". Si logramos que el cliente pueda ver en reportes diarios, semanales, quincenales y mensuales de cómo gestionamos su seguridad y tener reuniones periódicas para ofrecer nuevas gestiones, sin duda, tendremos cliente para rato.
- **Nuevos modelos de negocio.** La 4ª Revolución Industrial abre grandes oportunidades digitales. Sólo es necesario contratar o consultar a las personas que saben del tema y generar oportunidades que nosotros quizás no podemos ver. Sólo con buscar en LinkedIn: "gerente o director de transformación digital" y verás cómo empresas importantes ya están dando ese paso. Seguramente la generación de oportunidades será mucho mayor que la inversión.
- **Optimización de procesos.** Para crecer hay que delegar. ¿Cuántas veces escuchamos eso? La digitalización es una de la forma de hacerlo. Crear procesos digitales acompañando los que ya tenemos, y garantizar el cumplimiento de los mismos, asegura el cumplimiento.

Ya es hora entonces, es inminente, se viene la 5ª Revolución Industrial, Inteligencia Artificial a servicio de las personas. No dejes pasar la oportunidad de ser diferente.

La procrastinación es la acción o hábito de retrasar actividades o situaciones que deben atenderse, sustituyéndolas por otras situaciones más irrelevantes

Crear procesos digitales acompañando los que ya tenemos, y garantizar el cumplimiento de los mismos, asegura el cumplimiento

Fotos: FreePick

La 4ª revolución industrial abre grandes oportunidades digitales. Sólo es necesario contratar o consultar a las personas que saben del tema y generar oportunidades que nosotros quizás no podemos ver

Diego Escobal, DSE, especialista en digitalización de procesos de seguridad, director de VEA Consultores y vicepresidente de ASIS Capítulo Península de Yucatán. *Más sobre el autor:*

Columna de GEMARC

hcoronanav15@yahoo.com.mx

Héctor Coronado Navarro, presidente de Grupo de Ejecutivos en Manejo de Riesgos Corporativos, A.C. (GEMARC) para el periodo 2023-2025.

Más sobre el autor:

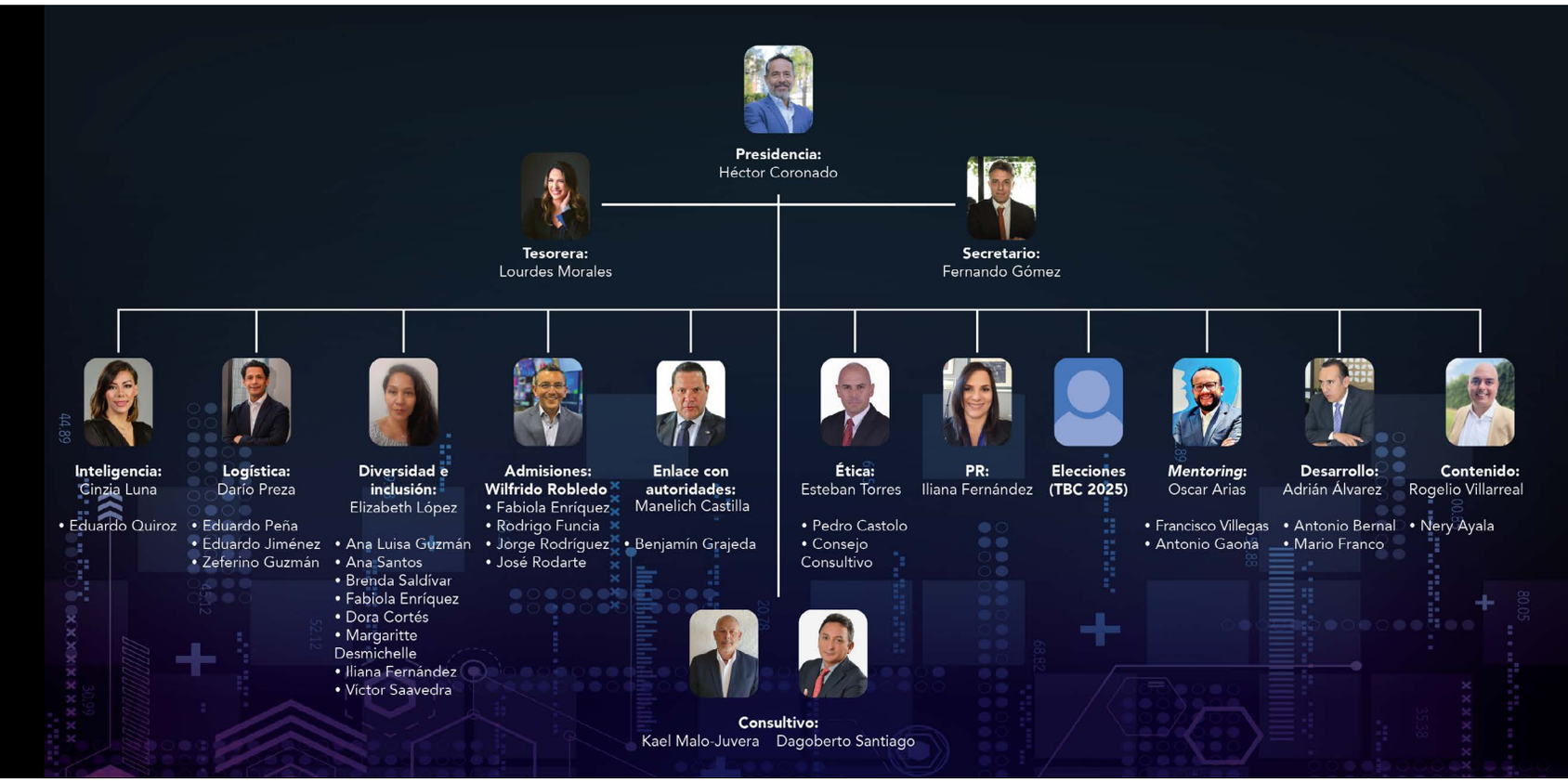
LOS COMITÉS EN GEMARC

MÉXICO

La fortaleza mayor que tiene GEMARC son sus miembros y a efecto de llevar a cabo el plan estratégico que se tiene en la asociación, GEMARC se apoya con distintos Comités, mismos que están liderados por uno de los miembros y estos a su vez acompañados por otros integrantes. Lo anterior, no demerita que todos los asociados aportan de forma indistinta en las diferentes actividades que tenemos en la asociación.

La conformación de los Comités es de la siguiente manera:

Además de la Presidencia, dirigida por Héctor Coronado; la Tesorería, por Lourdes Morales; y la Secretaría, por Fernando Gómez, se tienen los siguientes Comités:



COMITÉ DE ADMISIONES (LÍDER: WILFRIDO ROBLEDO)

El Comité de Admisiones de GEMARC busca fortalecer la red de ejecutivos en manejo de riesgos corporativos mediante la incorporación de los máximos responsables de la seguridad en México de empresas nacionales y trasnacionales. Entre las funciones del Comité están:

- Actualizar y aplicar los requisitos para ingresar a la asociación.
- Mantener actualizado el directorio de miembros activos.
- Promover la incorporación de los máximos responsables de la seguridad de empresas nacionales y trasnacionales a la asociación, de acuerdo a los lineamientos de ingreso.
- Identificar sectores que actualmente no estén representados en la asociación.
- Ser un canal de vinculación entre la membresía y la mesa directiva.
- Elaborar un perfil de los miembros.
- Velar por la confidencialidad de los datos de los miembros.

Entre los proyectos en los que se encuentra trabajando el Comité están: la actualización de los lineamientos y requisitos de la solicitud de ingreso a GEMARC y la creación de un modelo de membresía que permita a nuestros miembros acreditarse como parte de la asociación.

Actualmente, el Comité está integrado por Fabiola Enríquez, de Grupo Presidente; Jorge Rodríguez, de Grupo Soriana; Rodrigo Funcia, de ABBVIE; José Rodarte, de Nike, y coordinado por Wilfrido Robledo Luna, de Grupo Imagen Multimedia.

COMITÉ DE ÉTICA (LÍDER: ESTEBAN TORRES)

El objetivo de este comité es promover los valores y las buenas prácticas a través de un foro en el que se discutan las cuestiones que puedan afectar, a nivel moral, a GEMARC o sus miembros.

Dentro de sus funciones principales están son las de desarrollar un código de ética que establezca los principios y valores éticos que deben guiar las acciones y decisiones de todos los miembros del grupo, así como promover la integridad y la honestidad en todas las actividades, estableciendo políticas y procedimientos claros relacionados con la conducta de sus miembros.

Además, nos enfocaremos de manera proactiva en brindar orientación y capacitación a los miembros del grupo, sobre cuestiones éticas y cuando sea necesario, el investigar cualquier denuncia relacionada con conductas que se consideren que van en contra de lo establecido por los lineamientos y/o violaciones del código de ética que sea establecido.

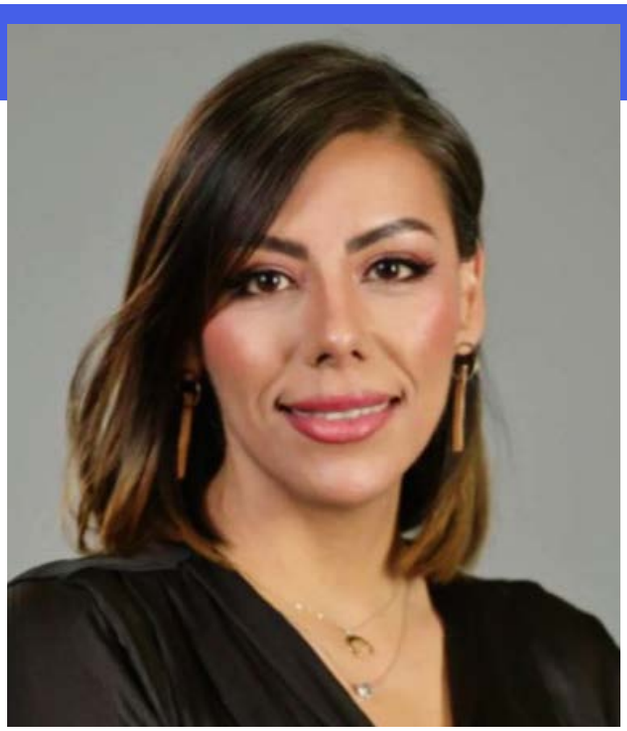
Este comité está encabezado por Esteban Torres, quien estará llevando a cabo los trabajos junto a Pedro Castolo y los miembros del Comité Consultivo, Kael Malo-Juvera y Dagoberto Santiago.

COMITÉ DE DIVERSIDAD E INCLUSIÓN (LÍDER: ELIZABETH LÓPEZ)

El objetivo de este Comité es promover una cultura de igualdad, equidad e inclusión a través de actividades de concientización dentro de la seguridad corporativa.

Dentro de las acciones propuestas, se fomentará la diversidad en la contratación, implementar programas de capacitación y sensibilización para los empleados sobre la importancia de la diversidad, inclusión y eliminación de prejuicios en el lugar de trabajo, colaborar con los diferentes equipos para revisar y actualizar políticas y prácticas asegurando que sean inclusivas y reflejen el compromiso con la diversidad, fomentar igualdad de oportunidades, crear una cultura inclusiva, colaborar con otras organizaciones, apoyo a grupos de afinidad, participar en mediciones que nos permitan tener una evaluación de todo ello; así como compartir las mejores prácticas que existen en el mercado.

Este Comité será liderado por Elizabeth López, apoyada por Ana Guzmán, Ana Santos, Brenda Saldívar, Dora Cortés, Fabiola Enríquez, Iliana Fernández, Margaritte Desmichelle y Víctor Saavedra.



COMITÉ DE INTELIGENCIA (LIDER: CINZIA LUNA)

Liderado por Cinzia Luna, *Country Security Manager* de ENGIE, con el valioso apoyo de Eduardo Quiróz, director de Seguridad de Grupo Águila - Ammunition. Ambos con amplia trayectoria en Inteligencia, en el sector público y privado.

El Comité de Inteligencia busca transformar la información en conocimiento para la mejor toma de decisiones, que garantice el desarrollo y continuidad del negocio de las empresas representadas en GEMARC.

El comité enfrentará el reto de reducir la incertidumbre en la que operamos como responsables de seguridad, a través de productos de inteligencia operable. Esto llama a una dinámica de cooperación entre los miembros de GEMARC para el acopio de información de calidad que nos permita un ciclo de inteligencia impecable, desde el acopio hasta la difusión y retroalimentación.

COMITÉ DE *MENTORING* (LÍDER: OSCAR ARIAS)

Uno de los grandes atributos de GEMARC son sus miembros, en el cual con la suma de conocimientos y cantidad de un sinnúmero de experiencias vividas en el campo de Seguridad Corporativa, el objetivo específico de este comité es el de inspirar a las nuevas generaciones a través de un esquema de Mentores & *Mentees*, por medio de vínculos de comunicación asertiva con aprendizaje de doble vía para trazar metas en común, planes de desarrollo, proyectos de corto, mediano y largo plazo, por medio de valores éticos y profesionales que demanda el campo de seguridad.

Este comité está conformado por Antonio Gaona, actualmente director de Seguridad para CODERE; Francisco Villegas, DSE, subdirector de Protección Patrimonial en Christus Murgueza Sistemas Hospitalarios; y coordinado por Oscar Arias, *Regional Security Officer LATAM* para Grupo DANONE, donde tenemos el reto de crear una estructura y estrategia de mentores altamente comprometidos al objetivo de este comité.

Alcance propuesto:

- **Fase 1:** colaboradores de los miembros de GEMARC, que estén en desarrollo y/o crecimiento en sus organizaciones como parte de sus planes de carrera.
- **Fase 2:** universidades vinculadas al ramo de Seguridad a través de convenios colaborativos.

Nota: todo esto previo a la revisión del Comité de Ética y aprobación de nuestras organizaciones como un valor agregado al ser miembro de GEMARC.

COMITÉ DE DESARROLLO (LÍDER: ADRIÁN ÁLVAREZ)

El objetivo del Comité de Desarrollo Profesional es fomentar el crecimiento y la excelencia de los miembros de esta organización.

Nuestro propósito es brindarles las herramientas, recursos y oportunidades necesarias para adquirir nuevas habilidades, conocimientos y competencias que les permitan alcanzar su máximo potencial profesional, convirtiendo en aspiracional el desarrollo profesional *per se*.

Principales metas y funciones:

- **Capacitación y formación:** diseñar programas de capacitación y formación que estén alineados con los objetivos estratégicos de las empresas en las que nos desempeñamos y las necesidades individuales de los agremiados. Estos programas se enfocarán en mejorar las habilidades técnicas, el liderazgo, la gestión de proyectos, las habilidades gerenciales y directivas y otros aspectos relevantes para el desarrollo profesional de los ejecutivos de Seguridad.
- **Desarrollo de talento:** identificar y potenciar talentos, preparándolos y fomentando el crecimiento profesional en las oportunidades de mercado. Asimismo, se buscará detectar las necesidades de talento emergentes y trabajar en el desarrollo de opciones de aprendizaje.
- **Evaluación del desempeño:** implementar sistemas de evaluación que permitan a los agremiados conocer sus áreas de mejora. A través de estas evaluaciones, se buscará establecer planes de desarrollo.
- **Gestión del conocimiento:** facilitar la transferencia de conocimientos y buenas prácticas dentro de la organización, creando una cultura de aprendizaje y colaboración. Esto incluye el uso de plataformas de aprendizaje en línea y presenciales, sesiones de *mentoring* y la promoción de comunidades de práctica.
- **Programas de desarrollo de liderazgo:** diseñar programas específicos para el desarrollo de habilidades de liderazgo y gestión. Se busca cultivar líderes efectivos y empáticos que inspiren a sus equipos y promuevan un ambiente de trabajo positivo.
- **Seguimiento y medición:** realizar un seguimiento periódico de los resultados de los programas de desarrollo profesional y medir su impacto en el rendimiento individual y profesional. Esto permitirá realizar ajustes y mejoras continuas.
- **Desarrollo de base de conocimientos:** desarrollo de materiales de consulta técnica-científica-pedagógica, especialmente de forma electrónica dentro de una biblioteca virtual universal.

Al cumplir con estos objetivos, el Área de Desarrollo Profesional contribuirá al crecimiento sostenible de los integrantes y agremiados y al fortalecimiento del talento humano, asegurando ejecutivos altamente capacitados, motivados y comprometidos con el éxito personal y de su organización.

Los integrantes de este equipo de trabajo se conforman por Mario Alberto Franco, Antonio Bernal y Adrián Álvarez.

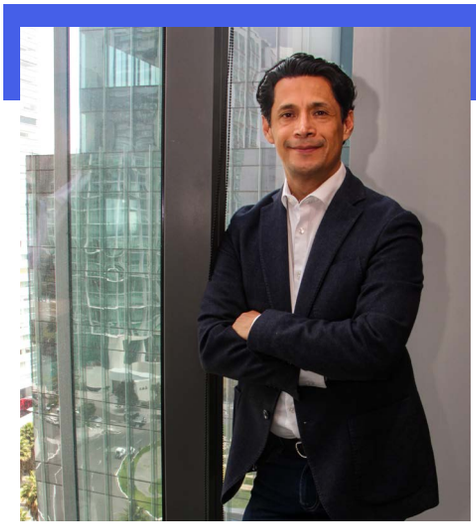
COMITÉ DE CONTENIDO (LÍDER: ROGELIO VILLARREAL)

El Comité de Contenido se encarga de gestionar las necesidades de información para GEMARC y sus miembros. Nuestra labor principal consiste en proponer reglas básicas para la generación de encuestas y *benchmarks*, garantizando que el repositorio de información sea accesible y confiable.

Somos el primer punto de contacto para los miembros cuando requieren alguna encuesta, verificando la existencia previa de información relevante. Además, brindamos apoyo en la generación de encuestas mediante plataformas digitales que facilitan la obtención y análisis de la información. Asimismo, nos destacamos por asegurar la confidencialidad de la información sensible que se genere, implementando rigurosos métodos de protección.

Actualmente, estamos trabajando en un proyecto para establecer un reglamento que garantice la efectividad de las encuestas y su almacenamiento en un repositorio de información confiable. Nuestro objetivo es favorecer la accesibilidad y usabilidad de dicho repositorio.

El Comité de Contenido está integrado por Nery Ayala y Rogelio Villarreal, quien asume el rol de coordinador. Nuestro enfoque profesional se orienta a satisfacer las necesidades de información de manera eficiente y confiable para todos los miembros de GEMARC.



COMITÉ DE LOGÍSTICA (LÍDER: DARÍO PREZA)

Conocida también como seguridad a la cadena de suministro, este Comité lo lideran Darío Preza, Eduardo Jiménez, Zeferino Guzmán y Eduardo Peña, nuestro objetivo es compartir mejores prácticas para la prevención de los robos al transporte de mercancías en las autopistas y carreteras del país, buscando una reducción significativa de este delito.

Al ser una afectación de alto impacto para las empresas daña seriamente la reputación de México e incrementa los costos de los productos; por ello buscamos generar sinergias con asociaciones e instituciones públicas así como privadas para estudiar, analizar, medir y prevenir este delito.

Crear guías, lineamientos, capacitación para el desarrollo de los ejecutivos de seguridad corporativa para la aplicación y uso de tecnología de procesos, así como estrategias de seguridad preventiva para proteger a las personas, activos, materias primas, mercancías, clientes y miles de productos que transitan diariamente en nuestro país.

foto: El Heraldo

COMITÉ CONSULTIVO (LÍDERES: KAEL MALO-JUVERA Y DAGOBERTO SANTIAGO)

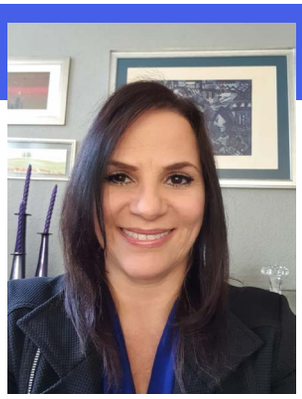
Este Comité, de reciente creación, conformado por Kael Malo-Juvera y Dagoberto Santiago, mismos que son ex presidentes de GEMARC en los periodos 2019-2021 y 2021-2023 respectivamente; estarán por un lado apoyando al Comité de Ética en la toma de decisiones y por otro lado, servirán al presidente en curso, cuando así se les requiera, como un medio de asesoría y consulta en temas coyunturales para la asociación.

Se agregó este Comité, tomando en cuenta, no sólo por las posiciones honoríficas de los actuales ex presidentes, sino por considerar de gran valía su experiencia previa durante sus gestiones en GEMARC.

COMITÉ DE ENLACE CON AUTORIDADES (LÍDER: MANELICH CASTILLA)

El Comité de Enlace con Autoridades, conformado por Manelich Castilla Craviotto y Benjamín Grajeda Regalado; pretende construir un esquema de atención para los integrantes de GEMARC ante situaciones que, por su relevancia, exijan hacer de conocimiento de las áreas operativas en materia de seguridad pública y/o procuración de justicia del país, alguna contingencia en curso o que requiera seguimiento.

Dada la diversidad de giros de las empresas representadas en GEMARC, el Comité ha considerado como prioritarios los casos de extorsión y secuestro para el establecimiento de estos enlaces institucionales, en el entendido de que en el mediano plazo debe construirse una agenda integral y de mayores alcances, después de escuchar y analizar las inquietudes de todos los miembros del Grupo.



COMITÉ DE RELACIÓNES PÚBLICAS (LÍDER: ILIANA FERNÁNDEZ)

La función de Relaciones Públicas dentro de GEMARC ayudará en la coordinación de eventos y enlace con los miembros. Uno de los principios y fortalezas de GEMARC, es la relación cercana entre los socios en donde las actividades dentro de la organización consolidan dichas sinergias. Iliana Fernández en la encargada de dicha función, quien seguirá aportando valor a la asociación.

COMITÉ DE ELECCIONES (LÍDER: POR DEFINIR)

Este Comité se encarga de establecer las reglas de las elecciones para la selección del presidente de GEMARC, las cuales se dan cada dos años de forma democrática. Actualmente no se ha establecido, toda vez que el presente periodo comenzó a mediados del presente año y una vez que se esté próximo a la culminación de la actual administración, se nombrará el mismo a efecto de dar el seguimiento y debido proceso. ■

Fotos: GEMARC

LA TECNOLOGÍA Y EL SOPORTE TÉCNICO

APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA

38 ANIVERSARIO

- INDUSTRIAL • RESIDENCIAL
- COMERCIAL • GOBIERNO• FRACCIONAMIENTOS
- PARQUES DE ENERGIA • AEROPUERTOS
- CORPORATIVOS • PLATAFORMAS PETROLERAS

REGISTRO FEDERAL DGSP/303-16/3302 PERMISO SSP PUEBLA
SSP/SUBCOP/DGSP/114-15/109
REPSE AR10508/2021

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD ALAS SOCIO ALAS

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

Achilles No. 329,814

COPARMEX

222 141 12 30

gerenciacomer@pem-sa.com

WWW.PEM-SA.COM

El especialista en Seguridad Integral, David Macoto Nancarrow Sugiura, se une como nuevo director operativo y consejero a GRIP, empresa liderada por Gonzalo Senosiain Baixeras

好きこそ物の上手なれ.

Proverbio Japonés ("Suki koso mono no joozo nare" - "para aprender algo lo principal es que a uno le apasione")

MÉXICO

Mónica Ramos y Antonio Venegas / *Staff* Seguridad en América

Una de las empresas de seguridad privada más reconocidas en el país, es GRIP (Global Risk Prevention), fundada y liderada desde hace casi 15 años por Gonzalo Senosiain Baixeras, teniendo como principal característica el cuidar desde casa a sus colaboradores. Este año, GRIP le da la bienvenida como nuevo director operativo y consejero a un experto en Seguridad Integral, David Macoto Nancarrow Sugiura, quien comparte los valores de todo GRIPer: compromiso, lealtad, humanidad.

"Gonzalo y yo, tenemos una visión muy similar hacia la dignidad del guardia y su calidad de vida, siempre hemos trabajado compartiendo experiencias para mejorar la calidad de vida del guardia, sus zonas de trabajo y hacer que el cliente entienda esa parte de no ver al guardia como objeto, sino como ser humano", recalcó Mako.

Fortalecer el papel del guardia, cuidarlo y brindarle todos los elementos para realizar los servicios que le fueron asignados, son los principales aspectos que GRIP contempla en su día a día, tanto interna como externamente, los GRIPers son un ejemplo de vida para estos expertos en seguridad.

La seguridad privada en México lleva años trabajando en la profesionalización del sector, y uno de los métodos que más ha funcionado, es la unión del gremio. Algo similar sucede de forma interna en GRIP, ya que Macoto Nancarrow se integra a la empresa, sumando a las estrategias y filosofía de GRIP, los aprendizajes que la cultura japonesa —raíces maternas de Mako— le ha dejado a lo largo de su vida y que ha implementado en su carrera profesional dirigiendo otras empresas de seguridad privada.

"Todos estos valores que vienen muy arraigados de la cultura japonesa, no se van a cambiar por ser mexicanos, pero sí los podemos permear un poco, al final se puede generar un guardia y una empresa muy diferente a todas las que están establecidas", comentó Mako.

Por su parte, Gonzalo Senosiain hizo hincapié en que ambos coinciden en la visión que tienen sobre la seguridad, por ejemplo, sus procesos operativos son casi idénticos. La llegada del nuevo

"La calidad humana que hay en GRIP y en esta alianza no la hay en otros lugares", **Mako Nancarrow**

"Como dueños y directores tenemos la obligación de atender a la persona y solucionarle cuanto antes, estamos para escucharlos, todos nuestros colaboradores saben que la puerta está abierta para resolver cualquier duda", **Gonzalo Senosiain**

ALGUNOS VALORES DE GRIP:

1) Si no es mío, le pertenece a alguien más.
2) Sé un engrane.
3) Disfruta tu trabajo.
4) Reconoce, hazte responsable, corrige y aprende de tus errores.
5) Aunque en GRIP se reconoce el esfuerzo, lo que se premia es el resultado.
6) Trata como quieras que te traten.

GRIPer a la empresa busca continuar promoviendo la importancia de crear un ambiente laboral y una vida con calidad para los GRIPers, que al ser cuidados, transmitan este valor de protección y lealtad a los clientes, que sirvan como reflejo de la identidad de la empresa al momento de tratar con éste.

"Parte de esto es seguir dignificando al guardia, pagando un sueldo adecuado y a tiempo, darle al GRIPer el trato digno que amerita, hablar con el cliente y hacerle entender que tiene que ser parte del equipo", comentó Gonzalo Senosiain.

Macoto proviene de una familia de migrantes, madre japonesa, padre norteamericano, pero comparte su ascendencia con el orgullo que México le genera y con la pasión que la seguridad le ha brindado desde que se integró a este sector, esa cultura materna es la que integrará y ampliará a la visión de GRIP.

Los japoneses son conocidos por colocar al trabajo en el número uno de sus prioridades, además de que el conservar un solo empleo toda su vida, les otorga dignidad y respeto, aunado a esto, la puntualidad y la ética, valor que los lleva a buscar la perfección, el autocontrol y la autodisciplina, siendo resilientes a los cambios; que si los relacionamos con un GRIPer, encajan perfectamente y no sólo en la creación de un trabajo que les motive e impulse a generar relaciones interpersonales saludables, sino también generan en el cliente esta sensación de humanidad y respeto, de cuidado y protección, ya que GRIP, cuida, previene y asegura.

EN GRIP NO BUSCAMOS EXCUSAS, ¡ENCONTRAMOS SOLUCIONES!

Dado que Mako y Gonzalo coinciden en las estrategias de seguridad, el solucionar conflictos o problemáticas también es similar. Ambos expertos consideran que se deben atender las solicitudes de un cliente de manera inmediata, sobre todo cuando se trata de la seguridad de sus bienes e indudablemente de la protección a personas.

"Algo que es muy importante, es el entender cuál es la necesidad final del cliente y a qué se dedica. Si el cliente vende algún producto, entender cómo, desde nuestra área, podemos contribuir para darle un valor agregado a ese producto; si entendemos cuál es lo más importante para él, lograremos que el objetivo de nuestro servicio, se cumpla, y además en beneficio para todos. En GRIP no buscamos excusas, encontramos soluciones", puntualizó Gonzalo Senosiain.

En la empresa también destaca la importancia de la comunicación, los directivos tienen una línea abierta tanto para los clientes como para los colaboradores internos, con la finalidad de atender quejas, sugerencias, agradecimientos o cualquier comentario que se pueda tener. Esto tiene como objetivo garantizar la atención de cualquier problemática presentada en el servicio, ellos siempre tendrán una respuesta.

"Como dueños y directores tenemos la obligación de atender a la persona y solucionarle cuanto antes, estamos para escucharlos, todos nuestros colaboradores saben que la puerta está abierta para resolver cualquier duda", mencionó Gonzalo. Mako coincidió con esto, "mucha gente lo ve como un negocio de números, pero es tan valioso y delicado el recurso humano, por eso es tan importante que el cliente sepa que puede contar contigo cuando sea, al final es lo que brinda tranquilidad. La calidad humana que hay en GRIP y en esta alianza no la hay en otros lugares".

De esta manera, esta importante unión busca garantizar en el cliente y en el colaborador ese sentido de pertenencia, trabajo en equipo y tranquilidad, mediante el desarrollo profesional de la seguridad. ■

Fotos: Antonio Venegas / SEA

SEGURIDAD EN ESTADIOS DE FÚTBOL

Fotos: FreePick

MÉXICO

Violeta E. Arellano Ocaña

El objetivo principal de la seguridad en eventos deportivos no es responder a las amenazas, sino evitar que se produzcan

Los estadios de fútbol son el escenario perfecto para eventos de esparcimiento familiar, sin embargo, también han sido sede de varios eventos desafortunados de violencia a consecuencia de riñas entre porras.

Uno de los incidentes más lamentables ocurridos en nuestro país fue el 05 de marzo de 2022 en el estadio Corregidora en Querétaro, México, que dejó 26 heridos, personas detenidas, autoridades cesadas, y sanciones para el inmueble, clubes deportivos y empresa de seguridad privada a cargo.

ELEMENTOS A TOMAR EN CUENTA PARA DEFINIR UN DISPOSITIVO DE SEGURIDAD EN UN PARTIDO DE FÚTBOL

Primeramente, conocer la normatividad correspondiente. Existe regulación nacional e internacional, entre ellas, el manual general de PC "Estadio Seguro", el reglamento de seguridad para partidos oficiales de la Federación Mexicana de Fútbol y el reglamento FIFA de Seguridad en los estadios.

Todos ellos coinciden en que debe realizarse un análisis de riesgos previo que incluya riesgos internos y externos: éstos pueden ir desde la ubicación del estadio, la infraestructura con la que cuenta, condiciones meteorológicas, el ambiente socio político de la ciudad, históricos de comportamiento de las porras o barras.

Con base en este análisis, se tienen que tomar medidas de prevención para mitigar los riesgos detectados. En el caso específico de las porras, se les puede separar desde el ingreso al estadio, elaborar un diseño de flujos para que no se encuentren dentro de las instalaciones, ubicarlas en las cabeceras, bajo vigilancia de elementos de seguridad pública y privada.

MONTERREY / CANCÚN / VERACRUZ / / COATZACOALCOS / VILLAHERMOSA

GORAT
SEGURIDAD
PRIVADA

ALARMAS

GPS

CCTV

GUARDIAS

ESCOLTAS

CUSTODIA DE TRANSPORTE

SERVICIOS INTEGRALES DE SEGURIDAD

800 00 46728 / www.tecuidamos.mx

OFICINA C4 RIVIERA / +52 229 193 5519

Plaza Portal Conchal, Local 4 y 5 Carr. Boca del Rio a Anton Lizardo Km 2.5 Fracc. Lomas Residencial

MANAGED BY: GRUPO ABREU Y MORENO S.A. DE C.V.

Otro punto en el que toda la normatividad coincide, es que la seguridad de los asistentes, es responsabilidad compartida entre autoridades locales, responsables de los estadios y de los clubes deportivos, por lo que es indispensable la presencia y colaboración entre seguridad pública y seguridad privada.

Con respecto a la cantidad de personal de seguridad, el Reglamento FIFA de Seguridad en los Estadios recomienda un elemento por cada 250 espectadores para un partido de bajo riesgo y un elemento por cada 100 espectadores en caso de alto riesgo.

CONDICIÓN LEGAL DE UNA EMPRESA DE SEGURIDAD PRIVADA

Las empresas de seguridad privada deben contar con un Registro federal y/o local expedido por la Secretaría de Seguridad Ciudadana a través de la Dirección General de Seguridad Privada para la prestación de servicios de seguridad, así como su registro como empresa prestadora de servicios especializados, conocido como REPSE, que emite la Secretaría del Trabajo y Previsión Social.

PROTOCOLO A SEGUIR PARA DETENER LOS DISTURBIOS

Es muy importante que el personal tanto de seguridad pública y privada estén pendientes de las reacciones del público en todo momento, para que, al menor indicio de conductas de desorden, se les haga un llamado a comportarse, bajo amenaza de sacarlos o si ya la violencia es inminente, pedir refuerzos, encapsularlos y sacarlos inmediatamente del recinto y entregarlos a personal de seguridad pública para el tratamiento correspondiente. De esa forma se impide que la riña crezca, ya que una vez que se convierte en batalla campal, el personal de seguridad pública y privada será insuficiente para poder retomar el control.

¿CUÁL DEBE SER LA CAPACITACIÓN DEL PERSONAL DE SEGURIDAD PRIVADA PARA PARTICIPAR EN EL OPERATIVO DE SEGURIDAD DE UN PARTIDO DE FÚTBOL?

El personal de seguridad privada debe tener los conocimientos básicos para desarrollar sus funciones, por ejemplo, control de accesos, terminología de seguridad, detección de situaciones de riesgo, adicionalmente para las actividades en un estadio, debería capacitárseles en control de masas y procedimientos de actuación en casos de emergencia con la finalidad de que tengan muy en claro sus funciones y no haya necesidad de improvisar.

Otro punto importante, es contratar empresas con experiencia comprobable en eventos deportivos y masivos. ■

Debe realizarse un análisis de riesgos previo que incluya riesgos internos y externos: éstos pueden ir desde la ubicación del estadio, la infraestructura con la que cuenta, condiciones meteorológicas, el ambiente socio político de la ciudad, históricos de comportamiento de las porras o barras

Fotos: FreePick

Es muy importante que el personal tanto de seguridad pública y privada estén pendientes de las reacciones del público en todo momento, para que, al menor indicio de conductas de desorden, se les haga un llamado a comportarse, bajo amenaza de sacarlos o si ya la violencia es inminente, pedir refuerzos, encapsularlos y sacarlos

Violeta E. Arellano Ocaña, gerente de Seguridad Integral en Corporación Interamericana de Entretenimiento (CIE).
Más sobre la autora:

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

BUENAS PRÁCTICAS Y CONSIGNAS PARA EL PERSONAL DE SEGURIDAD *(PARTE I)*

MÉXICO **Hermelindo Rodríguez Sánchez**

En esta ocasión nuestro especialista invitado muestra este sistema de prácticas para el guardia de seguridad, que contiene las funciones e indicaciones para que el vigilante de seguridad desempeñe y desarrolle su labor con profesionalismo

Cada formación del guardia debe ser emitida con las consignas específicas para cada servicio en particular y debe contener en su interior indicaciones referentes a higiene y seguridad, medidas de seguridad física, emergencias, de tal modo que, mientras más amplio y robusto sea en sus instrucciones.

Un Manual del Guardia se transforma en un Manual de Procedimientos, Operaciones y Lineamientos Técnicos para el guardia de seguridad que contiene temas más profesionales tales como llamada amenazante o extorsiva, ciberterrorismo, paquetes y mensajería sospechosa, higiene y seguridad, combate de incendios y atención a emergencias, control de monitoreo, etc.

A continuación te compartimos las consignas más comunes y recurrentes para la elaboración de un manual del guardia de seguridad.

CONSIGNAS PARA EL GUARDIA

Objetivo: custodiar las instalaciones, controlar la entrada o salida de mercancía, mobiliario y equipo, insumos y materiales, reportar el uso o abuso de los recursos de la empresa, vigilar que se cumplan y hacer cumplir las indicaciones y procedimientos, a manera de minimizar los riesgos que causen desestabilidad y pérdida.

Las funciones del cuerpo de vigilancia son:

1) Cooperar con acciones de seguridad y vigilancia en la empresa, dentro y fuera de ella.
2) Coordinar la evacuación del personal en caso de siniestro o amenaza.
3) Participar activamente en prácticas y simulacros como parte de su capacitación.
4) Prevenir y minimizar la sustracción de activos, robo y/o ataque a los recursos materiales de la empresa.
5) Detectar y reportar situaciones de sabotaje en la empresa, sus instalaciones y sus activos.
6) Prestar un servicio amable, eficiente y versátil al personal (colaboradores y empleados), así como a sus visitantes y clientes.
7) Atender las incidencias que surjan y se relacionen con la seguridad y vigilancia en la empresa.
8) Identificar actos inseguros y prácticas que pongan en riesgo al personal y las instalaciones.
9) Reportar de manera oportuna, clara y detallada, las novedades surgidas y actividades realizadas durante su jornada de trabajo, mediante la Bitácora de Registro o del Reporte de Novedades.

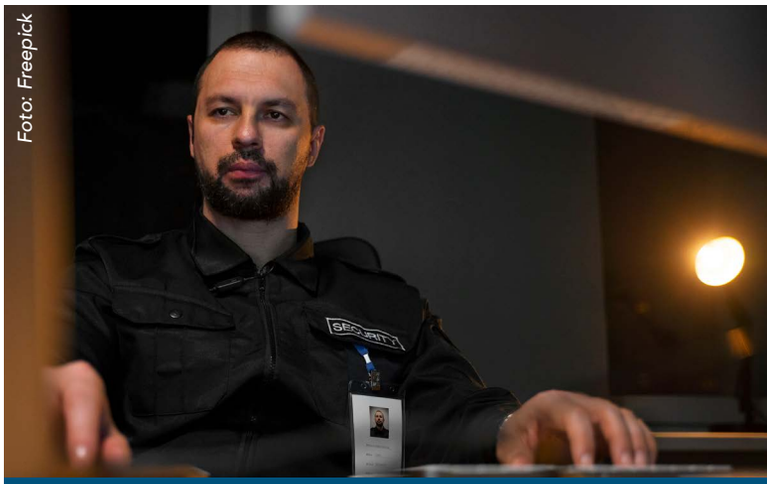


Foto: Freepick

El guardia de seguridad debe verificar en cada recorrido, las condiciones y ubicación de los elementos de protección y combate de incendios, sensores, alarmas, cerraduras, iluminación y barreras perimetrales

10) Realizar recomendaciones y propuestas sobre la implementación de recursos para incrementar el nivel de seguridad en las instalaciones, de ser necesario, sugerir el incremento de la plantilla del personal de vigilancia.

