SEGURIDAD® EN AMÉRICA

Año 25 / No.147
Noviembre-Diciembre

www.seguridadenamerica.com.mx

Especiales:

Seguridad en petróleo y energía

Soluciones de seguridad en *Data Centers* y TI

Reportaje: Seguridad en la industria alimentaria

COBERTURA NACIONAL

A QUIEN VALOR MERECE

- SERVICIOS DE MONITOREO
- SISTEMAS ELECTRÓNICOS DE SEGURIDAD
- CUSTODIAS DE TRANSPORTE
- TÉCNICOS EN SEGURIDAD PATRIMONIAL

@MultiprosegOficial @MULTIPROSEGOFICIAL MULTIPROSEG OFICIAL

ALGUNOS DE NUESTROS CLIENTES

AUDI, TELCEL, CEMEX, DAIMLER TRUCK, NIKE, PROLOGIS, GENERAL ELECTRIC, FEMSA

AMESP

CDMX
CIUDAD DE MÉXICO

CNS

ASIS INTERNATIONAL

redconocer
de prestadores de servicios
Entidad de Certificación y Evaluación

ISO

BAC

ema
entidad mexicana
de acreditación, a.c.

ANERPV

COPARMEX

REPSE
Registro de Prestadores de Servicios Especializados u Obras Especializadas

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

Contamos con cobertura
EN TODOS LOS ESTADOS DE LA REPÚBLICA MEXICANA
con la estructura de oficinas regionales
y un CORPORATIVO.

AV. ARMADA DE MÉXICO 1500,
RESIDENCIAL CAFETALES,
C.P 04930, DELEG. COYOACÁN.

+ 52 (55) 79599598

INFO@MULTIPROSEG.COM.MX

SEGURIDAD EN AMÉRICA

Dirección General
Samuel Ortiz Coleman, DSE
samortix@seguridadenamerica.com.mx

Asistente de Dirección
Katya Rauda
krauda@seguridadenamerica.com.mx

Coordinación Editorial
Tania G. Rojo Chávez
prensa@seguridadenamerica.com.mx

Coordinación de Diseño
José Arturo Bobadilla Mulia

Administración
Oswaldo Roldán
oroldan@seguridadenamerica.com.mx

Reportera
Mónica Ramos
redaccion1@seguridadenamerica.com.mx

Medios Digitales
Estefania Hernández
mdigital@seguridadenamerica.com.mx

Circulación
Alberto Camacho
acamacho@seguridadenamerica.com.mx

Actualización y Suscripción
Elsa Cervantes
telemarketing@seguridadenamerica.com.mx

María Esther Gálvez Serrato
egalvez@seguridadenamerica.com.mx

Ejecutivas de Ventas
Gabriela Rueda
grueda@seguridadenamerica.com.mx

Luz María González Medina
luz@seguridadenamerica.com.mx

Año 25 / No. 147 / Noviembre | Diciembre / 2024

Portada:
SISSA

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

COMPARTE ESTA REVISTA
COMPARTIR ES RECICLAR

Conmutador: 5572.6005
www.seguridadenamerica.com.mx

Apoyando a:

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

Veinte años brindando servicios profesionales de seguridad

ASIS

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

EDITORIAL

El Índice Gallup de Seguridad Pública 2024 evalúa las experiencias de la población en 140 países frente a delitos violentos (robos, asaltos, atracos), su percepción de seguridad en general y su confianza en las fuerzas del orden durante el año. Según el reporte, América Latina y el Caribe siguen siendo una de las regiones donde la gente se siente más insegura y una de las áreas con menor confianza en la policía a nivel global.

De acuerdo con InSight Crime, detrás de esto está la inseguridad impulsada por el narcotráfico, el crimen organizado y la corrupción, que ha alimentado un sentimiento de vulnerabilidad en los habitantes de la región. Esto ha llevado a que América Latina haya sido clasificada como una de las regiones con peor percepción de seguridad a nivel global desde 2015, cuando comenzaron las encuestas del Índice Gallup de Seguridad Pública.

Pese a esta realidad, las cifras han mostrado una lenta, pero constante mejoría a partir de 2017. Sin embargo, las percepciones de seguridad varían ampliamente entre los países de la región, con algunos experimentando profundas crisis de violencia, mientras que otros han logrado mejorar sus indicadores.

Entre los países latinoamericanos incluidos en el índice, aquellos que mostraron una mejora en sus puntajes respecto al año anterior fueron El Salvador, Uruguay, Guatemala, Honduras, Paraguay y República Dominicana. En contraste, Chile, Argentina, Colombia, Perú y Ecuador experimentaron un descenso en sus resultados, mientras que Venezuela y México mantuvieron los mismos niveles que el año anterior. Sin embargo, el estudio tiene algunas limitaciones, no cubriendo algunos países como Haití, que desde 2021 se encuentra sumido en una crisis de seguridad.

PANORAMA EN MÉXICO

Durante el primer semestre de 2024, 14.2% de la población adulta en México ha tenido contacto con autoridades de seguridad pública, de ese porcentaje, 47.5% declaró haber sufrido, al menos, un acto de corrupción por parte del personal de las instituciones de seguridad, según datos del Instituto Nacional de Estadística y Geografía (INEGI).

De acuerdo con la Encuesta Nacional de Seguridad Pública Urbana (ENSU), se calcula que durante el primer semestre del año casi 26% de los hogares tuvo, como mínimo, un integrante que fue víctima de al menos un delito, como: robo total o parcial de vehículo, robo en casa habitación, robo o asalto en la calle o transporte público, así como robo en forma distinta a las anteriores o extorsión.

Ante los números de crímenes y la percepción de la inseguridad, 39.3% la población encuestada señaló que ha modificado rutinas en cuanto a permitir que sus hijos o hijas menores salgan de su vivienda; 38.8% dijo que habían cambiado sus hábitos al caminar por los alrededores de su vivienda después de las 08:00 de la noche y el 24.3% cambió su rutina relacionada con visitar parientes o amistades.

De la población encuestada que percibió como muy o algo efectivo el desempeño de las instituciones de seguridad pública para prevenir y combatir la delincuencia, 86.9% identificó de manera positiva a la Marina; 82.9% al Ejército; 82.4% a la Fuerza Aérea Mexicana; 74%, Guardia Nacional; 56.8%, policía estatal, y 48.7% a la policía preventiva municipal.

Estimado lector, ¿qué percepción tuvo usted de la inseguridad en su país durante 2024? Envíe sus comentarios y/o sugerencias a prensa@seguridadenamerica.com.mx

***Seguridad en América** le desea felices fiestas y un próspero año nuevo 2025, lleno de abundancia y seguridad.* ■

SISSA DIGITAL

Aliados de la transformación digital

www.sissadigital.com

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 Jesús De Miguel Sebastián, Coronel del Ejército de Tierra de España en Retiro y socio fundador de Two Worlds Collaborative Intelligence, 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 acerca del experto, consulte su currículo:

ENTREVISTA EXPRÉS CON

Elías Valencia Gómez,

gerente de Desarrollo de Negocios en SISSA Monitoring Integral

¿Considera al Nearshoring como una oportunidad de negocio para la seguridad electrónica?

El *nearshoring* en México es una oportunidad muy interesante de negocio para la seguridad electrónica, ya que esta estrategia atrae una gran cantidad de inversión extranjera debido a su proximidad con Estados Unidos y otros mercados clave. Las necesidades de seguridad electrónica en estas inversiones son siempre latentes, especialmente para proteger instalaciones, datos y activos críticos. Además, va de la mano con la reducción de riesgos, optimización de costos y eficiencia operativa, factores esenciales para que el negocio sea exitoso. México, con su infraestructura en crecimiento, presenta un entorno ideal para implementar soluciones avanzadas en este ámbito. ■

Uncover The Unseen™

GARRETT

¡Paragon establece el estándar para el futuro!

Ambiscan

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

ESCANEAR PARA MÁS INFORMACIÓN

MADE IN THE USA

ÍNDICE

Noviembre | Diciembre


Con Grupo IPS, aterriza en el
futuro de la seguridad
IPS
Conoce más de nosotros
30 AÑOS DESDE 1995
ESR
Great Place To Work.
GPTW
SUPER EMPRESAS 2024
COPARMEX CIUDAD DE MÉXICO
ASLIME
CCE
55-5525-3242
grupoipsmexico.com

SCATI ANALYTICS, REVOLUCIONE LA VIDEOVIGILANCIA CON IA

Una solución avanzada que permite a los profesionales de la seguridad y a los analistas de negocio obtener información valiosa de las imágenes de sus cámaras de videovigilancia en tiempo real

ESPAÑA

SCATI, fabricante de soluciones inteligentes de seguridad, presenta SCATI ANALYTICS, una suite avanzada de analíticas de video basada en inteligencia artificial (IA), diseñada para ofrecer un nivel sin precedentes de seguridad y eficiencia operativa.

Esta innovadora solución no sólo mejora significativamente la seguridad, sino que ofrece un valor agregado significativo en el ámbito de la inteligencia de negocio, permite a los usuarios finales anticiparse a los eventos, protegiendo activos y optimizando operaciones estratégicas.

Además, ofrece un amplio abanico de analíticas avanzadas, adaptándose a las necesidades más dinámicas de la seguridad y de la inteligencia de negocio.

SCATI ANALYTICS REVOLUCIONA LA VIDEOVIGILANCIA CON IA Y ADEMÁS PERMITE:

1) **Reducir falsas alarmas:** Mediante sofisticados algoritmos de IA, SCATI ANALYTICS reduce significativamente las falsas alarmas, permitiendo a los usuarios concentrar sus recursos en alertas verídicas y relevantes, optimizando así la eficiencia y eficacia del sistema de seguridad.
2) **Detectar amenazas de manera proactiva:** La capacidad de identificar comportamientos inusuales y amenazas potenciales en tiempo real permite una respuesta rápida y eficaz, garantizando una seguridad preventiva y proactiva.
3) **Analizar comportamientos:** Más allá de la mera observación, SCATI ANALYTICS analiza patrones de comportamiento, ayudando a prever situaciones antes de que ocurran y optimizando la gestión de la seguridad.
4) **Fácil de usar y gestionar:** La administración centralizada de todos los servidores desde el VMS SCATI WATCHER permite una gestión integral y eficiente, con recepción de alarmas en tiempo real y registros históricos accesibles para revisiones y análisis posteriores.
5) **Integración con Business Intelligence:** SCATI RECKON permite la explotación avanzada de metadatos, ofreciendo la capacidad de crear gráficas y cuadros de mando personalizados para una mejor gestión de los sistemas de seguridad y una consciencia situacional completa.