CONSIGNAS PARA EL ELEMENTO DE SEGURIDAD

El guardia de seguridad debe presentarse 15 minutos antes de su hora de inicio de actividades, perfectamente uniformado, con el equipo complementario completo, atento y alerta a las novedades del día.

Queda estrictamente prohibido a los elementos de seguridad y vigilancia todo tipo de distracciones durante su servicio, tales como lectura de revistas, periódicos, libros, folletos, ver televisión, escuchar la radio (salvo para escuchar la hora o los noticieros), etc. Los oficiales que presten el servicio diurno deberán anunciarlo.

Las instalaciones deberán contar con los recursos suficientes de iluminación, detección y videovigilancia para la protección del espacio defendible y para minimizar el riesgo de intrusion o ataque a los guardias de servicio nocturno. El guardia de seguridad debe verificar en cada recorrido, las condiciones y ubicación de los elementos de protección y combate de incendios, sensores, alarmas, cerraduras, iluminación y barreras perimetrales. Elaborar el Reporte de Novedades en caso de detección de irregularidades en el equipo de protección y defensa de las instalaciones.

TRASECO

Training Security Company

PERSONAL OPERATIVO CUALIFICADO

(Valores, Capacitación y Adiestramiento)

Guardias intramuros

Tu tranquilidad nuestra pasión

Seguridad TRASECO Privada

Custodia y vigilancia

Protección ejecutiva

Consultoría y capacitación

SOMOS UNA NUEVA OPCIÓN EN PROTECCIÓN

Equipo Directivo con 30 años de experiencia en el ramo

Porfirio Díaz # 67 int. 3,
Barrio San Juan, Tultitlán,
Estado de México, C. P. 54900

5524493906

5618829950

CONTRATACIONES:
ventas@traseco.com

CONSEJO NACIONAL CNSP SEGURIDAD PRIVADA A.C.
EMPRESAS DE CALIDAD

AMEXSI

CONSIGNAS PARA CONTROL DE ACCESO EN RECEPCIÓN

Establecer las directrices, lineamientos y responsabilidades que deben observarse por todo el personal de la empresa, sus empleados y visitantes en el acceso a las instalaciones, determinar las acciones que incrementen las medidas de seguridad, se custodie la integridad de los empleados, se resguarden los activos y se proteja la información de la empresa.

Alcance:

Esta política aplica a todo el personal administrativo y operativo (producción, almacén, distribución, servicios generales), y personal externo en general (proveedores, visitantes y contratistas).

AL MOMENTO DE ABRIR LA PUERTA DE LA ESCLUSA PEATONAL, EL GUARDIA DE SEGURIDAD DEBE ASEGURARSE DE NO ABRIR LA SEGUNDA PUERTA HASTA QUE LA PRIMERA HAYA CERRADO COMPLETAMENTE

DEFINICIONES:

Credencial de empleado:	Documento por medio del cual se identifica a la persona como colaborador de la empresa y se permite el acceso a las instalaciones.
Identificación oficial:	Documento que contiene fotografía e información general del portador, que lo identifica oficialmente. Este documento puede ser la credencial del INE (Instituto Nacional Electoral), licencia de conducir, cartilla del SMN (Servicio Militar Nacional) o pasaporte.
Gafete de visitante:	Documento de identificación que se proporciona al personal visitante y que le permite el ingreso y permanencia dentro de las instalaciones.
Proveedores o contratistas	Empleados de compañías externas que prestan o suministran bienes o servicios a la empresa.
Visitantes:	Personas sin relación directa a la empresa y que requieren del ingreso a las instalaciones con motivos comerciales o personales.

LINEAMIENTOS DEL CONTROL DE ACCESO

Sólo se permitirá el acceso a las instalaciones a personas que presenten Identificación Oficial Vigente, como recurso confiable.

El guardia de seguridad debe solicitar identificación oficial del visitante, y mediante un breve cuestionamiento, verificar el motivo de la visita, comprobar la información con la persona que recibe la visita y sea quien proporcione la autorización para el ingreso.

Una vez que haya cumplido con el procedimiento de identificación y control a través del registro de sus datos generales, el guardia de seguridad realizará el intercambio de un gafete numerado como recibo de su identificación, la cual permanecerá en vigilancia hasta que el visitante se retire.

El gafete de identificación es propiedad de la empresa y de uso obligatorio, por lo que el usuario debe portarlo siempre en un lugar visible.

Al momento de abrir la puerta de la esclusa peatonal, el guardia de seguridad debe asegurarse de no abrir la segunda puerta hasta que la primera haya cerrado completamente. Esta acción permitirá mantener "regulada" la entrada y cumplir con el objetivo de la esclusa: permitir la entrada a un espacio controlado antes de que el visitante ingrese a las instalaciones.

En caso de ser una visita confirmada al área de oficinas, será recibida en una "sala de espera". Por ningún motivo, las visitas pueden trasladarse solas por el interior de las instalaciones.

En caso del personal externo que acude con frecuencia a las instalaciones, como en el caso de mensajeros, paquetería, surtidores de agua o recolectores de basura, se consultará la relación proporcionada por el cliente en cuanto a horarios de atención y servicio.

Cuando por motivos de trabajo, el empleado deba permanecer en horario extraordinario el guardia de seguridad debe verificar la autorización a través del formato correspondiente, correo electrónico o indicación directa. La solicitud debe indicar el horario, las actividades a realizar y las áreas donde puede permanecer mientras realiza el trabajo. El documento debe contener el nombre y firma de la persona que autoriza la permanencia.

Todo el personal operativo (y en algunos casos el personal administrativo), tienen un rango de tiempo de tolerancia, después de transcurrido este tiempo, el guardia de seguridad deberá hacer mención del retardo y solicitar la autorización al área correspondiente para que el empleado pueda ingresar a laborar.

Cuando el personal operativo o administrativo llegue tarde a sus labores, deberá realizar el llenado de una solicitud de permiso. Al momento, el guardia de seguridad dará aviso a la Gerencia de Recursos Humanos o quien tenga facultad para determinar la situación del trabajador.

Cuando el personal que ingresa a laborar en turno nocturno llegue con algún retraso, el guardia de seguridad deberá informar al jefe inmediato para que éste tome las medidas pertinentes. En ningún caso, deberá regresarlo a fin de evitar que el empleado quede expuesto ante el riesgo de sufrir un asalto o accidente. El guardia de seguridad se limitará a registrar la situación en su bitácora de novedades. ■

Hermelindo Rodríguez Sánchez, CPO, CSSM, DSI, DES, CEO y fundador de la Consultoría en Seguridad y Protección Integral (Cosepri). *Más sobre el autor:*

Cursos de Manejo Evasivo y Defensivo

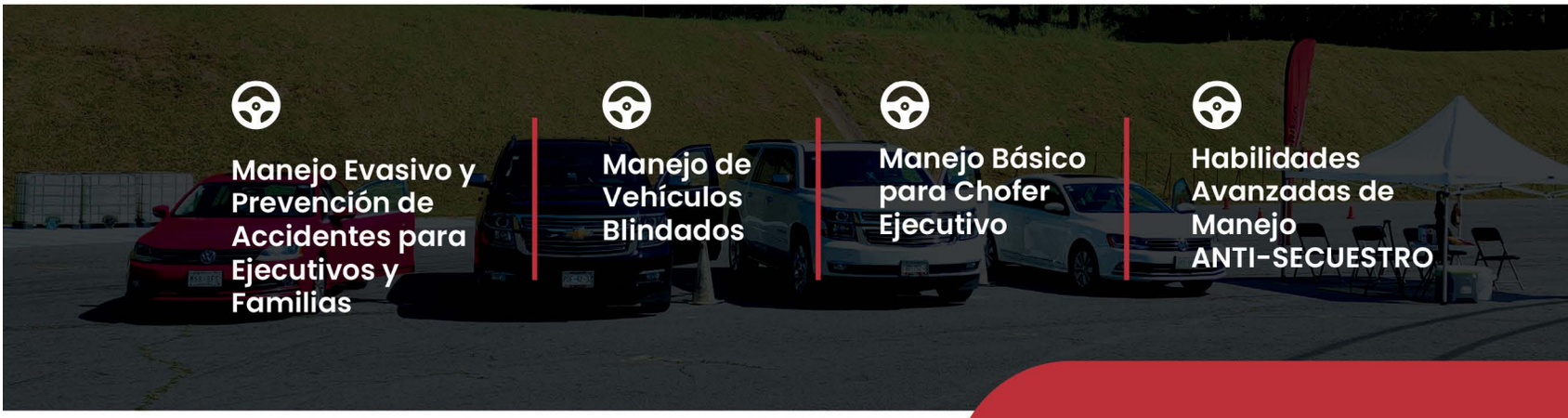
La capacitación más avanzada del mundo

Desarrolla habilidades de conducción avanzadas que te **permitán prevenir accidentes y delitos comúnes. Aprende junto a los pilotos profesionales más experimentados de México**.

Nuestro compromiso, desde hace 10 años, ha sido el crear los mejores programas de capacitación especializada en dinámica de vehículo con técnicas de entrenamiento basadas en ciencia, utilizando instrumentos de medición que puedan garantizar que se generen habilidades reales para aplicaciones reales.

- **Las mejores instalaciones de México.**
- **Único curso en México medido por computadoras que producen datos que sustentan la creación de habilidades reales demostrables.**
- **Reportes de desempeño emitidos por computadora que proporcionan una herramienta vital para toma de decisiones tácticas y de planeación.**

Programas de Capacitación



- Manejo Evasivo y Prevención de Accidentes para Ejecutivos y Familias
- Manejo de Vehículos Blindados
- Manejo Básico para Chofer Ejecutivo
- Habilidades Avanzadas de Manejo ANTI-SECUESTRO

Contáctanos

Capacita a tu personal y familia en las técnicas de manejo evasivas y defensivas más avanzadas del mundo.

Email
contacto@as3.mx

Web
as3.mx

Teléfono
+52 1 55 4181 8373

Columna de la

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

Más sobre la autora:

Jaquelin León Velázquez, secretaria del Comité ALAS México y gerente de Marketing y Comunicación para CAME México.

TECNOLOGÍAS APLICADAS A LA SEGURIDAD EN EVENTOS

Fotos: FreePick

MÉXICO

Los encuentros deportivos que se dan en nuestro país y países hermanos de Latinoamérica son un referente cultural muy fuerte con la capacidad de unir familias y amigos así como de dividirlos, por la pasión con la que se vive el deporte de competencia.

Tal pasión conlleva al fanatismo a vulnerar la sana convivencia; sin irnos muy lejos en el tiempo, en México el último evento deportivo que se registró de alto impacto fue en el año 2022 con el enfrentamiento entre asistentes durante un partido de futbol en el estadio Corregidora que dejo más de 20 heridos graves.

FAN ID EN EL MUNDIAL DE FUTBOL

El resultado de estos enfrentamientos puso al sector de la seguridad en el mapa ya que dos años atrás de este evento se había lanzado el primer piloto de control de fanáticos "FAN ID" en el mundial de Rusia, el cual constaba en crear un registro digital del rostro de quienes estarían acudiendo de manera presencial a los estadios, dicho piloto logró que se considerara la credencial de fanático como una identificación oficial para poder recorrer como turista de manera segura, entre otros beneficios.

Con estos hallazgos, en marzo del presente año, se hizo oficial la implementación del FAN ID para México sin excepción de equipos o estadios, por lo que en este caso. Las tecnologías aplicadas en el entorno de la seguridad para eventos deportivos se convirtieron en una herramienta indispensable para los responsables de la seguridad o bien usuarios finales al frente de la gestión y control de personas que puedan vulnerar la tranquilidad y seguridad tanto de los asistentes como el del inmueble.

Dicho lo cual, la organización y control de los eventos deportivos actualmente se encuentra en una transformación tecnológica, que sin duda está marcando historia en el campo de las tecnologías aplicadas en la seguridad y el control que reta a todos los involucrados en la cadena de valor para acercar soluciones que apoyen al objetivo de promover la cultura de la sana convivencia en eventos deportivos, claro sin dejar de lado la delicadeza de crear atmósferas de protección de datos personales.

Los invito a conocer a los socios corporativos y profesionales que son parte de la Asociación Latinoamericana de Seguridad ALAS para conocer las tendencias tecnológicas, así como los alcances en integración que impulsan el desarrollo de ciudades seguras. ■

TRUSTGROUP MR

En Seguridad, “Nadie Conoce México Como Nosotros”.

- Protección Ejecutiva.
- Seguridad Física.
- Seguridad Logística.
- Traslado de Valores.
- Capacitación y Entrenamiento.
- Administración de Crisis.
- Estudios de Integridad.
- Proyectos Integrales de Seguridad.

Contamos con los permisos de la Secretaría de Seguridad y Protección Ciudadana, la Secretaría de la Defensa Nacional en todas las modalidades para la portación de armas de fuego en todo el territorio nacional, así como de la Secretaría del Trabajo y Previsión Social.

www.trustgroup.com.mx

Más de quince años brindando servicios profesionales de seguridad

Nuestros Ejecutivos son miembros activos de:
ASIS INTERNATIONAL CAPÍTULO MÉXICO 217
*ASIS es la mayor empresa, a nivel mundial, de Profesionales de Seguridad

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.
"Dos Décadas de Representar Empresas de Calidad"

Prolongación Paseo de la Reforma 1232 Torre A Piso 1 Col. Lomas de Bezares CP 11910
Ciudad de México Tel. 55 2167 1231 y 55 6811 2618 | contacto@trusgroup.com.mx

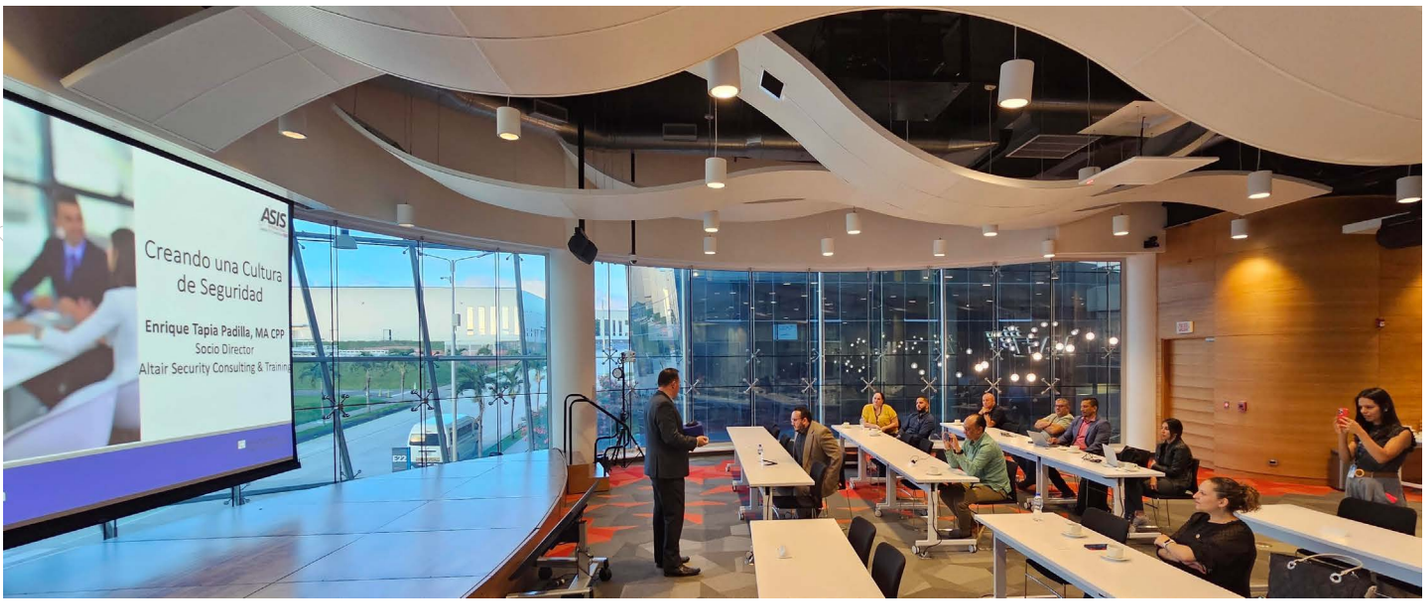
Columna de
Enrique Tapia Padilla, CPP
etapia@altair.mx

Socio director,
Altair *Security*
Consulting & Training.

Más sobre el autor:

INVOLUCRANDO A LAS PERSONAS EN LA IMPLANTACIÓN DE UNA CULTURA DE SEGURIDAD

(PRIMERA PARTE)



En un mundo con cada vez más retos de seguridad y muchos de ellos de rápida evolución, multifactoriales y además que suceden por diversos flancos, resulta indispensable repensar la seguridad y hacernos de todos los recursos disponibles.

No obstante, los colaboradores de manera involuntaria o deliberadamente pueden comprometer a cada momento la seguridad, por ello comunmente se menciona en seguridad que son el eslabón más débil, pero también pueden ser un gran aliado. Para lograrlo, las organizaciones deben implementar una serie de medidas y estrategias que aseguren los entornos, entre ello, crear una cultura de seguridad. Pareciera difícil porque muchos hablan de que los cambios son necesarios pero en ocasiones pocos quieren formar parte de ellos e involucrarse. Y es que muchas personas no se sienten parte de ello ni consideran que sus acciones individuales tienen gran impacto, nada más alejado de la realidad.

La importancia de que los colaboradores estén involucrados es imperativa. Las estrategias pueden ser variadas pero deben ser contundentes para asegurarnos que la seguridad sea un comportamiento de cada uno de ellos y no sólo se quede en un departamento, el departamento de seguridad.

Hace casi tres años, escribí un vasto artículo en dos secciones donde explicaba, paso a paso, cómo crear una cultura de seguridad; no obstante, ahora quiero enfocar este ensayo en el trabajo que se debe realizar con las personas para lograrlo.

EL PAPEL DEL LIDERAZGO

Un buen liderazgo sin duda resultará en el éxito del proyecto. Pero, ¿qué es el liderazgo? Una definición que me gusta por la profundidad que abarca es, "una disciplina que produce deliberadamente una influencia en un grupo determinado, con la finalidad de alcanzar un conjunto de metas preestablecidas de carácter beneficioso, útiles para la satisfacción de las necesidades verdaderas del grupo de influencia".

El papel del liderazgo en este sentido es crucial para establecer el tono y crear un entorno de apoyo para las iniciativas de seguridad. Implica estar disponible y proveer un apoyo cordial y propositivo, aceptando retroalimentación y sugerencias, involucrando verdaderamente a las personas, creando alianzas internas y beneficios grupales, privilegiando las relaciones y colaboraciones a largo plazo. El liderazgo está centrado en el desarrollo de los valores, en la motivación con claridad y respeto, con credibilidad y empuje. Al ser la creación

de la cultura de seguridad un trabajo de largo plazo, la disciplina, inteligencia emocional y la resistencia a la frustación serán muy valoradas.

LA IMPORTANCIA DE UNA CONCIENCIA EN SEGURIDAD COLECTIVA

Una cultura de seguridad comienza con la sensibilización; comprender que como ente debemos evolucionar a una conciencia situacional colectiva. Cuando una persona es consciente de su entorno y de los riesgos que pudieran implicar las acciones, comenzamos por buen camino. Por ello, es importante hacerles saber cuáles son los retos de seguridad y modo de operación de los adversarios, de manera que, en lugar de una vacía y nociva paranoia, exista una conciencia donde tomemos parte activa, sabiendo que la mayoría de los riesgos se pueden prevenir siguiendo sencillas medidas de seguridad.

Comprendiendo la forma en que se materializan las amenazas y el impacto que pudiera tener a su seguridad o a la de sus colaboradores, desarrollando un sentido de responsabilidad y corresponsabilidad, comprometiéndose con las medidas de seguridad a llevar a cabo. Involucrarlos y alentarlos permanentemente a la mejora continua.

EDUCACIÓN Y FORMACIÓN

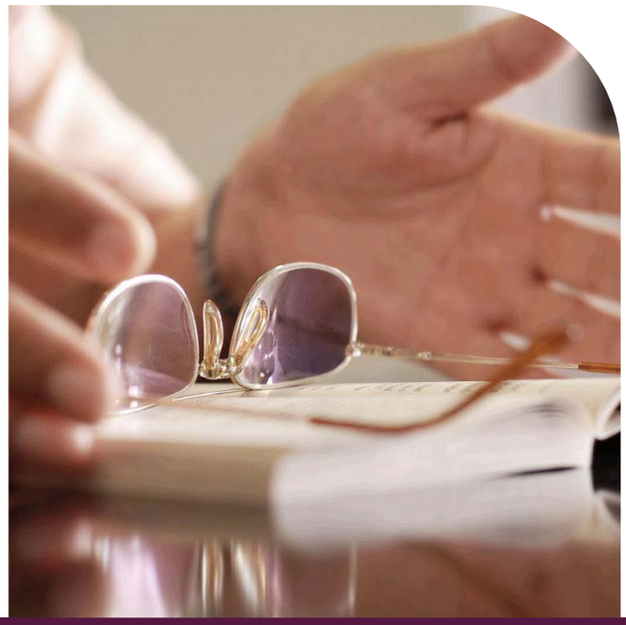
Los esfuerzos de capacitación a través de seminarios y cursos, *coaching*, infografías, comunicados, procesos y otras herramientas en seguridad resultan fundamentales para lograr que la cultura de seguridad permee en la organización, que forme parte de su naturaleza. Al sensibilizar de los riesgos, pero también de las medidas de prevención y de reacción que disminuyan los niveles de riesgo aumentando así los de seguridad, no sólo en el entorno laboral, sino también en los entornos social y familiar, podríamos lograr un compromiso con el proyecto.

Si bien los esfuerzos aislados sirven de alguna forma, debe aspirarse a una inmersión y capacitacion continua de todo el personal, sólo así lograremos mantener a los empleados informados sobre las amenazas presentes y las mejores prácticas de neutralización y prevención. Lograr que los métodos de entrenamiento sean más amigables, atractivos e inspiradores para fomentar la seguridad, la participación activa de los colaboradores y la retención de conocimientos, considerando escenarios y experiencias de la vida real.

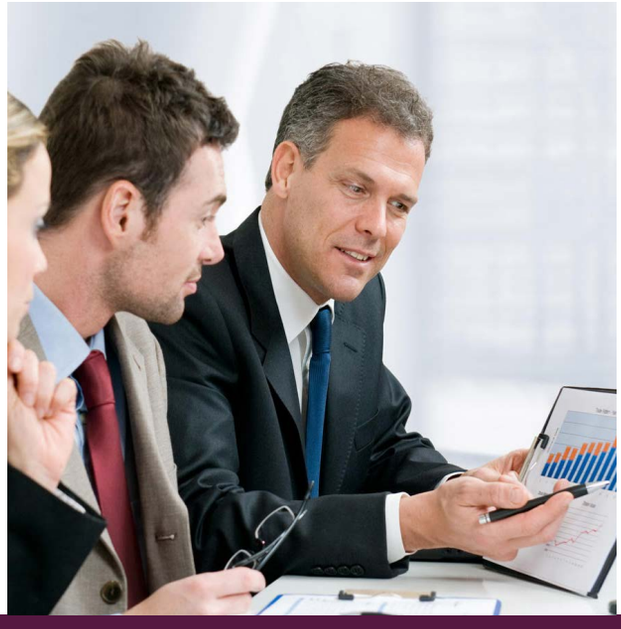
Como leen, resultará importante trazar una estrategia y esfuerzos alineados para conseguir que el proyecto funcione. En la siguiente entrega hablaré de otras estrategias indispensables para el éxito del proyecto. Nos leemos pronto.

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

Fotos: Cortesía Enrique Tapia



El liderazgo está centrado en el desarrollo de los valores, en la motivación con claridad y respeto, con credibilidad y empuje. Al ser la creación de la cultura de seguridad un trabajo a largo plazo, la disciplina, inteligencia emocional y la resistencia a la frustación serán muy valoradas



Comprendiendo la forma en que se materializan las amenazas y el impacto que pudiera tener a su seguridad o a la de sus colaboradores, desarrollando un sentido de responsabilidad y corresponsabilidad, comprometiéndose con las medidas de seguridad a llevar a cabo. Involucrarlos y alentarlos permanentemente a la mejora continua

FACTORES CLAVE PARA APLICAR LA PREDICTIVIDAD EN LA GESTIÓN DE LA SEGURIDAD

Fotos: FreePick

La seguridad predictiva puede ayudar a las organizaciones a reducir el riesgo de filtraciones de datos, interrupciones del sistema y otros incidentes de seguridad costosos

VENEZUELA | **Alfredo Yuncoza**

En el panorama actual de amenazas en constante cambio y cada vez más complejo, las organizaciones están bajo más presión que nunca para adoptar medidas de seguridad proactivas. La seguridad predictiva es una herramienta poderosa que puede ayudar a las organizaciones a identificar y responder a las amenazas antes de que se materialicen.

¿QUÉ ES LA SEGURIDAD PREDICTIVA?

La seguridad predictiva es un enfoque de seguridad que utiliza el análisis de datos y el aprendizaje automático para identificar patrones y anomalías que pueden indicar una posible amenaza a la seguridad. Al identificar y responder proactivamente a las amenazas, las organizaciones pueden reducir el riesgo de violaciones de datos, interrupciones del sistema y otros incidentes de seguridad costosos.

FACTORES CLAVE PARA APLICAR LA PREDICTIVIDAD EN LA GESTIÓN DE LA SEGURIDAD

Hay una serie de factores clave que las organizaciones deben tener en cuenta al aplicar la predicción en la gestión de la seguridad. Éstas incluyen:

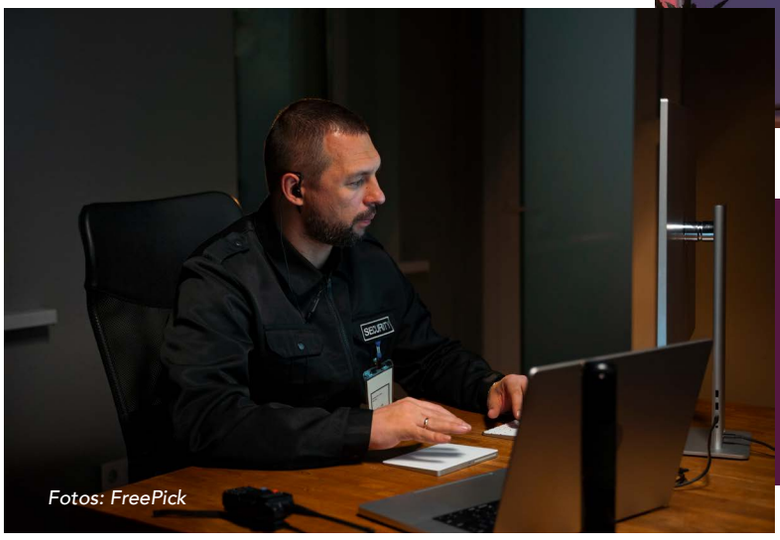
- **Recopilación y análisis de datos:** el primer paso en la seguridad predictiva es recopilar y analizar datos de una variedad de fuentes, como el tráfico de la red, el comportamiento del usuario y los registros de seguridad. Estos datos se pueden usar para entrenar modelos de aprendizaje automático para identificar patrones y anomalías que pueden indicar una posible amenaza a la seguridad.
- **Desarrollo de modelos:** una vez que se recopilaron y analizaron los datos, se pueden desarrollar modelos de aprendizaje automático para identificar patrones y anomalías. Estos modelos se pueden utilizar para generar alertas cuando se detectan amenazas potenciales.
- **Respuesta y remediación:** cuando se detecta una amenaza potencial, es importante contar con un plan para responder y remediar la amenaza. Esto puede implicar tomar medidas para bloquear la amenaza, investigar el incidente y tomar medidas para evitar que ocurran incidentes similares en el futuro.

BENEFICIOS DE LA SEGURIDAD PREDICTIVA

La seguridad predictiva ofrece una serie de beneficios para las organizaciones, que incluyen:

- La seguridad predictiva puede ayudar a las organizaciones a obtener una mayor visibilidad de su postura de seguridad, lo que puede ayudarlas a tomar mejores decisiones sobre cómo asignar los recursos de seguridad

Fotos: FreePick



Fotos: FreePick

La seguridad predictiva puede ayudar a las organizaciones a mejorar la eficiencia de sus operaciones de seguridad al automatizar muchas de las tareas involucradas en identificar y responder a las amenazas

- **Riesgo reducido:** la seguridad predictiva puede ayudar a las organizaciones a reducir el riesgo de filtraciones de datos, interrupciones del sistema y otros incidentes de seguridad costosos.
- **Eficiencia mejorada:** la seguridad predictiva puede ayudar a las organizaciones a mejorar la eficiencia de sus operaciones de seguridad al automatizar muchas de las tareas involucradas en identificar y responder a las amenazas.
- **Mayor visibilidad:** la seguridad predictiva puede ayudar a las organizaciones a obtener una mayor visibilidad de su postura de seguridad, lo que puede ayudarlas a tomar mejores decisiones sobre cómo asignar los recursos de seguridad.

DESAFÍOS DE LA SEGURIDAD PREDICTIVA

Hay una serie de desafíos que las organizaciones deben tener en cuenta al implementar la seguridad predictiva. Éstas incluyen:

- **Calidad de los datos:** la calidad de los datos utilizados para entrenar modelos de aprendizaje automático es fundamental para el éxito de la seguridad predictiva. Si los datos no son precisos o completos, los modelos no podrán identificar amenazas potenciales de manera efectiva.
- **Precisión del modelo:** incluso con datos precisos, los modelos de aprendizaje automático no siempre son 100 % precisos. Es importante contar con un plan para manejar los falsos positivos y los falsos negativos.
- **Costo:** la seguridad predictiva puede ser una inversión costosa, especialmente para las grandes organizaciones.

La seguridad predictiva es una herramienta poderosa que puede ayudar a las organizaciones a mejorar su postura de seguridad y reducir el riesgo de incidentes de seguridad costosos. Sin embargo, es importante ser consciente de los desafíos que implica implementar la seguridad predictiva y tomar medidas para mitigar estos desafíos. ■

Alfredo Yuncoza, presidente del Hispanic Advisory Board IFPO. *Más sobre el autor:*

BLINDAJE AUTOMOTRIZ: UNA HERRAMIENTA QUE SALVA VIDAS

La inseguridad, violencia y la delincuencia organizada, son las principales razones del incremento en el blindaje automotriz

Foto: cortesía Equipos Tácticos y tecnológicos de Seguridad ETTS

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

El blindaje automotriz es una industria que ha presentado un incremento en México en los últimos años, esto debido al alza de la inseguridad y la manera en que la violencia ha invadido distintas regiones del país. De acuerdo con el Consejo Nacional de la Industria Balística (CNB), los autos más blindados son camionetas familiares, principalmente con motores V6, de modelos recientes, dependiendo de las zonas geográficas, de la actividad del usuario y del tipo de protección que esté buscando.

Los estados con más solicitudes de blindaje automotriz son: Ciudad de México, Estado de México, Guanajuato, Jalisco, Nuevo León, Puebla, Tamaulipas y Veracruz, precisamente son los estados en donde se presentan más robos, donde está presente la delincuencia organizada y el narcotráfico. Pero esta herramienta ya no es sólo para empresarios, ejecutivos, políticos, actualmente se está extendiendo su uso para las personas civiles, como una medida preventiva y para el cuidado de la familia.

Es importante considerar ciertos aspectos al momento de blindar un automóvil, mismos que sólo los expertos conocen y que de hacer caso a todas las indicaciones y valoraciones, el blindaje automotriz puede salvar vidas. Es por eso que realizamos una entrevista a Gadi Mokotov, presidente de la Comisión de Blindaje Automotriz del Consejo Nacional de la Industria de la Balística (CNB).

GADI MOKOTOV

Seguridad en América (SEA): ¿Cuáles considera que son los principales retos a los que se enfrentan las empresas blindadoras en México?

Gadi Mokotov (GM): al ser México uno de los principales países en el ramo del blindaje a nivel mundial, el principal reto al que nos enfrentamos como empresas blindadoras, es seguir el ritmo de las nuevas tecnologías, lo que genera una competencia por ofrecer la mejor y mayor solución de seguridad para el cliente final. El blindaje siempre estará evolucionando, por lo que otro reto importante de una blindadora, es seguir buscando esas variantes que marquen la diferencia; nuevos desarrollos, materiales, nuevas técnicas, la búsqueda de un producto diferente que resalte entre el resto de las blindadoras, es decir, poder ofrecer no sólo productos con una mayor calidad, sino también precios competitivos.

SEA: ¿Qué aspectos debe considerar un usuario final al momento de blindar su vehículo?

GM: se debe considerar que al ser un vehículo modificado, aun-

Foto: cortesía Equipos Tácticos y Tecnológicos de Seguridad ETTS

que sea mínimo, siempre habrá diferencias en comparación con la versión original del vehículo. Una de las principales consideraciones está en el peso, ya que éste traerá consigo una diferencia notable en la conducción. Se debe ser consciente y responsable ante este cambio de peso del vehículo, porque habrá un cambio en los hábitos normales de manejo.

Otro punto importante que debe tener en cuenta el usuario, es que, un vehículo blindado siempre se hace pensando en salvaguardar la integridad de los ocupantes y que la función principal del blindaje, es que el usuario pueda escapar de una situación de riesgo, que su vehículo le permita salir ileso, pero siempre pensando en que el vehículo es una herramienta de escape y no de ataque. Por lo que se deben de considerar, técnicas de manejo táctico, lo cual ayudará a sacar el máximo provecho a un vehículo blindado.

SEA: ¿Cuál es la importancia de la industria del blindaje automotriz en México?

GM: la industria del blindaje permite generar empleos, así mismo implementar nuevas tecnologías a nivel nacional, aporta soluciones reales a la problemática del país, relacionada con la delincuencia organizada que afecta el transporte de carga, también el aumento de casos de secuestro, entre otros.

SEA: ¿Puede compartirnos cuáles son los objetivos del CNB?

GM: algunos de nuestro objetivos como Consejo Nacional de la Industria de la Balística, además de estar constantemente informando de todo lo relacionado al blindaje, son que las empresas se encuentren legalmente establecidas y debidamente registradas ante la autoridad (DGSP), que cuenten con certificados y soluciones específicas y, por supuesto, que todas las empresas de blindaje se comprometan a actuar contra todas las formas de corrupción, incluyendo extorsión o soborno anteponiendo siempre la verdad y oferta honesta a los usuarios de sus servicios.

Realizamos colaboraciones en conjunto para beneficio del sector junto con instituciones y autoridades, entre otros. Además de tener un enorme interés en el sector de la industria del blindaje, para nosotros como CNB buscamos el bienestar del usuario y contribuir a tener un México seguro.

SEA: ¿Cuál es el panorama actual del blindaje automotriz en México, crece o disminuye?

GM: el continuo aumento de la delincuencia y el crimen organizado en el país, hace pensar que la industria del blindaje automotriz seguirá en aumento, así como se ha estado registrando año con año. Con un aumento del 8% en la fabricación de vehículos en 2023. Por lo tanto, el incremento del blindaje automotriz es algo inevitable.

SEA: ¿Cómo se regulan las empresas de blindaje automotriz en México y qué sucede con aquellas que no cumplen los requisitos?

GM: una empresa de blindaje debe estar registrada ante la Dirección General de Seguridad Privada (DGSP), que depende de la Secretaría de Seguridad y Protección Ciudadana, lo que nos permite a las blindadoras emitir una constancia de autentificación con un código QR, respaldando el nivel de blindaje, también con el número oficial (placa de identificación) en cada uno de los vehículos que dicha empresa produzca, actualmente en el mercado mexicano, existen muchas empresas que no están registradas y que incluso ofrecen precios que hacen dudar de la calidad de sus materiales.

La única forma de regular el blindaje en México es por medio de la NOM-142-SCFI-2000, esta norma indica los niveles y especificaciones de protección balística resistente a impactos de bala y proyectiles, así como los métodos de prueba. Hoy en día no existe un ente que regule y certifique todos los vehículos con cualquier tipo de blindaje y con ello se garantice que los materiales utilizados en este proceso, cumpla con las normas nacionales y/o internacionales.

SEA: ¿Se tiene el dato de cuántas empresas de blindaje automotriz existen en el país?

GM: de acuerdo al oficio recibido por la DGSP en octubre de 2022 referente al número de empresas registradas en blindaje automotriz, se tuvo la información de que se tenían en la modalidad VII, submodalidad "a", 136 empresas registradas. "a" es la actividad relacionada directa o indirectamente con la instalación o comercialización de sistemas de blindaje con todo tipo de vehículos automotores.

NÚMERO DE AUTOS BLINDADOS EN MÉXICO

*Número de hologramas emitidos por la DGSP (unidades blindadas)
Comparativa desde el año 2018 a 2022:
2018: 3953
2019: 1511
2020: 2425
2021: 3775
2022: 3640

BLINDAJE AUTOMOTRIZ (COSTOS APROXIMADOS)

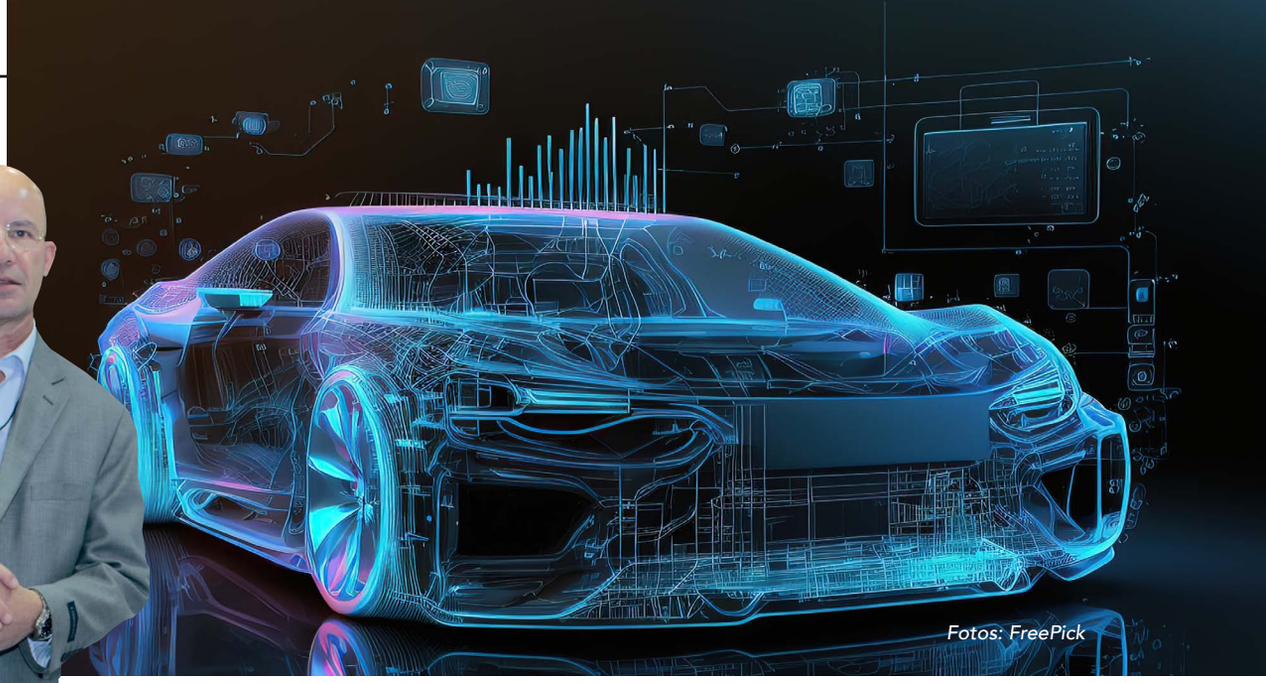
Nivel 2 Antiasalto urbano
- Protección de calibre .357 Magnum e inferiores.
- En autos los precios comienzan desde los 25 mil a los 28 mil dólares más IVA.

Nivel 3 Antiasalto urbano
- Protección de calibre .44 Magnum e inferiores.
- En autos los precios comienzan desde los 33 mil a los 43 mil dólares más IVA.
- En las SUV's los precios comienzan desde los 35 mil a los 45 mil dólares más IVA.

Nivel 4 Antisecuestro
- Protección de rifle de asalto AK-47 en inferiores.
- En autos los precios comienzan desde los 55 mil a 60 mil dólares más IVA.
- En las SUV's los precios comienzan desde los 60 mil a 61 mil dólares más IVA.

Nivel 5 Antiatentado
- Protección de FAL 7.62 X51 e inferiores.
- En autos los precios comienzan desde los 70 mil a 73 mil dólares más IVA.
- En las SUV's los precios comienzan desde los 75 mil a 80 mil dólares más IVA.

*En niveles altos los precios van de acuerdo a la configuración solicitada por el cliente.



Fotos: FreePick

MAURICIO NATALE

CITY SAFE: UNA SOLUCIÓN CONFIABLE Y SEGURA

Una de las empresas más representativas de la industria del blindaje automotriz, es City Safe. A continuación les compartimos la entrevista que le realizamos a su director general, Mauricio Natale.

SEA: en la actualidad, ¿hacia quiénes está dirigido el blindaje automotriz y por qué?

Mauricio Natale (MN): debido al alza en los índices de asalto, secuestro, robo de mercancía, y asaltos urbanos a mano armada, muchos ciudadanos mexicanos se sienten inseguros, al grado en el que, su vehículo es el sitio en el que más se sienten vulnerables a ser víctimas de algún delito. Es debido a esto, que el blindaje se convirtió en una solución real y eficaz para garantizar la seguridad de nuestros clientes con el mejor sistema de blindaje y protección de vehículos.

Esto se traduce en eficiencia, menos desgaste mecánico y mayor seguridad al momento de conducir.

Blindarse hoy en día en un tema de responsabilidad personal. Tener un vehículo blindado permite resguardar nuestra integridad, cuidar de nuestros seres queridos, patrimonio y bienes. De igual manera, es una forma de coadyuvar con las autoridades pues el blindaje, por su efectividad, es un real disuasivo para los delincuentes.

SEA: ¿Cuáles son los cinco aspectos a considerar antes de blindar un auto?

MN: aspectos relevantes a considerar:

1) No asumir que todos los blindajes son iguales y tener una idea clara de en qué tipo de instalaciones se realizará el blindaje, y comprobar si tienen o no la calidad necesaria. Esto permitirá evaluar el monto de inversión.
2) Evaluar diversas blindadoras y verificar que cuenten con materiales certificados que cumplan con la Norma Oficial Mexicana o su equivalente internacional. Buscar que la blindadora cumpla con una experiencia mínima de mil vehículos blindados para garantizar una mayor calidad en el servicio.
3) Tener especial cuidado con los productos sustitutos. No recomendamos adquirir un blindaje en una autoboutique o mediante recomendaciones de terceros con precios más económicos.
4) Tomar en cuenta la actividad desempeñada para conocer el nivel


Foto: cortesía CITY SAFE


Foto: cortesía CITY SAFE

de riesgo al que se puede enfrentar. En caso de no conocerlo puede acudir a una blindadora para obtener recomendaciones precisas.

5) Asegurarse de que se firme un contrato con las especificaciones del blindaje y que la empresa cuente con la certificación de que el blindaje del vehículo está legalmente registrado.

SEA: ¿Cuáles son los aspectos a considerar para definir qué tipo de blindaje requiere el cliente?

MN: el cliente debe tener claridad en:

1) Su nivel de riesgo, no es el mismo que corre un director o ejecutivo a otros sectores como emprendedores y jefes de familia.
2) Evaluar el índice delictivo de la zona en la que habita o trabaja.
3) Tomar en cuenta el tipo de actividades que realiza.
4) Evaluar su entorno y su estilo de vida, para poder contemplar todos los factores de riesgo.

SEA: ¿Qué características debe tener un auto para poder ser blindado?

MN: debe tener como mínimo:

1) Capacidad motriz suficiente para poder moverse adecuadamente con el blindaje.
2) Características de tamaño y tipo de vehículo a elegir, según la necesidad actual y real del cliente es el nivel de blindaje que se sugiere adquirir.
3) Blindar un vehículo con el que realmente se sienta a gusto y utilice a diario.
4) Algunos recomiendan autos de baja gama, para bajar el perfil del cliente y disminuir el riesgo, pero es un punto discutible, ya que no lo va a utilizar diariamente.

SEA: ¿Por qué blindar con City Safe?

MN: somos una compañía legalmente establecida con una experiencia profesional de más de tres décadas de experiencia y resultados de éxito en la industria del blindaje en Colombia, Medio Oriente y México. Lo que nos permite ofrecer una solución de alta calidad, funcionalidad y ante todo seguridad a todos nuestros clientes.

SEA: ¿Cómo se define City Safe?

MN: en tres palabras:

- **Liviano:** diseñamos blindajes que agregan un peso mínimo al vehículo. Esto se traduce en eficiencia, comodidad y durabilidad.
- **Seguro:** todos nuestros materiales están certificados a nivel internacional y contamos con técnicos e ingenieros expertos para lograr el mejor producto del mercado.
- **Confiable:** la calidad es una de nuestras prioridades en todo momento. Por lo tanto, otorgamos atención personalizada en la asesoría, venta de productos, servicio y garantías para lograr la total satisfacción de nuestros clientes. ■

SEGURIDAD EN EVENTOS DEPORTIVOS

Fotos: FreePick

México alberga a dos eventos deportivos de gran envergadura: el ATM y la F1, mismos que requieren de estrategias de seguridad preventivas y reactivas

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

¿A quién no le gusta al menos un deporte en la vida? Lo practique o no, la mayoría de las personas sienten cierta afición a algún deporte en particular, en México queda claro que el futbol es por quien se desviven cada fin de semana; Estados Unidos, el futbol americano; Nueva Zelanda, rugby; y hay otros que exportan deportistas de diferentes categorías, como Brasil, en donde tienen aptitudes muy marcadas para futbol, pero también para voleibol. Es decir, el deporte forma parte de la vida de las personas de alguna manera.

Pero no todo es pasión y alegría, la historia nos ha mostrado que hay una línea delgada entre afición y fanatismo, entre los que disfrutan de esta actividad y aquellos que la utilizan para violentar. En México, se llevan a cabo eventos deportivos de gran envergadura, como lo son el Abierto Mexicano de Tenis (AMT), y la Fórmula 1 (F1), ambos con excelente organización y con una seguridad a cargo de expertos en la materia, que tienen presente la importancia de estas estrategias para que los espectadores continúen disfrutando del deporte.

FÓRMULA 1 GRAN PREMIO DE LA CIUDAD DE MÉXICO

Se acerca el mes de octubre, y con él, uno de los eventos deportivos más esperados del país, la Fórmula 1 Gran Premio de México. Del 27 al 29 de octubre, el Autódromo Hermanos Rodríguez (Ciudad de México), recibirá a aficionados, corredores, *staff*, patrocinadores, y los diferentes participantes.

"Para prevenir y preservar la seguridad de todos los participantes de la Fórmula 1, implementamos videovigilancia, control de accesos, seguridad privada, relaciones con autoridades y capacitamos al personal de staff sobre actuación en caso de emergencias", **Violeta Arellano Ocaña**

Aunque no es un evento al que cualquier aficionado puede ir, en México ha tomado gran relevancia y la derrama económica tanto para la empresa organizadora, como para la CDMX es importante. Este año, los boletos van de los ocho mil pesos (470 dólares) hasta los 29 mil pesos (mil 700 dólares), más el consumo al interior. Pero como todo evento masivo, requiere de una planeación y seguridad estratégica.

PREVENCIÓN Y REACCIÓN

En entrevista, Violeta Arellano Ocaña, responsable de Seguridad Corporativa en una de las empresas de entretenimiento más importantes del mundo, Corporación Interamericana de Entretenimiento (CIE), y quien forma parte de la organización de la F1, nos comentó cuáles son las medidas de seguridad en este evento.

"Cada evento tiene sus particularidades, amenazas y niveles de riesgos, que van desde las condiciones geográficas, climáticas e incidencia delictiva del sitio, las condiciones socio políticas que se vivan en ese momento, así como historial de violencia entre los aficionados de los equipos deportivos. Para prevenir y preservar la seguridad de todos los participantes de la Fórmula 1, implementamos videovigilancia, control de accesos, seguridad privada, relaciones con autoridades y capacitamos al personal de *staff* sobre actuación en caso de emergencias", señaló la experta.

Y agregó que se realizan revisiones a todas las instalaciones en cumplimiento con la normatividad de Protección Civil, además de contar con el apoyo de autoridades de la Ciudad de México, como lo son Seguridad Ciudadana, Protección Civil, Bomberos, Ministerio Público, Tránsito, Policía Turística, Turismo, Secretaría de Movilidad, entre muchas otras.

De forma particular, ante un incidente durante una carrera de Fórmula 1 en México, derivado de un extenso análisis de riesgos, se toman medidas preventivas y se determinan procedimientos de actuación para cada uno de los riesgos identificados que incluyen paro parcial o total de actividades, evacuaciones parciales o totales, activación de equipos de emergencia, revisiones técnicas de instalaciones y determinación de condiciones para reanudar operaciones.

"La naturaleza del evento, las condiciones del inmueble y de la CDMX, generan una gran gama de situaciones de riesgo, entre ellas, sismo, incendio, fugas, derrames, lluvias torrenciales, vientos de máxima velocidad, tormentas eléctricas, contingencias ambientales, epidemias, manifestantes, riñas, robos, asaltos, accidentes en pista que afecten a las áreas de público y viceversa... adicionalmente a las medidas mencionadas, se cuenta con un puesto de mando con responsables de operaciones clave y representantes de autoridades donde se determinan, de manera colegiada, las acciones a realizar en caso de crisis, accidentes o incidentes importantes", señaló.

Violeta Arellano explicó que es de alta importancia el contar con infraestructura técnica y humana en eventos masivos, tomando en cuenta que en la actualidad, sucesos como terrorismo o vandalismo se pueden presentar, para esto recomienda contar con un Centro de Comando dentro de las organizaciones para poder realizar monitoreo en medios y redes sociales y así poder detectar intentos de boicot o convocatorias de actos violentos por parte de porras, barras, aficionados, opositores y grupos de interés.

"Estos elementos proporcionan información vital para elaborar análisis de riesgos que contemplan las condiciones citadas en el punto anterior, con los que de determinan las acciones preventivas disuasivas y reactivas que incluyen invariablemente dispositivos de control de acceso, que incluyen cacheos, arcos detectores, direccionamiento de flujos, así como asignación de espacios para porras o barras. Adicionalmente, existe la videovigilancia de interiores y exteriores, así como enlace con autoridades para identificar grupos violentos, manifestantes o disturbios en las inmediaciones y rutas hacia los inmuebles".

Para la seguridad de los deportistas, la experta sugiere aplicar técnicas de "Seguridad Profunda y Seguridad Endurecida", "se realizan dispositivos de vigilancia y control de accesos, que incluyen personal de seguridad interna, privada y pública. Nos apoyamos además con tecnología como videovigilancia, custodia y rastreo de unidades y un sistema bastante robusto de registro y control de acreditaciones que filtran qué personas están autorizadas paras ingresar a áreas restringidas de acuerdo con nivel de riesgo y funciones específicas", concluyó.

ABIERTO MEXICANO DE TENIS

El Abierto Mexicano de Tenis (AMT) celebró su trigésimo aniversario en la edición de febrero de este año (inició en 1993), en Acapulco, Guerrero, dejando una derrama económica de más de mil 200 millones de pesos (71 mil 40 mil dólares).

"Gracias a la realización de este evento (el AMT), Acapulco tuvo una exposición mediática en 170 países a través de los medios de comunicación internacionales y una afluencia turística de poco más de 189 mil visitantes; otro importante aspecto en materia económica, es que la empresa organizadora contrata habitantes de Acapulco para el 90% de los empleos que se generan durante este torneo, generando desarrollo local y fomentando un mayor sentido de pertenencia", informó en su portal el gobierno del estado de Guerrero[1].

No sólo es un evento significativo para la economía del país, sino para el turismo y la relevancia que tiene su organización y seguridad a nivel mundial. En entrevista, Víctor Manuel Vergara, director Operativo de Seguridad del Abierto Mexicano de Tenis Acapulco/Los Cabos/León por parte de la empresa Mextenis S.A. de C.V., explicó que los principales retos de seguridad en este evento se pueden definir a partir de dos ópticas:

1) Los que son visibles para todos los que acuden al evento.
2) Los que son manejados fuera del radar de los aficionados, pero que de no atenderse podrían generar un riesgo en el desarrollo del evento.

"Los retos visibles, de inicio los tendríamos que relacionar a la inseguridad de la región y todas sus variantes que lamentablemente mantienen números preocupantes desde hace muchos años, sin embargo, saliéndonos de una visión común, existen retos complejos como el manejo de masas en horarios de alto flujo como el inicio y cierre; el Abierto Mexicano es un evento que tiene jornadas muy extensas, sumando el factor clima, por lo que la administración y rendimiento del personal que opera la seguridad es muy importante, asimismo, dentro del evento y de forma simultánea, se realizan diferentes eventos, como fiestas y mini conciertos, por lo que debe existir una completa concentración y supervisión de distintos escenarios, así como un equipo listo para atender cualquier incidente que se presente", señaló el experto.

Y agregó que por otro lado, también se deben contemplar los delitos comunes como la reventa, y buscar una transportación segura del aficionado. "Dentro de los retos no visibles, podría encontrarse la rotación con autoridades del sitio, la coordinación con autoridades externas, que, si bien año con año muestran todo el apoyo para el desarrollo del evento, la coordinación llega a ser compleja en algunos momentos. Finalmente, redes de apuestas no autorizadas, falsificación de identificaciones, *tickets* o claves de ingreso, son parte de los retos que el equipo de seguridad debe atender y mantenerse a la vanguardia para no ser sorprendidos".

"Cuando logras una interacción y perfecto balance entre los tres pilares básicos de protección (Protección Civil, Física y del Talento) y convences a los organizadores de que son una necesidad, ahí es donde se puede empezar a construir la estética y el disfrute del espectador", **Víctor Manuel Vergara**

Los eventos masivos tienen en común aspectos a considerar para desarrollar una estrategia efectiva de seguridad, como las características del lugar donde se llevará a cabo, el tipo de evento, las inmediaciones del lugar, el transporte y accesos, entre otros.

"Al igual que en cualquier evento masivo, existen aspectos que deben ser considerados de forma obligatoria, desde mi experiencia, el tener tres análisis básicos: Protección Civil, Protección Física y Protección al Talento, permitirá establecer un esquema de seguridad adecuado para los asistentes, *staff* operativo, comité organizador y jugadores. También, debemos mantener una evaluación de riesgos del lugar en donde se llevará a cabo el evento, no sólo del interior sino del exterior, incluyendo las vías de conexión y acceso al sitio", señaló.

También se debe desarrollar una evaluación del tipo de aficionados o público que asistirá al evento, para establecer el nivel de protección adecuado, incluso en el tenis, se deben cuidar a los contrincantes en los partidos para saber si existen barras, porras o aficionados que requerirán mayor atención.

Fotos: FreePick

HERRAMIENTAS TECNOLÓGICAS

La tecnología es una herramienta de seguridad que sin duda debe estar presente en un evento masivo, en el caso de eventos deportivos, en otros países ya se cuenta con estadios inteligentes que poseen, por ejemplo, tecnología biométrica para un acceso más seguro e identificar a los asistentes y tener un mejor control ante incidentes.

"Podemos utilizar toda la tecnología que facilite el control de la seguridad, desde un estacionamiento automatizado en el ingreso, formato de pago y salida; hasta un filtro que sea menos invasivo como arcos detectores de metal, lectores de *tickets* de ingreso o brazaletes de acceso rápido. Así como tecnología adicional: drones, reconocimiento facial, lectoras de gafetes que rápidamente se puedan programar para autorizar o denegar accesos, esto beneficiará el trabajo del equipo de seguridad y permitirá generar registros para que exista rastreabilidad en caso de ser necesario", explicó Víctor Vergara.

Una de las estrategias de seguridad que ha funcionado no sólo en los eventos deportivos, sino en los distintos sectores: *retail*, transporte, industria automotriz, manufacturera, etc., es el compartir información sobre la delincuencia, las zonas de alto riesgo, y apoyarse de las autoridades.

"Un punto alterno a la tecnología, es el compartir información con otros torneos y/o con la asociación que regula el deporte, esto muchas veces te ayuda a anticipar algún riesgo que pudiera estar latente en tu evento, con ello la decisión de incrementar o no tecnología se vuelve muy relevante".

SEGURIDAD DENTRO Y FUERA

En este tipo de eventos internacionales, la organización no sólo depende del país o estado sede, sino también de la empresa responsable del torneo, en este caso, de la Asociación de Tenistas Profesionales (ATP), y como lo explicó Víctor Vergara, se requiere de una planeación entre organizaciones para contemplar todos estos aspectos y que el evento sea un éxito, como lo ha sido a lo largo de sus treinta ediciones, así como para la seguridad de los tenistas.

"Inicialmente tenemos una reunión y estrecha comunicación el equipo de Seguridad de la ATP, con el Supervisor del Torneo (también de la ATP) y el Comité Organizador local, esto permite emitir un sólo mensaje para todos los jugadores sobre los riesgos a los que pudieran estar expuestos. Posteriormente, se define cuáles son los jugadores que requerirán protección dedicada, que no siempre son los de mayor *ranking* en el torneo, y asignarles un equipo entrenado capaz de anticipar cualquier riesgo al que el deportista pudiera estar expuesto".

Dentro de los hoteles sede o alternos, existe una adecuada coordinación con el equipo de seguridad del lugar y un blindaje previo de los sitios de mayor concurrencia, para que los tenistas puedan desempeñar sus actividades con una menor invasión y no se altere tampoco el desarrollo de las actividades del hotel para sus huéspedes.

El experto explicó que fuera del *venue* o arena, las estrategias básicas como avanzadas, red de contactos locales, apoyos de autoridades, etc., ayudarán a que el nivel de exposición de los tenistas se reduzca, sin dejar de lado que deberá existir una comunicación proactiva con el mismo deportista o con el equipo que lo acompañe (*manager*, *coach*, etc.). El AMT 2024 se llevará a cabo en la Arena GNP Seguros, y el hotel sede será el Hotel Princess Mundo Imperial, el estadio principal recibirá a más de 10 mil espectadores, por lo que la comunicación con las autoridades locales y estatales es de suma importancia.

"Durante estos 20 años de experiencia, no sólo cubriendo el AMT, sino otros eventos masivos, he aprendido que la protección de estos te exige equilibrar distintas disciplinas de la seguridad y mantener un enfoque durante el desarrollo del evento, su planeación e incluso días después de su término. Cuando logras una interacción y perfecto balance entre los tres pilares básicos de protección (Protección Civil, Física y del Talento) y convences a los organizadores de que son una necesidad, ahí es donde se puede empezar a construir la estética y el disfrute del espectador, considerando casi todos los escenarios de riesgo para poder reaccionar de la mejor forma con el menor de los impactos. La seguridad siempre debe tener un nivel de calidad excepcional", finalizó. ■

Referencias:

[1] *"Deja el Abierto Mexicano de tenis una derrama económica de más de mil 200 MDP", Gobierno del Estado de Guerrero. 05/03/2023.*

SEGURIDAD EN LA INDUSTRIA FARMACÉUTICA

foto: freepik

La Industria Farmacéutica mexicana tiene un valor cercano a los 300 mil millones de pesos, además de ser el segundo mercado más grande en Latinoamérica, con un crecimiento del 10% en 2023, mismo que incentiva a mejorar los procesos de seguridad ante los riesgos que corre este sector en el país

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

De acuerdo a declaraciones de Rafael Gual Cosío, director general de la Cámara Nacional de la Industria Farmacéutica (CANIFARMA), ésta tuvo un crecimiento aproximado del 10% en lo que va del año, con un valor cercano a los 300 mil millones de pesos[1]; además de que México es el segundo mercado más grande de Latinoamérica de la IF. Este mejoramiento de los últimos años, se debió a raíz de la pandemia por COVID-19, por ejemplo, en el año 2020 generó 79 mil puestos de trabajo, cifra que representó un crecimiento de 3.6% respecto a 2019.

Pero así como crece la productividad de la Industria Farmacéutica (IF), los riesgos a los que se enfrenta también han ido incrementando, por ejemplo el mercado ilegal o la falsificación de medicamentos. En el décimo segundo Congreso Nacional de Farmacias en Ciudad de México (México, 2022), Juvenal Becerra, presidente de la Unión Nacional de Empresarios de Farmacias (Unefarm), comentó que "el mercado irregular repuntó un 20% en 2021 hasta alcanzar un valor de 28 mil millones de pesos (cerca de 1,365 millones de dólares), entre medicinas caducas, falsificadas y robadas, además de insumos como cubrebocas o gel antibacterial sin certificaciones"[2]. Para lo que Rafael Gual agregó que el robo y falsificación de medicamentos representa un 6% del comercio total de fármacos.

Ante esta situación, los responsables del área de Seguridad de la IF han creado estrategias para combatir los efectos de la inseguridad en el mercado, además de todo lo que implica la propia industria para que su funcionamiento sea el adecuado. Es por eso que realizamos una serie de entrevistas a expertos de esta industria quienes nos comparten su experiencia y aprendizaje.

RIESGOS DE SEGURIDAD

La falsificación de medicamentos es un problema que la industria farmacéutica enfrenta desde hace varios años, además de la venta ilegal de estos en el mercado negro, y actualmente en redes sociales y páginas de Internet, de donde se desconoce su procedencia, sin dejar de lado los riesgos de cualquier industria frente al contexto político-social del país.

*"La educación continua al paciente sobre comprar sus medicamentos en establecimientos autorizados es clave en el combate a la falsificación", **Nery Ayala***

"Desafortunadamente, la industria farmacéutica enfrenta diversos desafíos, algunos de los que tienen mayor impacto en la salud de los pacientes son: la falsificación, adulteración y desvío de producto; el *e-commerce* de medicamentos sin los debidos controles de seguridad; el robo a transporte, la tipificación de los delitos por parte de la autoridad, la poca sinergia entre entidades regulatorias de salud y de aplicación de la ley, así como la poca concientización de la población sobre su salud al adquirir medicamentos de dudosa procedencia o en canales de venta no autorizados", señaló Alan Vara, *Country Security & SHE Sr. Manager* en Roche México.

*"La industria farmacéutica enfrenta diversos desafíos, algunos de los que tienen mayor impacto en la salud de los pacientes son: la falsificación, adulteración y desvío de producto", **Alan Vara***

La falsificación de medicamentos o la venta ilegal de estos, no sólo causa un daño económico al sector, sino que es un riesgo para la salud de quien los consuma, donde le puede provocar desde la no mejora ante una enfermedad, hasta la muerte. De acuerdo con Alan Vara, esta mala práctica se debe a la necesidad de los pacientes, la demanda de producto (que no necesariamente alcanza a cubrir las necesidades del mercado) y el costo del medicamento. Anteriormente, explicó el experto, los medicamentos más falsificados eran los de alta especialidad, por la ganancia en cuanto al costo, sin embargo, en la actualidad, pero en menor escala, incluso se han encontrado productos de acceso general o de venta libre que se ofrecen a los pacientes sin receta médica.

"De acuerdo con la situación actual permanecen lamentablemente los riesgos comunes de todas las industrias, el robo a transporte, las intrusiones a las instalaciones y, con todo ello un daño financiero enorme y un desprestigio reputacional invaluable. Además, existe un nuevo reto que es la preparación defensiva ante la incursión de la delincuencia utilizando IA para generar daño y engaño, es un peligro nuevo y difícil de descifrar rápidamente, y ya han dado sus primeros golpes con teleconferencias replicando falsamente a presidentes de compañías ordenando transferencias millonarias, luego descubren que fue una imagen y voz falsificadas por la IA (inteligencia artificial)", comentó Gerardo Corchado, consejero de la Comisión de Seguridad de CANIFARMA.

Por su parte, Nery Ayala, experto en Seguridad Corporativa, explicó algunos aspectos para garantizar la autenticidad y la integridad de los medicamentos en el mercado. "Toda la industria tiene altos estándares en la fabricación y la palabra clave es trazabilidad. Por trazabilidad entendemos que todos los medicamentos deben tener un número de lote, fecha de manufactura y fecha de caducidad. Cualquier producto farmacéutico que no tenga esta información representa una bandera roja. No hay que perder de vista que lo más importante es la seguridad de los pacientes. En la parte reactiva cuando tenemos una sospecha de falsificación, la industria tiene a la mano diversas herramientas para confirmar si el producto es genuino (revisar los lotes en sistema para ver sitio de manufactura, a donde el lote fue distribuido, análisis de laboratorio si se tiene la muestra para determinar que el producto tiene el ingrediente activo, etc.). La educación continua al paciente sobre comprar sus medicamentos en establecimientos autorizados es clave en el combate a la falsificación".

Rodolfo García, coordinador de Seguridad en Novartis Farmacéutica México, también visualiza los siguientes problemas de seguridad en la IF:

- Delincuencia organizada (control de plazas, carreteras, etc.).
- Competencia desleal (venta de producto robado, tianguis, mercados, etc.).
- Piratería.

CANIFARMA FRENTE A LA FALSIFICACIÓN DE MEDICAMENTOS

La Cámara Nacional de la Industria Farmacéutica (CANIFARMA) está conformada por 170 empresas del sector, y busca generar propuestas y estrategias, tanto preventivas como reactivas, para que tanto la industria y las empresas, puedan implementarlas por sí mismas y en conjunto con las autoridades, federales y locales, encargadas de la seguridad de la población y la seguridad de los insumos para la salud.

"En CANIFARMA buscamos vinculación con autoridades locales y federales para minimizar los riesgos: con reuniones periódicas de seguimiento y actualización (Dirección General de Seguridad en Carreteras de la Guardia Nacional) – GN, en sus instalaciones de Base CONTEL", señaló Jesús Islas, presidente de la Comisión de Seguridad de CANIFARMA y *Protective Security Lead* en Novartis.

*"En 2021 hubo un incremento de más de 143% del valor del mercado negro de medicamentos respecto a 2020, al pasar de 11 mil 500 mil millones de pesos (MDP) en 2020 a 28 mil MDP en 2021", **Jesús Islas***

*"La Seguridad Estratégica debe estar cimentada desde prevención, que inicia en tener políticas y procedimientos robustos pero que permitan tener agilidad", **Alfredo Jiménez***

Jesús explicó que aunque por su naturaleza el mercado negro de medicamentos es un fenómeno complejo de medir, estimaciones propias de CANIFARMA señalan que alrededor del 6% de los medicamentos que se venden en el mercado mexicano podrían ser falsificados. A nivel mundial, la Organización Mundial de la Salud (OMS) estima que este porcentaje podría ser del 1% en países desarrollados, 10% en países en vías de desarrollo y hasta del 30% en algunas zonas de Asia, África y América Latina.

"En nuestro país, se observó en 2021 un incremento de más de 143% del valor del mercado negro de medicamentos respecto a 2020, al pasar de 11 mil 500 mil millones de pesos (MDP) en 2020 a 28 mil MDP en 2021. Aunque este crecimiento puede atribuirse a la pandemia por COVID-19, una encuesta realizada por el Instituto Mexicano de la Propiedad Intelectual (IMPI), reveló que sólo el 10% de las personas que compran productos falsificados consideran que ponen en peligro su vida y su salud", agregó el experto.

Ante esta situación, la CANIFARMA lanzó la "Campaña de Comunicación contra la Falsificación", con el objetivo de brindar información de forma concreta y precisa sobre los riesgos que representa el mercado ilegal de insumos para la salud y la falsificación de medicamentos en nuestro país, enfocado de acuerdo con el grupo que se visita. También se realizó una alianza con el Instituto de Química de la UNAM para impartir la plática a los alumnos residentes, y se tiene planeado expandir esta estrategia a otras instituciones educativas, como Universidad La Salle.

Dentro de la CANIFARMA, existen diferentes Comisiones y Consejeros, uno de ellos es Gerardo Corchado, quien comentó que la principal función de la Comisión de Seguridad, es el intercambio de conocimientos y experiencias en seguridad, para lograr la obtención de las *'best practices'* (las mejores prácticas) que se puedan compartir e implementar con las empresas agremiadas.

FABRICACIÓN Y ALMACENAMIENTO: ESTRATEGIAS DE SEGURIDAD

México es un país productivo en todas las industrias, y cada una requiere ciertas especificaciones para su desarrollo, en el caso de la industria farmacéutica, los productos resultados de este proceso, requieren de un almacenamiento y transportación con medidas para su seguridad y funcionamiento, muy específicas y totalmente necesarias.

"En el sector Farmacéutico, se debe contar con una serie de medidas y estrategias de seguridad implementadas desde la fabricación y almacenamiento para garantizar la integridad de los productos farmacéuticos, entre ellas comparto las siguientes:

- **Control de acceso.** Las instalaciones deben contar con sistemas de control de acceso físico, como tarjetas de proximidad, torniquetes en los filtros, CCTV en todas las áreas y seguridad en profundidad para limitar la entrada a áreas restringidas.
- **Seguridad del perímetro.** Se deben implementar cercas, cámaras de seguridad, iluminación adecuada y sistemas de alarma en el perímetro de las instalaciones para prevenir intrusiones no autorizadas.
- **Monitoreo de seguridad.** Se debe contar con un sistema de monitoreo y vigilancia, lo ideal es tener una central de monitoreo propia que opere 24/7, así como sistemas de detección de intrusos, para supervisar las áreas de almacenes.
- **Almacenamiento adecuado.** Los productos deben almacenarse en condiciones adecuadas de temperatura, humedad y luz para preservar su integridad y eficacia.
- Las instalaciones deben cumplir con las regulaciones y estándares de la industria, como las Buenas Prácticas de Almacenamiento entre muchos otros, para garantizar la calidad y la integridad de los productos", comentó Octavio García Peregrina, CPP, responsable de Seguridad y Protección en Farmacéuticos Maypo.

Por su parte, Alfredo Jiménez Garibay, especialista en Seguridad Corporativa, compartió algunas estrategias de seguridad para fábricas de medicamentos de gran longitud.

"La Seguridad Estratégica debe estar cimentada desde prevención, que inicia en tener políticas y procedimientos robustos, pero que permitan tener agilidad, un sistema de reclutamiento de personal que no sólo considere las capacidades técnico-laborales, sino también tenga un foco en la integridad, una campaña permanente de concientización del personal para tener una verdadera cultura de la seguridad, instalaciones basadas en CPTED, hasta la seguridad física tradicional para fines de disuasión, detección, contención e investigación".

*"Debemos contar con un Sistema de Gestión Control y Seguridad que tenga todas las políticas y procedimientos certificados para garantizar la seguridad en la cadena logística", **Octavio García Peregrina, CPP***


Tracking®
Systems
de México S.A. de C.V.
Soluciones Integrales
para RASTREO SATELITAL
Recuperación
98.5%
Aviso en menos
de 30 minutos*
25 AÑOS
DE EXPERIENCIA
+ de
50,000
equipos
instalados
24/365 DÍAS
Monitoreo de
equipos
WEB
APP
Desarrollo de
WEB y APP
Tecnología
3G/4G/Satelital
amazon
web services
Azure
Infraestructura
sustentada por
AWS y Azure
Contamos con
puntos estratégicos
en todo el país
*APLICAN RESTRICCIONES.
ALGUNOS ACCESORIOS Y EQUIPOS REQUIEREN ACTUALIZACIONES
Y/O CONFIGURACIONES ESPECIALES.
Más Información:
amesis
Socio Amesis
amesis.org.mx
Contáctanos
55·5374·9320

SEGURIDAD EN LA INDUSTRIA FARMACÉUTICA

"Los problemas de seguridad de la industria son: delincuencia organizada, competencia desleal y piratería", **Rodolfo García**

Prevención del Delito mediante el Diseño Ambiental (CPTED) es una metodología que busca disminuir los actos delictivos y de violencia en espacios urbanos, a través de la modificación de los factores de riesgo, creando, recuperando y adaptando los espacios públicos para hacerlos visiblemente seguros.

Además de las estrategias mencionadas anteriormente, la tecnología es fundamental para disminuir los riesgos y complementar al factor humano. "Se puede generalizar en que el 90% de la producción en la industria farmacéutica está automatizada, desde que la materia prima entra a las máquinas hasta que sale empacada lista para subir al transporte. Eso garantiza de alguna manera la seguridad de la cadena de producción. La tecnología también es factor decisivo en la cadena logística, que incluye desde almacenaje, *picking*, hasta la distribución. El eslabón más débil sigue siendo las personas por lo que la llegada de camiones autónomos reducirá de forma importante este riesgo", comentó Eduardo Téllez, *Chief Security Officer* en Laboratorios Liomont.

LOS RIESGOS EN LA CADENA DE SUMINISTRO

El transporte de carga en el país se ha visto afectado por el aumento de robo y violencia por parte del crimen organizado, ante esta situación, Octavio Peregrina, CPP, nos compartió algunos aspectos a considerar dentro del Sistema de Gestión de Riesgos en la cadena de suministro para asegurar que los productos lleguen seguros y adecuados a los puntos de distribución y/o venta:

- Debemos contar con un Sistema de Gestión Control y Seguridad que tenga todas las políticas y procedimientos certificados para garantizar la seguridad en la cadena logística" Octavio García Peregrina, CPP.
- Que el sistema de gestión esté auditado y acreditado por BASC (alianza de negocio para un comercio seguro).
- Procesos en cada una de las fases de la distribución del producto o medicamento, para tener una trazabilidad de las rutas desde el origen hasta la entrega con los clientes o instituciones.
- Sistema de monitoreo dedicado al proceso de logística que opere 24/7 y cuenta con protocolos de seguridad durante la cadena de logística.
- Sistema de reacción a nivel nacional que nos apoya y responde en caso de emergencias, robos o riesgos a los que se puede enfrentar los transportes durante el desarrollo de la entrega.

Alan Vara agregó el uso de custodias para el transporte de producto, establecer rutas, horarios y protocolos de seguridad para la distribución, implementar dispositivos de geolocalización en las unidades de transporte, la correcta destrucción de producto y las auditorías a proveedores del proceso E2E.

Hablando de México, explicó Alfredo Jiménez, la combinación del incremento de la incidencia delictiva con la disminución de las capacidades y voluntad por parte de las autoridades encargadas de la seguridad en las carreteras, se han convertido en el mayor reto de la cadena de suministro de esta industria.

Por su parte, Jesús Islas resaltó la importancia de una coordinación muy estrecha con los diferentes actores involucrados en la cadena de distribución (*Supply Chain*), para generar estrategias adecuadas encaminadas a minimizar el nivel de riesgo en la cadena de suministro.

"Es importante realizar evaluaciones constantes a los socios de negocio: transporte, almacenes, aduanas, casas de monitoreo (GPS) para evaluar sus procesos y procedimientos que garanticen la seguridad de nuestros productos; así como la evaluación constante de rutas de distribución para crear corredores seguros".

Mientras que Rodolfo García, suma a todo lo anterior:

- Visibilidad a lo largo de toda la cadena.
- Imágenes holográficas en el etiquetado.
- Cintas de seguridad en el Contenedor Primario.
- Rastreo Satelital.
- No parar el transporte durante su trayecto (cajero, comer, gasolina) en la medida de lo posible.
- No dejar al transporte nunca solo, siempre tener visibilidad.

Otra parte importante es el cuidado y protección de los empleados de la IF, para ello Nery Ayala compartió algunas medidas que se toman para garantizar la seguridad de los empleados en los laboratorios farmacéuticos y las plantas de producción.

"La principal función de la Comisión de Seguridad, es el intercambio de conocimientos y experiencias en seguridad, para lograr la obtención de las 'best practices', **Gerardo Corchado**

SOMOS PROFESIONALISMO
COMPROMISO
LEALTAD

GRUPO CORPORATIVO DE PREVENCION S.A. DE C.V.