SCATI ANALYTICS se adapta a cualquier tamaño de instalación, desde pequeños negocios hasta grandes corporaciones. Gracias a su capacidad de aprendizaje continuo, mejora constantemente su precisión y eficiencia a lo largo del tiempo. Su flexibilidad permite una integración con los sistemas existentes y herramientas avanzadas para optimizar la seguridad y apoyar la toma de decisiones estratégicas. ■

Fuente y fotos: SCATI

GSI

FABRIL S.A. DE C.V.®

VER CATÁLOGO

NUESTRA SEGURIDAD BANCARIA ES LA GARANTÍA DE SU TRANQUILIDAD

BLINDAJE

Blindaje personalizado para vehículos y sucursales bancarias, garantizando seguridad con materiales de alta resistencia que superan los estándares de calidad establecidos en el mercado.

SEGURIDAD BANCARIA

Fabricamos ventanillas, esclusas, cofres, muros blindados y puertas de seguridad para bancos, ofreciendo protección confiable contra amenazas, con materiales de alta calidad

CAJAS DE SEGURIDAD

Desarrollamos cofres de seguridad de alta tecnología con nuestra patente exclusiva de núcleo cerámico, brindando máxima protección y durabilidad ante cualquier intento de vulneración.

www.gsifabril.com | ventas@gsifabril.com.mx | WhatsApp: +52 1 5611785324 @gsi.fabril

TRANSPORTE SEGURO DE MERCANCÍAS

Establecer acciones y controles son una necesidad para todas las empresas que brindan servicios de transporte

Foto: Freepik

COLOMBIA | **John Mario Pérez Morales**

Colombia como los demás países que son hacen parte de la región han expresado su interés por fortalecer los controles relacionados con su cadena de suministro nacional e internacional, a través de diferentes esfuerzos que han sido señalados por la Organización Mundial de Aduanas OMA[1], a través del reconocimiento que otorga al Operador Económico Autorizado (OEA), a aquellas empresas que demuestren su compromiso en materia de seguridad, en toda su cadena logística, adoptando no sólo las mejores prácticas sino dando cumplimiento a los requisitos establecidos en sus componentes.

A nivel global siempre hemos pensado en la profesionalización del hombre de seguridad, siendo ésta una prioridad para las empresas que brindan servicios de seguridad privada, para ello hemos considerado un sinnúmero de factores que involucran habilidades, conocimientos, entrenamientos y evaluación de integridad. Las necesidades y alcances de los servicios de seguridad hoy van más allá del manejo de controles de acceso y monitoreo en salas de circuito cerrado de televisión, las compañías requieren un soporte robusto en la seguridad y monitoreo de la carga, la inspección en el llenado de contenedores, así como el seguimiento de rutas hasta la entrega de productos en última milla.

En los planes de continuidad del negocio (BCP), dedicamos un capítulo específico al aseguramiento de la carga, siendo esta responsabilidad parte de acuerdos de nivel de servicio de las compañías, establecidos en sus relaciones contractuales, tiempo de entrega, condiciones de la carga y seguridad que permitan a las compañías alejarse de posibles contaminaciones, riesgos que deben estar identificados y tratados, con un riesgo residual, producto de controles efectivos que puedan evaluarse periódicamente.

La forma como se embalan los productos cuando se trata de estibas paletizadas, con almacenamiento adecuado y cubitaje cuando se trata de producto a piso o, como comúnmente se le conoce, arrume negro, que eviten en destino averías por errores cometidos durante el procedimiento, así como el medio de transporte adecuado, pueden evitar pérdidas innecesarias, algunas empresas no consideran importante este aspecto y transportan cargas en cama bajas aseguradas solamente con bandas, sin carpa, con exposición total al impacto climático y al posible accionar criminal de los delincuentes.

DESDE ORIGEN

La seguridad de la carga inicia desde los despachos de nuestra mercadería en origen desde donde nos deben indicar en qué condiciones realizaron el llenado del contenedor o demás unidades de carga, continuando con su llegada a puertos o aeropuertos donde la agencia de aduanas que opera para las compañías deberá reportar de forma inmediata al área de Seguridad, si un despacho ha sufrido apertura por etiquetado o inspección antinarcóticos.

Aquí es importante precisar que estos controles de la fuerza pública son aleatorios y se producen en cualquier momento. Una vez surtido el proceso de desaduanamiento inicia el monitoreo terrestre y trazabilidad de la carga, seguimiento que realizamos a través de plataformas tecnológicas de rastreo satelital. Las operaciones pueden variar de cara a los diferentes sectores de la economía, pero es importante comprometer a los aliados estratégicos para que generen sus reportes de recepción de la carga, ya sea insumos y materia prima que pasarán a proceso de maquila o a zonas de almacenamiento con producto terminado.

Durante la asignación de conductores que hacen parte de la flota de transporte de la carga de las compañías, se requiere la identificación completa de los mismos, así como el conocimiento previo de las condiciones del contenedor que será utilizado en procesos de exportación, esta actividad que puede ser evidenciada mediante *e-mail*, evita gastos innecesarios a la operación, toda vez que se vuelve en un control inicial del estado real del contenedor, evitando así cambios

FACILITAR SOLUCIONES QUE BRINDEN CONFIANZA PARA UN MEJOR FUTURO

www.sissamx.com

que generarán demoras en el cargue afectando la reserva y tiempos de entrega en motonave.

Las empresas de transporte deberán aportar su plan de contingencia donde contemplen los riesgos que han identificado en su operación, así como: las acciones de mitigación, como accidentes de tránsito, robos, bloqueos, protesta y conflictividad social, afectaciones viales por factores climáticos, cierre de aduanas, fallas mecánicas, cambio de ruta, daño de vehículos, transbordo, sabotaje, cargue o descargue, inspecciones de seguridad, como los más importantes.

ESTANDARIZAR PROCESOS

Las compañías que brindan los servicios del transporte de mercancías son parte del grupo de asociados de negocio, y como tal requieren una verificación de cumplimiento, con barrido de listas restrictivas nacionales e internacionales, así como el *vetting* que debe realizarse a sus conductores, aquí debo hacer precisión porque muchas compañías manejan la figura del conductor y vehículo fidelizado, sin importar la relación contractual todos deberán contar con una verificación que incluya antecedentes criminales, dicha actividad deberá tener un periodo de actualización específico.

Estandarizar procesos y procedimientos con acciones de control y evidencias que permitan mantener la seguridad en una facilidad se vuelve entonces en un reto para las empresas de seguridad privada, ya que son ellos quienes apoyan los resultados de la gestión de seguridad y riesgos, hombres bien entrenados, con roles claramente definidos generan excelentes resultados a las compañías. No podemos confundir la reducción de costos de un presupuesto con eliminar posiciones en seguridad que dejen brechas o una alta exposición a la materialización de riesgos. La tecnología apoya la acción o reacción del factor humano.

Los programas de inducción y reinducción para divulgar las políticas y estándares de seguridad de una organización, así como los escenarios de amenazas son una obligación, pues nos permiten minimizar exposiciones, generar consciencia y mantener actualizada especialmente a la fuerza de venta del riesgo público y los escenarios de afectación.

RIESGOS Y CÓMO ENFRENTARLOS

El transporte de la carga está expuesto a diferentes factores que pueden comprometer no sólo la integridad del producto, sino también la seguridad de los operadores, me permito mencionar algunos:

- **Averías.** Producto del mal manejo de la mercancía, durante el llenado o descarga.
- **Accidente de tránsito.** En algunas ocasiones producto de micro sueños que terminan en colisiones por alcance, volcamiento, con lesiones o muertes y pérdida total de la mercancía.
- **Casos de hurto bajo la modalidad de piratería terrestre o asalto.** Casos de hurto en movimiento de mercancía, o eventos de acciones criminales planeadas.
- **Hurto en Centros de distribución.** En muchas ocasiones y bajo la experiencia de múltiples investigaciones, el hecho de encontrar productos en el mercado con varias referencias del portafolio por debajo del costo real del mismo, puede tratarse de saqueo.
- **Condiciones ambientales extremas.** Excesiva lluvia con vehículos carpados que puedan llegar a afectar la mercancía.
- **Riesgo cibernético.** Hackeo de los sistemas de gestión de transporte, comprometiendo la información propia y de clientes de la organización.
- **Riesgo público.** Que se puede materializar como ataque terrorista, vandalismo y la más grave contaminación de la carga por narcóticos o armas.

Establecer acciones y controles serán entonces una necesidad para todas las empresas que brinden servicios de transporte, para ello deberán considerar o implementar mínimas medidas de seguridad entre las cuales están:

- Capacitación constante del personal.
- Uso de tecnología avanzada para el monitoreo y rastreo de mercancías.
- Implementación de protocolos de seguridad robustos.
- Contratación de seguros adecuados para cubrir posibles pérdidas o daños.
- Colaboración con proveedores de transporte confiables y experimentados.
- Cumplimiento estricto de las regulaciones y normativas aplicables.

Estas estrategias pueden ayudar a reducir significativamente los riesgos y asegurar un transporte más seguro y eficiente de las mercancías.

El reto estará entonces en lograr impactar toda la operación de manera positiva siendo un soporte transversal a todas las áreas funcionales, buscando un objetivo común que es mantener la continuidad del negocio. ■

Referencias:

[1] *OMA (Organización Mundial de Aduanas.*

John Mario Pérez Morales, oficial en uso de buen retiro de la Policía Nacional y especialista en seguridad.
Más sobre el autor:

EMPRESA DE SEGURIDAD ELECTRÓNICA

SYSTEM AI

- Sistema de CCTV
- Sistema de Alarmas
- Detección y Extinción de Incendio
- Control de Acceso
- Project Management
- Centro de Monitoreo
- Domótica

COMEXA 30 años

Totalmente conectado a ti

comexa_seguridad · comexa · ComexaSeguridad

www.comexa.com.mx • ventas@comexa.com.mx

Ignacio Zaragoza 73 • Col. Barrio Santa Catarina • Coyoacán, 04010 • CDMX

55 5685 7830 † 55 5685 7837 • 800 2 COMEXA

III EDICIÓN DE LA CUMBRE **DE SEGURIDAD CORPORATIVA**

Más de 200 responsables de seguridad reunidos para fortalecer y actualizar sus conocimientos en Prevención, Tecnología, Metodología y Seguridad en la Cadena Logística

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Seguridad en América, fuente de conocimiento y actualización, llevó a cabo la III edición de la Cumbre de Seguridad Corporativa, los días 28 y 29 de agosto en el Hotel Courtyard Mexico City (CDMX), en donde se reunieron más de 200 responsables del área de Seguridad para escuchar en voz de reconocidos y certificados especialistas, temas como: Estrategias de prevención contra el robo de carga en México; Métricas de Seguridad en la Cadena de Suministro; Diseño e implementación de KPIs para mitigar incidentes y pérdidas; Modelos de seguridad privada y su adaptación regulatoria, laboral y tecnológica; entre otros.

Durante la ceremonia de inauguración, Samuel Ortiz Coleman, director general de **SEA**, reiteró la importancia de este tipo de foros para compartir información, análisis, estrategias y tecnología que fomenten la seguridad, no sólo de las compañías a las que representan, sino también a la seguridad de México. "Este año, y contemplando la situación actual del país y sus distintas industrias, decidimos enfocarnos en la cadena logística, la cual enfrenta retos diferentes cada día, y de la que dependen millones de personas", comentó.