Servicios:

- **Guardias Intramuros**
- **Custodia a Transporte de Carga**

SÍGUENOS EN REDES SOCIALES

@grupocorporativodeprevencion

CONTACTO

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

Contamos con las Afiliaciones y Certificaciones:

ASIS INTERNATIONAL · AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C. · CNSP Consejo Nacional de Seguridad Privada A.C. Empresas de Calidad · BASC · Circulo Logistico · ISO 9001:2015 Certified Company

*"Siempre se debe dar preferencia a la vida e integridad física de las personas antes que a la de cualquier bien tangible o intangible", **Eduardo Téllez***

"La industria en general tiene altos estándares de capacitación para los empleados que laboran en áreas productivas y comerciales, además de conocer los procedimientos de reporte cuando se presentan quejas de sospechas de falsificación. Además, las plantas productivas cuentan con sistemas de control de seguridad electrónica (circuito cerrado de televisión, control de acceso, controles en las líneas de producción, seguridad en el transporte, etc.) que permiten tener una trazabilidad del producto. Adicionalmente, todos los empleados deben conocer al detalle los procedimientos de reporte cuando se tienen sospechas en una muestra".

*Como invitado especial, **Luis Monge Cuéllar**, Regional Security Manager México-Belice en Abbott Laboratories*

Sobre la seguridad de los empleados en los laboratorios farmacéuticos y las plantas de producción, Eduardo Téllez comentó que los colaboradores pueden ser distribuidos en diferentes grupos dependiendo su actividad y/o conocimiento y/o acceso a procesos.

"Una persona que está en la etapa final de la cadena de distribución tiene un riesgo muy diferente a quien está en Producción, Calidad o Recursos Humanos. Con base en esto, se hacen análisis de riesgos por posición y se integran al Plan de Crisis y Continuidad de Negocio, para reducir la probabilidad de que se rompa, o, en su caso, se pueda hacer una recuperación del negocio lo más pronto posible. Asimismo, es necesario diferenciar la seguridad desde el punto de vista laboral en la integridad, y salud de la persona de los riesgos y problemas de inseguridad en la vía pública y la vida fuera de las oficinas o plantas productivas. Dentro de esta última, siempre se debe dar preferencia a la vida e integridad de física de las personas antes que a la de cualquier bien tangible o intangible", puntualizó.

Referencias:

[1] *"La Industria Farmacéutica mexicana es la más importante de Latinoamérica", Código F. 01/04/2023. Código F (codigof.mx).*

[2] *"Las farmacéuticas en México prevén crecimiento de 36 % en medio de las crisis". EFE/José Méndez- CONCANACO. 04/08/2022 https://www.concanaco.com.mx/prensa/tepuedeinteresar/las-farmaceuticas-en-mexico-preven-crecimiento-de-36-en-medio-de-las-crisis*

*Fotos: Mónica Ramos / **SEA***

Este reportaje especial fue realizado gracias al patrocinio de SISSA Monitoring Integral.

Agradecemos todas las facilidades otorgadas por Hacienda de Los Morales para la realización de este reportaje.

TIMUR
Latinoamérica

GALEAM

NUESTRO VALOR, SU SEGURIDAD






SERVICIOS

PROTECCIÓN EJECUTIVA

GUARDIAS INTRAMUROS

CONSULTORÍA

[www.galeam.mx]
[www.timurlatinoamerica.com]

info@galeam.mx | info@timurlatinoamerica.com
55 6840 1036 / 56 3048 9610 / 56 3700 0133

CERTIFICACIONES

SEGURIDAD EN LA INDUSTRIA AUTOMOTRIZ

foto: freepik

La industria automotriz en México incrementó sus ventas en un 20.1% este año, pese a la pandemia por COVID-19, la inflación y la interrupción en la cadena de suministro, sin embargo, sigue siendo un blanco para la delincuencia

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La industria automotriz en México ha ido estabilizándose después de los estragos que dejó la pandemia por COVID-19, la cual también alteró toda la cadena de suministro a nivel mundial, ejemplo de ello, es que en enero de este año, se reportó un crecimiento del 20.1% en ventas de vehículos en el país, en comparación con el mismo mes, pero del año 2022.

De acuerdo a José Zozaya, presidente ejecutivo de la Asociación Mexicana de la Industria Automotriz (AMIA), durante una entrevista otorgada a Forbes[1], tan sólo en enero de este año, se produjeron 280 mil 315 unidades y se exportaron otras 238 mil 135, dejando a la vista las grandes oportunidades que tiene esta industria para los posibles inversionistas, pero también sigue siendo un blanco para la delincuencia.

En junio de este año, un grupo de delincuentes, detuvo con violencia una "madrina" que transportaba camionetas en la Autopista León-Aguascalientes, a punto de pistola se llevaron las camionetas sin que nadie pudiera detenerlos. Este tipo de asaltos han ido incrementando principalmente en carreteras del corredor Jalisco, Michoacán y Guanajuato.

Guillermo Rosales, presidente de la Asociación Mexicana de Distribuidores Automotores (AMDA), dio a conocer en entrevista con El Financiero, que "entre mayo de 2022 y abril de este año se han robado 8 mil 645 equipos, es decir, un incremento de 24.4 por ciento. Por el contrario, la recuperación de unidades por parte de las aseguradoras cayó 58 por ciento"[2].

"Los principales problemas de seguridad en la industria son: robo de materiales, componentes en tránsito, robo hormiga, extorsión, secuestro exprés", **Gustavo Melo**

Como invitado ***José Manuel Allende,*** *Head of Security México en General Motors*

Es por ello que realizamos una serie de entrevistas a expertos de seguridad en la industria automotriz, para saber qué se está implementando ante esta situación, y cómo están protegiendo una de las industrias más importantes para el país.

PRINCIPALES RIESGOS

Como cualquier otra industria, la automotriz tiene sus propios riesgos de acuerdo a su movilidad y funcionamiento, al igual que aquellos a los que se enfrentan los demás sectores, que dependen del área geográfica, el contexto socio cultural y la inseguridad en el país, etc.

De acuerdo con Gustavo Melo, *Corporate Security Manager* en Daimler Truck México; los riesgos actuales de seguridad a los que se enfrentan son: robo de materiales, componentes en tránsito, robo hormiga, extorsión, secuestro exprés.

Por su parte, José Luis Valderrábano, gerente de Seguridad para México y apoyo a Latinoamérica de Nissan Mexicana, agregó, además, que "uno de los riesgos que afectan a la industria es precisamente la inseguridad que vive actualmente el país, en todas las aristas, por ejemplo, los atracos en el traslado de los vehículos o autopartes, que afectan al producto terminado y/o materias primas, de la misma manera el traslado del personal a sus casas y a las plantas".

Ahora bien, sobre los riesgos que enfrentan los usuarios finales de los vehículos, Gustavo Melo explicó que entre ellos se encuentra principalmente el robo total del vehículo con o sin violencia; aunque por ejemplo los vehículos de gama alta cuentan con llaves de proximidad inteligentes, y adicionalmente se pueden dotar de equipos de rastreo y localización satelital, sin dejar la importancia de contar con un seguro de autos.

CADENA DE SUMINISTRO

La cadena de suministro de la industria automotriz, aún se encuentra recuperando de las consecuencias que dejó la pandemia por COVID-19 en todo el mundo, así como la guerra entre Rusia y Ucrania, pues uno de los problemas a los que se enfrentó sobre todo en años como 2021 y 2022, fue el desabasto de materia prima y autopartes para la fabricación y armado de los vehículos, lo que llevó a la espera de los consumidores hasta por cinco meses para obtener un vehículo. Sin embargo, ese periodo de espera ha ido disminuyendo.
Por otra parte, también trabajamos en conjunto con las autoridades, en mesas de trabajo, a través de varias asociaciones como AMIA o el CEEG en las que hemos impulsado fuertemente y con el apoyo de las autoridades, la implementación de nuevas rutas en el 'operativo escalón'".

Respecto a este tema, Natalia Cerutti Pereyra, *gerente de Seguridad de Mercedes-Benz Mexico International,* comentó que el uso de tecnología ayuda a complementar la seguridad en la cadena de suministro, por ejemplo el uso de GPS (en inglés: Global Positioning System) y monitoreo, así como el ir conociendo y adaptando el uso de AI en la seguridad logística.

Sobre el traslado de los vehículos y considerando los riesgos a los que las "madrinas" enfrentan actualmente, José Luis Valderrábano explicó que se ayudan de información generada por el propio sector, asociaciones y autoridades, para conocer cuáles son las mejores rutas para transportar los vehículos, cuáles son zonas calientes, los horarios y paraderos seguros, entre otras.

Por su parte, Enrique Arellano Balcázar, gerente de Seguridad Corporativa de Mercedes-Benz Mexico, compartió algunas estrategias de seguridad para el traslado de los vehículos.

"Es importante controlar quién tiene y recibe la información de los embarques, crear y mantener la sinergia con las líneas transportistas para una mejora constante, así como realizar auditorías a los transportistas en los esquemas de OEA y C-TPAT, que los mantengan con esquemas seguros en el traslado de los vehículos, crear y mantener la comunicación efectiva hacia los contactos correctos para el apoyo de los recursos federales y finalmente, la estrategia de corredores seguros que permiten un traslado sin contratiempos o perdidas", indicó.

"Uno de los riesgos que afectan a la industria es precisamente la inseguridad que vive actualmente el país en todas las aristas", ***José Luis Valderrábano***

"Las alianzas con las autoridades de seguridad son necesarias, y mantener constante comunicación directa con ellas; así como realizar ajustes en la logística de las madrinas para evitar robos", **Natalia Cerutti**

Natalia Cerutti coincidió en estas estrategias y agregó otras más para enfrentar el robo de vehículos en tránsito. "Las alianzas con las autoridades de seguridad son necesarias, y mantener constante comunicación directa con ellas (Operativo Escalón, Laica, grupos de mensajes/respuesta directa y más rápida); realizar ajustes en la logística de las madrinas (horarios, convoyes, monitoreo, etc.), cambio en algunos procesos (llaves por separado), participación activa en AMIA y CAMEXA+Embajada Alemana (comité de seguridad de las empresas alemanas en México) entre otras asociaciones".

PROTECCIÓN DE DATOS Y EMPLEADOS

Al ser una industria en la que la propiedad intelectual y la confiabilidad por parte de los empleados es necesaria, los expertos en la materia han creado diferentes estrategias, con ayuda también de tecnología, para proteger tanto los datos sensibles, como al personal ante la situación que en algunos estados se vive por el crimen organizado.

"Nosotros creamos estrategias de identificación de empleados, utilizamos seguridad física, control de acceso, identificación de contratistas y proveedores e identificación y revisión de vehículos", explicó Gustavo Melo, y José Luis Valderrábano, agregó el uso de tecnología como la videovigilancia.

VEHÍCULOS ELÉCTRICOS: PREVENCIÓN ANTE ACCIDENTES

La producción de vehículos eléctricos o híbridos ha ido en aumento, el interés y la búsqueda constante de nuevas tecnologías y diseños que logren la emisión cero más un autoeficiente, está manteniendo ocupada a esta industria en todo el mundo. José Zozaya, presidente de la AMIA, comentó en la misma entrevista a Forbes, que "en los últimos dos años, se han anunciado inversiones por más de 3 mil 500 millones de dólares de diversas empresas asociadas a la AMIA, que se destinarán a actividades de producción de baterías y autos eléctricos, desarrollos en materia de automatización, introducción de procesos con energía de fuentes renovables, entre otras actividades derivadas de la importante transformación histórica de la industria hacia la producción de vehículos de cero emisiones"[3].

Y añadió que de enero a noviembre de 2022 hubo un crecimiento del 52.9% con 45 mil 249 unidades con este tipo de tecnologías, sin embargo, aún falta más infraestructura y cultura en el país para aumentar el uso de estos vehículos. Ejemplo de ello, es el desconocimiento que se tiene hacia cómo reaccionar ante un accidente en estas unidades, ya que no pueden ser los mismos procedimientos de rescate en un accidente vehicular que incluya un auto eléctrico.

"Las características de los autos eléctricos son completamente diferentes, ya que las condiciones cambian radicalmente y el manejo e intervención en los autos eléctricos es distinta; por un lado tenemos cableado de alto voltaje en algunas áreas del vehículo que no deben estar en contacto como si fuera un auto a combustión; también los fluidos que se maneja en un auto eléctrico son ácidos que no pueden manejarse a la ligera por ser tóxicos, pero dentro de todo este entorno completamente distinto a los autos de combustión, existe un estándar alto de seguridad para los ocupantes de un auto eléctrico, este estándar les permite desplazarse y hacer recargas de manera segura sin poner en riesgo su integridad", explicó el experto.

Ante estas características y el no poder dejar de lado los posibles accidentes vehiculares que los usuarios de los vehículos eléctricos puedan tener, Mercedes-Benz México está implementando capacitaciones a los cuerpos de Bomberos y Protección Civil.

"Esta estrategia es una iniciativa de nuestro CEO, el cual desea que los equipos de respuesta inmediata puedan recibir directamente de la marca la información básica y primordial al momento de tener que actuar e intervenir algún vehículo eléctrico que este envuelto en un accidente vial ya sea con o sin pasajeros. Por eso es que buscamos obtener por medio de nuestra área de Relaciones de Gobierno en conjunto con Seguridad Corporativa, la sinergia con los contactos claves y responsables del Heroico Cuerpo de Bomberos, iniciando con los equipos de toda la Ciudad de México, posteriormente impartir

"Las características de los autos eléctricos son completamente diferentes, ya que las condiciones cambian radicalmente y el manejo e intervención en los autos eléctricos es distinta", **Enrique Arellano Balcázar**

esta capacitación al Estado de México y avanzar con los estados de Jalisco y Nuevo León, sin dejar a un lado los equipos de Latinoamérica, ya que veremos cada vez más los vehículos eléctricos de Mercedes-Benz en esta región del continente", finalizó.

La industria automotriz continúa estabilizándose a nivel mundial, sin embargo no es ajena a los problemas de seguridad de cada región o país, y ahora también debe adaptarse a las nuevas tecnologías y lo que estas impliquen en su implementación.

Alejandro Barrera,
gerente de Seguridad
en General Motors

Referencias:

[1 y 3] *"2023: año de grandes oportunidades para el sector automotriz en México", Forbes, 06/05/2023 https://www.forbes.com.mx/2023-ano-de-grandes-oportunidades-para-el-sector-automotriz-en-mexico/*

[2] *"'Triángulo del horror' en México: Tráileres llenos de autos son robados en Altos de Jalisco", Fernando Navarrete, El Financiero. 12/07/2023 https://www.elfinanciero.com.mx/empresas/2023/07/12/triangulo-del-robo-en-mexico-traileres-llenos-de-autos-son-atracados-en-altos-de-jalisco/*

*Fotos: Mónica Ramos / **SEA***

Este reportaje especial fue realizado gracias al patrocinio de SISSA Monitoring Integral.

Agradecemos todas las facilidades otorgadas por Hacienda de Los Morales para la realización de este reportaje.

SOLUCIONES CONTRA INCENDIO

foto: freepik

MÉXICO | Mónica Ramos / *Staff* Seguridad en América

En México se registra un promedio de 260 incendios urbanos y no urbanos al día en todo el país, de los cuales, el 55.6% ocurre en edificios y condominios, dejando alrededor de 700 víctimas letales al año, y la mejor solución ante este grave problema, es la prevención

El INEGI (Instituto Nacional de Estadística y Geografía) dio a conocer que anualmente se registran más de 95 mil incendios urbanos y no urbanos, en promedio 260 al día en todo el país, y según datos de la National Fire Protection Association (NFPA), de cada 100 incendios en zonas urbanas, el 55.6% ocurre en edificios y condominios; 34.1% en comercios; 21.1% en casas de una sola familia; 3% en hoteles y moteles; 3% en industrias y 4.3% en otros edificios[1].

Desafortunadamente, se han registrado alrededor de 700 víctimas letales al año por incendios; además de que las edificaciones que presentan este siniestro, pierden un gran porcentaje de su patrimonio, y de acuerdo con aseguradoras, el impacto económico por incendios en el país en los últimos cinco años, fue de 34 mil millones de pesos[2].

La mejor medida de seguridad ante este siniestro, es la prevención. Es por ello que realizamos una serie de entrevistas a expertos en el tema, para conocer las mejores medidas y tecnologías contra incendios en distintos sectores del país.

ROBERTO JARAMILLO, CONSULTOR EN *SAFETY* Y PROTECCIÓN CIVIL

Maestro en Administración de Empresas y Director de Proyectos, con una especialidad en Habilidades Directivas. Fue voluntario en la Cruz Roja Mexicana, formándose como Paramédico, Rescatista Urbano, Operador de Radio y de Vehículos de Emergencia e Instructor. Perteneció a grupos voluntarios, entre ellos el Escuadrón de Rescate y Urgencias Médicas (ERUM) de la Ciudad de México. Fue integrante de la Policía Federal en la División de Inteligencia, posteriormente colaboró en el C5 de la CDMX como director de Vinculación y responsable del Centro de Operaciones de Emergencia (COE) y de 2019 a 2023 fue director general de Protección Civil y Salud en el trabajo en el Consejo de la Judicatura Federal.

Seguridad en América (SEA): de acuerdo con su experiencia, ¿cuáles son las principales causas de un incendio en México?

Roberto Jaramillo (RJ): las generadas por riesgo eléctrico y por la acumulación de materiales que generan cargas de fuego. Esto aunado a una laxa cultura de prevención respecto a este riesgo, que genera al año más de 98 mil incendios estructurales en el país.

SEA: ¿Cuáles son las principales construcciones en México que presentan incendios?

RJ: vivienda de interés social y medio, seguidas por actividades industriales de transformación, en donde se almacenan grandes cantidades de producto bajo condiciones de riesgo, en donde predomina la falta de sistemas de detección y supresión.

SEA: ¿Qué medidas de seguridad recomienda para prevenir un incendio?

RJ: en viviendas, revisión periódica de las instalaciones eléctricas y de gas, así como conocimientos básicos de combate a fuegos incipientes, sobre cargar las líneas eléctricas (extensiones y multicontactos sin protección termo magnética) incrementa considerablemente el riesgo de corto circuito e incendio. En la industria y servicios, observar y verificar los procedimientos preventivos, eliminación de riesgos por cargas de fuego acumuladas, preparación especializada de las brigadas y, dependiendo del nivel de riesgo, auxiliarse de sistemas automatizados de detección y supresión donde estos sean necesarios, más que por cumplimientos normativos, por sentido común.

5 tips de seguridad al momento de presenciar un incendio, por Roberto Jaramillo:

- Mantener la calma y recordar la preparación.
- Si no existe forma de iniciar un ataque inicial o secundario no se arriesgue innecesariamente.
- Muévase rápido y active a las demás personas en el recinto, debe actuar más rápido que el fuego.
- Nunca combatir un fuego si no se cuenta con equipo de protección adecuado.
- Active por cualquier medio disponible de inmediato a los servicios de emergencia, el tiempo de respuesta de éstos, hace una gran diferencia en los resultados del siniestro.

JACQUELINE FLORES ALVARADO, ESPECIALISTA EN *SAFETY*

Lic. en Administración de Empresas Turísticas por la UVM, cuenta con una Maestría en Administración con especialidad en Dirección del Factor Humano por la misma institución. Está certificada en la Elaboración de Programas Internos de Protección Civil por el Centro Nacional para la Prevención de Desastres (CENAPRED), y participó como expositor en el Diplomado de Dirección de Programas de Protección Civil del CENAPRED. También contribuyó en el establecimiento de las bases de la protección civil en el Grupo Financiero Banamex y en CIGrupo. Laborando para la primera Instutución por 24 años y en la segunda desde 2017 hasta la fecha, al frente de la protección civil. Cuenta con más de 30 años de experiencia en Protección Civil.

SEA: ¿Cuáles son las soluciones contra incendios que más recomienda utilizar?

Jacqueline Flores Alvarado (JF): la prevención es el elemento más importante cuando se trata de proteger la integridad del personal, de los bienes y valores de cualquier instalación expuesta al riesgo de incendio. Esta debe de ir acompañada de medidas y acciones que contribuyan a mitigar los posibles efectos de un incendio tales como:

- Sensibilizar e informar a los socios y/o dueños de empresas o negocios sobre la importancia de invertir en medidas de prevención, así como en la adquisición, instalación y mantenimiento de equipo contra incendio con tecnología de punta, que evitará pérdidas importantes, lo cual, a corto o mediano plazo, redundará en un retorno de inversión para éstos (ROI).
- Realizar inversiones en equipo vs. incendio contratando con empresas autorizadas que instalen sistemas certificados de detección de humo, de supresión de incendios, hidrantes, extintores, etc.
- Conocer, adoptar y aplicar leyes y reglamentos en materia de prevención de incendios.
- Realizar puntualmente análisis de riesgos y atender de inmediato las anomalías detectadas.
- Desarrollar un agresivo programa de capacitación en la prevención y combate de incendios.

Todo lo anterior, puede contribuir a que disminuya la vulnerabilidad o exposición al riesgo de incendio, lo cual redundará en la protección del personal y activos de las empresas, reduciendo la posibilidad de verse envueltos en acciones de carácter legal con autoridades o con terceros que pudieran ser afectados.

SEA: ¿Cuáles son los protocolos de seguridad ante un incendio?

JF: los protocolos para el personal que labora en una empresa:

Antes:

- Ubica las rutas de evacuación.
- Identifica las salidas de emergencia más cercanas.
- Conoce a tus brigadistas.
- Conoce el significado de la señalización.
- Ten localizados los extintores en tu área de trabajo y verifica que estén vigentes en su mantenimiento.
- Ubica las estaciones manuales contra incendio y su uso.
- Participa en los simulacros.

Durante:

Conserva la calma y transmítela.

- Si es un conato de incendio y conoces el uso de un extintor, trata de apagarlo, si no lo logras, retírate, activa la estación manual contra incendio y da la voz de alerta.
- Si es un fuego declarado o conflagración, ¡aléjate! Activa la estación manual contra incendio más cercana, da la voz de alarma a tus compañeros y evacua el lugar lo más rápido posible sin correr.
- Da aviso al personal de seguridad.
- Si hay humo en el área y es denso, cubre nariz y boca con un trapo húmedo y desplázate en cuclillas o a gatas hasta la salida de emergencia más cercana.
- No portes contigo mochilas u objetos personales que pudieran afectar el flujo de evacuación.
- Sigue la columna de evacuación en orden.
- Ubícate en el punto reunión externo y espera instrucciones del personal brigadistas y/o de seguridad.

Después:

- Mantente en el punto de reunión externo hasta recibir indicaciones.

SALVADOR GÓMEZ MARTÍNEZ, PRESIDENTE DEL CONSEJO DE INSTALA

Ingeniero civil egresado de la UNAM con 39 años de experiencia en ejecución y supervisión de obras, especializado en protección contra incendio, con certificación CPO de la IFPO y certificación DES por parte de ASUME y la Universidad Panamericana. CEO de Meridian Global e INSTALA, y ex presidente de la NFPA Capítulo México, ALAS Comité México y AMERIC.

SEA: ¿Cuáles considera que son los lugares o edificaciones más propensos a un incendio y por qué?

Salvador Gómez Martínez (SG): aquellos que en el análisis de riesgos tienen como resultado un riesgo extraordinario, así como los que tienen instalaciones eléctricas y de gas en condiciones de falta de mantenimiento, incumplimiento de normas o deterioro severo, y finalmente, aquellos que carecen de sistemas de detección de incendios y de extinción automática de incendios.

SEA: ¿Cuáles son las soluciones contra incendios que más recomienda utilizar?

SG: para sistemas de alarma y detección de incendios, la detección temprana por aspiración, debido a su alta efectividad, y en sistemas de extinción, los rociadores automáticos o los sistemas híbridos de nitrógeno con agua pulverizada para riesgos especiales.

MAK MR
EXTINGUISHER

MAKSeguridad

Prevenir es Proteger:
Extintores Efectivos con Mantenimiento de Calidad

¿Estás preparado para enfrentar el fuego? No dejes la seguridad al azar. Utiliza el extintor adecuado y mantén su funcionamiento con nuestro servicio de mantenimiento especializado. ¡Actúa hoy y protege lo que más importa!

www.makseguridad.com

SOLUCIONES CONTRA INCENDIO

SEA: ¿Considera que México está al mismo nivel que otros países en materia de capacitación, elementos de protección civil, tecnología contra incendios? ¿Qué considera puede mejorar en el país sobre ese tema?

SG: contamos en México con expertos que proveen capacitación adecuada en esta materia, particularmente en las asociaciones especializadas en seguridad como AMPCI (Asociación Mexicana de Protección Contra Incendios, anteriormente NFPA Capítulo México); CONAPCI (Consejo Nacional de Protección Contra Incendios), y los organismos certificadores de la NFPA como el IIAR (Instituto Internacional de Administración de Riesgos).

En cuestión tecnológica estamos a la vanguardia, ofreciendo las últimas soluciones aprobadas y listadas por UL/FM. Un área que se debe de revisar es la actualización de manera práctica, sencilla y factible de ser cumplida, de los Planes y Programas Internos de Protección Civil solicitados por la autoridad correspondiente, además de incorporar de manera obligatoria las normas de la NFPA, mediante la adopción de los códigos NFPA-1 Código Nacional contra Incendios y NFPA-101 Código de Seguridad Humana, como se ha hecho en varios países de Latinoamérica.

JOSÉ ANTONIO MOLLEVI PALACIOS, DIRECTOR DE SEGURIDAD CORPORATIVA & RELACIONES LABORALES PARA LAUREATE MÉXICO

Lic. en Derecho egresado de la UNAM, iniciando como litigante en el despacho Barrera, Siqueiros y Torres Landa, colaborando años después en laboratorio Merck, Sharp & Dohme, como director de Compliance para Mexico & Centroamérica, actualmente es el director de Seguridad Corporativa & Relaciones Laborales para Laureate México, siendo responsable de la seguridad de 38 campus con una población de alumnos, docente y personal administrativo de alrededor de 230 mil personas.

SEA: de acuerdo con su experiencia, ¿cuáles son las medidas contra incendios más eficientes en un centro escolar?

José Antonio Mollevi (JA): en nuestro caso, empezamos con un análisis de riesgo de incendio, lo cual nos ayuda a verificar nuestras áreas de oportunidad. Una vez concluido, verificamos las medidas de mitigación tales como: hidrantes, extintores, detectores de humo, detectores de calor, detectores de gas, válvulas sísmicas. Adicional, se contempla la integración de brigadistas para atención de cada área, así como pláticas de inducción a estudiantes, docentes y administrativos.

En nuestra experiencia, los ejercicios de simulacros también han servido para reforzar las medidas de prevención, ya que los brigadistas ponen en práctica lo aprendido en capacitaciones y los protocolos de actuación en caso de un conato de incendio.

Por otro lado, debemos considerar que, como buena práctica, la sinergia que hagamos con las autoridades es de gran ayuda para una atención inmediata; ya que gracias a que llevamos una buena relación con las autoridades bomberos y/o protección civil, nos ha ayudado a tener los canales de comunicación abiertas y una atención a emergencias más oportuna.

SEA: ¿Cuáles son los procedimientos de evacuación en caso de incendio en sus instalaciones?

JA: se identifica el lugar donde inicio el conato de incendio, si es controlable, la brigada de incendios actúa para su control; en caso de tener que evacuar, se activa protocolo de evacuación a través de alerta sonora, los brigadistas y docentes, dirigen a los estudiantes a los puntos de reunión más próximos; en paralelo, se activa el Comité de Atención de Emergencias, quienes contactan a las autoridades pertinentes, verifican la concentración de estudiantes, y toman acciones sobre la atención a esta emergencia.

SEA: ¿Realizan capacitación contra incendios tanto a estudiantes, empleados, padres, en su instituto?

JA: sí, hablando primeramente de estudiantes, en las pláticas de inducción se les informa de nuestros protocolos de actuación en caso de incendio, así como los mecanismos preventivos que tenemos para su contención, y se realizan prácticas para el uso y manejo de extintores.

TRUST ID

VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL

La Solución de Certificación y Verificación de Personal

más rápida, efectiva y confiable

99%
CONFIABILIDAD

- PROCESOS ULTRA RÁPIDOS
- ACEPTADA EN LOS PRINCIPALES CEDIS
- EN LÍNEA DESDE TU CELULAR
- CERTIFICADO Y CREDENCIAL DIGITAL E IMPRIMIBLE
- ESPECIALISTAS EN LOGÍSTICA

Más Información:

DESCARGA LA APP

ANDROID APP ON Google play

Download on the App Store

Grupo® UDA

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

trustid.mx

55 5374 9340

55 4141 6451

En el caso de colaboradores, se les da pláticas de inducción para el actuar en caso de un incendio y, se refuerza sus conocimientos a través de cursos que deben realizar semestralmente. Es importante mencionar que también contamos con un manual de consulta que pueden traer los colaboradores digitalmente en su celular, para conocer los protocolos de actuación que contempla diferentes escenarios de emergencias o amenazas.

Por último, para nuestros brigadistas voluntarios que son colaboradores, se les capacita semestralmente y se refuerza sus conocimientos en ejercicios de entrenamiento a fuego real en campo (Ejemplo: La posta).

MIDORI LLANES, SUBDIRECTORA DE SEGURIDAD E HIGIENE EN AXA MÉXICO

Egresada de la primera generación de la Maestría en Administración de Seguridad con especialidad en Ciberseguridad de la UDLAP Jenkins. Certificada como Profesional de la Protección (CPP, por sus siglas en inglés), siendo parte de las tres primeras latinoamericanas en aplicar en español. Su preparación académica a nivel internacional ha sido en Estados Unidos, España, Colombia y Venezuela. Cuenta con más de 25 años de experiencia en Seguridad y ha trabajado en diversas empresas transnacionales como líder de Seguridad Corporativa. También fue presidenta de ASIS Capítulo México.

SEA: de acuerdo con sus conocimientos, ¿qué edificaciones son las más propensas a incendios y por qué?

Midori Llanes (ML): más allá del tipo de edificio, lo más importante son las medidas que toman para reducir las vulnerabilidades. Aquellas instalaciones que no dan mantenimiento eléctrico periódico, almacenan sustancias combustibles en lugares inapropiados o no usan extensiones, son las más propensas a sufrir un incendio. Debido a lo anteriormente mencionado, usualmente las instalaciones que pasan tener un uso como oficinas o casa-habitación, a ser almacenes o fábricas improvisadas, muestran una mayor probabilidad de tener incendios.

SEA: ¿Puede compartirnos algunas estrategias preventivas contra incendios?

ML:

- Dar mantenimiento preventivo y correctivo a los sistemas eléctricos.
- Brindar entrenamiento a las brigadas y comisiones de Higiene y Seguridad de las empresas o edificios.
- Consolidar una cultura de detección de riesgos por medio de campañas de comunicación para que todos sepan cómo prevenir incendios.
- Contar con sistemas de extinción como rociadores automáticos, extintores e hidrantes.
- Capacitar al personal en medidas de acción si existe algún brote de fuego o incendio.

ESTELLE HASCOET, SUBDIRECTORA DE SUSCRIPCIÓN HOGAR Y PYMES EN AXA MÉXICO

SEA: ¿Puede platicarnos sobre la importancia de los seguros contra de protección del patrimonio que ofrece AXA y si en él se contemplan a los incendios?

Estelle Hascoet (EH): únicamente 6.5% de las viviendas y cerca de 18% de los negocios en México cuentan con la protección de un seguro. Para respaldar el patrimonio que estos significan para las familias y emprendedores mexicanos, existen los seguros de daños. En 2022 y lo que va de este año, hemos atendido más de 6 mil casos en la cobertura por incendio entre nuestros asegurados de empresas y hogares que significaron un costo promedio de alrededor de 300 mil pesos (17 mil 975 dólares). En el caso de nuestra oferta, tanto el seguro Hogar Integral para casas como 'Planprotege Daños' para pequeñas y medianas empresas, tienen contemplada la cobertura contra incendio dentro de las básicas.

SEA: ¿Cuáles son los cinco aspectos a considerar para contratar un seguro de daños (que incluya incendios)?

EH:

Identifica tus necesidades de protección para así contratar las coberturas necesarias. Además de las básicas como edificio y contenidos, rotura de cristales, robo de bienes, responsabilidad civil a terceros; puedes contratar adicionales para amplificar el alcance.

- **México es un país altamente expuesto a riesgos por catastróficos.** Por ello, es recomendable contratar las coberturas por fenómenos hidrometeorológicos, terremotos y erupciones volcánicas.
- **Consulta las condiciones generales en la página web de tu aseguradora para que sepas con transparencia lo que incluye y lo que no tu seguro.** Además, podrás conocer cuáles son las asistencias y beneficios a los que tienes acceso.
- **Asesórate con tu agente experto** para que te explique los términos que puedan ser complicados como el coaseguro, deducible o suma asegurada.
- **Úsalo en caso de incendio.** Si ocurre este tipo de incidentes, no olvides llamar a la aseguradora. En AXA México, desde hace 15 años, tenemos la misión de proteger mejor a más mexicanos. Actualmente contamos con la confianza de más de 180 mil hogares y negocios en el país.

JOSÉ LUIS CORIA ARREGUIN, GERENTE NACIONAL DE PROTECCIÓN CIVIL EN CODERE MÉXICO

Egresado de la Universidad de Valle de México, de la Licenciatura en Sistemas Computacionales Administrativos. Cuenta con un Diplomado por la Universidad Iberoamericana en "Seguridad Pública y Protección Civil"; Certificado CONOCER en Estándar de Competencia en el ramo de "Auditor de Sistemas de Gestión de Seguridad". Agente capacitador registrado ante Secretaría del Trabajo y Previsión Social, en temas de safety y security. Del año 2000 a 2013, como funcionario de mando medio en temas de Security, en dependencias federales.

SEA: de acuerdo con su experiencia, ¿cuáles son las medidas contra incendios más eficientes en un casino, incluyendo la tecnología?

José Luis Coria (JL): principalmente hay que considerar la participación del factor humano, en la formación y capacitación conforme a NOM-002 y 026, de la mayoría de los colaboradores quienes realizan sus actividades en cada Unidad de Negocio, para formar equipos de primera respuesta con la finalidad de prevenir y actuar debidamente ante situación declarada de Emergencia, conforme a los protocolos establecidos a cada inmueble.

Para:

- Salvaguardar la vida de clientes y colaboradores.
- Mantener la continuidad de Operación.
- Imagen corporativa, desde la perspectiva de instalaciones seguras.
    - Llevar un adecuado seguimiento al mantenimiento de instalaciones, primordialmente a las de Alto Riesgo, como son gas, electricidad, estructural, conforme a la Normatividad establecida.
    - Evitar el almacenamiento o acumulación de material obsoleto, que pueda representar altas cargas combustibles, sólidos y líquidos, debidamente contenidos e identificados, con el propósito de reducir los factores aplicables a la Clasificación del Riesgo de Incendio.
    - Mantener un adecuado y oportuno mantenimiento preventivo a Sistemas de Alertamiento temprano, redes de hidrantes y extintores, con proveedores certificados.
    - Establecer procedimientos de recorridos preventivos (por lo menos dos por turno), con la finalidad de verificar el óptimo funcionamiento y operación de rutas de evacuación, salidas de emergencia, señalética, puntos de reunión y equipo contra incendio.

SEA: ¿Cómo protege Codere sus bienes, instalaciones y personal ante un incendio o contra éste?

JL: siendo Codere una empresa líder a nivel mundial en el giro de entretenimiento seguro, se cuenta con una amplia gama de Pólizas de Seguros con cobertura global y las requeridas en específico por autoridades de cada país para su operación, para todas y cada una de las Unidades de Negocio.

Para el caso de nuestras Unidades de Negocio en México, contamos con una Póliza de Seguro de Responsabilidad Civil, la cual brinda la Protección requerida para, clientes, colaboradores e instalaciones, en caso de cualquier fenómeno natural o perturbador. Conforme a lineamientos de Secretaría del Trabajo y Previsión Social, todo colaborador está suscrito al régimen del Seguro Social y también cuenta con el beneficio de una Póliza de Gastos Médicos Mayores.

JULIETA MUÑOZ CORNEJO, CONSULTORA EN SISTEMAS DE SEGURIDAD CONTRA INCENDIO

Inició en el área de Protección Contra incendios en el año 2002 en el área de Ventas y posteriormente se especializó en la parte técnica tanto en la normatividad como sistemas, ya que se certificó en programación de tableros vs incendio y en el diseño de sistemas de supresión limpios, de agente espumante, de agua nebulizada, de sistemas en aerosol y sus diferentes aplicaciones. También está certificada en sistemas de BMS. Así como CPP ante ASIS Internacional, y Dirección de Seguridad de Empresas (DSE) y retomando sus estudios para la certificación de Seguridad Física de ASIS (PSP).

SEA: de acuerdo con su experiencia, ¿cuáles son las medidas contra incendios más eficientes en una tienda de autoservicio?

Julieta Muñoz (JM): los incendios estructurales en este tipo de instalaciones representan un riesgo muy tangible y, a la vez, no muy obvio a la vista del ojo público. En estos inmuebles conviven equipos y materiales muy variados pero con riesgos altos de incendio como lo son las cámaras de refrigeración, agentes refrigerantes, tuberías de gas, almacenamiento de sustancias y productos altamente inflamables, aerosoles, muchas instalaciones eléctricas que podrían ser temporales por equipos que pueden usarse en promociones y no necesariamente fijos en el piso de venta.

Es decir, todo lo que representa vivir en este sector implica que se garantice la seguridad del personal y de ahí la instalación de medios de detección, primordialmente, para contar con tiempo de usar equipos de primer ataque y evitar propagación por la velocidad de crecimiento que estos eventos podrían tener y, en segundo lugar, los equipos de supresión, ya sean portátiles (extintores), fijos (hidrantes) o automáticos (rociadores) que bien puedan ser parte de la línea de la red contra incendio, o automáticos en los casos de riesgos especiales como son cocinas o áreas de sistemas. Un aspecto también muy importante para garantizar que esta protección sea eficaz es la educación, la capacitación y primordialmente, la creación de conciencia de riesgo de incendio que tenemos.