Los encargados de realizar el corte de listón, fueron los presidentes de las asociaciones más importantes de Seguridad en México, entre ellos: Armando Zúñiga Salinas, presidente de ASUME; Luis Enrique Villatoro, analista de Inteligencia y miembro del Consejo Directivo de ANERPV, en representación de David Román Tamez, presidente de ANERPV; Ana Guzmán, presidenta de AMEXSI; Carlos Martínez, presidente de ALAS Comité Nacional México; Gabriel Bernal, presidente de AMESP; Gadi Mokotov, presidente del CNB; Héctor Romero, presidente de Círculo Logístico; Héctor Coronado, presidente de GEMARC; José Luis Alvarado, presidente de ASIS Capítulo México; Ricardo Bustamante, presidente de AMESIS; Ricardo León, secretario general del CNSP, y en representación de Adalberto Ortiz Ávalos, presidente de COPARMEX Ciudad de México, Manuel Arcos Aguirre, integrante del Órgano de Gobierno de COPARMEX CDMX.

"Hoy más que nunca, la colaboración y el intercambio de conocimiento son esenciales. La Cumbre de Seguridad Corporativa reúne a especialistas, líderes y profesionales del sector, los cuales forman parte de reconocidas empresas a nivel nacional e internacional, creando un espacio para compartir experiencias, innovaciones tecnológicas y estrategias efectivas de prevención, gestión de riesgos, reacción y continuidad del negocio, un aporte invaluable para poner en práctica, gracias a todos ellos por sumarse a esta iniciativa de profesionalización", expresó Samuel Ortiz Coleman.

TENDENCIAS TECNOLÓGICAS PARA LA CADENA LOGÍSTICA

Uno de los objetivos de la Cumbre es compartir la tecnología que fomenta la prevención, reacción y aseguramiento de la cadena logística. Es por eso que diferentes socios comerciales presentaron, en el área de *networking*, las soluciones más innovadoras en seguridad, entre ellos: detecta, MOPEC Security, Verkada, M360, SCATI, Solcat, Multiproseg, Altair, Cymez, Prosegur Security, IPS, itisa, Bosch, MSPV Seguridad Privada, JVP, y Eagle Eye Networks.

"A lo largo de estos dos días, tendremos la oportunidad de escuchar a ponentes destacados, y las soluciones que nos ofrecen nuestros socios comerciales, a quien agradezco la confianza, compromiso e interés por ser parte de esta tercera edición y quienes son fundamentales para el éxito de esta Cumbre, con ellos podremos establecer conexiones valiosas que fortalecerán nuestra red de seguridad", puntualizó el director general.

SEA: FUENTE DE CONOCIMIENTO Y ACTUALIZACIÓN

Con un total de 12 conferencias a cargo de más de 25 ponentes, los asistentes a la III Edición de la Cumbre de Seguridad Corporativa realizaron un total de 16 horas de formación académica. La primera conferencia llevó por título: "Fortaleciendo la Seguridad: Colaboración Empresarial y Gubernamental en la Cadena de Suministro", a cargo de César Cruz González, *Head of Security & Criminal Compliance* de Sigma Alimentos, junto con Klaus Ortiz Lohse, director de Seguridad de Grupo Alfa. Este binomio destacó la importancia de realizar estrategias de seguridad que integren a las autoridades, y así puedan robustecer la reacción ante el robo en tránsito o la recuperación de éste.

La siguiente conferencia fue impartida por Eduardo Hernández Ruíz, *Supply Chain Security Council* del Consejo de Seguridad en Cadena de Suministro; y Gastón Cedillo Campos, director del Laboratorio en Sistemas de Transporte y Logística, con el tema "Seguridad en Cadena de Suministro en el Contexto del *Nearshoring*". Por su parte, Octavio García Peregrina, CPP, gerente de Seguridad y Protección de Farmacéuticos Maypo; y José Luis Sánchez Gutiérrez, DSE, director de Protección Patrimonial, hablaron sobre la "Seguridad en Movimiento: Protegiendo la Cadena Logística".

Y uno de los especialistas que no podía faltar en la Cumbre, ya que su aporte es de suma importancia por toda la trayectoria que tiene en el sector, y fue Antonio Gaona Rosette, director de Seguridad de Codere, quien, junto con Raúl Rojas González, *Country Security Facility Manager* de CEMEX, hablaron sobre las experiencias de éxito que han tenido en la cadena logística de la Industria del Tabaco, *Retail* y Construcción.

Uno de los binomios que sorprendió con la dinámica de la conferencia, fue el de Natalia Cerutti Pereyra, *Sr. Global Security Manager* de Marelli; y Darío Preza, *Head of Corporate Security* de Mabe Global, planteando si acaso la Seguridad a la Cadena de Suministro en México es una misión imposible, percatándose a través de diferentes preguntas a los asistentes, sobre cuáles son los principales retos y riesgos a los que se enfrentan, no sólo las industrias del país, sino los propios habitantes, que de alguna manera esa situación contribuye o afecta la seguridad de estas.

En esta edición, se realizó un panel de especialistas en seguridad logística integrado por: Luis Enrique Villatoro Martínez, director de Inteligencia LATAM de Overhaul; Yolanda Bernal Sánchez, Líder de Comité logístico de ASIS Capítulo México; David Román Tamez, presidente de ANERPV; Juan Omar Trujillo Zurita, CPP, director general de GC-Protección Seguridad Privada; y José Luis Alvarado Martínez, presidente de ASIS Capítulo México, quienes compartieron diferentes estrategias de prevención contra el robo de carga en México.

Para finalizar la primera jornada de conferencias, el Cap. Julio César Balderas Mora, director de Seguridad Patrimonial de Casa Cuervo, y Francisco Reynoso Chávez, gerente de Seguridad Patrimonial de Casa Cuervo, hablaron sobre la importancia y el valor de "la confianza" en las empresas. Tanto la que generas con tus propios colaboradores, como la que, de estos, parte hacia los clientes.

SEGUNDA JORNADA DE NETWORKING

El segundo día de conferencias inició con José Manuel Rodarte Méndez, consultor *senior* de PPR Consulting; y Héctor Raúl Martínez Galván, *Global Security Manager* de Bombardier, con el tema "Puntos a considerar en la estrategia de Seguridad para la Cadena de Suministro". Le siguió el binomio conformado por José Luis Saavedra Hernández, gerente Corporativo de Seguridad Patrimonial de Grupo Corporativo Papelera; y Miguel Vázquez Narváez, capacitador y asesor en carga aérea para recintos fiscalizados, quienes hablaron sobre los tópicos de Seguridad en la Cadena de Suministro de la Carga Aérea.

Por su parte, Dagoberto Santiago Toledo, director de Seguridad *Senior* LATAM de PespsiCo; y Enrique Sansores Barreda, director de Seguridad de PepsiCo México, expusieron el tema: *'Perfect Delivery'*. Mientras que Eduardo Jiménez Granados, *Corporate Security Manager* de Diageo México; e Isadora de Ávila Ruíz, de Kellogg´s, explicaron cuáles son y cómo pueden utilizarse las métricas de Seguridad en la Cadena de Suministro, su diseño e implementación de KPIs para mitigar incidentes y pérdidas.

El siguiente binomio estuvo integrado por David Bautista Mata, director de Seguridad e Inteligencia de Detecta, y Jorge Uribe Maza, director Comercial de Grupo IPS México, quienes dieron una charla sobre los modelos de seguridad privada y su adaptación regulatoria, laboral y tecnológica.

Y para cerrar la tercera edición de la Cumbre de Seguridad Corporativa, Julio César Porras Avitia, gerente de Seguridad Corporativa de Cil Group; y María Araceli Rivera Murillo, *Foreign Trade Customs & Compliance* México de Grupo Daltile, subieron al escenario para hablar de las estrategias a implementar para construir una Cadena de Suministro segura, requiriendo el involucramiento y la colaboración de todos los participantes en ésta. ■

Fotos: Mónica Ramos / SEA

JVP
LOGÍSTICA

PROTECCIÓN
Ejecutiva
Especializada

BENEFICIOS:

MONITOREO
24/7

- Flota aérea con disponibilidad inmediata.
- Análisis y seguimiento de ruta en tiempo real.
- Personal local en la mayoría de las principales ciudades en la República Mexicana, Sudamérica, EU y Europa.
- Traslados de seguridad ejecutiva especializada.

jvplogistica.com

@jvplogistica

@jvplogistica

55 81 08 05 87

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:

INTRODUCCIÓN A LA RESISTENCIA AL FUEGO

EUA

La resistencia al fuego (RF) se refiere a la habilidad de un material o estructura para soportar la exposición a las altas temperaturas de un incendio, sin perder su integridad estructural o convertirse en un peligro para la seguridad de los ocupantes del edificio o los bomberos que tratan de controlar el incendio. Se mide sometiendo un material o ensamblaje a una prueba estandarizada en un laboratorio de resistencia al fuego. La prueba mide cuánto tiempo el material puede mantener su capacidad de carga, aislamiento e integridad mientras está expuesto al fuego. La duración del tiempo en que el material mantiene esta integridad exitosamente se registra como su clasificación de resistencia al fuego.

Por consiguiente, la resistencia al fuego se mide en términos de tiempo, en horas o minutos, aunque esto no necesariamente denota cuánto tiempo un material podría soportar un incendio antes de que falle o pierda su eficacia. Sin embargo, la metodología para determinar la RF de un elemento constructivo y lo que implica esa resistencia al fuego, son temas mucho más complejos que trataremos de discernir a continuación.

En el Manual de Protección Contra Incendios de la NFPA, yo escribí lo siguiente sobre la resistencia al fuego: "Muchos aspectos relacionados con este tema son para nosotros en Latinoamérica conceptos que intuitivamente pensamos que son ventajosos para nuestra manera de construir. Tenemos todavía una construcción robusta basada en ladrillo y concreto, que en la mayoría de los casos tiene una resistencia al fuego importante. Por otro lado, construimos edificios relativamente pequeños donde tradicionalmente no hemos tenido mayores problemas de protección contra incendio".

"Sin embargo, el problema de la protección contra incendios en Latinoamérica está centrado en los edificios grandes, edificios que estamos construyendo cada vez más con arquitecturas abiertas y novedosas, con elementos estructurales más expuestos, con terminados interiores altamente combustibles y copiando la arquitectura de países más desarrollados, donde existe una tradición arraigada de seguridad contra incendios. Es allí donde estamos encontrando problemas"[1].

Debería dejar por sentado que los métodos constructivos que se utilizan en edificios grandes, como el de la Foto 1, son muy similares en Estados Unidos como en Latinoamérica, típicamente con concreto o elementos no combustibles. La principal diferencia entre los Estados Unidos y nosotros se centra en la construcción residencial, donde en el país del norte, ésta es principalmente en madera, como se muestra en la Foto 2.