SEA: si el incendio ocurre en algún CEDIS que surta a las unidades de autoservicio, ¿cuál es el procedimiento de reacción y qué ocurre con el contenido?

JM: cuando las tiendas de autoservicio reciben sus mercancías a través de centros de distribución, el reto es aún mayor en el sentido de que casi siempre, estos CEDIS se encuentran dentro de parques o bodegas industriales que no se encuentran siempre protegidas con rociadores ni medios de detección de incendio que garanticen la respuesta ante un evento. El reto de los CEDIS es que el arrendador, cuenta con un sistema que protege al parque en su generalidad mas no en los contenidos de las empresas que arrendan estos espacios o bodegas.

De ahí que se asegure que no se puede contar con la certeza de protección total en estos espacios, porque la manera de garantizarla sería contar con un sistema propio de alarma y supresión, con suministro de agua propio y en eso, al ser superficies en renta, hacen que las inversiones de los que arrendan, no se contemplen como mejora de inmueble salvo que se negocien cláusulas especiales en los alcances de los contratos de arrendamiento y se tenga una visión a largo plazo.

CRISTIAN GODÍNEZ, SUPERVISOR DE REACCIÓN INMEDIATA DE LA CENTRAL DE MONITOREO EN UNA PRESTIGIOSA CASA DE EMPEÑO

Cuenta con una Licenciatura en Administración, y otra en Seguridad Pública; es diplomado en Habilidades Directivas, y está certificado como CPO (Certified Protection Officer), con más de 12 años de experiencia como Profesional en Seguridad Integral, y desde hace 10 años en una prestigiosa casa de empeño

SEA: ¿Qué tecnología contra incendios recomienda para espacios que contienen piezas valiosas como lo es una casa de empeño?

Cristian Godínez (CG): puede ser desde un sistema de detección de incendio básico, como lo es un panel de detección de incendio dedicado, hasta un sistema de detección de alertamiento temprana, como un sistema de aspiración Vesda o un sistema de extinción de incendios mediante un agente limpio, como lo es un Gas Novec o un FM20.

SEA: ¿existe un protocolo de comunicación con los bomberos y servicios de emergencia locales en caso de incendio?

CG: por supuesto, un protocolo de reacción en caso de incendio es básico. Una de las principales actividades es solicitar el apoyo de los cuerpos de Emergencia, así como notificar a las áreas internas que deben conocer el incidente, ya sea Operaciones, Legal, Seguridad, Seguros y Fianzas, entre otras áreas que participan cuando suceden este tipo de situaciones de riesgo.

SEA: ¿Cuenta con un Plan de Continuidad de Negocios específico ante un incendio?

CG: sí existe un Plan de Continuidad de Negocios, pero no para cada tipo de incidente, ya que un BCP (por sus siglas en inglés), debe abarcar todos los escenarios posibles a los que puede enfrentarse la empresa, recomiendo ampliamente contar con uno para saber qué se debe hacer en determinadas circunstancias, que puedan afectar a las personas, las instalaciones o las operaciones de la empresa, el no contar con un BCP puede resultar en grandes consecuencias para la empresa, desde pérdidas económicas, hasta daño a la imagen y la reputación.

SEA: ¿Cuáles son los requisitos básicos de seguridad contra incendios en los lugares de trabajo?

CG: contar con un análisis de riesgos que nos permita identificar los riesgo potenciales que podrían afectar a cada una de las unidades de negocio, las instalaciones de resguardo de bienes y valores, y todas aquellas instalaciones donde podría suscitarse un incidente; así como identificar las herramientas tecnológicas y sistemas adecuados para cada uno de los lugares que debemos salvaguardar.

Fotos: Mónica Ramos / **SEA**

Referencias:

[1] *Incendios urbanos en México. CONAPCI*

[2] *"México, territorio en llamas por los incendios urbanos", Reporte Indigo, 06/09/2022.*

Con la participación de Norma Liliana Jiménez, coordinadora regional de Protección Civil México en BBVA

Este reportaje especial fue realizado gracias al patrocinio de SISSA Monitoring Integral.

Agradecemos todas las facilidades otorgadas por Hacienda de Los Morales para la realización de este reportaje.

19 DE SEPTIEMBRE: ¿UNA TERRIBLE COINCIDENCIA?

Ante los terremotos de septiembre en México, los especialistas en seguridad se actualizan y profesionalizan para tener una reacción que puede salvar vidas, ejemplo de ello, el trabajo realizado en la Comunidad de Protección Civil de ASIS 217

Foto: Freepick

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Llega el mes de septiembre y la alerta sísmica es el sonido más temido en México, sobre todo en los estados que han sido sacudidos por la naturaleza, especialmente desde 1985 y hasta 2017. En más de un año se ha repetido la actividad sísmica ese mismo día, inevitablemente se recuerda la tragedia de ambas fechas y el dolor de quienes perdieron seres queridos en alguno de los terremotos.

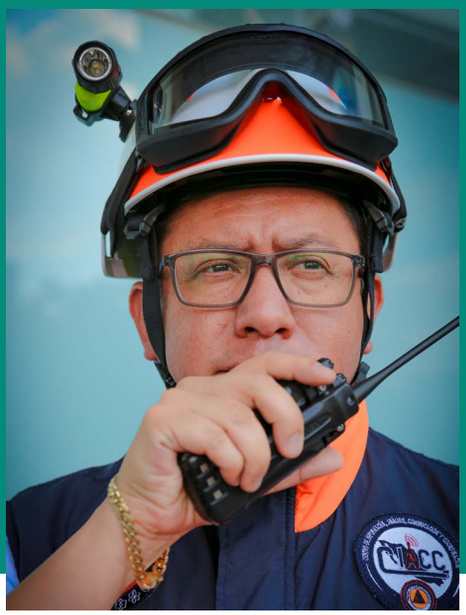
El terremoto de 1985 tuvo una magnitud de 8.1 grados en la escala de Richter, sucedió el jueves 19 de septiembre a las 07:17 h y el epicentro se localizó en el océano Pacífico en las costas de Michoacán; mientras que el terremoto del mismo día, pero del año 2017, fue de 7.1 grados en la escala de Richter, localizado en el límite estatal entre Puebla y Morelos, a 120 kilómetros de la Ciudad de México, justo a las 13:14 h, siendo la Ciudad de México en donde más personas fallecieron (228 de 369 personas).

El terremoto de 2017 dejó a la vista las consecuencias de la falta de supervisión en los permisos y técnicas de construcción sin las inspecciones necesarias y estrictas para edificaciones, tomando como ejemplo el complejo Residencial San José, ubicado en Zapata 57 y Tlalpan, colonia Portales, de seis torres con 24 departamentos, de los cuales se colapsaron seis de ellos con tan sólo tres meses (en 2017) de haber sido entregados a sus compradores. Asimismo, inmuebles como el Multifamiliar de Tlalpan (en donde nueve personas perdieron la vida) y el edificio de Álvaro Obregón 286 (49 lamentables decesos) dejaron a la luz la falta de medidas de reforzamiento en inmuebles que ya habían presentado daños en sismos previos (había evidencia desde 1997) o cuyas estructuras no cumplían con los estándares de las normas arquitectónicas actuales.Tampoco se puede dejar de lado la tragedia derivada de la construcción fuera de norma del colegio Rébsamen y los permisos otorgados para operar así, lo cual dejó 26 personas fallecidas, de las cuales 19 fueron niños y niñas. El 19 de septiembre de 2022, a las 13:05 h por más extraño o casual que pareciera, volvió a temblar por más de 90 segundos con una magnitud 7.7; el epicentro fue en las costas de Michoacán, frente a la población de Coalcomán; haciendo vibrar a la Ciudad de México, Hidalgo, Guerrero, Puebla, Morelos, Jalisco, incluso a la región sur de Chihuahua.

La memoria de las y los mexicanos en este mes, está dividida, entre la tragedia y la unión que ésta provocó con el único objetivo de levantarse y seguir adelante, pero ¿habremos aprendido la lección? ¿A partir de estos trágicos sucesos cambió la perspectiva y seguridad de las personas, las edificaciones y la capacidad de reacción y resiliencia ante una emergencia?

¿UN TERREMOTO SE PUEDE PREVENIR?

El Servicio Geológico Mexicano denomina a los sismos como movimientos de la corteza terrestre, siendo la interacción entre Placas Tectónicas, la principal causa de éstos, aunque no es la única. "Cualquier proceso que pueda lograr grandes concentraciones de energía en las rocas puede generar sismos cuyo tamaño dependerá, entre otros factores, de qué tan grande sea la zona de concentración del esfuerzo"[1]. Los terremotos son entonces sismos de grandes dimensiones… la pregunta es si realmente se pueden prevenir.



ROBERTO JARAMILLO, CONSULTOR EN *SAFETY* / PROTECCIÓN CIVIL

"Mi historia dentro los servicios de emergencia y la seguridad se remonta al año 1990, cuando tenía 16 años y me uní a las filas de la Cruz Roja Mexicana como voluntario, ahí me formé como Paramédico, Rescatista Urbano, Operador de Radio y de Vehículos de Emergencia e Instructor. En 2001 me integré a grupos voluntarios, entre ellos el Escuadrón de Rescate y Urgencias Médicas (ERUM) de la Ciudad de México. Del 2009 al 2017 fui integrante de la Policía Federal en la División de Inteligencia, posteriormente colaboré en el C5 de la CDMX como director de vinculación y responsable del Centro de Operaciones de Emergencia (COE) y del 2019 al 2023 fui director general de protección civil y salud en el trabajo en el Consejo de la Judicatura Federal. Soy maestro en administración de empresas y director de proyectos, cuento con una especialidad en habilidades directivas, así como diversos diplomados y certificaciones en gerencia integral de la seguridad, criminología, táctica policial, inteligencia, intervención en emergencias / catástrofes, sistema de comando de incidentes, así como evaluación y asistencia post-sísmica".

"Los terremotos, como uno de los fenómenos geológicos más devastadores y súbitos, no pueden prevenirse y quien lo afirme está mintiendo. Existe en el mundo tecnología de alertamiento oportuno ante la ocurrencia de los sismos (en al menos 16 países) y México ha sido un país pionero en el desarrollo de estas tecnologías desde hace varias décadas y eso hoy ha ayudado a que muchas personas hayan salvado la vida ante estos eventos. Lo que sí se puede prevenir son los efectos de los sismos a partir de los análisis de riesgos y vulnerabilidad que realicen las comunidades y los profesionales de la seguridad y la protección civil", comentó en entrevista Roberto Jaramillo, consultor en *Safety /* Protección Civil.

Dicho lo anterior, la prevención se basa en aceptación de que este fenómeno natural puede suceder en cualquier momento y de distintas magnitudes, de acuerdo con nuestro entrevistado, la región del Pacífico Mexicano es la más propensa a los sismos, esto debido a que el "cinturón tectónico" conocido como cinturón de fuego, que es donde más sismos ocurren a lo largo del planeta, prácticamente atraviesa las costas mexicanas.

Este "cinturón" está formado por placas de subducción (que se hunden una debajo de otra) que al moverse provocan estos fenómenos, los cuales suelen afectar, no sólo los estados costeros, sino otros estados aledaños, entre los que se encuentran: Morelos, Jalisco, Puebla, Tlaxcala y la Ciudad de México. De igual forma, la zona de Baja California puede considerarse de riesgo mayor ante su proximidad con la falla de San Andrés, que es el límite entre el cinturón de fuego y la placa norteamericana. Es entonces en estas zonas donde deberán existir más medidas de prevención ante estos fenómenos.

MEDIDAS DE PROTECCIÓN

Los científicos no dejan de estudiar los fenómenos naturales, sobre todo en esta era donde el cambio climatológico y las acciones de la humanidad han contribuido a esta fatal situación, modificando los procesos naturales. Debido a las diferentes catástrofes que han sucedido en el planeta, los especialistas y los responsables de cada área han ido incrementando las medidas de seguridad para evitar los menores daños posibles, pero, sobre todo, la pérdida de vidas.

La ingeniería sísmica ha avanzado mucho en el mundo a partir de grandes catástrofes del pasado entre las que podemos mencionar el terremoto de Valdivia en Chile en los años 60; Fukushima en Japón en el 2011 y desde luego el sismo de 1985 en México.

"Frente a un terremoto ya no puedes hacer mucho, pero preventivamente sí hay mucho qué hacer. El análisis geológico adecuado, la selección del diseño, los materiales, los elementos estructurales y sistemas de mitigación sísmica (amortiguadores, muros de corte de placa y estructura diagonales de soporte por mencionar algunos) permiten que se pueda construir de manera segura en zonas altamente sísmicas, grandes estructuras seguras como es el caso de la Torre Mayor o la Torre BBVA en México son muestra de ello. En lo personal, pienso que el enfoque 'Build Back Better' acordado en el marco de Sendai por parte de Naciones Unidas, aporta elementos esenciales para incrementar la seguridad de las construcciones en el mundo", explicó Roberto Jaramillo.

La Ley "*Build Back Better*" (reconstruir mejor) fue impulsada por el presidente de Estados Unidos, Joe Biden, y en forma resumida, se trata de invertir y generar alianzas para financiar medidas que contrarresten los impactos de la pandemia por COVID-19, pero también otros aspectos sociales y de infraestructura con un pensamiento enfocado en la sensibilización y concientización del cambio climático. Este enfoque invierte en aspectos específicos de la sociedad que mejoren su calidad de vida, así como en aspectos que reduzcan los efectos del cambio climático y mejoren la economía del país sin dañarlo.

MÉXICO FRENTE A LOS TERREMOTOS

Ante la incertidumbre de si el 19 de septiembre ocurrirá otro terremoto, o las *fake news* de que pronto sucederá otra catástrofe similar, los responsables de Protección Civil y de Seguridad continúan trabajando en las medidas ante estos fenómenos. Sobre todo, después de haber sido evidenciada la corrupción y falta de severidad en los permisos de construcción, ejemplo de ello, el Colegio Rébsamen (Tlalpan, CDMX), en el que Mónica García Villegas, directora del Colegio y dueña de las instalaciones, había ampliado y construido

"Los terremotos, como uno de los fenómenos geológicos más devastadores y súbitos, no pueden prevenirse y quien lo afirme está mintiendo"

ilegalmente un piso de más de 230 toneladas que la estructura origanal no soportó.

De esta tragedia, cuatro personas fueron detenidas, la directora en 2019, y otros tres responsables de la obra, Juan Mario Velarde (arrestado en 2018 y condenado a 208 años de prisión); Juan Apolinar Torales (2019), y Francisco Arturo Pérez (2022).

"Considero que, desde la concepción del Sistema Nacional de Protección Civil (SINAPROC) como resultado del terremoto de 1985 en el país, México avanzó mucho en la materia, al darle forma a un mecanismo preventivo que a su vez permitió el reforzamiento y la coordinación de los servicios de emergencia. Sin embargo, también considero que el papel de las autoridades en la materia debe fortalecerse para generar en la sociedad mecanismos más sólidos de participación conjunta que privilegien un pensamiento resiliente y dejen de lado la concepción de que las autoridades deben resolver todo en torno a una calamidad como son los terremotos", señaló nuestro entrevistado.

Y también agregó que el Sistema de Alertamiento Sísmico Mexicano (SASMEX, por sus siglas) es el único sistema de alerta temprana oficial que opera desde 1987 y es una compleja red de estaciones de monitoreo (96) y centrales de alertamiento público (7) que todo el tiempo están evaluando la actividad sísmica en las costas del Pacífico.

Cuando ocurre un evento, cuyas características se asemejan a los algoritmos preestablecidos, se alertará el sistema y en el caso de sismos mayores, activarán las alertas públicas en radio, televisión, así como los altoparlantes que están ubicados en los postes de los C4 y C5 de diferentes regiones del país. Respecto a su efectividad, él considera que es un sistema muy maduro y robusto reconocido por autoridades científicas y tecnológicas del mundo que, en más de 30 años de funcionamiento y gracias a su desempeño, ha salvado millones de vidas.

MÉXICO SIEMPRE UNIDO

Ante la escena impactante de los edificios colapsados, la oscuridad y la desesperación por encontrar a familiares y amigos, las calles de la Ciudad de México, tanto en 1985 como en 2017, se llenaron de mexicanos, mexicanas y extranjeros, dispuestos a ayudar. México siempre unido al menos en la tragedia, buscando la forma de salir adelante y ayudar a quien lo necesita. En el terremoto de 2017, las llamadas de auxilio se viralizaron por redes sociales y en algunas colonias llegó primero la gente a ayudar, que las propias autoridades, y es que a veces desconocemos quiénes son los encargados ante estas situaciones.

"Existen diferentes instituciones pertenecientes a los gobiernos estatales y municipales, así como organismos no gubernamentales como la Cruz Roja Mexicana que, se han profesionalizado de forma importante para dar una respuesta oportuna y técnicamente calificada ante estos eventos.

Sólo por mencionar algunos, se encuentran los equipos de búsqueda y rescate (USAR, por sus siglas en inglés) del gobierno de Jalisco; la Cruz Roja de las delegaciones CDMX, Tijuana y el grupo voluntario Rescate Urbano México A.C., cuyos programas de entrenamiento han sido supervisados por los mejores especialistas en la materia en diferentes partes del mundo, lo anterior sin menoscabo de la gran labor y esfuerzo que realizan los Heroicos Cuerpos de Bomberos del país y las Unidades de Protección Civil estatales y municipales, a pesar de las precarias condiciones en que muchas veces se encuentran", añadió Roberto Jaramillo.

El sector de la seguridad privada no puede dejar de lado este tema, y en asociaciones como ASIS Capítulo México se cuenta con la Comunidad de Protección Civil, la cual encabeza Roberto Jaramillo, en la que se abordan las mejores estrategias de seguridad ante estas situaciones.

"Resumiré en una sola frase el objetivo de la Comisión: salvar vidas. La Comunidad de Protección Civil ASIS tiene como objetivo principal el crear una cultura de prevención y preparación real y dejar de lado la respuesta a incidentes como una solución de fondo a estos temas; hoy, después de tantos años de andanza en las emergencias, puedo decir que la prevención y el entrenamiento anticipado son una de las mejores inversiones que pueden hacer las instituciones y sobre todo los profesionales de la seguridad", comentó.

EN MEMORIA DE TODAS LAS PERSONAS QUE FALLECIERON EN LOS TERREMOTOS

Puedo asegurar que la vida de una persona que vivió el terremoto de 1985 o y/o el terremoto de 2017 cambió totalmente, no sólo algunos se quedaron sin casa, sin sus pertenencias, sino que también perdieron seres queridos, amigos, y en su memoria queda el terrible recuerdo de cada segundo en que el suelo de su ciudad se sacudió imparablemente.

¿Habremos aprendido cómo evitar tantas perdidas en un terremoto y estar de pie para seguir adelante? En seguridad sí.

"Considero que, a pesar de que los mexicanos solemos dejar la historia en el olvido, eventos como los antes mencionados han dejado una profunda mella emocional en la sociedad, acompañada de un gran dolor y desesperación por las pérdidas humanas y materiales que se han visto reflejados en una mayor participación e involucramiento ciudadano, pero sobre todo, estos eventos han ido fortaleciendo en los profesionales de la seguridad la consciencia sobre la importancia de estar preparados con antelación, para poder hacer frente de manera exitosa a estos eventos, que, como todos sabemos, no podemos prever y pueden ocurrir en cualquier momento", concluyó el especialista. ■

Referencias:

[1] *"SISMOS: Causas, características e impactos", Servicio Geológico Mexicano | 02 de octubre de 2017 https://www.gob.mx/sgm/es/articulos/sismos-causas-caracteristicas-e-impactos?idiom=es*

Asistencia Legal

ALES

Gestoría Jurídica
en materia de
Seguridad Privada

Más de 30 años de experiencia en el sector a nivel nacional

Asumimos la responsiva de su empresa en los siguientes rubros:

· Obtención de autorizaciones iniciales, revalidaciones y modificaciones, para empresas de seguridad privada en todas las modalidades y en cualquier estado de la República.

· Mantenimiento y asesoría de los permisos de seguridad privada, cumplimiento de obligaciones Municipales, Estatales y Federales.

· Análisis jurídico y atención a cualquier procedimiento administrativo de cada permiso.

· Representación, atención y respuesta a visitas de verificación, supervisión o de inspección.
· Atención a multas y sanciones mediante recursos legales idóneos.

· Juicios de nulidad y amparo administrativo.

· Registro de personal directivo, administrativo y/o técnico-operativo a nivel Federal y Estatal hasta la obtención de CUIP o CIP.

· Alta o registro de agente capacitador interno o externo, planes y programas de capacitación, constancias laborales de capacitación DC-2, DC-3, DC-4 y DC-5.

· Elaboración de manuales operativos o de capacitación.

· Evaluaciones de Perfiles médicos, físicos, psicológicos, toxicológicos, entorno social.

· Permiso para el uso de armas de fuego, así como alta y registro de armamento ante SEDENA.

· Inscripción de Reglamento Interior de Trabajo, ante el Centro Laboral de Conciliación y Registro Laboral, Juntas Locales.

licdantegarciamtz@outlook.com

Whats: 477 828 1291

11 DE SEPTIEMBRE DE 2001, UN PARTEAGUAS EN LA SEGURIDAD MUNDIAL

Han pasado 22 años de los terribles atentados terroristas a las Torres Gemelas y al Pentágono (EUA), ¿además de intensificar las estrategias de seguridad, el terrorismo cambió su modus operandi?

Fotos: FreePick

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Es imposible olvidar un suceso tan trágico como lo fueron los atentados terroristas del 11 de septiembre de 2001, en los que 19 hombres pertenecientes al grupo terrorista al Qaeda, dirigidos por Osama bin Laden, y quienes secuestraron cuatro aviones comerciales estadounidenses, de los cuales dos fueron impactados en el World Trade Center (New York); uno en el Pentágono (Washington); y otro a las afueras de Shanksville, Pensilvania, cobrando la vida de dos mil 977 personas, incluyendo a los pasajeros de los aviones, policías, bomberos y agentes portuarios que llegaron a auxiliar.

A partir de ese momento, el terrorismo tuvo mayor atención en todo el mundo, pese a que ya existía desde las décadas de los años 80 y 90, fue hasta las 08:46 h cuando el vuelo 11 de American Airlines (que viajaba de Boston a Los Ángeles) golpeó la torre norte del World Trade Center, ahí el mundo mantendría la mirada en el terrorismo sin poder descansar.

"El terrorismo existe mucho antes que los lamentables atentados del 11 de septiembre de 2001. Podemos remontarnos a la década de los 80, 90; por ejemplo, en Egipto con la hermandad musulmana, o la guerra entre Rusia y Afganistán, así como en los 90 en Argelia; el terrorismo está muy asociado al mapa geopolítico y a las tensiones políticas entre naciones a nivel mundial. Y este se ha ido modificando de acuerdo a sus intereses. Hemos de contemplar un cambio muy importante, los terroristas de Afganistán se fueron a la parte de Sub-Saharan (África), extendiéndose de Burkina Faso a Somalia con los famosos 'piratas', y han evolucionado, ya no lo hacen por una causa político-religiosa, se ha vuelto un negocio lucrativo", explicó Mustapha Sahalí, director general de PSI Seguridad, y quien nació en Argelia y tiene un amplio *expertise* en materia de terrorismo.

El experto también comentó que hoy en día, los grupos terroristas también se están fusionando con la piratería en los océanos, con el robo de mercancía en carretera, la venta y tráfico de drogas, transporte de drogas y de armas, con el secuestro, es decir, está diversificando sus actividades. El terrorismo es un negocio, y deja mucho dinero, por lo que no se ha podido controlar del todo.

VIAJAR YA NO ES COMO ANTES

El terror y la desconfianza fueron sentimientos que por muchos años permanecieron en los pasajeros recurrentes de los aeropuertos de todo el mundo, después por supuesto de los atentados del 11-M, pero sobre todo del mismo país, que no podía aceptar que hubiesen ocurrido dichos atentados pese a la seguridad con la que ya contaban, por lo que en el año 2001

"A partir del 11-M se extremaron las medidas de control en las fronteras, en la vía aérea en particular y han optado los gobiernos por intercambiar información sobre los movimientos de los grupos terroristas"

fue creada la Administración de Seguridad de Transporte (TSA) en Estados Unidos, la cual ahora forma parte del Departamento de Seguridad Nacional (Homeland Security, creado en 2002) y quien se encarga de supervisar la seguridad de más de 400 aeropuertos estadounidenses.

"No sólo Estados Unidos incrementó los controles de seguridad en sus aeropuertos, todos los países de todo el mundo lo hemos hecho. Nuestra forma de viajar cambió. A partir del 11-M se extremaron las medidas de control en las fronteras, en la vía aérea en particular y han optado los gobiernos por intercambiar información sobre los movimientos de los grupos terroristas, e inclusive ha causado tanto impacto esta amenaza, que en España hay un diplomado sobre terrorismo, se ha vuelto una especialidad analizar la conducta de estas personas", agregó el experto.

Esas medidas de seguridad se esparcieron en el mundo, así como diferentes actos terroristas no sólo hacia Estados Unidos, además de que se ha vuelto una mala práctica entre los gobiernos para amedrentar y tener poder.

"Las tendencias actuales del terrorismo que se pueden observar, de acuerdo a mi experiencia, es que el terrorismo Yihadista va a disminuir, pero lo que sí puede aumentar es una escalada de actos terroristas entre Rusia y Ucrania, porque es un arma para desestabilizar a los gobiernos. Se podría pensar que habrá atentados contra Rusia, pero ésta es un Estado policiaco que tiene un gran control y que ha impedido que alguien atente contra ese lugar, o si lo han intentado, al menos lo impidieron y fue mediatizado el hecho. Retomando a Estados Unidos, hace unos meses el presidente de esa nación, Joe Biden, comentó sobre una de las preocupaciones de seguridad del país, y es el terrorismo doméstico o los grupos radicales, la supremacía blanca contra latinos, negros y demás. Hoy se presentan más atentados domésticos en Estados Unidos, que actos terroristas, incluyendo los tiroteos de sus propios residentes", sentenció Mustapha.

EL NARCOTRÁFICO ¿TERRORISMO O NO?

La idea de clasificar a los cárteles mexicanos de droga, como grupos terroristas, es algo que desde el ex presidente de los Estados Unidos, Donald Trump, se ha sugerido, sin embargo, el gobierno mexicano rechazó la propuesta de Trump, quien en su propia voz declaró que le ofreció al presidente de México, Andrés Manuel López Obrador, venir y "limpiarlo". Su argumento es que al año el país norteamericano pierde a 100 mil estadounidenses a causa del narcotráfico mexicano.

Esta situación se ha intensificado por la presencia del fentanilo. "Casi 70 mil personas en Estados Unidos murieron por sobredosis de drogas que involucraron fentanilo en 2021, un aumento de casi cuatro veces en cinco años. Para 2021, aproximadamente dos tercios de todas las muertes por sobredosis involucraron al potente opioide sintético, según el informe. Se pueden informar varias drogas en un certificado de defunción, y el fentanilo a menudo se encuentra junto con otras, según los CDC (Centros para el Control y la Prevención de Enfermedades de EE.UU)"[1].

Es evidente que los cárteles mexicanos son la principal amenaza de seguridad de este país, cada vez más expanden su territorio, sin embargo, para el gobierno mexicano, que Estados Unidos los declare como terroristas, significa una violación a la soberanía del país.

"En México sí estamos viviendo un terrorismo procedente de los cárteles de la droga, pero como no hay bombas o granadas, no lo consideran así. Lo que preocupa es el tipo de ataques de estos cárteles de la droga, el cómo amedrentan a la autoridad estatal, municipal, en el estado que sea y que pueden llegar a usar otro tipo de armamento, porque hoy, con lo que cuentan, pueden 'rafaguear' a las instituciones, a un oficial de policía, un cuartel de policía, al ministerio público, o hasta una iglesia. La gente está abandonando su lugar de residencia por los constantes enfrentamientos entre cárteles y policía o ejército, ejemplo de ello, los estados de Zacatecas, o Chiapas", comentó Mustapha Sahalí.

El experto comentó que es un tema muy delicado, porque Estados Unidos "con su arrogancia y abuso de poder, mismo que lo ha llevado a ser el país más odiado en el mundo, y que muchos países se hayan aliado y hecho acuerdos comerciales con China y Rusia, cansados de la arrogancia de Estados Unidos".

MUSTAPHA SAHALÍ, DIRECTOR GENERAL DE PSI SEGURIDAD

Con un Doctorado en Administración de Empresas (España), Mustapha Sahali tiene más de 17 años en el sector de la seguridad, enfocándose desde un principio sobre todo en el área comercial. En 2019, fundó la empresa de seguridad privada PSI Seguridad (Profesionales en Seguridad Integral), la cual ofrece los servicios de: Seguridad física, Seguridad Electrónica y Consultoría en seguridad, con un equipo de expertos profesionales que cuentan con diversas certificaciones de nivel internacional tales como: CPP, DSE y DSI.

"Estamos muy vulnerables porque vivimos en una sociedad en la que la violencia se ha normalizado, se ha perdido esa sensibilización a la vida"

Fotos: FreePick

Para el país vecino es más sencillo responsabilizar en su totalidad a México, "a los republicanos se les hace muy fácil decir que el narcotráfico en México es terrorismo e intentar meter sus manos, pero cuando se habla de la participación de los estadounidenses, de la aduana en el paso de las drogas, toda la responsabilidad es de México, en lugar de que ellos asuman y actúen. No podemos dejar que ellos etiqueten y consideren terrorismo al narcotráfico cuando no ha habido ningún atentado a su país", externó.

EL CIBERTERRORISMO

La tecnología y la vida virtual en la que nos encontramos inmersos, no podía quedarse fuera de estas estrategias de control violentas y repudiables. El ciberterrorismo existe, y es aquel que a través de hackeos obtiene información o logra dañar a quien decida de acuerdo a sus ideologías.

"El ciberterrorismo no cuesta vidas humanas de los atacantes, no cuesta dinero en armamento y la logística es mucho más sencilla: un tipo con una computadora y listo", comentó Mustapha Sahalí. Como cualquier ataque cibernético, la prevención es fundamental para asegurar la información, integridad, operación y demás aspectos que los ciberterroristas quieran atacar.

A 22 AÑOS DE LOS ATENTADOS 11-M

Las víctimas de los atentados del 11 de septiembre de 2001 son más de dos mil 977 personas, pues con los años, algunos de los rescatistas han perdido la vida a causa de cáncer o problemas respiratorios relacionados con el humo, los gases que se desprendieron con el derrumbe de las Torres Gemelas, sus muertes han sido clasificadas como homicidios, y hay que agregar las familias que se quedaron sin sus seres amados.

¿Cuál es la importancia de tener presente lo sucedido en el 11-M? Recordar que todos estamos expuestos a un ataque contra nuestra persona, que como expertos en seguridad, la prevención, la capacitación y la búsqueda de más herramientas tecnológicas y estratégicas, ayuden a mitigar y evitar estas tragedias.

"Hoy por hoy, nos queda muy claro que todos estamos expuestos a algún ataque. Estamos muy vulnerables porque vivimos en una sociedad en la que la violencia se ha normalizado, se ha perdido esa sensibilización a la vida humana, hasta a la vida animal, y tenemos que replantearnos muchas cosas, la educación en la escuela, en las casas. Hay factores geopolíticos que pueden influir en la conducta de la persona y que se puede convertir en terrorismo, en una persona que atenta contra terceros, no importa la razón; hoy por hoy no estamos exentos de nada", señaló el entrevistado.

Las redes sociales además de sus funciones del círculo social, son una herramienta poderosa para detectar posibles actores y terroristas. De acuerdo con nuestro experto, el terrorismo sí se puede prevenir, porque lo que hace falta es la labor de inteligencia y contrainteligencia. "Un acto terrorista no es espontáneo, lleva toda una planeación, y algunos de ellos se pueden detener, de ahí la importancia de estar siempre alerta, monitorear las redes sociales, tener inteligencia y contravigilancia, sólo así algunos de ellos serán identificados y evitados", finalizó. ■

Referencias:

[1] *"Nuevo informe detalla el aumento mortal de sobredosis con fentanilo en EE.UU" CNN en ESPAÑOL. Deidre McPhillips. 03/05/2023*

[2] *https://cnnespanol.cnn.com/2023/05/03/informe-aumento-mortal-sobredosis-fentanilo-eeuu-trax/*

FACEit

PLATAFORMA TECNOLOGÍCA EN LA NUBE
PARA COMPAÑÍAS DE SEGURIDAD

GRUPO SALUS
SEGURIDAD Y BIENESTAR

FACEit es un poderoso software para dirigir y controlar la operación de su empresa beneficiando todas las áreas como:

- "**Supervisión** en tiempo real de las operaciones de seguridad."
- "**Optimización** en la gestión del personal de seguridad."
- "**Generación** de informes detallados en cuestión de minutos."
- "**Aumento** en la eficiencia."
- "**Y ahorros de tiempo** con el uso del software."

SOLUCIONES SIMPLES A PROBLEMAS COMPLEJOS

Conoce nuestros servicios en nuestro sitio web www.gruposalus.com.mx

Tel. +52 55 2560 7642

WWW

WWW.GRUPOSALUS.COM.MX/FACEIT

CONTÁCTANOS
Y SOLICITA TU DEMO

SEGURIDAD PERSONAL EN ÁREAS DE ALTO RIESGO (PARTE II)

Consejos para no ser víctimas de la violencia urbana

Fotos: FreePick

GUATEMALA | **Enrique Jiménez Soza**

Nada está garantizado en un 100% cuando se trata de seguridad: 90% prevención, 5% reacción y 5% suerte. La prevención representa un 90% en seguridad, por eso las acciones se deben concentrar en esta etapa.

MEDIDAS DE SEGURIDAD EN EL ESTACIONAMIENTO

Dejar el auto en la calle siempre es peligroso, por lo que se aconseja que deje su vehículo en los estacionamientos. Y tome en cuenta las siguientes recomendaciones:

- Planifique el horario de llegada y de salida. Después decida dónde va a dejar el auto. Muchas veces usted llega cuando es de día y hay bastante movimiento en la calle, pero cuando vuelve al automóvil, la calle está desierta y oscura.
- Si desconfía de algo o de alguien, pase de largo por su auto y reevalúe la situación. Ante cualquier duda, llame a la policía (911).
- Saque siempre la llave de contacto, aún cuando esté detenido sólo algunos instantes.
- No deje las llaves de su casa dentro del vehículo. Las pueden usar después para asaltar su casa, sobre todo si el auto tiene calcomanías, facturas o cualquier otra cosa que identifique su dirección.
- Nunca permanezca dentro del auto estacionado. Si usted lo hace se convierte en la víctima perfecta. No deje ningún objeto dentro del auto; ponga todo en el baúl.
- Si usted se estaciona siempre en la misma zona y le robaron la tapa del tanque de nafta, cambie todas las llaves de su auto. Hay delincuentes que roban la tapa para hacer copias de las llaves.
- Antes de estacionar (o cuando vuelva) mire a su alrededor para ver si hay una persona o una situación sospechosa.
- Si al volver a su auto usted observa un desperfecto que impide poner en marcha el motor, llame de inmediato a algún contacto de confianza. Alguien pudo haber provocado el desperfecto para simular ayudarlo.
- Si hay personas sospechosas a su alrededor, hay poco movimiento o es de noche, no permanezca cerca de su auto.
- Si ve a alguien abriendo su auto, nunca se acerque. Busque ayuda sin que lo noten y recuerde: nunca cierre el espacio entre usted y el delincuente.

CUANDO MANEJA

No coloque en su auto calcomanías que permitan identificar dónde vive, dónde trabaja, qué lugares frecuenta, a qué universidad concurre. Esto se puede usar contra su persona.

Mantenga los vidrios siempre cerrados, o muy poco abiertos para permitir solamente la entrada de aire. Las puertas deben estar siempre trabadas. Si viaja en taxi, pida al conductor que trabe las puertas y cierre los vidrios.

Fotos: FreePick

Si observa por el espejo retrovisor que las personas del auto de atrás tienen aspecto sospechoso, no se detenga; diríjase a un lugar concurrido, preferiblemente donde haya policías o personal de seguridad, y si la intención era asaltarlo, esas personas no lo seguirán.

Si esto ocurre de noche o en lugares desiertos "nunca" se detenga, aunque no desconfíe de los ocupantes de otro auto.

Si se pincha un neumático de noche, o en lugares poco transitados, no pare. Conduzca hasta un puesto o un lugar concurrido, es preferible sufrir desperfectos en el vehículo antes que correr el riesgo de ser asaltado.

Los abordajes a un vehículo sólo son posibles si el vehículo está detenido, ya que un delincuente nunca trata de abordar un auto en movimiento; por eso es imprescindible que, en todo lo posible, evite detenerse. Estando parado, usted se vuelve un blanco muy fácil.

Por más inhumano que parezca, no se detenga para ayudar a alguien de noche o en lugares poco concurridos es preferible que llame por teléfono a la policía (911) y dé los datos sobre el lugar donde está la persona que necesita ayuda. No deje de ayudar, pero no se detenga. Los delincuentes utilizan mujeres y niños para hacer emboscadas.

Se recomienda que al abordar el vehículo, primero se ponga en marcha, trabe la puerta y parta inmediatamente, posteriormente podrá colocarse el cinturón de seguridad, encender la radio, acomodar objetos, etc. Esto se sugiere en ese orden ya que cuanto más tiempo permanezca detenido, mayor será el riesgo de un abordaje.

El delincuente no quiere tener sorpresas desagradables por lo que, en general, elige los blancos más fáciles; y dado que los vidrios polarizados se prestan a la incertidumbre, el uso de éstos puede inhibir la acción de los asaltantes.

Si usted piensa que lo está siguiendo otro vehículo no altere su forma de manejar, mejor diríjase a un puesto policial o un lugar concurrido, donde haya personal de seguridad o policías. Nunca detenga el vehículo ni trate de protegerse en estaciones de servicio, porque éstas son poco concurridas y los delincuentes las conocen bien. Al llegar a su casa, antes de detener el auto, observe la calle, lugares donde se puedan esconder personas, árboles cercanos, etc. Si nota la presencia de alguien sospechoso, no se detenga.

Evite las rutinas. Procure diversificar sus caminos, y si es posible, sus horarios de salida y de llegada. No descuide el mantenimiento de su vehículo. Mantenga en condiciones los neumáticos, los faros, el sistema eléctrico, las trabas, el motor, la batería, etc. Esto evitará fallas que le obliguen a detener el vehículo. Si ocurre esto y no puede evitar detenerse, trate de resolver el problema lo más rápido posible y salir del lugar peligroso. Tenga siempre a mano los teléfonos de remolques. El celular es una herramienta sumamente útil. Tenga uno y asegúrese de que funcione sin dificultades.

Si se pincha un neumático de noche, o en lugares poco transitados, no pare. Conduzca hasta un puesto o un lugar concurrido, es preferible sufrir desperfectos en el vehículo antes que correr el riesgo de ser asaltado

Si usted está manejando y cae algo líquido sobre el parabrisas no conecte los limpiaparabrisas. Se sabe que hay un tipo de resina que al volcarse sobre un vidrio y extenderse con los limpiaparabrisas forman una película opaca que obliga al conductor a detenerse.

Cuando desciende del auto lo abordan los delincuentes que están esperando más adelante. De la misma forma no detenga su vehículo si es alcanzado por piedras o cualquier otro objeto.

ASALTO EN EL AUTO

Si alguien lo aborda proceda de la siguiente forma:

1) **Tenga calma y pida calma:** mantenga la calma y pida al delincuente que mantenga la calma. Hágale sentir que él es el que tiene el control de la situación. Un delincuente con miedo puede reaccionar de forma impredecible.
2) **Obedezca rápidamente:** obedezca las órdenes del asaltante y trate de cumplirlas con calma, pero con rapidez.
3) **Informe lo que va a hacer:** mantenga las manos donde el asaltante pueda verlas (en el volante). Si tiene que tomar objetos, soltar el cinturón de seguridad o abrir la puerta, informe al agresor y haga movimientos suaves. Recuerde que el asaltante está nervioso y movimientos rápidos o bruscos pueden alterar la situación.
4) **Si tiene que salir del auto hágalo en la forma correcta:**

- La forma equivocada es cuando, al bajar del auto, la persona queda entre la puerta y el delincuente. Como éste tiene apuro por abandonar el lugar, puede empujarla hacia adentro y terminar llevándosela junto con él.
- La forma correcta y segura para la víctima sería que al bajar del vehículo, la persona se aparta del delincuente, dejándole la entrada libre. Como el delincuente tiene apuro, no va a tratar de arrastrar a la persona hacia adentro, sino que va a entrar al auto para abandonar el lugar cuanto antes. ■

Enrique Jiménez Soza, asesor profesional de seguridad. *Más sobre el autor:*

CÁRCELES EN LATINOAMÉRICA (PARTE I)

Crisis, exigencias y retos

Fotos: FreePick

ESPAÑA

Manuel Sánchez Gómez-Merelo

El sistema penitenciario está en crisis en toda Latinoamérica con mayores o menores niveles de gravedad pero, en cualquier caso, con un deterioro creciente por el reducido espacio físico, el incremento de la población carcelaria y la obsolescencia del sistema.

Esta situación de inseguridad revoluciona Latinoamérica y no tiende a mejorar en casi ningún país dada la reducida inversión pública y las casi nulas políticas de reinserción para los reclusos. Se mira para otro lado y se asume, con un alto coste, los siniestros provocados por esas difíciles e insalubres condiciones de vida, que conducen inevitablemente al deterioro de la convivencia, la violencia, la propia corrupción funcionarial y la frustración de la sociedad.

LAS CÁRCELES ESTÁN SATURADAS

Periódicamente, la ONU denuncia la sobrepoblación en las cárceles latinoamericanas y alerta de la grave situación. La crisis en las cárceles es estructural. Son una muestra de la impunidad, corrupción e ineficiencia del sistema penitenciario, incluso del judicial.

En general, todo el sistema penitenciario de la región vive en el omnipresente problema del hacinamiento y el de la falta de inversión, que facilita la presencia de organizaciones criminales que imponen su ley en cárceles deterioradas, insalubres y con funcionarios frecuentemente corruptos.

En la actualidad, de media, las cárceles albergan casi 40 por ciento más de reclusos de lo que deberían y, en muchos casos, se llega hasta el 300 por ciento, lo que facilita las tragedias acaecidas y pronostica otras, difíciles de evitar si no se aborda seriamente la problemática largamente denunciada.

Desde México a Argentina, el hacinamiento, que acaba desembocado en motines e importantes conflictos, es moneda de cambio en todo el continente. La situación en los penales es gravísima pues, buena parte de los establecimientos penitenciarios existentes, vienen del siglo pasado.

Cada país tiene sus particularidades pero, a las pésimas condiciones de vida, hay que sumar el abuso de la detención preventiva, la falta de salubridad y atención médica, la insuficiente alimentación, la ausencia de políticas de rehabilitación y de reinserción, la corrupción y los escasos e inadecuados recursos humanos.

Las condiciones de hacinamiento en las que se encuentran las cárceles latinoamericanas propician el que se sigan reproduciendo organizaciones delictivas en el interior, que se produzcan conflictos entre bandas rivales, que haya mafias y jerarquías entre los presos, sumado a la carencia de espacios adecuados para albergar a aquellos de mayor peligrosidad.

Así, el hacinamiento, las peleas entre bandas, la corrupción, los motines, fugas, etc. han dado lugar a la terrible cifra de más de dos mil internos muertos en siniestros ocurridos en las cárceles de Latinoamérica en los últimos dos años.

DELINCUENCIA Y CORRUPCIÓN

El descuido y abandono en las cárceles fomenta la inseguridad en toda Latinoamérica. Las carencias de personal, tecnología y obsoleta arquitectura facilitan la acción de criminales y mafias.

Si para nadie es desconocida la crisis carcelaria de Latinoamérica, tampoco lo es su vínculo con los más de 40 años de guerra contra el narcotráfico. En este sentido, el creciente número de presos es directamente proporcional al peso que se asigna al combate contra las drogas.

Pero, hay más, dentro de los propios centros penitenciarios, existen: extorsiones, corrupción, prostitución, drogas, mercados ilegales, mafias, intimidación, sicarios, robos, asesinatos, secuestros e intimidación, porque se han convertido en lugares en los que los cárteles de la droga y las bandas criminales realizan grandes negocios y delinquen con muy pocos límites, tanto fuera como dentro de los centros penitenciarios.

El narcotráfico en toda la región ha llenado las cárceles en las últimas tres décadas, convirtiendo al hacinamiento y a la violencia en un mal menor y común de las cárceles de Latinoamérica, según confirman también muchos analistas.

La corrupción en las cárceles latinoamericanas es deplorable y grave. La Comisión Interamericana de Derechos Humanos critica el deterioro y abandono de los centros penitenciarios, y señala que, en muchos casos, la corrupción permite que los funcionarios dejen entrar habitualmente en los propios recintos armas, drogas y teléfonos móviles. Así, el crimen organizado controla y se encuentra permanentemente conectado con el exterior, donde continúan sus actividades delictivas.

Fotos: FreePick

DERECHOS HUMANOS

La situación actual presenta un negro panorama en las cárceles latinoamericanas, según la organización Human Rights Watch (HRW) que recientemente señaló que, en la actualidad, hay un problema generalizado de abandono, brutalidad policial y hacinamiento carcelario, según el informe anual presentado en Washington, Estados Unidos.

El incremento de la población penal, la falta de presupuesto o la mala administración, entre otros aspectos, ha desembocado en que el sistema penitenciario en Latinoamérica sea un sistema fallido o descontrolado.

Los protocolos de emergencia en las cárceles son problema común para los gobiernos latinoamericanos, y se han institucionalizado como verdaderos sistemas del delito controlados por los propios internos.

Actualmente, existen desafíos importantes en los sistemas penitenciarios de Latinoamérica, desde el planteamiento de nuevas normativas y estructuras organizacionales hasta las propias condiciones de vida dentro de las prisiones, lo que hace necesario atender un gran número de factores para garantizar los derechos humanos de las personas privadas de libertad.

Por otro lado, carecen de soluciones alternas al encarcelamiento, como la libertad vigilada para autores de delitos menos graves o no violentos, trabajos comunitarios o la disposición de brazaletes electrónicos de control.

Con todo ello, la realidad es que en Latinoamérica los detenidos no van a la cárcel sino al infierno, a esos recintos hacinados y obsoletos donde se juntan los delincuentes confesos con los que cumplen su aún inexistente condena en régimen preventivo, además de las víctimas de la obsoleta legislación, que hace que todas las leyes deriven en el derecho penal, criminalizando conductas que no revisten auténtica gravedad.

CLASIFICACIÓN Y TRATAMIENTO

La base del sistema y ordenamiento penitenciario se fundamenta en la clasificación y tratamiento de los internos con los siguientes principios generales:

- Intervención de equipos multidisciplinarios, que atiendan las diferentes variables desencadenantes de la conducta desadaptada.
- Intervención continua y programada que establezca las fases y pautas de cambios de conducta individual y su evolución.
- Diseño de programas formativos orientados a desarrollar las aptitudes de los internos, enriquecer sus conocimientos y mejorar sus capacidades técnicas o profesionales.
- Potenciar y facilitar los contactos del interno con el exterior colaborando con los recursos de la comunidad como instrumentos fundamentales en los programas de reinserción.

Igualmente y como objetivos específicos del tratamiento podríamos señalar los siguientes:

- Garantía del sistema en el cumplimiento de la pena respetando los derechos y haciéndoles cumplir sus deberes.
- Disminución de la conflictividad interna (seguridad y disciplina) a través de la clasificación y separación entre módulos para lograr una convivencia ordenada y segura.

Fotos: FreePick

Uno de los factores que impide la reinserción real de los penados es la falta de oportunidades y los escasos programas que existen para la rehabilitación social

- Ocupación de los internos la mayor parte del tiempo posible a través de asistencia a cursos, talleres, deportes y otras actividades de tipo recreativo y cultural.
- Formación académica con el desarrollo de programas básicos y de especialización de educación.
- Formación laboral con el desarrollo de programas y establecimiento de talleres de trabajo ocupacional, incluso remunerado.
- Creación y mantenimiento de hábitos de autocuidado, conservación y mantenimiento de las dependencias y sus instalaciones.

REINSERCIÓN Y RESOCIALIZACIÓN

Uno de los factores que impide la reinserción real de los penados es la falta de oportunidades y los escasos programas que existen para la rehabilitación social. Hay que considerar que muchos internos no tienen la educación básica ni media completa, por lo que establecer convenios con instituciones públicas y/o privadas para propiciar la educación, o que se les propicie algún oficio o especialización es de vital importancia.

Las experiencias con internos que han culminado sus estudios en la cárcel son muy positivas aunque, lamentablemente, en Latinoamérica, lo son con porcentajes bastante bajos.

Las instalaciones penitenciarias en Latinoamérica están lejos de lograr la reinserción y resocialización de los penados, pues en la región sólo se atiende la coyuntura urgente, es decir, se gestionan los problemas e incidentes que ya son graves en lugar de resolverlos cuando apuntan a un deterioro evitable y a un necesario cambio del sistema.

Por otro lado, llama la atención la falta no sólo de recursos e inversión, sino también de personal, además de su escasa cualificación para hacerse cargo del tratamiento de los reclusos o tener capacidad de reacción cuando se desatan los incidentes y, sobre todo, en caso de especial gravedad.

En varios países latinoamericanos se está formando y capacitando más al personal de centros penitenciarios, pero también hay que aumentarles los salarios y valorar el hecho de que su profesionalidad redundará en la mejora de un servicio social muy importante.

La cultura de prevención, así como la implementación de nuevos programas de reinserción en los penales son temas prioritarios y debe de ser tarea y responsabilidad de todas las partes implicadas. ■

Manuel Sánchez Gómez-Merelo, consultor internacional de Seguridad y ex-coordinador de Seguridad en Instituciones Penitenciarias.
Más sobre el autor:

Las instalaciones penitenciarias en Latinoamérica están lejos de lograr la reinserción y resocialización de los penados, pues en la región sólo se atiende la coyuntura urgente

Fotos: FreePick

México – Jordania – Serbia – Israel – Italia – Rusia – Colombia - Venezuela

La capacitación que marca la diferencia

GRUPO CIPI®

CURSOS:

- *Protección a funcionarios 360°*
- *Medicina táctica*
- *Manejo táctico antisecuestro*
- *Manejo de armas y defensa personal*
- *High level protection*
- *Inteligencia contra inteligencia antisecuestro*
- *Protección ejecutiva antisecuestro*
- *Blindajes / seguridad privada*

DIPLOMADOS:

- *Gestión integral de riesgos (protección civil)*
- *Protección Ejecutiva*
- *Seguridad Privada*
- *Seguridad Pública*

56 1181 7875 *56 1264 3517*

cipi@consultoresenproteccion.com

ISO 17024:2012 ISO 9001:2015 ISO 18788:2015 redconocer

ADULTOS MAYORES CON PROBLEMAS DE DEMENCIA SENIL O ALZHEIMER SON MÁS DIFÍCILES DE LOCALIZAR

Desde el año 2010, desaparecieron en nuestro país diez mil personas mayores de 65 años. La gran mayoría tienen enfermedades neurodegenerativas

Fotos: FreePick

MÉXICO

Ricardo Nava Rueda

Un adulto mayor con problemas de salud mental, demencia senil o Alzheimer son muy difíciles de localizar cuando se llegan a extraviar, al igual que otras personas con discapacidad mental.

El primer problema al que se pudieran enfrentar es un accidente, pues ellos van caminando por la calle sin saber qué es lo que pasa y están distraídos.

El segundo problema que se presenta, es sí van a ser "atrapados" o caerán en situación de calle, ya que pueden pasar días, semanas, meses o hasta años y su vestimenta o aspecto es muy diferente de cuando se extraviaron, incluso para las autoridades y familiares será bastante complicado reconocerles.

Sumado a lo anterior, también pueden ser captados para trata de personas en particular para explotación laboral, ya que en principio será muy fácil dominarles y también para el ciudadano les preocupará (por su aspecto, estado o condición) el darles dinero o alimentos, que sólo serán para quienes les exploten.

En tema de prevención es ya no dejarles solos o salir a la calle. Avisar a los vecinos y personas cercanas que el familiar padece un trastorno, que aparentemente no se puede notar.

También una propuesta particular es poner un tatuaje pequeño con su nombre completo, me han preguntado si es conveniente la ropa bordada con su nombre, lo considero que al paso del tiempo ya tendrán otra que alguna persona les pueda regalar, de igual manera me preguntan por una placa con su nombre de la persona, vamos a pensar que caiga en manos de un explotador y será lo primero que le quite o sirva para cometer una extorsión.

Una propuesta en 2002 de su servidor a la PGR (Procuraduría General de la República de México), entre otras, es que se lleve un censo con fotos de personas en situación de calle, en este 2023 puede ser más fácil con la tecnología (biometría), con la seguridad que muchos están en proceso de búsqueda y localización, simplemente en la Ciudad de México se calculan siete mil personas en situación de calle.

Nombraré ejemplos de lo varios casos que me han tocado:

CASO 1

El Sr. Guillermo se perdió tres veces, la segunda vez caminó desde el metro San Cosme hasta Plaza Galerías, unos dos kilómetros, ahí retuvo un policía, le preguntó que a dónde iba, le dijo: "a Xochimilco", cuando él vive en Azcapotzalco. De acuerdo con su familia, tiene Alzheimer.

OFRECEMOS SOLUCIONES EN LA CADENA LOGÍSTICA CON UN ENFOQUE EN LA SEGURIDAD PRIVADA, CREANDO ESTRATEGIAS PARA PROTEGER LOS BIENES DE CADA UNO DE NUESTROS CLIENTES.

SEGURIDAD EN
LA CADENA LOGÍSTICA

CORPORATIVO EN SEGURIDAD

ALFIL

ADMINISTRADORES EN SERVICIOS
INTEGRALES DE SEGURIDAD, S.A. DE C.V.
SEGURIDAD PRIVADA

Custodia de mercancías, bienes y/o valores:

- Patrullas y/o Motos con sistema GPS
- Custodia civil o armada
- Sistema de video a bordo
- Tripulación de 2 elementos
- Sistema de comunicación seguro
- Flota con modelos recientes 2021a 2023
- Monitoreo dedicado y activo 24/7
- Candados de seguridad
- Candados GPS

- Consultoría especializadas.
- Escolta ejecutiva.
- Sistemas integrales GPS.
- Aplicaciones de seguridad.
- Análisis de riesgo.

Monitoreo Logístico, prevención, control de pérdidas e investigaciones.

Protegemos con estrategia e inteligencia



Equipo Centurión

Acciones
Seguimiento
Reducción de costos

CERTIFICACIONES

ISO 9001-2015 EMPRESA CERTIFICADA

CERTIFIED ISO 28000

Alce Blanco 55 Fracc. Industrial Alce Blanco, Naucalpan de Juárez, 53370. Estado de México

www.corporativoenseguridadalfil.com

informes@corporativoenseguridadalfil.com

Tel. 55 53 58 97 59

SOCIO

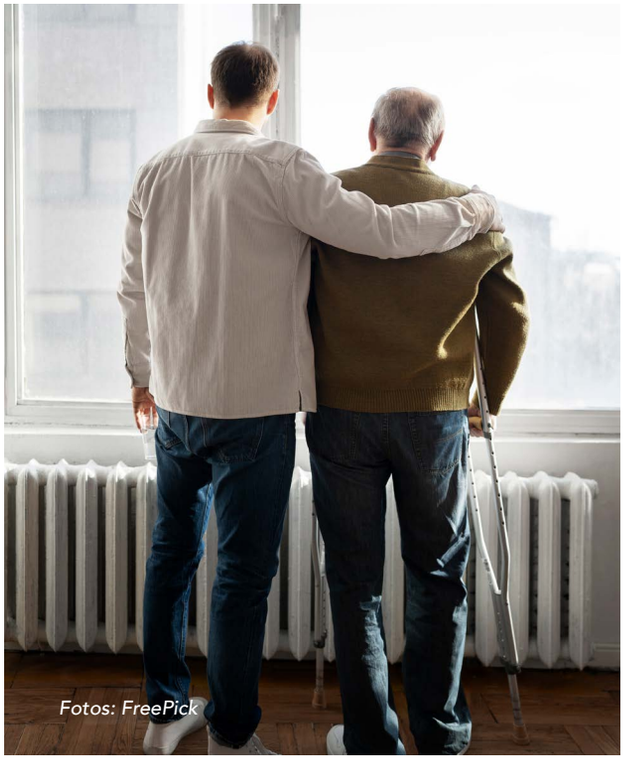
ASIS INTERNATIONAL CAPÍTULO MÉXICO 217

9mesis

FEPASEP Federación Panamericana de Seguridad Privada

TSR Certified TAPA Transported Asset Protection Association

CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C. CNSP EMPRESAS DE CALIDAD



Fotos: FreePick

En tema de prevención es ya no dejarles solos o salir a la calle. Avisar a los vecinos y personas cercanas que el familiar padece un trastorno, que aparentemente no se puede notar

CASO 2

La Sra. Cristina era mamá de un amigo, los dos ya fallecieron. Cristina siempre estaba afuera de su casa, como a ocho metros siempre que veía a alguien nos decía: "me voy contigo", yo le decía "si Cristi, ahora regreso por ti", varias veces le dije a su hijo Horacio: "Un día se va a perder tu mamá", pero siempre me contestaba: "no, sólo sale a la esquina y se regresa". En una ocasión Horacio nos fue a buscar a mi pareja y a mí, muy espantado: "Lupita, Ricardo, no encuentro a mi mamá, dicen que iba del brazo de una muchacha".

Entre los vecinos nos organizamos para la búsqueda, unos vecinos nos refieren que la vieron que entraba a una unidad habitacional, de clase alta, el jefe de vigilancia nos dijo que sí llegó acompañada de una mujer a la que sólo la conocían como "la colombiana", pero que no les dejó entrar por instrucciones del dueño del departamento. Como no me dejó ver los videos, hicimos presión con los vecinos y policía, el jefe de vigilancia nos pidió unos minutos, como a los 30 minutos bajó con Cristina, ella muy alterada, pero se la regresaron a su hijo, había una denuncia por privación ilegal de la libertad, pero le voltearon a su hijo la denuncia por omisión de cuidados. Cristina, con Alzheimer.

CASO 3

"Lalito" salió de su casa en Xochimilco, Ciudad de México, se le ubica a casi tres semanas de extraviado, se le vio por Ecatepec, Estado de México, y finalmente lo encontramos en Av. México-Tacuba, no habla nada, él padece autismo.

CASO 4

Un viernes por la noche me pidieron apoyo para buscar a un adulto mayor de 80 años, venía la familia de Mexicali, Baja California, me refirió su yerno que al mediodía fue de compras con su hija y nieta a Plaza Antara, CDMX, en un momento su hija y nieta entraron a comprar ropa y él les dijo que las esperaba afuera, lo perdieron de vista y preocupadas pidieron los videos y se ve que le da dos vueltas al centro comercial.

Al acompañar a su yerno a la Fiscalía Especializada en la Búsqueda, Localización e Investigación de Personas Desaparecidas (FIPEDE) le pregunté si su suegro padece Alzheimer u otro problema, me dijo que no, pero me comentó que tenía un mes de haber enviudado, reflexionó a mi pregunta y me dice: "fíjate que ayer después de comer se durmió un rato y después se alteró, preguntó que dónde estaba, cuando ya varias veces habían llegado a su departamento de Polanco".

Al día siguiente lo encontramos en el Parque Lincoln, los policías que tuvieron contacto con él le preguntaron si estaba bien, les contestó que sí, que estaba esperando a su hija y nieta que fueron a comprar, ya habían pasado casi 24 otras.

CASO 5

Este adolescente se salió de su casa, ya que su abuela dijo que lo regañó y que el chico se espantó, esto fue un lunes, y el miércoles siguiente me llamaron para pedir apoyo para buscarlo por parte de la Policía Escolar, el jueves empezamos la búsqueda, él se perdió en Iztapalapa, CDMX. Ubicamos un sitio donde había pernoctado en Tlalpan y finalmente lo localizamos en Coyoacán (por Ciudad Universitaria), él estaba muy combativo, pues no había tomado sus medicamentos en tres días, lo canalizamos al psiquiátrico.

Su problema es esquizofrenia, de acuerdo con su abuela.

CASO 6

El Sr. Gerardo salió de su casa y, de acuerdo con su esposa, tiene demencia senil, pero que iba y regresaba a casa. Un día no regresó, lo seguimos buscando, lo más seguro es que esté en situación de calle.

Y como estos casos, desafortunadamente hay muchos. Cuidemos a nuestros adultos mayores, ellos nos necesitan. ■

Ricardo Nava Rueda, *"Lost Boy"*, director de Difusión y Relaciones Públicas de la Asociación Mexicana de Niños Robados y Desaparecidos, A.C. y líder del proyecto Encuéntrame de Seguridad por México (Iniciativa Chapultepec, A.C.). *Más sobre el autor:*

5 razones para *afiliarme*

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

1 MÁS DE 25 AÑOS DE TRABAJO

ASIS CAPÍTULO MÉXICO es el tercer capítulo más grande del mundo, agrupa a más de 350 profesionales de la seguridad en México.

2 NETWORKING

Nuestra membresía está conformada por directores de seguridad de empresas privadas, consultores, CEO´s usuarios finales del sector público y privado.

3 CRECIMIENTO PROFESIONAL

Obtén un asenso en tu carrera profesional a través de nuestros webinars, cursos, talleres, comunidades temáticas y bolsa de trabajo sin costo.

4 VÍNCULOS CON ASIS INTERNACIONAL

Obtén acceso exclusivo a las Guías & estándares de ASIS Internacional así como a la base de datos de más de 34 mil profesionales de seguridad alrededor del mundo.

5 REUNIONES MENSUALES

Este evento reúne a los Profesionales de la Seguridad para abordar temas relacionados con la seguridad, protección, management y liderazgo, así como intercambiar experiencia y establecer una red de networking.

Trabajando **juntos por ASIS, crearemos posibilidades infinitas** para cada miembro de nuestro Capítulo.

!Súmate!

Linktree

Todo lo que necesitas de ASIS a 1 clik de distancia.

#JuntosXASIS
#PosibilidadesInfinitas

MAYOR INFORMACIÓN:

55 3437 6890
55 1321 1289
55 1233 3446
55 3578 6160
info@asis.org.mx

CRIMINOLOGÍA DEL DESARROLLO: ESTUDIO DEL DESARROLLO EN LA FORMACIÓN DE LA CONDUCTA CRIMINAL

Cambios que se han producido durante los años en los individuos en cuanto a la conducta antisocial

Fotos: FreePick

MÉXICO

Wael Sarwat Hikal Carreón

LOS ESTUDIOSOS DESARROLLISTAS EN CRIMINOLOGÍA

Si se consultan los textos de Criminología, en general se podrá observar que este campo especializado tiene fuentes históricas; le antecede quienes trabajaron sobre el tema del desarrollo dirigido al estudio de la criminalidad, entre ellos: Lombroso, Ferri, Garófalo, Di Tullio, De Greeff, Pinatel, Freud, hasta los continuadores de estos, hoy también clásicos: Baratta, Ingenieros, Bernaldo De Quirós, Quiroz Cuarón, Solís Quiroga, Tieghi, Zaffaroni y Marchiori, Reyes Calderón, Reyes Echandía, Herrero Herrero. Lo esencial es mirar de vuelta al pasado los antecedentes previos a cometer su conducta antisocial, esto debe ser básico en la etiología del crimen (Criminología Etiológica-Multifactorial).

LOMBROSO Y LA OBSERVACIÓN ANTROPOLÓGICA DE LOS DELINCUENTES

Lombroso siendo médico italiano, es considerado innovador de los estudios ordenados de la Criminología. Investigó en numerosos militares, delincuentes de guerra y en cárceles, procuró investigar características antropométricas de los criminales, pensando haber encontrado el origen de la criminalidad analizando los cráneos de delincuentes, así como anomalías y deformaciones corporales, posteriormente se amplían los estudios a la influencia de los factores culturales, no sólo los físicos.

Indicaba que la criminalidad es un tipo de violencia extraña y patológica, reflexionando que el crimen es consecuencia de la interacción entre los factores biológicos, psicológicos y culturales. Considera al criminal un ser sin empatía, de personalidad descompuesta. Lombroso junto con Ferri y Garófalo, destacan también la importancia de estudiar las causas del delito durante el desarrollo del individuo y la interacción de diversos factores durante su vida.

Se destaca la importante de hacer las observaciones y clasificaciones de los delincuentes, en aquel entonces y en la actualidad, se clasificaba según el delito, pero también con sus rasgos físicos, culturales, además de los diagnósticos psicológicos y psiquiátricos. De tal manera, conoceremos sus antecedentes que lo llevaron a tal conducta, y estar en posición de reconstruir su vida orientándola a una recuperación sana.

DI TULLIO Y EL TRATAMIENTO BASADO EN LOS FACTORES DE RIESGO

Alumno de Lombroso, está otro médico, Di Tullio, quien vislumbra a la Criminología Clínica como "la ciencia de las conductas antisociales y criminales basada en la observación y el análisis profundo de casos individuales, sean estos normales, anormales o patológicos" (Pérez González, Rodríguez Jorge y Loy Vera, 2018, p. 13). Al hacer referencia a un examen a profundidad, involucra el investigar las causas lo más próximo a su totalidad; lo que implica un estudio penetrante, histórico y reconstructivo de la vida del individuo.

Todas las personas, en contextos particulares pueden llegar a cometer algún crimen, pues hay una lamentable tendencia en el desarrollo individual y cultural y a procesos de integración en la personalidad, con ciertas perturbaciones graves en la vida. Por tanto, es preciso realizar el estudio de un sujeto criminal en su personalidad global; es decir, investigando sus factores biopsicosociales (Pérez González, Rodríguez Jorge y Loy Vera, 2018).

Para Di Tullio, el tratamiento clínico debe basarse en el conocimiento integral de la personalidad del delincuente. Éste reconocía que transformarla es complejo, pero según el avance de la ciencia y los tratamientos, se podrá lograr. Sugería un tratamiento conformado por las áreas: psicológica, médica, psicológica, psiquiátrica,

ISIS®
SEGURIDAD INTEGRAL

Creamos entornos **seguros**

Servicios:

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

AFAC
AGENCIA FEDERAL DE AVIACIÓN CIVIL

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE
CERTIFICATION /CERTIFICACION Nº MEXGDL00175-1

CONSEJO NACIONAL CNSP SEGURIDAD PRIVADA A.C.
EMPRESAS DE CALIDAD

ASIS INTERNATIONAL

mesis®

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

pedagógica, de trabajo social y sociológico, lo cual implica tener una comprensión profunda del individuo.

Por otra parte, Di Tullio sería secretario general (1937-1949) de la Sociedad Internacional de Criminología durante el periodo de 1937 a 1949, ulteriormente fue presidente de 1949 a 1950 (International Society of Criminology, 2016).

INGENIEROS Y LA ETIOLOGÍA DEL CRIMEN

En Argentina, los trabajos de Ingenieros mediante la Psicología Clínica y la Criminología Clínica se crearon en el Instituto de Criminología de la Penitenciaria Nacional de Argentina. Con una óptica etiológica-criminal, éste indica que: "Todo acto delictuoso es la resultante de causas" y especifica la labor integradora criminológica en tres áreas:

1) **Etiología criminal.** Estudia las causas determinantes de los delitos. En lugar de presuponer el "libre albedrío" del delincuente, busca el "determinismo" de su acto antisocial: en su constitución orgánica y en las condiciones del ambiente en que vive.
2) **Clínica criminológica.** Estudia las múltiples formas en que se manifiestan los actos delictuosos y los caracteres fisiopsíquicos de los delincuentes. No trata de establecer la "responsabilidad" del delincuente, sino de fijar su grado de "temibilidad" según el peligro que pueda resultar de su convivencia en la sociedad.
3) **Terapéutica criminal.** Estudia las medidas, sociales o individualizadas, de profilaxis o de represión del delito; no trata de "castigar" al delincuente porque le supone libre de preferir el mal al bien, sino porque procura asegurar la "defensa social" contra su actividad morbosa, mediante instituciones preventivas y por la segregación en establecimientos apropiados a los diversos casos (Tieghi, 2004, p. 51).

Su trabajo lo realizó cuando ocupaba el cargo de jefe del Gabinete de Psicología Clínica Experimental y examinó a cada uno de los internos elaborando informes denominados: Boletín médico-psicológico, conformado por un estudio de la personalidad, examen somático y cultural. Ingenieros estudió las causas de la criminalidad y la influencia de los factores que determinan los crímenes, específicamente el estudio psicopatológico. Además agrupó las medidas de tratamiento:

a) **Medios preventivos:** enfocados a impedir los factores que pueden inducir la externalización de las predisposiciones criminales.
b) **Medios represivos:** donde sugiere penas versátiles para casos particulares, según las características criminales como edad, sexo, profesión, costumbres, etcétera (Marchiori, 2004).

A la tradición de Ingenieros le prolonga Loudet, médico y profesor de diversas instituciones de salud, sería también el fundador de la Sociedad Argentina de Criminología, consideraba al criminal como un enfermo; por ello, el estudio clínico sugería se hiciera con técnicas antropológicas y clínicas, para establecer en cada particular los factores endógenos y exógenos, además la técnica de la historia psiquiátrica para evaluar el grado de peligrosidad del delincuente a través del estudio de la personalidad (Ferro, Rodríguez Sturla y López, 2016). "El estudio del criminal patológico desde el aspecto biopsicológico y sociológico (factores endógenos y exógenos), conllevó al Dr. Loudet a describir el estado peligroso de los sujetos delincuentes desde un polimorfismo psicológico-social" (Ferro, Rodríguez Sturla y López, 2016, p. 26).

DE GREEFF Y LA PSICOLOGÍA CRIMINAL

De Greeff, es calificado como "padre de la Psicología Criminal", logrando la cualidad de haber aplicado la ciencia psiquiátrica al entendimiento de la mente criminal, sintetizando los estudios biológicos, sociológicos y patológicos. Razonó fundamental el estudio de la personalidad que lleva al conocimiento de la variedad de factores de riesgo y la dinámica entre estos para la conducta criminal, ya que ésta es consecuencia de la interacción biopsicosocial (Pauwels y Verhage, 2019).

Es menester comprender al sujeto en su integridad. Indicó que hay que conocer al delincuente en relación a su pasado y vinculándolo con el momento actual. De Greeff considera obligadamente necesario para el diagnóstico de personalidad los rasgos de egocentrismo, agresividad e indiferencia afectiva (Landecho Velasco, 1967).

De Greeff fue el cofundador de la escuela de Criminología en Bélgica, ulteriormente cofundó la Sociedad Internacional de Criminología, misma que otorga un premio que lleva su nombre: "Etienne De Greeff." (International Society of Criminology, 2016). Además de haber sido profesor de Pinatel, quien trabajó en los estudios clínicos y fenomenológicos de la criminalidad (Pauwels y Verhage, 2019). También De Greeff fungió como primer presidente de la comisión científica de 1949 a 1950 (International Society of Criminology, 2016).

PINATEL, LOS NIVELES DE OBSERVACIÓN Y LOS COMPONENTES DE LA PERSONALIDAD ANTISOCIAL

Pinatel considera que la etiología criminal consiste en un saber integral que conduce a realizar el tratamiento de los delincuentes y articular las herramientas para los programas de prevención de la criminalidad. Llegar a ese conocimiento sería a través de la investigación, análisis y tratamiento del delincuente, esta para Pinatel es un concepto toral, un instrumento clínico, que permite conocer el grado de peligrosidad y evaluar los efectos del tratamiento (Beristain Ipiña, 1999).

Señalaba que el fenómeno criminal se puede estudiar en tres niveles de interpretación o niveles de observación: individual, conductual y general, en el cual se emplean diversas disciplinas para obtener un conocimiento holístico del problema criminal (Tieghi, 2004).

Utilizó y popularizó el término de personalidad criminal, la cual se puede tomar de modelo, paradigma o esquema bajo el análisis de cuatro variables: la agresividad, la labilidad, la indiferencia afectiva y el egocentrismo del delincuente (Beristain Ipiña, 1999).

Pinatel además de ser cofundador (junto con Di-Tullio) de la Sociedad Internacional de Criminología, desempeñó el cargo de secretario general, en los períodos de 1950 a 1956 y 1956 a 1966, esta última en la presidencia de Sellin. Consecutivamente fue presidente de la misma por dos períodos, de 1971 a 1978 (Beristain Ipiña, 1999). En 1975 fue premiado con la

SOLUCIONES ESTRATÉGICAS

RE & MI
S.A. DE C.V.

SEGURIDAD PRIVADA

BOTAS PARA
GUARDIAS DE SEGURIDAD

Resistentes ***al agua***

Calidad

Alta ***tecnología***

Potros BOOTS

Informes al teléfono:

55 72 58 92 26

Fotos: FreePick

medalla: "César Beccaria", concedida por la Sociedad Alemana de Criminología (Kriminologische Gesellschaft, 2016). El Instituto Vasco de Criminología de la Universidad del País Vasco otorga el Premio de Investigación Jean Pinatel (Instituto Vasco de Criminología, 2016).

QUIROZ CUARÓN Y LA CLÍNICA CRIMINOLÓGICA

Quiroz Cuarón sugería que la Criminología puede tomar de la Medicina técnicas para observar, diagnosticar, pronosticar y tratar las enfermedades, vendría a ser una Criminología Médica. El ser humano es el sujeto de estudio de la Criminología Clínica y de este mismo nace la Antropología Criminal como un ser físico y cultural, la Sociología Criminal como ente que se desenvuelve en sociedad, de la Psicología Criminal al tener interacción lo interno mental con lo externo social y físico, etcétera, esto requiere un trabajo minucioso en las observaciones clínico-criminales.

Quiroz Cuarón se enfoca en cuatro rasgos patológicos de las personalidades psicopáticas: la irritabilidad, que ante estímulos mínimos la ira explota de manera no proporcional, la emotividad, que sería una reacción exagerada por la débil capacidad de autocontrol, la impulsividad, siendo espontánea e inesperada, y la inmoralidad, como estímulo prepotente y egoísta, sin control. "(...) también se deberían buscar las causas que habían influido para que se cometiera un acto antisocial, tipificado en la ley penal o no, además debería estudiar la personalidad antisocial, buscar sus componentes así como establecer su relación con otros trastornos mentales" (Varela Macedo, 2014, p. 1353).

Quiroz Cuarón estableció tres talantes esenciales en la práctica clínica:

1) La investigación clínica.
2) El establecimiento de un departamento de clínica criminológica en el sistema penitenciario, con enfoque interdisciplinario para el estudio del delincuente y establecimiento de su tratamiento.
3) La enseñanza universitaria de la Criminología (Varela Macedo, 2014).

HURWITZ Y LOS FACTORES CRIMINÓGENOS INDIVIDUALES Y SOCIALES

Para Hurwitz, la Criminología es el estudio positivo de los factores criminógenos individuales y sociales sobre los que se produce la conducta antisocial. La Criminología se sitúa preponderantemente hacia la etiología del crimen.

Hurwitz ejecutó un profundo análisis de bases biológicas de la conducta criminal, de los factores hereditarios en familias con antecedentes criminales y ahonda en la importancia de los factores psicológicos de la criminalidad refiriendo las distintas alteraciones mentales incumbidas con el crimen (Redondo Illescas y Pueyo, 2007).