Foto 1- Los métodos constructivos de edificios grandes son similares tanto en Estados Unidos como en Latinoamérica.

Foto 2 - Residencia en construcción con elementos en madera.

MEXSEPRO

SEGURIDAD Y PROTECCIÓN DE MÉXICO

Somos la primer empresa ***Next Generation*** en seguridad Privada

[SEGURIDAD | inteligente]®

Para tu seguridad, nuestros servicios constan de:

- **Control de riesgos efectivo y eficaz**
- **Nos basamos en los análisis de investigaciones, evidencia, indicadores y hechos históricos**
- **Diseñamos tu Sistema integral de seguridad**

5 años

como la única y verdadera seguridad inteligente en México, registrado ante el IMPI.

SESIM®

Sistema Empresarial de seguridad inteligente Mexsepro

Orgullosamente MEXICANOS

Contamos con plataforma propia para el control de nuestras Operaciones y de Capital Humano

Nuestras nuevas oficinas corporativas SP MEXSEPRO

Artemio Alpízar Ruz No. 341 Int. 02, Colonia San Miguel, Alcaldía Iztapalapa, C.P. 09360, Ciudad de México

- mexsepro.com
- (55)65854448
- (55)80620154
- facebook.com/MEXSEPRO
- instagram.com/mexsepro
- twitter.com/spmexsepro

CÓDIGOS DE CONSTRUCCIÓN

En esos países donde existe un código de construcción moderno, estos códigos, además de requerir sistemas contra incendios y medios de evacuación, establecen requisitos mínimos de RF para ayudar a mantener la integridad estructural. Tanto el Código Internacional de la Construcción (IBC) como el Código de Construcción y Seguridad (NFPA 5000), definen los tipos de construcción de los edificios basados en una certificación de la resistencia al fuego de los elementos estructurales.

Hoy en día, la RF que debería tener un edificio se establece a través de una evaluación de su área construida, número de pisos, altura, porcentaje de fachada y distancia a otros edificios, dependiendo de la ocupación del edificio. Esto quiere decir que un edificio con una ocupación más riesgosa, por ejemplo, un hospital, debe tener una resistencia al fuego más alta que la de un edificio similar con una ocupación menos compleja, como por ejemplo una tienda mercantil, aunque tengan la misma área constructiva, número de pisos y altura. El IBC o la NFPA 5000 explican esto con mayor detalle, donde se establecen, dependiendo del código, 9 a 10 tipos de construcción diferentes para los edificios. En la normativa NFPA, estos tipos de construcción están definidos en la NFPA 220, Norma Sobre los Tipos de Construcción de Edificios.

RF DE UN ELEMENTO CONSTRUCTIVO

Las resistencias al fuego de los elementos constructivos se evalúan bajo tres criterios o parámetros principales:

1) Mantener la integridad estructural, estabilidad o habilidad de soportar una carga a pesar de la exposición al incendio. En otras palabras, evitar colapso durante el incendio.

2) Proporcionar una barrera física para restringir la propagación del incendio, es decir evitar el paso de las llamas.

3) Proporcionar aislamiento térmico de manera que la transmisión térmica se limite de forma que no se produzca la ignición de la superficie no expuesta, ni de cualquier material situado en la proximidad a esa superficie.

La manera más conocida para establecer la RF de un elemento constructivo es a través de un ensayo en un horno de pruebas de resistencia al fuego, como el mostrado en la Foto 3. En este sentido, la RF de vigas, columnas, puertas, secciones de pared, protecciones de penetraciones y juntas, etc., queda determinada por su rendimiento en este horno que se calienta siguiendo la curva normalizada tiempo-temperatura. Estas pruebas están diseñadas para elementos constructivos donde su resistencia al fuego generalmente se determina en términos de una RF de 20 min, 30 min, 45 min, una hora, 1.5 horas, dos horas, tres horas o cuatro horas.

Foto 3 – Horno de pruebas de resistencia al fuego para elementos constructivos.

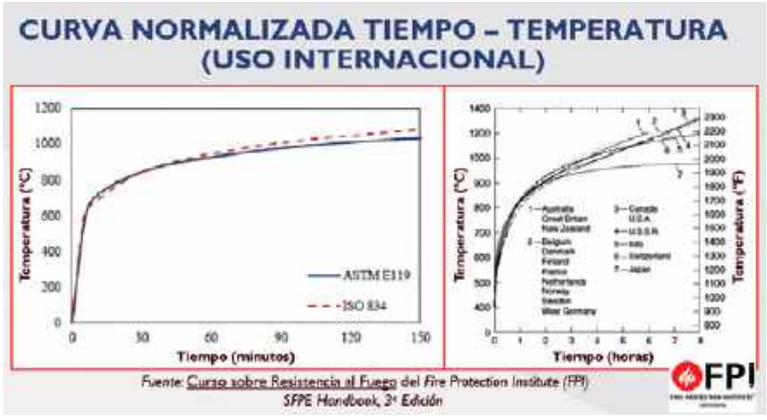
CURVA TIEMPO-TEMPERATURA NORMALIZADA

Los primeros conceptos de ingeniería de protección contra incendios que trataron de cuantificar la severidad de los incendios fueron sobre el impacto que los incendios tenían en la estabilidad estructural de los edificios. Una de las primeras pruebas a elementos RF se efectuaron en un club de arquitectos en Londres en 1790[2]. Pero no fue sino hasta un siglo después, luego del Gran Incendio de Baltimore en 1904, el cual fue iniciado por el colapso de un edificio de 10 pisos mientras estaba incendiado, que en la Universidad de Columbia en Nueva York se empezó a estudiar el tema de cómo probar la resistencia al fuego de un edificio[3].

Fue así como la curva normalizada tiempo-temperatura, que hoy día es utilizada de manera casi idéntica a nivel mundial, fue ideada. Esta curva tiempo-temperatura ha sido definida, por más de 100 años, en la ASTM E119, Métodos Estandarizados de Pruebas para Ensayos de Resistencia al Fuego de Edificios y Materiales de Construcción.

Las normas internacionales, lideradas por ISO 834, Ensayos de Resistencia al Fuego – Elementos Constructivos en Edificios, utilizan una curva tiempo-temperatura bastante similar a la de ASTM E119. Esto quiere decir que los especímenes constructivos que se ensayan en un horno de pruebas en la mayoría del mundo moderno, para establecer su RF, se analizan básicamente bajo la misma temperatura.

La figura anexa tomada de un curso que yo dicto sobre RF compara diferentes curvas tiempo-temperatura de uso internacional.



DIFERENCIAS ENTRE LAS PRUEBAS EUROPEAS Y LAS DE ESTADOS UNIDOS

Como ya se estableció, las curvas tiempo-temperatura utilizadas en Europa son similares a las que se utilizan en la normativa de los Estados Unidos. La normativa europea es extensa sobre este tema y establecer una comparación punto a punto entre los requerimientos europeos y los encontrados en NFPA sería casi imposible.

Pero en mi opinión si una puerta o una pared con RF similar, tienen certificación ya sea en Europa o en los Estados Unidos o Canadá, esta podría ser aprobada. Las pruebas bajo ASTM E119 requieren una prueba de chorro de agua (*hose test)* para garantizar que el elemento constructivo sea capaz de soportar el abuso de una manguera de extinción de incendios de alta presión, algo que a mí me parece muy práctico. Los europeos no requieren esta prueba.

CRNOVA SECURITY

Custodia de Mercancía

Guardia Intramuros

Monitoreo y Rastreo

ISO 9001 · ISO 28000 · BASC · ISO 18788 · ISO 37001

AMESP · ESR · ASIS INTERNATIONAL

crnovaoficial

crnovasecurity

www.crnova.com.mx

URBINA 19, OFICINA 3,PARQUE INDUSTRIAL NAUCALPAN, NAUCALPAN DE JUÁREZ,EDO. MÉX., CP. 53489.

En la tabla a continuación, se contrasta la normativa europea (BS EN 1364-1, Ensayos de Resistencia al Fuego para Elementos No Portantes. Parte 1: Paredes) con la de Estados Unidos (ASTM E119). Se puede observar que existen diferencias, pero estas no son importantes. A propósito, BS EN 1364-1 utiliza la curva tiempo-temperatura especificada en ISO 834.

MEDICIÓN EN LA PARED NO EXPUESTA AL FUEGO	ASTM E119	BS EN 1364
Incremento de temperatura promedio encima de la temperatura inicial (Clasificación I)	≤121°C	≤140°C
Incremento de temperatura máxima encima de la temperatura inicial (Clasificación I)	≤163°C	≤180°C
Evidencia que no hay llama sostenida (Clasificación E)	✓	✓
Evidencia que los gases calientes no ha encendido una almohadilla de algodón (Clasificación E)	✗	✓
Medición de la radiación (Clasificación W)	✗	< 15 KW/m^2 a 1 m de la pared
Prueba de chorro de agua	✓	✗

Tal vez una de las principales diferencias entre estas normas está en cómo se expresa la clasificación de la RF. La resistencia al fuego en la normativa NFPA se expresa típicamente en horas, excepto para elementos RF de menos de 1 hora, cuando se expresa en minutos. La normativa europea utiliza resistencias al fuego que se expresan en minutos, pero adicionalmente establecen independientemente la Integridad (E), Aislamiento Térmico (I) y Control de la Radiación (W). Estas clases de RF se pueden entender mejor con la siguiente gráfica.

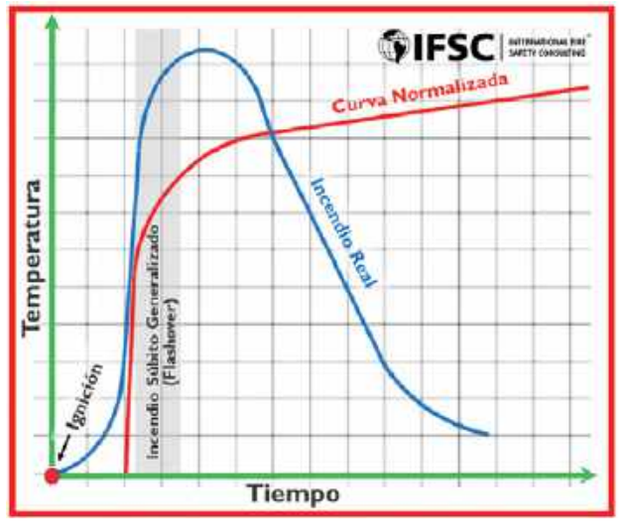
ENTENDIENDO LA RESISTENCIA AL FUEGO

Como ya lo mencioné, la resistencia al fuego se entiende como la aptitud de un elemento constructivo de mantener sus propiedades en presencia de un incendio durante un tiempo determinado.

Esto a veces se ha confundido con la severidad del incendio, el cual es una función de la intensidad y del tiempo del fuego expuesto. Aunque tiene sentido entender que la severidad de un incendio está relacionada con la resistencia al fuego, este concepto ha perdido razón de ser y se considera obsoleto.