También punteó que para el tratamiento hay que considerar ciertas fases del delito y del delincuente; por decir, la fase predelictiva, el delito y la fase postdelictiva; es decir, conocer los factores que han intervenido durante el desarrollo de cada una de las fases (Mejía A., 1966), nuevamente conocer los factores endógenos y exógenos. Hurwitz estuvo en la Comisión de las Naciones Unidas sobre crímenes de guerra en 1945 (The New York Times, 2016). ■

Referencias:

- *Beristain Ipiña, A. (1999). Jean Pinatel, criminólogo transnacional y hombre bueno. Eguzkilore, 13, 209-218. https://www.ehu.eus/documents/1736829/3343253/Eguzkilore+13-16.+Beristain.pdf*
- *Ferro, C.M., Rodríguez Sturla, P. y López, G. (2016). El Dr. Osvaldo Loudet y el análisis de la peligrosidad delictiva a través de casos clínicos. VIII Congreso Internacional de Investigación y Práctica Profesional en Psicología. Universidad de Buenos Aires. https://www.aacademica.org/000-044/125.pdf*
- *Instituto Vasco de Criminología (2016). X Premio de investigación Jean Pinatel. http://www.ehu.eus/es/web/ivac/jean-pinatel-saria*
- *International Society of Criminology (2016). Officers of the International Society of Criminology. International Society of Criminology. https://intercrim.com/former-presidents*
- *Kriminologische Gesellschaft (2016). Beccaria-Medaille. http://www.krimg.de/drupal/node/5*
- *Landecho Velasco, C.M. (1967). Apuntes de Clínica Criminológica. Instituto de Criminología y Universidad de Madrid.*
- *Marchiori, H. (2004). Criminología. Teorías y Pensamientos. Editorial Porrúa.*
- *Pauwels, L. y Verhage, A. (2019). Criminology in Belgium: from embryonic conception to contemporary currents in a nutshell: some food for thought. Criminology in Europe. https://biblio.ugent.be/publication/8661337/file/8661338*
- *Pérez González, E., Rodríguez Jorge, R.R. y Loy Vera, B. (2018). La aplicación de la criminología clínica en las investigaciones forenses actuales. Medicent Electrón, 22(1), 10-18. http://scielo.sld.cu/pdf/mdc/v22n1/mdc02118.pdf*
- *Redondo Illescas, S. y Pueyo, A.A. (2007). La psicología de la delincuencia. Papeles del Psicólogo. 28(3), 147-156. https://www.redalyc.org/pdf/778/77828302.pdf*
- *Tieghi, O.N. (2004). Tratado de Criminología. Universidad.*
- *The New York Times (2016). "Stephan Hurwitz, danish ombudsman". http://www.nytimes.com/1981/01/25/obituaries/stephan-hurwitz-danish-ombudsman.html*
- *Varela Macedo, M. (2014). Psicología jurídica y psicología criminológica. Temáticas y áreas de interés. Revista Electrónica de Psicología Iztacala, 17(4), 1349-1373. https://www.iztacala.unam.mx/carreras/psicologia/psiclin/vol17num4/Vol17No4Art2.pdf*

Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León, México. *Más sobre el autor:*

GRUPO LK

"Protegemos tu patrimonio con profesionalismo y pasión"

Oficiales de Seguridad

Monitoreo y Rastreo

Custodias de Transporte

Estudios de Vulnerabilidad

Lago Tana No. 77-B, Col. Torre Blanca, Miguel Hidalgo, 11280, CDMX.

grupolkseguridadprivada.com

55-8848-8264

EL SÍNDROME DE INDEFENSIÓN APRENDIDA COMO MECANISMO DE AUTORREGULACIÓN Y PROTECCIÓN EN VÍCTIMAS DE VIOLENCIA FAMILIAR

Foto: FreePick

GUATEMALA | **Juan Manuel Iglesias**

Entender al "síndrome" como autorregulador y a la enfermedad o patología como una "experiencia de sufrimiento"

En el artículo de la edición de octubre de 2020[1] analicé cómo las víctimas que se encuentran atravesadas por situaciones de violencia familiar desarrollan mecanismos de defensa adaptativos, que a su vez, como veremos en este artículo, permiten un autorregulación en un campo organismo/entorno de violencia y abuso.

Me refiero al "Síndrome de Indefensión Aprendida", que siguiendo a Graciela Ferreira (1989) se caracteriza por "el desamparo condicionado que anula toda posibilidad de reacción ante la desesperanza y el repetido fracaso en parar la violencia del hombre. Un impedimento psíquico concreto producto de la reiteración y acumulación de experiencias antes las cuales la voluntad y el esfuerzo fracasan y quedan al fin vencidos".

Esto implica la aparición de la siguiente sintomatología:

- La mujer parece apática y complaciente. No se queja ni se rebela, no desafía.
- Trata de razonar y dialogar.
- Se instala la certeza de que son inútiles los cuidados para evitar la violencia del marido.
- Los sentidos no están puestos en "provocar" sino en cómo evitar molestar al marido para que no la agreda.
- Puede haber autorreproche por no haber tenido todo en cuenta.
- Sentimiento de culpabilidad, deslealtad y convencimiento de incapacidad y falta de inteligencia.
- Cuando pide ayuda no lo hace por la violencia doméstica sino para que la ayuden a complacer al marido.
- La mujer no consigue admitir que las cosas pueden ser vistas de otra manera y no comprende que tiene posibilidades de salir de su encierro.

Desde un punto de vista clásico, esta sintomatología podría interpretarse como un desajuste, una neurosis a la cual se la combatiría con elementos "sanos", incluso verlo como una enfermedad.

Si bien es cierto que una persona atravesada por un campo de violencia se "enferma", y desarrolla síntomas como los arriba indicados, la propuesta de este artículo, siguiendo una mirada desde la Terapia Gestalt, es entender al "síndrome" como autorregulador y a la enfermedad o patología como una "experiencia de sufrimiento".

En este caso la víctima, para sobrevivir, como organismo creará este síndrome, siguiendo a Delacroix, para tratar de restablecer el equilibrio cuando éste se encuentre perturbado, incluso adoptando la forma de enfermedad.

Se produce una paradoja, ya que el organismo (la víctima) a través de la enfermedad trataría de establecer su equilibrio perturbado por la situación de violencia que se expresa muchas veces en el plano simbólico, psicológico, económico y físico

Fotos: FreePick

PROCESO DE AUTORREGULACIÓN

Entonces podemos hablar de un mecanismo no sólo de defensa, sino también de adaptación. Se produce una paradoja, ya que el organismo (la víctima) a través de la enfermedad trataría de establecer su equilibrio perturbado por la situación de violencia que se expresa muchas veces en el plano simbólico, psicológico, económico y físico: la enfermedad o el síndrome sería un proceso de autorregulación en acción, un proceso paradójico que produce el organismo para curarse a sí mismo. "Ya que el síndrome (síntomas) es a la vez expresión de la vitalidad y defensa contra la vitalidad".

Es decir, que si bien la víctima intenta autorregularse y protegerse también termina reforzando la situación de maltrato. Siguiendo a Delacroix, también podemos afirmar que la enfermedad aparece cuando, por ejemplo, la víctima pierde la capacidad de diferenciarse, es decir poder ser auténtica y ser reconocida por su singularidad. Sabemos que esto ocurre en contextos de violencia donde el victimario exige que la víctima se comporte como él quiere que sea, que piense de determinada manera, que adopte una nueva personalidad, lo que lleva muchas veces al desarrollo de formaciones reactivas y al lavado de cerebro.

Cuando esto sucede aparece la enfermedad bajo formas como son el síndrome de Indefensión Aprendida, del Esclavo, de Estocolmo o de la Mujer Maltratada. Como dice Delacroix, "la enfermedad sería una manifestación del organismo que nos significa que hemos perdido la capacidad de diferenciarnos o de posicionarnos ante los otros con nuestras diferencias".

En la indefensión vemos por un lado la "introyección" de aquellos valores productos de la "pedagogía negra" (Miller) que mandaban "reprimir" los contenidos vitales y creativos y negar las necesidades ya desde la infancia y por otro la "retroflexión" que al no poder enfrentar las reacciones del entorno porque eran muy amenazantes, tiene que reprimir esa agresividad en tanto energía vital.

En término gestálticos, con ello la víctima interrumpe el ciclo de contacto al negar sus diferencias, sus deseos profundos y sus necesidades. Se tiene que adecuar a las exigencias del entorno violento y es allí cuando aparece la enfermedad en forma de síndrome de Indefensión Aprendida.

Una de las funciones del síndrome, siguiendo a Delacroix "sería indicarnos que no llegamos a afirmarnos con nuestras diferencias, con nuestro deseo, con lo que es nosotros y que exige expresarse en su originalidad y ser reconocido por nosotros y por el otro".

Teniendo todo esto en cuenta es necesario para la recuperación de la víctima no estigmatizar ni demonizar la emergencia de estos síndromes, sino todo lo contrario, cuanto más consciente sea la víctima de este proceso, más podrá darse cuenta de cuál es la "metáfora", el mensaje de esa "enfermedad".

Como propone Delacroix "sería el único medio que queda a nuestro organismo para significarnos que sería oportuno reaccionar, atreverse con diferencia y esta vez de manera creadora".

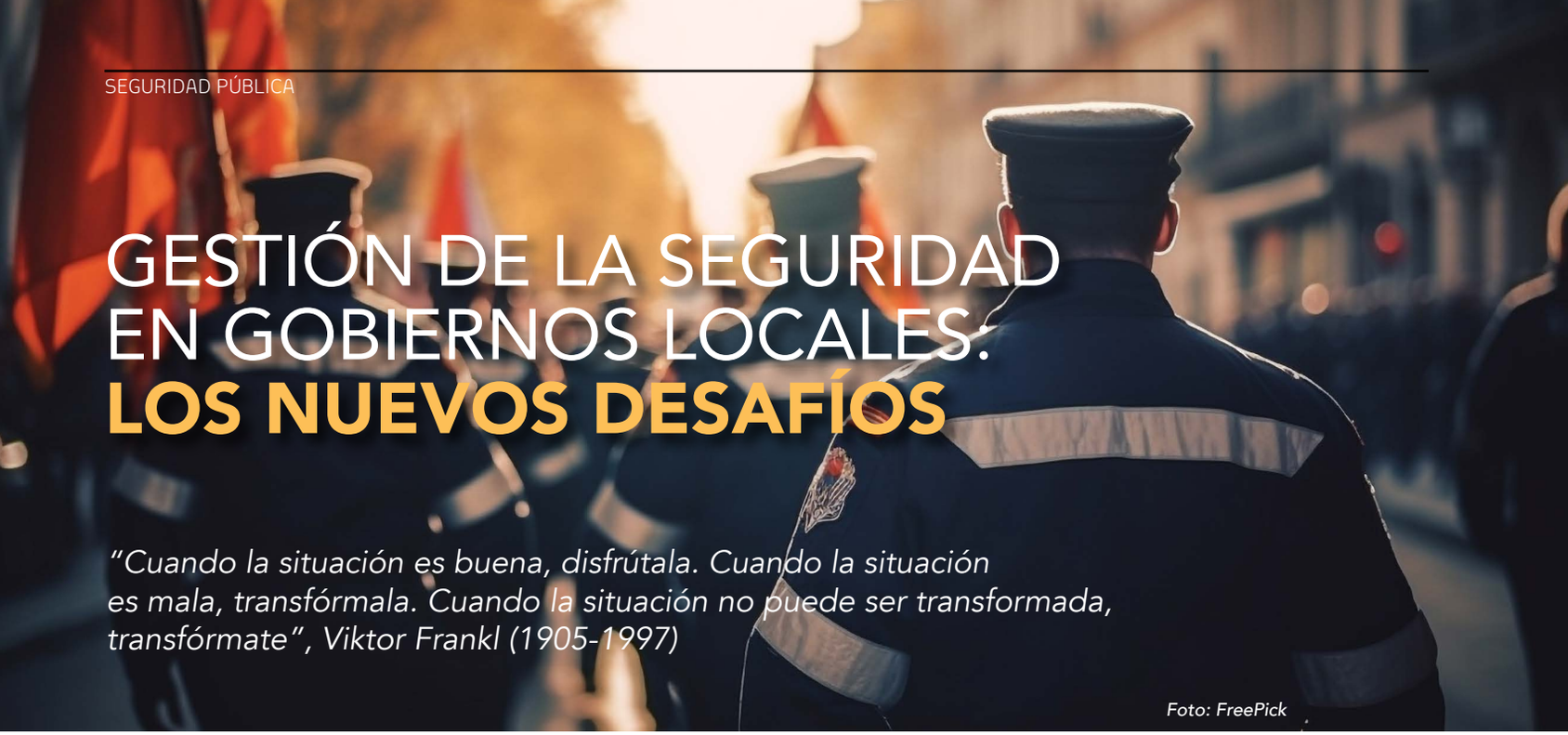
Pero sabemos que en el campo de la violencia, la víctima muchas veces queda bajo el dominio del síndrome y si bien la "enfermedad" es un llamado a un proceso de desdominio y de diferenciación, hay que establecer un andamiaje terapéutico y psicoeducativo que brinde apoyo al campo de la víctima para que pueda salir.
Es imprescindible el rol de los dispositivos victimológicos, los grupos de ayuda, el rol de la justicia y fuerzas de seguridad y demás organizaciones de la sociedad civil así como el reforzamiento de la red social y relaciones significativas que pueda tener la víctima. ■

Referencias:

[1] Se puede consultar mi artículo de la edición de octubre de 2020 "Violencia en la pareja: La importancia de cambiar las reglas de juego".

- Ferreira, G. (1992) Hombres Violentos-Mujeres Maltratadas. Aportes a la investigación y tratamiento de un problema social, Bs As, Sudamericana.

Juan Manuel Iglesias, magíster en Criminología, Victimología y Feminicidio. *Más sobre el autor:*



GESTIÓN DE LA SEGURIDAD EN GOBIERNOS LOCALES: LOS NUEVOS DESAFÍOS

"Cuando la situación es buena, disfrútala. Cuando la situación es mala, transfórmala. Cuando la situación no puede ser transformada, transfórmate", Viktor Frankl (1905-1997)

Foto: FreePick

ARGENTINA

Jorge Gabriel Vitti

La seguridad como tema de relevancia en la preocupación de la población, condiciona e influye en forma decisiva sobre los gobiernos locales como primer escalón de respuesta ante la petición ciudadana. Michael Lipsky (1980), desarrolló este nuevo objeto de análisis a comienzos de los años 80' en Estados Unidos, definiendo la "teoría de la burocracia de calle". Proporcionó una nueva forma de ver los dilemas de los trabajadores de la línea de frente del Estado, los gobiernos locales. Lipsky caracteriza a las burocracias de calle por su posición en la estructura organizativa estatal como "brazo operativo" del Estado, en contacto cotidiano con los ciudadanos. Su tarea se desarrolla en condiciones específicas, regulando beneficios y privando de acceso a solicitudes, según corresponda.

Pero, si bien su función es claramente delimitada y definida, no lo es así para quien peticiona ante ellos. En efecto, para ellos representan al Estado en general, en toda índole de necesidades. Los hechos delictivos en alza, han reforzado esa petición de los ciudadanos, teniendo como primer escalón receptor a los representantes de gobiernos locales. Binder (2016), refiere a esta situación arriba detallada, identificando tres momentos en la relación de los gobiernos locales con la agenda de seguridad:

1) Etapa de toma de conciencia del malestar y derivación de los reclamos a las autoridades provinciales y/o nacionales.
2) Etapa de cooperación, donde refuerzan las capacidades provinciales con recursos locales, aunque sin intervención directa.
3) Situación actual, en la cual se reconoce necesario aumentar la participación local del diseño y ejecución de políticas públicas a fin de no pagar los costos del malestar.

Al carecer orgánicamente del gobierno de la fuerza pública, han desarrollado una intensa actividad de gobernanza con los representantes locales de las fuerzas policiales, y explorado una serie de estrategias de prevención en un sentido más amplio y abarcativo, interpretable desde el concepto de seguridad humana. Seguridad humana concebida con centro en las personas, integral (seguridad económica, alimentaria, de la salud, ambiental, personal, de la comunidad y política). En este artículo, desarrollaremos puntualmente las facetas de la seguridad de las personas y la de la comunidad, aunque hay puntos de contacto con las otra por su visión integral sistémica. Dos son sus estrategias fundamentales: Protección (con foco sobre los sectores más vulnerables) y Empoderamiento (fomentando el desarrollo de los sectores postergados).

Protección (descendente) y Empoderamiento (ascendente)

¿CÓMO EVALUAR LA VULNERABILIDAD?

Es muy importante poder definir, entonces, cómo se debe evaluar la vulnerabilidad de los distintos sectores de la población para poder orientar la acción, a saber: exposición, fragilidad y resiliencia.

- **Exposición:** decisiones y prácticas que ubican al ser humano y sus medios de vida en la zona de impacto de un peligro. Ubicación geográfica.

Ejemplo actual de exposición: parada de colectivos a la madrugada

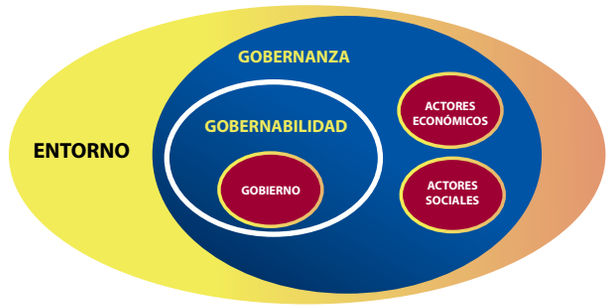
- **Fragilidad:** condiciones de desventaja o debilidad relativa del ser humano y sus medios frente al peligro. Características particulares de la persona. A mayor fragilidad, mayor vulnerabilidad.

Fragilidad, en este caso desventaja relativa por condición de la víctima

- **Resiliencia:** relacionada al nivel de asimilación o capacidad de recuperación del ser humano y sus medios frente a la ocurrencia de un daño. A mayor resiliencia, menor vulnerabilidad.

GOBERNABILIDAD Y GOBERNANZA

Esa gestión local es materializada a través de las funciones de gobernabilidad (con recursos orgánicos propios), y de gobernanza (con organismos no dependientes en relaciones de cooperación y coordinación). La fuerza pública, representada por las fuerzas policiales, constituye sólo un elemento (subsistema) que forma parte de un sistema superior (Sistema de Seguridad Humana), no el sistema en sí. Misma condición de subsistema también la revisten los gobiernos locales.



Gobernabilidad y Gobernanza

Dentro de las funciones de gobernabilidad, es decir, con recursos orgánicos propios, podemos citar, entre otras:

1) Creación o ampliación de estructuras de gobierno de la seguridad a nivel local.
2) Instalación o ampliación de centros de monitoreo urbanos.
3) Diseño de patrullaje municipal.
4) Estrategias de Prevención Situacional (iluminación, señalización, mantenimiento del espacio público).
5) Asistencia a víctimas de violencia intrafamiliar (género, niños, ancianos).
6) Centros de tratamiento de adicciones.
7) Observatorios locales de producción de información para toma de decisión.

En funciones de gobernanza (coordinación y cooperación), podemos citar:

1) Apoyo financiero y logístico a las fuerzas de seguridad y policía provincial (información territorial, instalaciones, policía adicional, combustible, compra y reparación de vehículos, etc.). Últimamente, y ante la carencia de personal policial, hay municipios que aportan conductores para los móviles policiales.
2) Coordinaciones operativas con la policía local, materializadas en corredores escolares, paradas seguras, y otras generadas en el análisis de la vulnerabilidad.
3) Promoción de la participación vecinal.
4) Programas de asistencia y reinserción social.
5) Participación en programas de justicia restaurativa.

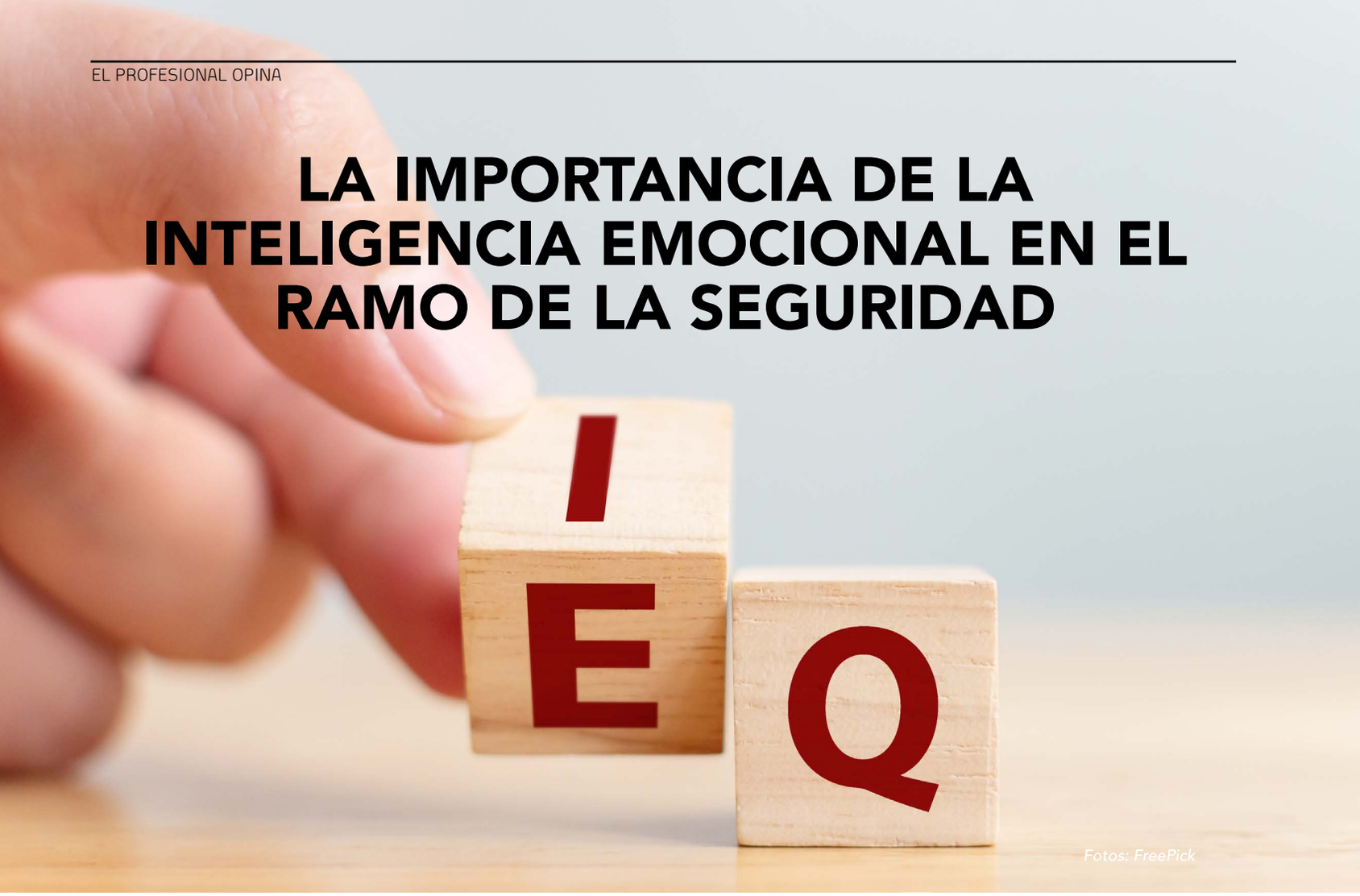
Como conclusión, podemos decir que, gradualmente, los gobiernos locales van asumiendo un mayor protagonismo en la agenda de seguridad. Sus posibilidades son limitadas por el marco normativo pero, a la vez, han buscado alternativas para dar respuesta al ciudadano como burocracias de calle que son. ■

Referencias:

- *BINDER, A. (2016), "Seguridad en el municipio y usos de la información sobre la criminalidad, la violencia y el conflicto", en T. Schleider y M. E. Carrasco (eds.), Municipios, los nuevos actores de la seguridad ciudadana, Buenos Aires, ILSED, pp. 19-31.*
- *LIPSKY, M. ([1980] 2010), Street Level Bureaucracy: Dilemmas of the Individual in Public Services. New York: Russell Sage Foundation.*

Jorge Gabriel Vitti, magíster en Inteligencia Estratégica por la Universidad Nacional de La Plata y Licenciado en Seguridad. *Más sobre el autor:*

LA IMPORTANCIA DE LA INTELIGENCIA EMOCIONAL EN EL RAMO DE LA SEGURIDAD



Fotos: FreePick

Más allá de las habilidades técnicas, la inteligencia emocional es fundamental para el éxito de los líderes y las organizaciones

AUSTRIA MÉXICO

Marcella Tapia

Con frecuencia se estereotipa al ramo de seguridad como un campo carente de emociones y todavía se siguen considerando las "habilidades blandas" como algo secundario. Sin embargo, la inteligencia emocional (IE) está basada en la ciencia y se reconoce más y más como una habilidad esencial para el buen desempeño en cualquier área en la que nos involucremos.

En los diferentes sectores y tamaños de empresas en donde se implementó la inteligencia emocional en los procesos de reclutamiento y en la educación, las investigaciones realizadas encontraron mejores resultados empresariales, como mayor compromiso de los empleados, la reducción de la rotación y el absentismo, y mayor rentabilidad. Un amplio estudio que se realizó en el ejército estadounidense mostró que la Fuerza Aérea logró reducir drásticamente la rotación de sus reclutadores y recortó sus pérdidas financieras en un 92%. Su iniciativa posterior de inteligencia emocional con los paracaidistas les ayudó a ahorrar 190 millones de dólares (Bar-On 2006).

¿QUÉ ES LA INTELIGENCIA EMOCIONAL?

Daniel Goleman, psicólogo y autor estadounidense, define la inteligencia emocional como "la capacidad de reconocer nuestros propios sentimientos, los sentimientos de los demás, motivarnos y manejar adecuadamente las relaciones que sostenemos con los demás y con nosotros mismos" (Goleman 1995). Cuando identificamos y gestionamos nuestras emociones, logramos tomar decisiones más inteligentes y acertadas y no nos volvemos prisioneros de nuestras propias emociones y pensamientos.

Hay varios modelos de la inteligencia emocional; explicaré el modelo de los cuatro dominios de Daniel Goleman (2014): autoconciencia, autogestión, conciencia social y gestión de relaciones.

La autoconciencia es el primer componente de la inteligencia emocional y la base esencial, ya que las demás habilidades de la IE no pueden desarrollarse sin tener esta habilidad. Tener autoconciencia significa ser consciente tanto de nuestro estado de ánimo como de nuestros pensamientos sobre el estado de ánimo (Mayer 1997). También implica conocer nuestros puntos fuertes y límites, así como tener confianza en nosotros mismos.

La autogestión es la capacidad de controlar nuestras propias acciones, pensamientos y sentimientos para obtener los resultados deseados. Es fundamental en la profesión de la seguridad, en donde es importante actuar con responsabilidad y madurez. Hay muy poco margen para el comportamiento inmaduro, la agresión, el sarcasmo o el pánico que podrían empeorar las situaciones.

La conciencia social es la habilidad de percibir las emociones de los demás y "leer" las situaciones adecuadamente. Se trata de detectar lo que piensan y sienten los demás y poder utilizar nuestra capacidad de empatía. Ahí también entran las habilidades de leer expresiones faciales, el lenguaje corporal, y la comunicación; todo esto es de suma importancia en el ámbito de la seguridad.

La gestión de las relaciones implica tener un sentido del trabajo en equipo y la colaboración, ser un líder inspirador y aprender a resolver conflictos.

Las personas que dominan este aspecto son capaces de liderar y motivar, de tomar la iniciativa y de reforzar las habilidades de los demás mediante la retroalimentación y la orientación.

El marco de competencias

Modelo de Inteligencia Emocional, Daniel Goleman (2014)

LA IMPORTANCIA DE LA INTELIGENCIA EMOCIONAL EN EL SECTOR DE LA SEGURIDAD

En general todos podemos beneficiarnos, tanto en la vida privada como en la vida profesional, de un alto grado de inteligencia emocional. Pero hay ciertas profesiones como médicos/as, enfermeras/os y maestros/as que requieren todavía un nivel más alto de estas habilidades. Lo mismo aplica para el ámbito de la seguridad. Muchos de los/las profesionales de seguridad se enfrentan a diario a desafíos, situaciones de estrés y experiencias traumáticas que pocas otras profesiones tienen con tanta frecuencia. Son precisamente estas situaciones extraordinarias en donde la inteligencia emocional resulta crítica.

A nivel operativo, a menudo el trabajo va acompañado de elevados riesgos para la integridad física y mental. Por lo mismo, el perfil del puesto exige que sean capaces de adaptarse y tratar con una gran variedad de situaciones y personas una y otra vez. Todavía más que la valentía y la fuerza física, el trabajo exige una comunicación inteligente y habilidades interpersonales que pueden pasar desapercibidas y ser subestimadas por el propio personal de seguridad, razón por la cual los líderes de seguridad deberían ser agentes proactivos de cambio con altos niveles de inteligencia emocional, para poder mejorar la cultura de su departamento u organización.

Muchos de los/las profesionales de seguridad se enfrentan a diario a desafíos, situaciones de estrés y experiencias traumáticas que pocas otras profesiones tienen con tanta frecuencia. Son precisamente estas situaciones extraordinarias en donde la inteligencia emocional resulta crítica

De hecho, según Daniel Goleman cuanto más alto ascienda un líder en la organización, más importancia adquiere la inteligencia emocional para tener éxito. Diversos estudios han demostrado que los líderes con una elevada inteligencia emocional dirigen con más éxito y son especialmente apreciados por sus colaboradores.

Para lograr sus objetivos, los líderes de seguridad necesitan habilidades para crear y reforzar alianzas y colaboraciones, tanto dentro como fuera de una organización. Dado que ayuda a mantener el autocontrol necesario para conservar la calma y el enfoque, la IE es un componente crucial de la negociación en situaciones de crisis. La capacidad de escucha activa, la autogestión, la empatía y el fomento de la confianza son esenciales para poder resolver conflictos con eficacia.

La buena noticia es que todos tenemos la capacidad de aumentar, cultivar y desarrollar nuestra inteligencia emocional. Algunos mitos sobre las "habilidades blandas" -empezando con el nombre, que de hecho debería cambiarse pronto a "habilidades esenciales"- no ayudan a tener todavía la aceptación debida. Sin embargo, los beneficios son enormes, especialmente para el sector de seguridad. ■

Referencias:

- *Bar-On, R. (2006) The Bar-On model of emotional-social intelligence (ESI) en https://www.psicothema.com/pdf/3271.pdf*
- *Goleman, D. (1995). Emotional Intelligence. New York, New York: Bantam Dell.*
- *Goleman, D. (2014). Liderazgo. El poder de la inteligencia emocional. B DE BOOKS*
- *Goleman, D., Boyatzis, R. & McKee, A. (2002). Primal Leadership: Realizing the Importance of Emotional Intelligence, Harvard Business School Press: Boston.*
- *Salovey, P. & Mayer, J. D. (1997). Emotional Development and Emotional Intelligence. New York, New York: BasicBooks.*

Marcella Tapia, M.A., *Coach* y entrenadora internacional de desarrollo personal y liderazgo. *Más sobre la autora:*

Omar A. Ballesteros, director general y CEO de Ballesteros y Barrera Servicios de Protección.
ballesteros.barrera@hotmail.com

Más sobre el autor:

ANÁLISIS DEL LENGUAJE CORPORAL: ROSTRO-CABEZA, TRONCO Y EXTREMIDADES

¡Siempre es un gusto, placer y honor! Mandarles un fuerte abrazo a todos ustedes que amablemente me siguen en mis redes sociales de LinkedIn, principalmente, donde con sus palabras me alientan a seguir buscando información más actual relativa al tema del lenguaje verbal o lenguaje corporal, por lo anterior cada vez son más amigos, que interesados en el tema, se suman a que su servidor sea *coaching* en el aprendizaje y mejoramiento de sus habilidades de expresión humana, llevando con ello a que no los engañen y puedan conseguir excelentes negociaciones para su beneficio.

En esta ocasión en la columna "EL SILENCIO HABLA", quiero expresar que mi amigo, el empresario Santiago Carranco, acaba de terminar su formación básica en este fascinante tema, que una vez que lo conoces te envuelve y te lleva a querer saber más. ¡Felicidades por terminar, amigo! Ahora comienza tu especialización.

La columna "EL SILENCIO HABLA", es para ustedes, y en esta ocasión hablaré de las tres partes del cuerpo que se tienen que denotar para poder analizar la expresión de una persona.

Las tres partes a revisar deben estar en sincronía, al menos dos:

1) Rostro-cabeza.
2) Tronco.
3) Extremidades.

Estas tres partes deben estar en coordinación, es decir, que cuando la cabeza expresa algo, las manos y los pies confirman dicha expresión, no es congruente que una persona que está llorando, tenga las manos metidas en las bolsas del pantalón, por mencionar un ejemplo, lo lógico es que las manos estén en la cara tocándola o acariciándola, o que los brazos envuelvan el tronco; a esto decimos que deben estar en sincronía.

Para aquellos que todavía no se inician en el tema del lenguaje no verbal, comúnmente se basan en lo que dice la persona, y no distinguen lo que los brazos y piernas quieren decir.

EJEMPLOS

Veamos la siguiente imagen:

En esta imagen aparece al centro Libia Denisse, que es la candidata del gobernador de Guanajuato, Diego Sinhue Rodríguez Vallejo, para suplirlo.

Según lo que se dice acá en Guanajuato, es que se debe realizar una selección "democrática" de la candidata para una competencia en suelo parejo, sin embargo, la foto muestra más que eso.

Veamos la foto más de cerca: el gobernador, claramente está expresando su apoyo a Libia, poniendo su mano izquierda en su hombro izquierdo, además de que tiene su tronco o cuerpo más cerca de ella, podría haber puesto su mano izquierda en su hombro derecho y de todos modos su expresión sería la misma, que es su apoyo a ella, pero no es el caso, podría haber puesto su mano izquierda como está, y haber alejado su cuerpo de ella, de tal manera que menciona de igual manera su apoyo, pero no es el caso.

Cuando quieres estar cerca de alguien, busca que tu persona o cuerpo esté más cerca de dicha persona

Analicemos:

1) Cuando quieres estar cerca de alguien, busca que tu persona o cuerpo esté más cerca de dicha persona. Como es el caso de la foto, más del 50% del cuerpo de Diego está detrás de ella. ¿Qué significa entonces? Expresa que quiere estar muy cerca de ella, puedo decir que le está llevando la campaña directamente. Hay favoritismo.
2) Si hubiera puesto la mano derecha en su hombro, expresaría que tiene una preferencia más allá que el trabajo, ya que la mano derecha tiene que ver con el afecto, en este caso no lo hay.
3) El cuerpo está ligeramente cercano a ella, sin estar encima de ella, lo que confirma, junto con la mano en la posición en la que está, su proximidad y cercanía con ella.
4) Si notan la cabeza está ligeramente alejada de ella, en la posición en la que está el tronco, la cabeza de Libia ve hacia al público, y por dar una orientación, está viendo hacia la izquierda de la foto, mientras que Diego está girando levemente en sentido contrario, eso también denota, que no hay acercamiento "afectuoso", si la cabeza estuviera inclinada hacia ella, podrá pensar a pesar del uso de la mano izquierda, que puede que haya sentimiento de él por ella.

Concluimos entonces:

- El gobernador tiene predilección por Libia.
- No tiene afecto con ella.
- Le da todo su respaldo muy notablemente (por lo que las demás candidatas se pueden despedir de un proceso parejo).
- Diego pretende estar muy cerca de ella, y controlar su agenda.
- Ella está conforme con la situación.

Hay expertos que se ostentan como "analistas del presidente", pero cualquiera que estudia la conducta y lenguaje corporal puede analizar al presidente, tengan cuidado con charlatanes.

Una expresión que todos vemos, de las personas con afecto, es la cercanía de las cabezas, como lo demuestra esta foto:

Algunos otros ejemplos de extremidades y troncos:

Las manos de ella quieren decir: "él es mío". Además él se toca las manos de una forma peculiar, eso quiere decir: "tengo un compromiso" (está tocando su dedo anular).

Las manos del hombre encima de la niña y la ligera expresión de la cara de la niña y sus manos abrazándose a sí misma, quieren decir: "tengo miedo", "tengo terror".

Estos amigos se abrazan, en hombros y cintura, en la forma en que lo hacen quiere decir: "apoyo y soporte", yo diría "hermandad".

Esta imagen me gusta, porque expresa dos cosas:

1) La forma de las manos del hombre es imposición.
2) La cara de ella, así como voltea la cabeza es incomodidad.

Estas señales son muy características del acoso.

Como siempre lo he dicho, se tiene que hacer mucha práctica para poder ser un analista con un acierto de más del 90%, debemos cometer errores como cualquier persona para podernos perfeccionar. Nadie tiene un acierto del 100%, sin importar las credenciales de todas las personas que hay que predican ser "lectores" de personas, y que son mega expertos, un experto serio sabe que a pesar de que tiene mucha práctica, existe al menos el 2% de probabilidad siempre, de que se equivoque, porque el análisis de la conducta y expresión de las personas tiene muchas variables.

Finalmente veamos esta última foto:

Te puedo decir todo lo que se ve, pero vale la pena que practiques, te dejé una ayudadita, hay unas señales amarillas en tronco y extremidades, que te dirán lo que sienten cada uno.

Para la siguiente edición hablaremos de los pies y la manos, te invito a que estés en contacto y no te pierdas la siguiente publicación.

Anímate hacer el análisis, y compártelo conmigo al correo: xcelencia.capacitaciones@gmail.com. ■

Fotos: Cortesía Omar Ballesteros

ASIS INTERNATIONAL™

CAPÍTULO MÉXICO OCCIDENTE 247

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Actualmente ASIS cuenta con 36 mil socios aproximadamente, afiliados en los más de 250 Capítulos en los cinco continentes, destacándola como la organización de seguridad más importante del mundo

ASIS International (American Society for Industrial Security), es la organización más importante del mundo que concentra a los profesionales de la seguridad, siendo un foro para profesionalizarse y compartir conocimientos. Actualmente ASIS cuenta con más de 250 Capítulos en el mundo, y uno de ellos ubicado en México es el Capítulo Occidente (247), presidido por Paul Messeguer Lamas, quien nos platica un poco de su trayectoria y los objetivos del Capítulo 247 de ASIS International.

Seguridad en América (SEA): ¿Qué significa para usted ASIS y el haber llegado hasta el día de hoy como representante del Capítulo Occidente?

Paul Messeguer (PM): hace 23 años que me hice socio del entonces "American Society for Industrial Security", a más de 18 años que me certifiqué CPP y que fui parte del equipo fundador de este capítulo, me siento profundamente honrado de estar de regreso y presidirlo.

Quiero mencionar a colegas como Jorge Septién e Iris Casco, actores fundamentales para el despegue y desarrollo del capítulo ASIS Occidente 247. Así como a cada uno de los fundadores, expresiden-

"A MEDIDA QUE CRECÍ, LA SEGURIDAD SE VOLVIÓ PARTE DE MI VIDA DIARIA"

tes y exmiembros de la mesa directiva por el tiempo y esfuerzo dedicado durante todos estos años de colaboración en ASIS.

Aprovecho para reiterar mi compromiso con el vicepresidente del Capítulo Jorge Guzmán Lara, la Mesa Directiva actual y nuestro RVP Región 7A Manuel Zamudio, quien nos representa ante esta comunidad global y diversa como lo es ASIS Internacional.

SEA: ¿Cuáles son sus objetivos como presidente de ASIS Capítulo 247?

PM: principalmente:

Fortalecer nuestra red de miembros.

Mejora de nuestras comunidades.

Proporcionar a nuestros miembros soluciones actualizadas a sus necesidades y aspiraciones educativas.

SEA: ¿Qué beneficios tienen los miembros de este Capítulo y cómo benefician al sector en general?

PM: los beneficios son varios, pero te puedo hablar desde mi experiencia:

1) Adquirir el conocimiento a profundidad de la seguridad y su integración a todas y cada una de las actividades tanto privadas como públicas.
2) Acreditación de los conocimientos adquiridos durante cualquiera de nuestras certificaciones.
3) Reconocimiento exponencial del profesionalismo, lo cual deriva en mejores oportunidades laborales.

¿Cómo beneficiamos al sector en general?

El principal beneficio es seguir agrupando y formando profesionales de seguridad con un alto conocimiento de sus funciones y enfocado a contribuir a los objetivos de las organizaciones.

SEA: ¿Cómo llegó al sector de la seguridad?

PM: inicié mis estudios en la Guadalajara de los 70 y mi formación profesional en IBM planta GDL a principios de los 90, este inicio fue en compañía de un grupo de profesionales de la seguridad que hoy en día son piezas clave en cada una de sus organizaciones, además de haber tenido la fortuna de tener como maestro al Ing. Sergio Delgado Torres.

SEA: ¿Por qué decidió desarrollarse en el área de la seguridad?

PM: para ser preciso, no es que yo lo había decidido (risa), a veces la vida te pone en el momento y lugar adecuado, y en mi caso así fue. La seguridad llegó a mi vida para llenar ese hueco que tenía a mis 20 años, y mis dudas sobre cuál sería el camino que tomaría, se despejaron inmediatamente.

SEA: ¿Qué es lo que más le apasiona de la seguridad?

PM: podría decir que la seguridad en todo su conjunto me apasiona. A medida que crecí, la seguridad se volvió parte de mi vida diaria.

SEA: ¿Cuáles considera que son los mayores retos como profesional en el sector de la seguridad?

PM: actualmente el mayor reto es la estabilidad del país, la cual afecta a todas y cada una de las actividades en las que como profesionales nos desarrollamos. Como ejemplo de esto sería que, nosotros debemos mantener seguras las operaciones de nuestras organizaciones en ambientes de riesgos variables, temporales, críticos e inestables.

SEA: en tres palabras, ¿cómo se define usted?

- Padre de tres hermosos hijos.
- Melómano.
- Profesional. ■

ACONTECIMIENTOS DE LA INDUSTRIA

Fecha: 30 de mayo de 2023.

Lugar: Bárbaro Club House del Hipódromo de las Américas, Ciudad de México.

Asistentes: más de 50 asociados.

Se celebra el Día GEMARC con conferencias y un nuevo presidente

El Grupo de Ejecutivos en Manejo de Riesgos Corporativos (GEMARC) llevó a cabo el "Día GEMARC", en donde se realizaron varias conferencias con profesionales como Rolando Rosas, titular de Ciberseguridad de la FGR (Fiscalía General de la República); Ana María Salazar Slack, CEO de Grupo Salazar Slack; Marion Reimers, periodista deportiva; y Tyrone Lara, agregado jurídico adjunto en la Embajada de los Estados Unidos en la Ciudad de México, además de presentar la entrega de resultados de Dagoberto Santiago, presidente saliente de la asociación.

Los miembros del Comité de Elecciones realizaron un informe de resultados acerca del proceso electoral, donde se hizo el anuncio de que, con la mayoría de los votos, el nuevo presidente de GEMARC es Héctor Coronado, *Head of Security Ops LATAM* en Mercado Libre. "De corazón, gracias, las puertas siempre estarán abiertas para todos. Algo que es muy importante es la unidad, no hay un protagonismo, no hay un presidencialismo, algo por lo que GEMARC será distinguido de otras asociaciones es que para mí es una familia, somos amigos, y contamos con cada uno de nosotros no sólo en lo profesional, sino también en lo personal. Esto se hace con el corazón, nada más", comentó Coronado. ■

Fecha: 06 de junio de 2023.

Lugar: Bárbaro Club House del Hipódromo de las Américas, Ciudad de México.

Asistentes: más de 50 participantes.

ASIS Capítulo México se reúne en un *Relax Meet & Learn*

Cap. Julio Balderas, director de Seguridad Patrimonial de Casa José Cuervo; y Brisa Espinosa, presidenta ejecutiva de ASIS Capítulo México

ASIS Capítulo México realizó su reunión mensual del mes de junio de una manera diferente, cambiando el desayuno por un *cocktail* en el que el Cap. Julio Balderas, director de Seguridad Patrimonial de Casa José Cuervo, ofreció la charla titulada "La importancia de la Inteligencia no verbal"; empezando con un ejercicio de relajación, para dar paso a la explicación sobre los tipos de comunicación no verbal que existen y que a veces no percibimos, como las expresiones corporales, gestos, símbolos, y cualquier otro método que a veces dicen más que las palabras, resaltando que en ocasiones tenemos prejuicios con la gente basándonos solamente en su apariencia o en las actitudes que expresan, pero que no manifiestan verbalmente.

Brisa Espinosa, presidenta ejecutiva de la asociación, otorgó el reconocimiento al Cap. Julio Balderas por su conferencia y a Miguel Ángel Champo, director general de Multiproseg, por su patrocinio. ■

Fecha: 07 de junio de 2023.

Lugar: Ciudad de México.

Asistentes: más de 150 participantes.

Seguridad en América realiza *Roadshow* "Seguridad en la industria farmacéutica"

Seguridad en América (**SEA**) realizó otra edición de los ya conocidos *roadshows* de seguridad, en esta ocasión enfocado en la Industria Farmacéutica, el cual contó con la participación de Alan Vara, *Security & SHE Sr. Manager* de la empresa ROCHE, quien se presentó con una charla magistral titulada "Salud + Seguridad = Operación de alto impacto".

CHARLA MAGISTRAL

Alan Vara comentó que nuestro país es el segundo mercado más grande del sector en Latinoamérica, el Estado de México, Jalisco y la Ciudad de México son las tres entidades en donde la industria farmacéutica más se ha desarrollado. Del total de empresas establecidas en México se abastece al Sistema de Salud en casi un 97%. De los más de 126 mil millones de habitantes en el país, sólo 92 millones 582 mil 812 de habitantes están afiliados a algún servicio de salud.

De acuerdo con Alan, las principales actividades delincuenciales ligadas a la industria farmacéutica son: robo a transporte de carga, desvío de insumos del Sector Público, mercado ilegal en establecimientos públicos, *e-commerce*, venta ilegal por plataformas de mensajería instantánea, adulteración y falsificación.

Lo que agrava la situación son las modificaciones en los procesos públicos de adquisiciones de insumos para la salud, la falta de capacidad técnica y carencia de infraestructura, la fragmentación de la persecución criminal de la actividad y sobre todo que no hay manera de medir efectivamente el impacto a la salud.

Las principales soluciones que presenta Alan son las alertas sanitarias emitidas por la COFEPRIS, principalmente realizadas por ROCHE en 2021 a 2023 por cuestiones de la pandemia. Destacó la presencia en asociaciones como Pharmaceutical Security Institute, CANIFARMA y GEMARC, enfocadas tanto en aspectos generales como específicos de la industria farmacéutica, de alcance nacional.

Javier Jarillo, Account Manager Access Control & Video Solutions en Johnson Controls

Alan Vara, Security & SHE Sr. Manager de la empresa ROCHE; y Alex Parker, Sales Manager de SEA

PATROCINADOR

Después fue turno de Javier Jarillo, *Account Manager Access Control & Video Solutions* de la empresa Johnson Controls, quien se presentó con la ponencia titulada "Seguridad física unificada para los retos del sector farmacéutico". Javier señaló los desafíos de la industria farmacéutica: el robo o clonación de fármacos, la logística, el cumplimiento normativo, los ataques de ciberseguridad, la eficiencia y control de procesos de calidad, materiales peligrosos y el reciclaje.

Johnson Controls se dedica a brindar soluciones inteligentes y unificadas que mejoren la seguridad, principalmente desarrollando tecnología más allá de la seguridad, entregando a cada uno de los clientes soluciones no sólo del área de Seguridad, sino de sistemas de gestión, refrigeración industrial, sistemas de aires acondicionados, protección contra incendios y por supuesto, la parte de seguridad, unificando estas soluciones en procesos de protección como la integración de video de detección con Ilustra Radar, control de accesos y monitoreo, grabación de acciones de alto riesgo, la cámara Multisensor Ilustra, entre otros dispositivos expertos en ciberseguridad.

También se contó con la participación de José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México; y Luis Miguel Dena, presidente de la Comisión de Tecnología de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), quienes hablaron de cada una de las asociaciones a las que representan. ■

Fecha: 19 de junio de 2023.

Lugar: Hacienda de Los Morales, Ciudad de México.

Asistentes: más de 100 socios.

La AMESP celebra su 11° aniversario con una reunión acompañada de una conferencia magistral

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) realizó una reunión especial con motivo de la celebración de su décimo primer aniversario, en donde Gabriel Bernal Gómez, presidente de la asociación, dio la bienvenida a los nuevos miembros de la AMESP, haciendo su unión oficial con la entrega del banderín y el pin a los representantes de las empresas Technical Armored Group, V21 Seguridad Privada y GPS Control. El presidente también mencionó el éxito obtenido en el Consejo Internacional sobre Seguridad Ciudadana realizado en Tijuana, Baja California, el pasado 18 y 19 de mayo, evento del cual la AMESP fue patrocinador.

Por su parte, Maribel Cervantes, *Head Protective Security Mexico & LAM* en HSBC, brindó la conferencia magistral "Cómo prevenir los delitos financieros en la seguridad privada", en la que habló de los delitos financieros, algo que desafortunadamente se ha popularizado en México en los últimos años. También mencionó los procesos de control de seguridad que se han implementado a partir de estas situaciones para la prevención del lavado del dinero. ■

Gabriel Bernal Gómez, presidente de la AMESP

Fecha: 20 de junio de 2023.

Lugar: oficinas de AMESP (Alcaldía Benito Juárez, Ciudad de México).

Asistentes: más de 50 socios.

La AMESP celebra la inauguración de sus nuevas oficinas

En el marco de la celebración de su décimo primer aniversario, la Asociación Mexicana de Empresas de Seguridad Privada (AMESP) realizó la inauguración de sus nuevas oficinas ubicadas en la alcaldía Benito Juárez de la Ciudad de México, en donde el actual presidente, Gabriel Bernal Gómez; Verónica Torres Landa, directora general, acompañados de miembros de la Mesa Directiva y ex presidentes de la asociación, realizaron un recorrido para los socios que asistieron al evento.

Gabriel Bernal ofreció unas palabras a los presentes, agradeció el apoyo de la Mesa Directiva y de todos los asociados, así como a sus predecesores en la presidencia, quienes se encontraban presentes. "Realmente este es un esfuerzo pensando en todos los asociados, es muy grato tener este espacio, un espacio digno, que le queda chico para lo que la asociación se merece, porque esta asociación se merece muchísimas cosas más", expresó. ■

Cap. Salvador López, presidente 2020 – 2022; Marcos Ossio, presidente 2014 – 2015; Mario Espinosa, presidente 2012 – 2014 y fundador de la asociación; Joel Juárez, presidente 2018 – 2020; y Gabriel Bernal, presidente actual de la AMESP

Fecha: 28 de junio de 2023.

Lugar: Hotel Marquis Reforma, Ciudad de México.

Asistentes: más de 100 participantes.

Seguridad en América realiza el "III Encuentro de Seguridad Bancaria 2023"

Diferentes directivos y responsables del área de Seguridad en el sector financiero y bancario, se reunieron en el "III Encuentro de Seguridad Bancaria 2023" organizado por **Seguridad en América** (**SEA**), *roadshow* dirigido y moderado por Samuel Ortiz Coleman, director general de **SEA**; y Alex Parker, *Sales Manager* de la misma casa editorial.

CHARLA MAGISTRAL

Samuel Ortiz Coleman agradeció la presencia de los asistentes al evento y presentó a los ponentes del panel titulado "Transformación de la Seguridad Bancaria en el Siglo XXI", los cuales fueron: Víctor Hugo Ramos Ortiz, director de Seguridad para Santander; José Manuel Díaz Caneja, director de Seguridad para BBVA; Hugo Montes Campos, director de Seguridad para CI Banco; Pedro Villanueva, subdirector de Prevención de Fraudes para INBURSA; Javier Hernández Vargas, director general de Banorte; y como mediador, Ciro Ortiz Estrada, director general de SEPROBAN.

PATROCINADORES

Posteriormente se presentó José de Jesús Arellano, *Vertical Sales Manager* de la empresa GENETEC, con la ponencia titulada "Desafíos, Riesgos y Necesidades Relacionados al Sector Bancario". En su charla, José analizó los riesgos del sector bancario y lo que conllevan, y cómo GENETEC puede apoyar a mitigar riesgos en la parte de seguridad física y seguridad cibernética, cómo pueden ayudar a hacer más eficiente la operación. La plataforma de la marca permite unificar a todos los departamentos para el trabajo en equipo, no sólo al de seguridad, sino que también comparte evidencias y recopilación de datos ante incidentes; la aplicación permite operar y generar procesos en tiempo real desde donde sea de manera segura, entre muchos otros beneficios.

Luego fue el turno de Alan Barrón, director de MAQYUD de la empresa SISSA, con una charla titulada "Soluciones de seguridad física en el sector bancario". Alan presentó dos soluciones para implementar en el sector bancario: Farfield, y Liberty Defense. La primera hace uso de tres herramientas: un fotosensor patentado capaz de eliminar patógenos que sirvan en épocas de pandemia o con virus simples como la gripa, éste se puede colocar en techos o muros, el monitor que mide la calidad del aire y un robot que permite la inspección en horas no laborales, todos buscando evitar la propagación de virus.

La segunda, enfocada en la seguridad física, una solución que permite la detección de armas metálicas, no metálicas, explosivos sólidos y otros elementos que se puedan considerar armas, es un escáner de personas

en movimiento, con el fin de complementar los controles de acceso.

Después se presentó Alberto Pérez, *Sales Director* de LATAM de SCATI, con el tema "El video como palanca transformadora del negocio: aplicaciones prácticas en la banca". Principalmente para ayudar a otras áreas del banco a que sirvan no sólo para la seguridad. Dentro de su amplio catálogo de productos y servicios, Alberto destacó algunas diferenciales de SCATI, fabricantes con su plataforma propia, personalización y adaptación en sus servicios, concentrándose en conceptos como conectividad, inmediatez y transformación digital, involucrando la seguridad física.

Posteriormente, fue el turno de la empresa BTV Mexicana, con una presentación titulada "Cómo evitar la suplantación de identidad en la Operación de los Contenedores de Efectivo", expuesta por Héctor Barbosa, director general; y Fernando Alberdi, presidente de la empresa. Ambos expertos reforzaron el concepto antes mencionado de seguridad física y la importancia de contar con equipo especializado en este sector. Hablando de la problemática de la suplantación de identidad, Fernando mencionó como ejemplo su nuevo sistema de Control de Acceso con combinaciones. Héctor habló acerca de las cerraduras que presentan con el objetivo de brindar soluciones reales a los clientes.

Luego fue turno de la presentación de tres marcas que se complementan: Density, Convergint y Omnicloud, con la ponencia titulada "Mi Banco Seguro", presentada por Issac Garrido, consultor de niebla; Ciro Ortiz, director de SEPROBAN; y Arturo Flores. Ciro explicó que la idea detrás de ese proyecto nació de la iniciativa de la autoridad de poder compartir las cámaras de los bancos con el servicio de C5, esto no se pudo realizar, sin embargo, el proyecto evolucionó en varias ideas que concluyeron en ver a los proveedores como aliados estratégicos y buscar una solución colaborativa para mitigar los ataques a cajeros automáticos.

El grupo contó con una demostración física de esta solución con un inflable que libera neblina. La plataforma conectada con el C5 recibe la alerta del botón de pánico de cualquier cliente o transeúnte en el banco donde se comparte la ubicación y video exterior en tiempo real para la atención de las autoridades, haciendo uso de herramientas digitales como el reconocimiento facial.

Después tocó el turno a la empresa HID, con una ponencia titulada "Soluciones SaaS HID – Uso de identidades digitales en la banca", presentada por Hugo Treviño, *Regional Sales Director* para México, Centroamérica y el Caribe de *Secure Issuance*; y Alejandro Espinosa, *PACS Director of Sales LAM North*. Ellos platicaron un poco sobre las tendencias globales de HID, destacando todos los procesos de fabricación bajo las diferentes marcas dependientes de HID, lo que permite tener mayor penetración de mercado, enfocándose en esta ocasión en dos: Control de Acceso Físico e Impresión Segura.

Más tarde se presentó Alberto López, *Sales Manager* México de la empresa Eagle Eye Networks, con la ponencia titulada "Avanzando hacia la Nube: la evolución de la seguridad física en la banca moderna". La empresa está focalizada en videovigilancia en la Nube. Alberto habló acerca de la evolución de la seguridad bancaria, entendiendo cómo la delincuencia se ha modernizado. Dado que la seguridad está migrando a la Nube, Eagle Eye ofrece sus plataformas de almacenamiento con conexión directa a las cámaras que operan y transmiten en vivo y que cuentan con otros servicios dependiendo del paquete, de fácil acceso y con información encriptada y comprimida para su manejo seguro.

Por último, se presentaron José Machado, gerente comercial de Latinoamérica y el Caribe de VERINT; y Everton de Brito Dias, ingeniero en Soluciones de la misma empresa, con una ponencia titulada "Ayudando a los Bancos a transformarse con Verint". La marca desarrolla soluciones para la industria financiera específicamente, garantizando dispositivos seguros y evitando la vulnerabilidad de sus datos. También ofrece herramientas para la actualización de los dispositivos y su programación periódica, almacena la información en video y analiza su manejo.

El "III Encuentro de Seguridad Bancaria 2023" finalizó con la rifa de grandes premios entre los que incluyeron un viaje a España otorgado pro SCATI y una Caja Fuerte otorgada por BTV, entre otros, otorgados por **Seguridad en América** y otros patrocinadores. ■

Fecha: 04 de julio de 2023.

Lugar: Bárbaro Club House del Hipódromo de la Américas, Ciudad de México.

Asistentes: más de 70 invitados.

ASIS Capítulo México realiza su Reunión Mensual de julio

Brisa espinosa, presidenta de ASIS Capítulo México; y Mtro. Ignacio Hernández Orduña, en ese entonces director de Seguridad Privada de la Secretaría de Seguridad y Protección Ciudadana

ASIS Capítulo México llevó a cabo su Reunión Mensual del mes de julio, en la que Brisa espinosa, presidenta de dicho Capítulo, presentó su informe semestral de actividades, de entre lo que destacó aspectos como: la participación de las comunidades, la importancia de la inclusión de las nuevas generaciones en el sector, los proyectos que se implementan como "Adopta una escuela", y las cuentas y los saldos positivos que presenta la asociación, entre otros.

El Mtro. Ignacio Hernández Orduña, en ese entonces director de Seguridad Privada de la Secretaría de Seguridad y Protección Ciudadana, brindó la conferencia "Deconstruyendo la industria de la Seguridad Privada, de la Ley y otros temas", en la que habló acerca de las principales problemáticas que existen en la seguridad privada como: los elementos de seguridad privada no colaboran con las fuerzas de seguridad pública, inseguridad jurídica y duplicidad de trámites para las empresas por la disparidad en la normatividad nacional, entre otros. ■

Fecha: 12 de julio de 2023.

Lugar: Ciudad de México.

Asistentes: más de 150 participantes.

Seguridad en América realiza *Roadshow* "Nuevo perfil de guardias y protección ejecutiva"

Se llevó a cabo otra edición de los *roadshows* de **Seguridad en América**, en esta ocasión titulado "Nuevo perfil de guardias y protección ejecutiva", con charlas magistrales a cargo de Rubén Fajardo, secretario ejecutivo de ASIS Capítulo México; e Ivan Ivanovich, socio VP de WSO. También estuvo José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México, quien, en representación de la presidenta, Brisa Espinosa, habló acerca de la asociación y los beneficios de formar parte de ella.

CHARLAS MAGISTRALES

La primera charla magistral estuvo a cargo de Rubén Fajardo, quien presentó la ponencia titulada "El nuevo perfil profesional del especialista en gestión de riesgos para profesionales de impacto crítico". En su plática, explicó la importancia que se le debe dedicar a la administración de recursos humanos, la formación y desarrollo de la protección ejecutiva, la cual debe ser constante y debe contener: educación continua, planes y programas de capacitación y adiestramiento, inventario de recursos humanos, evaluación del desempeño, desarrollo laboral y personal, planeación de carrera y vida, y otros factores que mejoren el desarrollo.

Por su parte, Ivan Ivanovich habló sobre la "Protección Ejecutiva en el Siglo XXI, la nueva doctrina", en la que compartió varios principios adecuados a la capacitación y desarrollo del guardia, sirviendo como una guía

de conceptos que se pueden adoctrinar para garantizar un excelente servicio, algunos de los principios expresados abarcan aspectos como la presentación, el manejo de información, los conocimientos adquiridos, las áreas de oportunidad para mitigar riesgos y prevenir situaciones de riesgo, entre otras.

PATROCINADORES

El primer patrocinador en presentarse fue Enrique Tapia, socio director de Altair, con la ponencia titulada "¿Tenemos a nuestros ejecutivos protegidos?". En sus propias palabras, la base en la formación de una cultura de prevención está en enseñar a la sociedad a auto protegerse. Refirmó la importancia de reconocer al guardia de protección ejecutiva para garantizar que él también ofrezca este servicio de seguridad. El objetivo detrás de esto es 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, minimizar el impacto consecuencial.

Posteriormente se presentó Mario Galván, *CEO & Founder* de la empresa JVP, con la presentación titulada "La aviación en la protección ejecutiva", en la que respondió cuestionamientos acerca de la aeronavegabilidad continua, como por ejemplo: ¿Cómo se garantiza que las actividades de mantenimiento sean acordes con las normas? Mario respondió con tres factores: las auditorías internas, auditorías externas y auditorias de calidad.

Después fue el turno de Lucas Banda, *Country Manager*

de Softguard, que se presentó con su ponencia titulada "*Apps* y tecnología para la seguridad ejecutiva", en la que reconoció la importancia de la identificación del guardia en el sector, presentó la *app* que Softguard desarrolla, VigiControl, la cual es capaz de realizar el control de guardias y hacer más eficiente su rol, en sí es capaz de realizar el control y auditoría completa del accionar del guardia.

Finalmente se presentó Héctor Robles, *VP Ops Globales* de FirstCall International y presidente del Capítulo México de la Fundación Internacional para Oficiales de Protección (IFPO), para hablar acerca de esta asociación y también de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), de la cual es miembro, destacando los beneficios de ambas y resaltando el crecimiento y el posicionamiento de las asociaciones de seguridad en México y en el mundo, las cuales benefician a los clientes finales y a las empresas de seguridad en su afiliación. ■

Fecha: 14 de julio de 2023.

Lugar: Hotel Courtyard Mexico City Revolución, Ciudad de México.

Asistentes: más de 150 invitados.

AMEXSI celebra 20 años de su fundación

Acompañada por ex presidentes de la Asociación Mexicana de Especialistas en Seguridad Integral A.C. (AMEXSI), Ana Guzmán, actual presidenta de la asociación, se mostró emocionada y orgullosa por la celebración de los 20 años de AMEXSI. "A lo largo de estas dos décadas, hemos enfrentado desafíos significativos, desde terremotos, terrorismo, crimen organizado y hasta una pandemia, sin embargo, AMEXSI ha demostrado su resiliencia y que sigue siendo un referente en el sector", comentó.

José Luis Alvarado, vicepresidente de AMEXSI, agradeció también a todos los asociados y al actual Comité Directivo por su arduo trabajo, así como a los patrocinadores del aniversario. Mientras que Rubén Fajardo Correa, director general de SIPROSI, y fundador del Diplomado "Desarrollo de Habilidades para el Directivo de Seguridad Integral", del que proviene AMEXSI, se mostró agradecido y satisfecho con los logros de la asociación. ■

Ana Guzmán, presidenta de AMEXSI; y Armando Zúñiga Salinas, presidente Grupo IPS (uno de los ex presidentes de AMEXSI)

Fecha: 17 de julio de 2023.

Lugar: oficinas de VIP Protection (CDMX).

Se lleva a cabo la firma de estatutos del CONAPECE

Se llevó a cabo la firma de los estatutos del Consejo Nacional para el Desarrollo Profesional de los Escoltas y Choferes Ejecutivos (CONAPECE), una nueva asociación civil que tiene como objetivo profesionalizar, capacitar y brindar mejores oportunidades laborales y académicas a los elementos de seguridad de estas dos categorías.

Al frente de este gran proyecto, se encuentra Víctor Aguirre Gutiérrez, director y fundador de VIP Protection, empresa que cuenta con más de 22 años de servicio en la industria de la seguridad privada; así como Gabriel Bernal Gómez, CEO de Grupo Paprisa; Luis Miguel Dena, presidente de Grupo BlackIND; David Macoto Nancarrow, director operativo y consejero de Grip; Kael Malo-Juvera, *Security Manager Mx & SSA North Region* en IBM; Pedro Sanabria, director general de Trust Group, entre otros conocidos expertos en seguridad privada. Además de miembros honoríficos como Perla Ortega Porcayo, directora general de Mak Extinguisher; y el Mtro. Juan Antonio Arámbula. ■

Fecha: 19 de julio de 2023.

Lugar: Ciudad de México.

Asistentes: más de 150 participantes *online*.

ASIS Capítulo México y AMESP presentan el *webinar* "Ciberterrorismo, la nueva amenaza"

ASIS Capítulo México y AMESP presentaron el *webinar* titulado "Ciberterrorismo, la nueva amenaza", impartido por el Dr. Eitan Azani, director de Investigación del International Institute for Counter-Terrorism-Israel. La reunión virtual se realizó como resultado de un continuo esfuerzo por trabajar y colaborar entre asociaciones; Brisa Espinosa, presidenta de ASIS Capítulo México y Gabriel Bernal, presidente de la AMESP, otorgaron unas palabras de bienvenida a los asistentes.

El Dr. Azani comenzó su presentación estableciendo un contexto de las tendencias del ciberterrorismo, específicamente en la zona de Medio Oriente, pero que han logrado bastante impacto en el resto del mundo. Estableció los principales grupos delictivos que tienen relevancia en el ciberterrorismo de esa región, de entre los que se encuentran los Jihad de Al-Qaeda, del Estado Islámico, *hackers* pro-palestinos, *hackers* pro-iraníes, grupos de extrema derecha, entre otros. ■

Fecha: 24 de julio de 2023.

Lugar: Club Piso 21, Ciudad de México.

Asistentes: 50 invitados.

CONOCER y la Seguridad Privada renuevan su compromiso con el sector

El Consejo Nacional de Normalización y Certificación de Competencias Laborales (CONOCER), representado por su presidente, Rodrigo A. Rojas Navarrete, llevó a cabo la Firma del Acta de Renovación del Comité de Gestión por Competencias del Sector de Seguridad Privada, del que es presidente Gabriel Bernal Gómez, acompañado de la Mesa Directiva de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), y del vicepresidente del Consejo de Gestión, Armando Zúñiga Salinas, quien también es el presidente de ASUME (Agrupaciones de Seguridad Unidas por México).

Durante el evento estuvieron presentes diferentes autoridades y representantes del sector de la seguridad privada, por parte del CONOCER, además de Rodrigo Rojas, José Omar Villarreal Ochoa, coordinador de Promoción y Desarrollo del CONOCER; Luis Alfredo Hernández Ortiz, coordinador de Operación y Servicios a Usuarios del CONOCER; así como presidentes de asociaciones de seguridad. ■

BUSINESS ALLIANCE FOR SECURE COMMERCE

OCCIDENTE DE MÉXICO

ACÉRCATE A NOSOTROS Y REDUCE LOS RIESGOS DE TUS OPERACIONES EN EL COMERCIO INTERNACIONAL

AFÍLIATE

CERTIFÍCATE

CAPACÍTATE

Transporte

Operador Logístico

Agentes aduanales

Más de **4,500** empresas certificadas

Servicios Temporales

Seguridad Privada

Manufactura

BASC OCCIDENTE MÉXICO

Capacitaciones Basc Occidente

W. www.bascoccidente.com.mx

C. promocion@bascoccidente.com.mx

T. (33) 2091 9402

Fecha: 26 de julio de 2023.

Lugar: Ciudad de México.

Asistentes: 150 participantes.

Seguridad en América realiza *Roadshow* "Soluciones contra incendio"

Seguridad en América (**SEA**) realizó otra edición más de los *roadshows* de seguridad, en esta ocasión centrado en el tema "Soluciones contra incendios", contando con dos charlas magistrales impartidas por Javier Fernández Soto, director occidente de Mak Extiguisher; y Gerardo Ibarra Vizcaino, *Lead Instructor* de FTech. Además de contar con espacios para las asociaciones ASIS Capítulo México y la AMPCI (Asociación Méxicana de Protección contra Incendio). El *roadshow* fue presentado nuevamente por el equipo de **SEA**, Samuel Ortiz Coleman, director general; y Alex Parker, *Sales Manager*.

CHARLAS MAGISTRALES

En primer lugar, se presentó Javier Fernández Soto, director occidente de Mak Extinguisher, con la ponencia titulada "Aspectos relevante de los sistemas contra incendios", en la que habló de los sistemas contra incendio, los cuales su principal función es salvaguardar y proteger la vida de las personas, detectando, evaluando y alertando. La mejor manera de protegernos de algo es conociendo a nuestro enemigo, diariamente convivimos con el fuego en muchas instancias, pero obviamente es un recurso peligroso.

Javier definió a un incendio como una ocurrencia de fuego no controlada que puede afectar o abrasar algo, el fuego no controlado de grandes proporciones, el cual puede presentarse de manera instantánea o gradual, pudiendo provocar daños materiales, pérdida de vidas humanas y afectación al ambiente.

Después fue el turno de Gerardo Ibarra Vizcaino, *Lead Instructor* de la empresa Fire Technologies and Loss Prevention Specialists (Ftech), quien realizó una presentación acerca de los riesgos en bombas de agua por recalentamiento y el uso de las válvulas de recirculación y alivio de presión para evitar su sobrecalentamiento. En sus palabras, en las bombas existe una cantidad importante de componentes internos que están en constante movimiento y estas partes en movimiento necesitan ser lubricadas para mantenerse a temperaturas adecuadas. Dentro de la bomba de agua, el lubricante por excelencia es el agua, mientras el agua este fluyendo, la bomba se mantendrá a temperaturas adecuadas de operación.

Posteriormente tomó la palabra José Arturo Ortega, director de la Asociación Mexicana de Protección Contra Incendios (AMPCI), para hablar un poco de la asociación. ■

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**
  - Investigaciones Corporativas
  - Respuesta a Emergencias
  - Protección ejecutiva y Servicios de Inteligencia
  - Monitoreo
- **Servicios de Tecnología**
  - Videovigilancia
  - Controles de acceso
  - Diseño, Ingeniería e implementación de servicios

Nuestro compromiso es contribuir a la construcción de una cultura de trato igualitario y no discriminación y por ello nos sumamos al **Consejo para Prevenir y Eliminar la Discriminación de la Ciudad de México (COPRED)**, *siendo la primera empresa de seguridad privada que se suma a este gran acuerdo.*

GRAN ACUERDO
POR EL TRATO IGUALITARIO
CDMX

Contáctanos

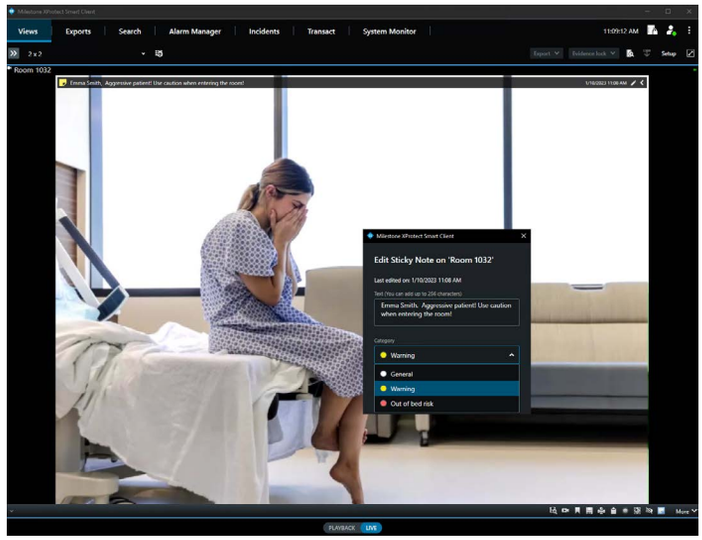
www.ausecurity.mx

(+52) 55 5337 0400

ALLIED UNIVERSAL®
SECURITY SERVICES
There for you.

Milestone Systems lanza XProtect ® Hospital Assist

XProtect ® Hospital Assist, ya disponible en el mercado, es una solución tecnológica de audio y video basada en datos, diseñada para optimizar la atención al paciente en entornos médicos. Este sistema avanzado permite a los profesionales de la salud monitorear de forma remota a varios pacientes al mismo tiempo, gracias a lo cual pueden responder rápidamente a posibles incidentes. Al agilizar las tareas diarias y mejorar la eficiencia del personal médico, XProtect ® Hospital Assist contribuye a aliviar de manera significativa la carga laboral que tienen los proveedores de atención médica en el dinámico entorno hospitalario de la actualidad. "No cabe duda de que el toque humano de los profesionales de la salud es esencial. Al incorporar tecnología de video basada en datos en sus actividades diarias, se potencia y mejora aún más su labor. XProtect ® Hospital Assist permite a los hospitales mejorar la calidad de la atención al paciente al ofrecer un respaldo adicional al personal médico", según afirmó Raúl Yadav, director de Tecnología de Milestone Systems. ■



SCATI presenta las cámaras Scati ThermalScan, visión 360° de grandes áreas sin puntos ciegos

SCATI lanzó las cámaras ThermalScan, que detectan, reconocen y rastrean un número ilimitado de objetivos (personas, vehículos, etc.) de forma automática, a gran distancia, incluso en las condiciones climáticas más adversas y en oscuridad total proporcionando imágenes de alta resolución. Cubren superficies de varios kilómetros de distancia sin dejar puntos ciegos gracias a su rotación de alta velocidad y al uso de avanzada tecnología de estabilización óptica de la imagen. Son ideales para la protección total de áreas muy extensas y con un perímetro irregular como puertos y aeropuertos, espacios naturales terrestres y marítimos, ya que su instalación minimiza los costes y simplifica la instalación y el mantenimiento frente a otras cámaras convencionales. Para la protección de las áreas más próximas al recinto a proteger, pueden tener asociadas Domos PTZ SCATI EYE, que se posicionarán automáticamente en aquellos puntos donde se detecte la intrusión. ■

CONSEJOS DE SEGURIDAD ANTE UN TERREMOTO

Septiembre es un mes en que la tragedia e incertidumbre viene a la memoria de los y las mexicanas, un mes en el que las coincidencias de la naturaleza han provocado desastres y un miedo inevitable en la población. Si bien, los sismos y terremotos no se pueden prevenir, sí se puede estar listo y reaccionar de la mejor manera para evitar una tragedia. A continuación le compartimos los cinco consejos de seguridad ante la presencia de un terremoto, que Roberto Jaramillo, consultor *Safety* / Protección Civil, nos compartió.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Siempre estar consciente de su entorno.** Conozca bien su vivienda, su lugar de trabajo, los sitios que frecuenta; ubique salidas de emergencia, rutas de evacuación y planes de emergencia.
2) **Prepárese y prepare a los suyos.** Tenga siempre a la mano una mochila de emergencia, que todos sepan el plan familiar de protección civil y capacitación básica para la supervivencia.
3) **Cuando escuche la alerta sísmica o el evento lo sorprenda, no pierda la calma y enfóquese.** Busque una zona de menor riesgo y repliéguese, espere a que el evento termine y siga las indicaciones del personal de seguridad o protección civil del lugar donde se encuentre. No salga corriendo, hoy sabemos que es más peligroso evacuar un inmueble como primera opción, ya que no conocemos los riesgos que hay afuera.
4) **No haga caso de la infodemia,** acuda a los sitios oficiales como el Centro Nacional de Prevención de Desastres y manténgase informado sólo por fuentes oficiales.
5) **Nunca olvide que… ¡Su vida es primero!** ■

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.

ÍNDICE DE ANUNCIANTES

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 2023	☐ $ 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 2023

ANERPV
Asociación Nacional de Empresas de Rastreo y Protección Vehicular

AMESP
Asociación Mexicana de Empresas de Seguridad Privada A.C.

ASIS INTERNATIONAL
CAPÍTULO MÉXICO 217

SEGURIDAD - PROTECCIÓN
CONFIANZA

ALARSEGM · B&A · UNIFORMAL · ασφάλεια · OEMPSA · Juvabe · INSTITUTO GAUDÍ

ασφάλεια
asfáleia
En Seguridad, el poder de la tecnología.

CREANDO IDEAS INNOVADORAS

MONITOREO DE FLOTAS - CONTROL DE ACCESOS - MONITOREO SATELITAL - GPS - CCTV

55 8438 2340 · GRUPOPAPRISA.COM · REDES SOCIALES

JUAN RACINE 112-PISO 3, POLANCO, POLANCO I SECC, MIGUEL HIDALGO, 11510 CIUDAD DE MÉXICO, CDMX

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.®

Guardias, guardias armados, custodias, custodias blindadas y custodias armada.

Cobertura a nivel nacional.

www.sepsisa.com.mx comercial@sepsisa.com.mx 55 5351 0402