Desafortunadamente en muchos de nuestros países, sobre todo en la parte sur de Sudamérica, los códigos piden que se ejecute un estudio de la carga de fuego del edificio para establecer la resistencia al fuego del edificio.

Este concepto, sin embargo, desde los años 80 se ha tildado como obsoleto, puesto que el incendio moderno tiende a tener una temperatura inicial mucho más alta que la mostrada en la curva normalizada tiempo-temperatura, pero tiende a extinguirse más rápidamente que lo que ocurría en los incendios hace 50 o más años, debido a la combustibilidad mucho más alta del mobiliario y contenidos de los edificios modernos. La figura anexa muestra, de manera conceptual, la diferencia entre la curva normalizada tiempo-temperatura y un incendio real.



¿CÓMO SE RECONOCE LA RF?

Típicamente esto se logra a través de pruebas en laboratorios de ensayos de resistencia al fuego. Estas pruebas son realizadas típicamente por un laboratorio independiente, siendo *Underwriters Laboratories* (UL) el laboratorio de ensayos más conocido. *Factory Mutual* también recientemente empezó a realizar estas pruebas. En Latinoamérica existen cuatro laboratorios de ensayos: IPT en Brasil, INTI en Argentina, y dos en Chile, IDIEM y DICTUC. Reitero no es válido que el fabricante del elemento constructivo certifique su propio producto, certificación que la debería determinar siempre uno de estos laboratorios de ensayo independientes. ■

Referencias:

[1] *Manual de Protección Contra Incendios de la NFPA, Quinta Edición, Moncada, J. y Moncada, J.A., editores, página10-1.*

[2] *The History of Fire Protection Engineering, NFPA-SFPE, Richardson, J.K., página 8.*

[3] *The History of Fire Protection Engineering, NFPA-SFPE, Richardson, J.K., página 9-12.*

Fotos: Cortesía Jaime A. Moncada

TIMUR
Latinoamérica

GALEAM

NUESTRO VALOR, SU SEGURIDAD

CONSULTORÍA

GUARDIAS INTRAMUROS

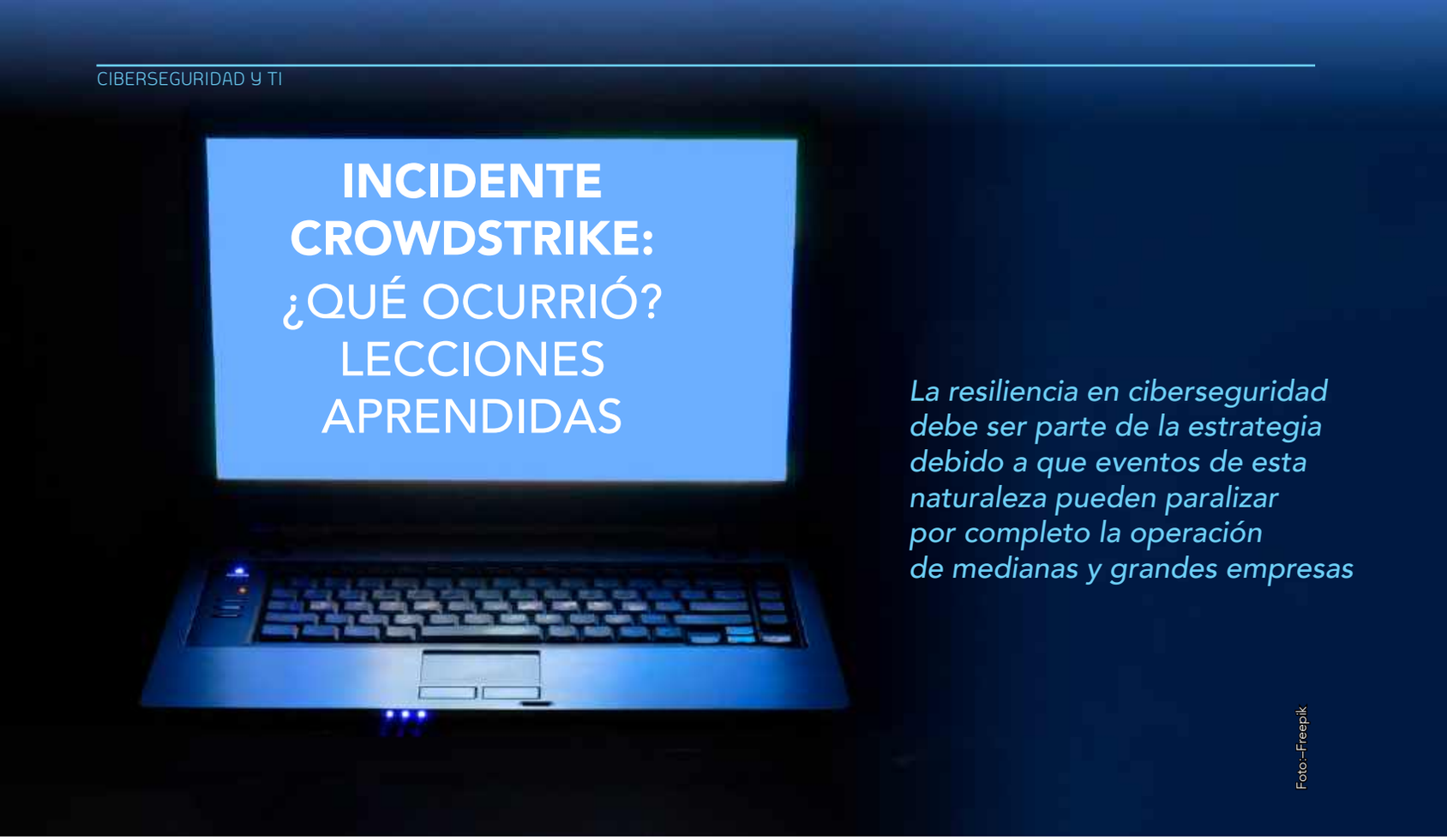
PROTECCIÓN EJECUTIVA

info@galeam.mx
info@timurlatinoamerica.com

56 3048 9610 / 55 6840 1036

www.galeam.mx
www. timurlatinoamerica.com

INCIDENTE CROWDSTRIKE: ¿QUÉ OCURRIÓ? LECCIONES APRENDIDAS



La resiliencia en ciberseguridad debe ser parte de la estrategia debido a que eventos de esta naturaleza pueden paralizar por completo la operación de medianas y grandes empresas

Foto:–Freepik

MÉXICO **Karen Elizabeth Heredia Miguel**

Actualmente, con el proceso acelerado de la digitalización de servicios las organizaciones, tanto del sector público como privado, han dirigido esfuerzos para proteger la infraestructura tecnológica que soporta sus operaciones, se incorporan soluciones que van a la vanguardia y que pueden ser robustas para el fortalecimiento de la estrategia de ciberseguridad.

Es importante considerar que las soluciones que se implementan coexisten en un ecosistema tecnológico, esto tiene ventajas al momento de proteger dicho ecosistema; sin embargo, es posible que se generen dependencias tecnológicas o incluso un fallo en alguna de las soluciones que puede impactar en los servicios de otras.

La pregunta es si las organizaciones están preparadas para eventos que puedan comprometer o interrumpir sus operaciones no sólo críticas, sino también en las estaciones de trabajo de sus colaboradores. En esta ocasión se abordará el caso ocurrido este año con el fabricante CrowdStrike, que proporciona servicios y productos para la protección contra amenazas cibernéticas.

En su sitio oficial[1], el fabricante publica una revisión del incidente el 19 de julio de 2024 a las 04:09 UTC que afectó al sensor de Falcon, el cual ofrece el servicio de protección de *endpoints* incorporando capacidades de inteligencia sobre amenazas y servicios de respuesta ante ataques a través del uso de *malware* o sin *malware*. La causa del incidente se deriva de una actualización de configuración de recopilación de telemetría sobre posibles técnicas sofisticadas de amenazas para este sensor de Windows, esta versión contenía un error no detectado lo que provocó un bloqueo en este sistema operativo con el famoso pantallazo azul (BSOD), las afectaciones se materializaron en los *hosts* con versión 7.11 y superior del sensor de Falcon. Los sistemas operativos que no tuvieron afectación fueron Mac y Linux.

Sin embargo, las preguntas son si este tipo de soluciones envía actualizaciones de forma constante ¿cuál fue la variante en este evento? O si ¿se trata de un hackeo? E incluso ¿las soluciones son realmente seguras? Estas preguntas se realizan en medio de una serie de afectaciones a diversas industrias, desde aeropuertos, bancos, puntos de venta, etc. Incluso es cuestionable el hecho de que la mayoría de las organizaciones tengan una dependencia en un sistema operativo el cual fue perjudicado por esta actualización, y las afectaciones se escalaron a nivel global.

El fallo declarado se debe a un error en la validación de contenido del paquete a liberar que, a pesar de pasar por un flujo de pruebas, donde se pasó de forma exitosa la verificación, debido a la confianza basada en comprobaciones previas que se liberó a producción, así que cuando el sensor recibía este contenido se generó una lectura de memoria fuera del límite generando una excepción inesperada que no se controló correctamente y ocasionó el bloqueo del sistema operativo Windows.

La solución identificada para tratar este incidente fue iniciar el sistema operativo en modo seguro, con la finalidad de renombrar una carpeta asociada al sensor y eliminar el archivo C-00000291*.sys alojado en la siguiente ruta C:\Windows\System32\drivers\CrowdStrike, y finalmente reiniciar el sistema, además de deshabilitar el servicio CSAgent.

Esta solución, aunque pareciera sencilla, tiene un impacto en los tiempos de atención que se pueden dar debido a que en primera instancia es una actividad que se requiere realizar de forma manual en cada uno de los *hosts* afectados, y replicar esta solución para una organización con altos niveles de operación y con el personal afectado en sus estaciones de trabajo alojadas en otra ubicación geográfica requiere sumar otros esfuerzos de logística y soporte de TI.

CONSECUENCIAS

Por parte del fabricante, este archivo que generó las afectaciones quedó obsoleto y en desuso en los sistemas operativos, y se agregó a una lista negra de Falcon en la Nube de CrowdStrike, a fin de evitar futuras interrupciones derivadas del uso de esta versión.

Ante las afectaciones que detuvieron la operación de diversas organizaciones, *hackers* malintencionados habilitaron dominios nuevos con la finalidad de crear campañas de *phishing* y otras actividades de carácter malicioso, ya que se ofrecían soluciones o asistencia profesional ante este evento.

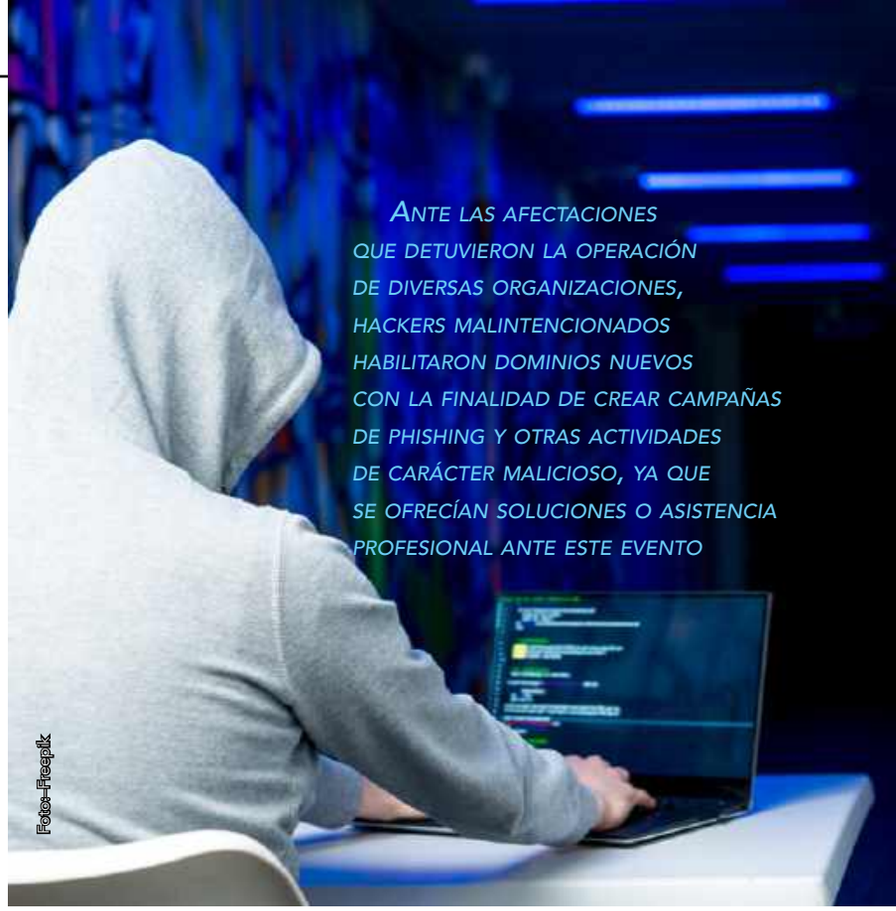
Considerando que parte de la efectividad de las campañas de *phishing* se logra a través del sentido de urgencia, y en este escenario diversas organizaciones requerían tener una solución inmediata ante el caos generado. La comunidad de ciberseguridad también alertó sobre estos dominios e indicadores de compromiso (IoC) para evitar otro tipo de incidentes materializados como resultado de la gestión del incidente principal.

Dentro de las lecciones aprendidas como organización es importante comprender el ecosistema tecnológico en el que se mantienen las actividades del negocio, con la finalidad de tener un posible plan de respuesta a incidentes que cumpla con los niveles de atención aceptables; considerando aquellas afectaciones que vienen a través de la cadena de suministro o por parte de los fabricantes mismos.

Es necesario tener controles aplicables a terceros que ayuden a gestionar los riesgos e impacto ocasionados por eventos que quedan fuera de los límites de responsabilidad de la propia compañía. Contar con un inventario de activos para conocer la dimensión de las afectaciones, cuántos de los sistemas utilizan las versiones de SO afectados, esto basándose en los Controles de CIS v8.1.

Además de mantener comunicado y capacitado al personal con el objetivo de seguir los protocolos de acción y remediación aplicables, para evitar que se generen nuevas afectaciones o fugas de información derivadas de una mala gestión de los eventos disparados por cualquier incidente.

Evaluar de forma constante los procesos críticos de negocio y contar con un plan de recuperación, para lograr restablecer los niveles de operación y servicio en los tiempos máximos y mínimos que la organización requiere.



La *ciberresiliencia* como parte de la estrategia debido a que eventos de esta naturaleza pueden paralizar por completo la operación de medianas y grandes empresas, y en la medida en que una empresa sea capaz de reducir los impactos y afectaciones le permite mantenerse "viva" en un mercado competitivo, genera confianza ante sus clientes e inversionistas, además de facilitar la recuperación de sus actividades de negocio.

Cada que se integra una nueva solución en el *stack* tecnológico de la empresa es importante evaluar qué proceso crítico soporta o si hay una dependencia hacia esa solución, lo que permite poner el foco para monitorear el estado del servicio de forma regular o las implicaciones de una caída o interrupción del servicio que brinda. Ya que, aunque para las organizaciones las tecnologías pueden ser una caja negra, es posible evaluar este tipo de posibles escenarios buscando si hay una forma de diversificar el manejo de la operación antes de "casarse" con una tecnología o fabricante, de esta forma las decisiones sobre adquirir o renovar un servicio son informadas y basadas en dicha evaluación de riesgos, presupuestos, implicaciones legales o posibles afectaciones. ■

Referencias:

[1] *Fuente: Centro de orientación y corrección de actualizaciones de contenido de Falcon | Huelga de multitudes (crowdstrike.com).*

Karen Elizabeth Heredia Miguel, arquitecto de Soluciones de Seguridad.
Más sobre la autora:

SEGURIDAD INFORMÁTICA EN MÉXICO: ¿ESTAMOS LISTOS PARA ENFRENTAR UN APAGÓN DIGITAL O UN CIBERATAQUE?

En México, la protección de la infraestructura digital y la resiliencia frente a las amenazas cibernéticas deben ser prioridades para las empresas

SISSA DIGITAL

MÉXICO

En un mundo cada vez más digitalizado, la seguridad informática se ha convertido en una prioridad crítica para gobiernos, empresas y ciudadanos. Recientemente, el mega apagón informático de CrowdStrike y el hackeo masivo de Anonymous a 325 sitios web del gobierno de Maduro en Venezuela han puesto de manifiesto la vulnerabilidad de los sistemas informáticos y la necesidad urgente de reforzar la ciberseguridad.

México no es ajeno a estos desafíos, con una economía en crecimiento y una digitalización acelerada, el país enfrenta constantes amenazas cibernéticas, por ello es esencial que, tanto el sector público como el privado, aumenten sus inversiones en tecnologías de ciberseguridad. La creación de infraestructura resiliente y la capacitación de profesionales especializados son fundamentales para proteger los datos y sistemas críticos.

MEJORES PRÁCTICAS

Es por ello que Héctor Gonzalo Castillo Vite, director de Desarrollo de *Software* de SISSA Digital, considera que es vital promover una cultura de seguridad informática entre la ciudadanía y las empresas. El Ingeniero Castillo compartió durante una entrevista, información sobre las mejores prácticas de ciberseguridad, las cuales pueden reducir significativamente el riesgo de ataques:

1) **Importancia de la Infraestructura:** La infraestructura tecnológica, como *firewalls*, sistemas de detección de intrusiones y respaldos, es crucial para prevenir y mitigar incidentes informáticos. También es esencial contar con planes de contingencia y procesos de recuperación.
2) **Soluciones de Respaldo:** Deben tener planes de contingencia, como *backups* y sistemas de virtualización para mantener el servicio en caso de fallos, es crucial.
3) **Cloudflare y AWS** son mencionados como herramientas útiles para mejorar la seguridad y la infraestructura en la Nube.
4) **Actualizaciones Automáticas:** Aunque las actualizaciones automáticas son útiles, no son la única solución. Las empresas deben tener un enfoque multidisciplinario que incluya un personal capacitado y procesos maduros para manejar problemas de seguridad.
5) **Incremento de Inversiones en Ciberseguridad:** Es esencial que tanto el sector público como el privado aumenten sus inversiones en tecnologías de ciberseguridad. Se recomienda asignar hasta un 25% del presupuesto a seguridad informática, aunque en la práctica esto varía según el sector y tamaño de la empresa.
6) **Concientización y Educación:** Es vital promover una cultura de seguridad informática entre la ciudadanía y las empresas. La educación y concientización sobre las mejores prácticas de ciberseguridad pueden reducir significativamente el riesgo de ataques.

7) SISSA ha trabajado en desarrollos para garantizar alta disponibilidad y seguridad, utilizando plataformas tanto en la nube como en servidores físicos, con monitoreo integral y capacidades de virtualización.

La ciberseguridad es una responsabilidad compartida que requiere el compromiso de todos los actores involucrados. "Desde SISSA Digital, reafirmamos nuestro compromiso de colaborar con diferentes sectores para fortalecer la infraestructura digital de México. Estamos convencidos de que, a través de una combinación de inversiones estratégicas, políticas adecuadas y una cultura de seguridad bien arraigada, podemos enfrentar y superar los desafíos cibernéticos que se presenten", mencionó Héctor Gonzalo Castillo. Los recientes eventos que han sacudido el mundo digital sirven como un poderoso recordatorio de que la seguridad informática no es opcional, sino una necesidad imperativa. En México, la protección de la infraestructura digital y la resiliencia frente a las amenazas cibernéticas deben ser prioridades para las empresas.

Héctor Gonzalo Castillo Vite,
director de Desarrollo de Software de SISSA Digital

Es momento de que el sector público y privado unan esfuerzos para construir un entorno digital seguro y confiable. La inversión en tecnologías de ciberseguridad, la cooperación internacional, la educación y la concientización, son los pilares sobre los cuales se debe cimentar la defensa cibernética del país. ■

Fuente y fotos: SISSA Digital

EL RETO MODERNO DEL ANALISTA DE SEGURIDAD / CIBERSEGURIDAD:
EL ARTE DE ANTICIPAR EN MEDIO DE LA NIEBLA

Foto: Freepik

COLOMBIA | Jeimy Cano

En la medida que la organización aprenda de los eventos conocidos, inusuales, desconocidos o emergentes, podrá crear y afinar una estrategia prospectiva de amenazas que le permita estar fuera de la zona cómoda y mantener una postura vigilante

El reto de los atacantes modernos es lograr comprometer sistemas o infraestructuras con el menor "ruido posible" para mantenerse dentro, de forma imperceptible o, por el contrario, generar el mayor "ruido posible" para crear una distracción creíble, para que luego que los analistas logren controlar los impactos del evento y cerrar las vulnerabilidades aprovechadas, el adversario pueda mantenerse oculto sin ser notado. En cualquiera de los dos eventos, el adversario tiene como fin lograr el "manto de la invisibilidad" lo que recuerda la frase del ExCEO de CISCO, John Chambers: "Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas".

Las cifras recientes sobre el tiempo de permanencia del adversario en la infraestructura antes de ser detectado (en inglés Dwell Time) (si es viable hacerlo), de acuerdo con el informe de Mandiant (2023), ha venido evolucionando de forma positiva para los analistas pasando en 2012 de 243 días a 16 días en 2022, lo que muestra un aumento de mejores y mayores estrategias de detección disponibles en las empresas, que de forma proactiva han venido calibrando sus sensores para cerrarle los espacios a los atacantes que quieren situarse de forma invisible en las infraestructuras de las empresas.

El gran logro que tienen los adversarios es "hacerles creer a las organizaciones que no han sido comprometidos y que los eventos que puedan revelar su presencia, responden a eventualidades o situaciones que son normales dentro de la dinámica de la infraestructura o sistemas". Es un ejercicio de inteligencia y engaño que busca confundir las mejores estrategias de detección e identificación de ataques, con el fin de mantener su ventaja estratégica basada en sorpresa, anonimato, velocidad y efectividad. En la medida que los adversarios tengan menos margen de acción, una vez han ingresado en la infraestructura, mayor será la capacidad de reacción de las organizaciones para visualizarlos y anticiparlos.

EL MAYOR RETO PARA LAS ORGANIZACIONES

El gran reto que tienen las organizaciones en la actualidad es situarse en las anomalías, las contradicciones y las rarezas (Charan, 2015) que las diferentes estrategias de defensa revelan, y analizarlas en tiempo real con la ayuda de soluciones basadas en inteligencia artificial, con el fin de, no sólo estudiar su contexto, sino tomar acciones efectivas, aun considerando los posibles falsos positivos o falsos negativos que se pueden generar por cuenta de la calibración necesaria de los algoritmos y sus bases de datos para su entrenamiento.

Así las cosas, los atacantes saben que en la medida que logren caracterizar mejor la dinámica de las infraestructuras o sistemas objetivo, mejor podrán generar su estrategia para mimetizarse en medio de su entorno normal de operación, pasar desapercibidos a los sensores especializados y crear situaciones de confianza y confort tanto para los profesionales de seguridad / ciberseguridad, como para sus ejecutivos. De esta forma, al no tener evidencia concreta de una posible actividad maliciosa, no habrá alertas y, por lo tanto, se reportará actividad "normal" de la infraestructura.

En este sentido, cuando lo anterior ocurre, el trabajo del analista de seguridad / ciberseguridad aumenta, pues ahora no sólo debe estar pendiente de aquello que se sale de lo esperado, sino crear un "nuevo normal" que implica revelar un "desquilibrio dinámico", esto es un "nuevo anormal" (Sheffi, 2020) que lo sitúe en un nivel de paranoia debidamente administrado que le permita afinar e hilar de forma fina lo que ocurre en la dinámica de su infraestructura con la ayuda de las herramientas de inteligencia artificial.

En este nuevo escenario, no sólo son necesarias las líneas base de operación de las infraestructuras, la aplicación de estándares y buenas prácticas (Oppliger, 2015), sino los ejercicios de simulación basados en escenarios, para mantener al equipo de ciberseguridad fuera de la zona cómoda, y desarrollar competencias claves para "ver en medio de la niebla" y actuar de forma efectiva desde la identificación de señales débiles, hasta

la detección de patrones conocidos, latentes y emergentes que permitan a la organización actuar de forma anticipada sobre posibles acciones incipientes del adversario en sus sistemas.

EL ARTE DE LA INVISIBILIDAD

El ejercicio de protección y prevención que se tiene en las organizaciones actuales se basa en todo aquello que es conocido. Bien se dice que sólo podemos protegernos de aquello que sabemos y conocemos. De esta manera, muchas de las inversiones en seguridad, siguiendo este paradigma y reafirmado por los equipos ejecutivos a través de los modelos de madurez, hace que los equipos de seguridad permanezcan con postura vigilante de aquello conocido, y generalmente desprevenido de lo que puede ser latente o emergentes. En consecuencia, el adversario tiene espacio suficiente no sólo para mantener la atención y distracción sobre el analista en su lectura "normal" (conocida), sino un lugar privilegiado para navegar debajo de los radares diseñados por las organizaciones.

El arte de la invisibilidad, no está solamente en tener la capacidad de "no hacerse notar", sino de pasar desapercibido a la luz del día, en mimetizarse con lo tradicional y la costumbre, pues de esta manera es posible encontrar mayor tiempo y espacio para crear el próximo evento inesperado que lleve a la organización a un nuevo engaño: una nueva crisis que cree haber controlado. Esto es, tener la tranquilidad de haber controlado la situación, cerrar las brechas identificadas, minimizar los daños y restaurar la tranquilidad en la organización.

Los avances acelerados de los adversarios con el uso de la inteligencia artificial establece desafíos más elaborados para los profesionales de seguridad / ciberseguridad, pues no sólo deberán reconocer eventos conocidos y desconocidos, sino aquellos elaborados por la inteligencia artificial adversarial, agregando un nivel más de complejidad y análisis que demandará no sólo capacidad para identificar esta nueva propuesta, sino especial énfasis en las capacidades novedosas que los nuevos desarrollos con inteligencia artificial traerán en el futuro y estar atentos a su posibles usos adversos, para desde ya comenzar a imaginar escenarios que puedan confundir o invalidar sus controles actuales (Ceschin *et al*., 2024).

Los analistas de seguridad / ciberseguridad deberán pasar de reportar no sólo las alertas tradicionales (basadas en eventos conocidos) a revelar alertas tempranas (basadas en patrones y tendencias) inmersas en los datos propios de los sistemas de monitoreo y control. Un ejercicio que implica un reto de comprensión e interpretación de los datos en contexto, para darle sentido a su nueva promesa de valor prospectiva que permita a la organización articular sus prácticas asociadas con el proteger y asegurar, con las capacidades necesarias para defender y anticipar. Un reto que busca no sólo reconocer al adversario antes de que tenga éxito, sino demorarlo, distraerlo, confundirlo y disuadirlo como nuevo paradigma de seguridad y control (Cano, 2023).

Es claro que los controles instalados y asegurados en las infraestructuras actuales lo que hacen es tratar de demorar al intruso para que ingrese, y en la medida de su nivel de calibración, dicha demora podrá ser corta o larga. En consecuencia, cada vez que un atacante emprende una acción específica sobre una infraestructura, necesitará tiempo y esfuerzo para recolectar toda la información clave que le permita tener un mayor conocimiento de su contraparte, para luego elaborar su plan de acción que genere mayor nivel de incertidumbre y daño en el objetivo, y las mayores certezas en la ejecución de sus estrategias.

Por lo tanto, los analistas de seguridad / ciberseguridad deben acuñar la frase de Carl Sagan: "La ausencia de evidencia, no es evidencia de ausencia", pues si los mecanismos de seguridad no reportan actividad maliciosa o sospechosa en la infraestructura, no significa que no exista actividad o señales débiles que indiquen algunos pasos que se vienen dando de forma imperceptible por parte del adversario, que serán visibles o no dependiendo de qué tan fino y especializado es el monitoreo y la línea base que tiene la organización frente a eventos inicialmente inusuales, que puedan llevar al descubrimiento de situaciones encubiertas.

Así las cosas, cualquier evento que resulte novedoso, frente a aquello que se conoce con anticipación deberá ser puesto inicialmente en observación, pues de esto dependerá la evolución e identificación de patrones emergentes, o la incorporación a la base de datos de eventos inusuales, como una manera de enriquecer el conocimiento y caracterización de la infraestructura asegurada. En la medida que la organización aprenda de los eventos conocidos, inusuales, desconocidos o emergentes, podrá crear y afinar una estrategia prospectiva de amenazas que le permita estar fuera de la zona cómoda y mantener una postura vigilante.

El reto al final no es que la organización llegue a ser "la mejor en su sector" en la defensa y anticipación de amenazas cibernéticas, sino "ser mejor ella misma cada día" teniendo en mente la inevitabilidad de la falla, sabiendo que tarde o temprano el adversario tendrá éxito y, por tanto, su capacidad resiliente será la que debe brillar cuando el evento adverso se materialice. Lo anterior implica, que el objetivo no es obtener un reconocimiento del sector por las prácticas y estándares que se aplican para proteger y asegurar las operaciones, sino desarrollar un estilo de vida vigilante y unas capacidades cibernéticas evolutivas, que basadas en el apetito de riesgo, los aliados estratégicos, los umbrales de operación y la caracterización de sus adversarios (Cano, 2021), hagan realidad la promesa de valor del área de seguridad / ciberseguridad: una confianza digital imperfecta. ■

Referencias:

- *Cano, J. (2021). Modos de operación de la ciberseguridad empresarial. Capacidades básicas para navegar en el contexto digital. Global Strategy. Global Strategy Report No. 44/2021. https://global-strategy.org/modos-de-operacion-de-la-ciberseguridad-empresarial-capacidades-basicas-para-navegar-en-el-contexto-digital/*
- *Cano, J. (2023). Security Risk Management and Cybersecurity: From the Victim or from the Adversary?. En: Jahankhani, H. (eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. 1-8. https://doi.org/10.1007/978-3-031-20160-8_1*
- *Ceschin, F., Botacin, M., Bifet, A., Pfahringer, B., Oliveira, L., Gomes, H. & Grégio, A. (2024). Machine Learning (In) Security: A Stream of Problems. Digital Threats: Reseach & Practice. 5(1). https://doi.org/10.1145/3617897*
- *Charan, R. (2015). The attacker's advantage. Turning uncertainty into breakthrough opportunities. New York, USA: Perseus Books Groups.*
- *Mandiant (2023). M-Trends 2023. https://services.google.com/fh/files/misc/m-trends-ig-2023-en.pdf*
- *Oppliger, R. (2015). Quantitative risk analysis in information security management: A modern fairy tale. IEEE Security & Privacy. 13(6). 18-21. doi: 10.1109/MSP.2015.118*
- *Sheffi, Y. (2020). The new (ab)normal. Reshaping business and supply chain strategy beyond covid-19. Cambridge, MA. MIT CTL Media.*

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.*

EL LADO AMARGO DE LAS *COOKIES* DE INTERNET

Foto: Freepik

Si bien las cookies proporcionan cierta "experiencia al usuario", la conveniencia que proporcionan tiene un costo: tu privacidad

MÉXICO

Gigi Agassini

En la era digital actual, es común encontrarnos con avisos en casi todos los sitios web que visitamos, preguntándonos si permitimos o no el uso de *cookies* en nuestro navegador. Esto refleja cómo las *cookies* están omnipresentes en nuestra experiencia en línea. Estos pequeños archivos de texto, almacenados en tu dispositivo por los sitios web, están diseñados para mejorar tu experiencia de navegación y hacerla más personalizada.

Recuerdan tu información de inicio de sesión, mantienen los artículos en tu carrito de compras y ayudan a personalizar el contenido. Sin embargo, aunque las *cookies* pueden ser convenientes, también presentan riesgos significativos y pueden representar una grave vulnerabilidad para la privacidad, que con frecuencia pasa desapercibida.

¿QUÉ EXACTAMENTE SON LAS *COOKIES*?

Las *cookies* son esencialmente archivos de texto con pequeños datos como nombre de usuario y contraseña que los sitios web envían a tu navegador y los utilizan para identificar tu ordenar cuando usas la red. Cuando visitas un sitio, éste almacena esos archivos en tu dispositivo, permitiendo que el sitio te reconozca en futuras visitas.

Se utilizan *cookies* específicas para la identificación de usuarios concretos y mejorar tu experiencia en la navegación. Los datos almacenados en una *cookie* son creados por el servidor al conectarte y estos datos se etiquetan con un ID exclusivo para ti y tu ordenar; por lo que cuando la *cookie* se intercambia entre un ordenador y el servidor de red, este último lee el ID y sabe que información mostrarte.

Todas las *cookies* funcionan de la misma manera, pero se han aplicado varios usos para estas. Existen varios tipos de *cookies*: las *cookies* de sesión, que expiran cuando cierras tu navegador; las *cookies* persistentes, que permanecen en tu dispositivo durante un período determinado; y las *cookies* de terceros, que son colocadas por anunciantes para rastrear tu actividad en línea a través de diferentes sitios web.

LOS RIESGOS PARA LA PRIVACIDAD

Debido a que las legislaciones globales están cambiando y una de las más fuertes y conocidas es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, así como varias estatales, provinciales de distintos países; es que muchos sitios deben solicitar permiso para usar ciertas *cookies* en los navegadores y proporcionar información acerca de cómo se utilizarán las *cookies* si son aceptadas.

La razón detrás de este cambio es que como mencioné en el inicio, las *cookies* guardan información privada que puede ser utilizada por ciberdelincuentes para espiar nuestra actividad en línea o piratear información personal.

Pero existen otras *cookies* que se instalan permanentemente en los ordenadores de usuarios y tienen capacidad única de reaparecer después incluso de haber sido "eliminadas". Estas son un gran riesgo, ya que en ocasiones este tipo de *cookies* pueden ser fabricadas por piratas informáticos y utilizadas para infectar los sistemas con virus o *software* malicioso.

Si bien las *cookies* proporcionan cierta "experiencia al usuario", la conveniencia que proporcionan tiene un costo: tu privacidad. Las *cookies*, especialmente las de terceros, pueden recopilar grandes cantidades de datos sobre tu comportamiento en línea. Esto incluye tu historial de navegación, consultas de búsqueda e incluso el tiempo que pasas en ciertas páginas. Con el tiempo, estos datos pueden ser agregados para crear un perfil detallado de tus hábitos, preferencias e incluso tu identidad. Las *cookies* de terceros no tienen impacto

alguno en la experiencia de navegación, es sólo lucrar con nuestros datos.

Este perfil detallado a menudo se utiliza para la publicidad dirigida. Los anunciantes usan esta información para mostrarte anuncios personalizados basados en tu historial de navegación. Aunque esto pueda parecer inofensivo, puede volverse invasivo rápidamente. Tus datos a menudo se comparten o se venden a terceros sin tu consentimiento explícito, lo que dificulta el control sobre quién tiene acceso a tu información personal.

LA IMPORTANCIA DE GESTIONAR LAS *COOKIES*

Dado el riesgo potencial, es crucial gestionar cuidadosamente tus *cookies* y no sólo dar clic en "aceptar todas". La mayoría de los navegadores modernos te permiten personalizar la configuración de las *cookies*. Puedes optar por aceptar sólo las *cookies* esenciales, bloquear las *cookies* de terceros o incluso rechazar todas las *cookies* por completo. Limpiar regularmente tus *cookies* es otra forma efectiva de minimizar los datos que los sitios web pueden recopilar sobre ti.

Además, considera utilizar navegadores o extensiones centradas en la privacidad que limiten el rastreo de *cookies*. Herramientas como estas pueden bloquear *scripts* de rastreo y anonimizar tu actividad de navegación, proporcionando una capa adicional de seguridad.

Eliminar o rechazar las *cookies* es sin duda una medida de mitigación de riesgos de violación de nuestra privacidad y aunque pareciera un poco contradictorio pues, por un lado ayudan a agilizar la experiencia en la navegación, por otro lado, pueden ser utilizadas para efectos totalmente contrarios.

Eliminar *cookies* normales es fácil, pudiera tener un impacto en la navegación de algunos sitios web. Sin *cookies* como usuario de Internet deberás volver a introducir todos tus datos en cada visita.

Mantener una higiene informática es esencial, el uso de herramientas que nos permitan eliminar *cookies* de rastreo persistentes, así como el uso de antivirus y VPN's son elementos que deben ser considerados para ayudarnos a gestionar mejor los riesgos.

LA IMPORTANCIA DE RECHAZAR LAS *COOKIES*

Rechazar *las cookies* no esenciales no se trata sólo de evitar anuncios intrusivos; se trata de proteger tu privacidad digital. Al limitar los datos que las empresas pueden recopilar, reduces el riesgo de que tu información personal sea explotada. Esto es particularmente importante a medida que las violaciones de datos y el robo de identidad se vuelven cada vez más comunes.

Foto: Freepik

Además, rechazar las *cookies* puede ayudar a combatir la difusión de desinformación. Cuando los anunciantes tienen menos acceso a tus datos, tienen menos herramientas para dirigirse a ti con contenido manipulador. Este es un paso pequeño, pero significativo hacia la creación de un entorno en línea más ético y transparente.

Las *cookies* son una espada de doble filo. Aunque pueden mejorar tu experiencia en línea, también conllevan riesgos significativos para la privacidad. Al tomar medidas para gestionar y rechazar las *cookies*, puedes proteger tu información personal y asegurar una experiencia de navegación más segura y privada. En un mundo donde los datos son una moneda valiosa, es esencial mantenerse vigilante y tomar control de tu huella digital. Proteger tu privacidad en línea comienza con entender los riesgos y tomar decisiones informadas sobre la configuración de tus *cookies*.

La ciberseguridad es un estilo de vida y comienza por ti.

¡Hasta la próxima! ■


Foto: Freepik

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

CASKA MÉXICO CELEBRA SU 15 ANIVERSARIO

MÉXICO

En septiembre, Caska México celebró su 15 aniversario con una reunión conformada por los socios fundadores, familias de ambos, amigos, colegas, colaboradores y clientes.

El evento dio inicio con la proyección de un video conmemorativo que contó la historia de la empresa desde su fundación en el 2009, cuando su principal producto eran estéreos para autos. Con los años, la empresa se convirtió en proveedora Tier1 de las dos principales armadoras automotrices en el país, así como un referente en la industria de la seguridad privada con los servicios de custodias, monitoreo satelital, guardias y blindajes.

En su discurso, Diego Peralta, socio fundador, agradeció a las personas que han formado parte de la historia de la empresa, por haber sido piezas fundamentales en el desarrollo y crecimiento de Caska México.

Por su parte, Fernando Ávila, también socio fundador de la empresa, habló del reto importante que significó abrir diferentes líneas de negocio, y que a pesar de las dificultades, siempre han sabido enfrentarlas con éxito.

Los asistentes fueron recibidos con diferentes activaciones y disfrutaron de una amena convivencia con música, bebidas y bocadillos. También se les obsequió un peluche en forma de planeta tierra llamado "EdMundo", como el nuevo integrante de la empresa.

CASKA
MÉXICO

Haciendo un mundo más seguro

Foto: Tania G. Rojo Chávez / SEA

Diego P. Peralta Mereles, socio fundador de Caska México

Foto: Tania G. Rojo Chávez / SEA

Fernando D. Ávila Muñoz, socio fundador de Caska México

RECONOCIMIENTO A LA DEDICACIÓN

Como parte de la celebración, se entregaron reconocimientos a los colaboradores más destacados que han aportado gran valor a la empresa, reconociendo su talento y dedicación.

- **José Luis Torres Seinos**
  Instalador
  13 años de servicio
- **Rosario Ávila Albarrán**
  Coordinadora administrativa de Custodias
  11 años de servicio
- **Sandro Juárez Razo**
  Gerente de Operaciones de Custodias
  8 años de servicio
- **Martín Juárez Sánchez**
  Coordinador de Patio
  8 años de servicio
- **Arturo Ramírez Díaz**
  Gerente Automotriz
  7 años de servicio
- **Ángel Rosas Trejo**
  Coordinador de Operaciones
  5 años de servicio
- **Itzel Sánchez Pérez**
  Directora Comercial
  5 años de servicio
- **Alberto Cordova Gama**
  Director de Seguridad
  4 años de servicio

Durante el festejo, **Seguridad en América** platicó con varios clientes de la empresa, quienes dedicaron unas palabras:

Francisco D. Moreno Sarmiento, Jefe de Seguridad Patrimonial de Grupo Axo, se sintió agradecido con Caska México, mencionó que a todos los clientes les hacen un traje a la medida muy funcional y les deseó muchos años más de éxito.

Agustín Castro, Ejecutivo de Logística de Importaciones de Mr. Pistacho, dijo que Caska desempeña un excelente trabajo, con gran profesionalismo, demostrando ser líderes en lo que hacen.

Esteban García Olmedo, Gerente de Seguridad de Multimarcas Promoda de Grupo Axo, agradeció a Caska por ser sus proveedores y por brindarles un excelente servicio, finalizó deseando que no sólo sean 15 años de éxito sino, muchos más.

MÁS SOBRE LA EMPRESA

A 15 años de su creación, Caska México cuenta con cinco oficinas corporativas, seis bases operativas, más de 230 unidades vehiculares y más de 400 mil productos anuales de venta en el sector automotriz. Además es un referente de las industrias de seguridad privada y equipamiento automotriz en el país, reafirmando su compromiso con más de 2 mil familias mexicanas. ■

Fuente y fotos: Caska México

DECÁLOGO PARA EL USUARIO DE SEGURIDAD PRIVADA

Foto:-Freepik

Conozca las recomendaciones de nuestro colaborador invitado

MÉXICO **Dante García Martínez**

La seguridad es responsabilidad de todos, y tanto la empresa que provee los servicios como quien los administra y posiciona en determinada empresa u organización, deben conocer las responsabilidades que cada uno tiene para lograr el objetivo en común: resguardar la integridad de las personas, y proteger los bienes. Es por ello que a continuación nuestro especialista invitado, nos comparte los diez aspectos que debe tener presente el usuario final.

1 **Analizaré** con sinceridad y respeto, las consignas que requiero de mi prestador de servicios.

2 **Estudiaré** coordinadamente las Cláusulas de los Contratos de Seguridad, con mi representada y aquellos que ofertan el servicio, para actuar equitativamente.

3 **Compartiré** los éxitos y reconocimientos, sin dejar de acotar los errores, que puedan servir de experiencia.

4 **Revisaré** con sumo detalle, toda deficiencia que afecte el cabal desarrollo del servicio de seguridad.

5 **Seré** respetuoso y amable con cada elemento operativo, sin distingo alguno.

6 **Aceptaré** la óptica de cada persona, valorando detenidamente, antes de dar una opinión.

7 **Rechazaré** involucrar mis intereses y deseos personales o familiares, con mi trabajo.

8 **Seré** responsable de mis opiniones y comentarios, ante quien represento, así como ante el prestador del servicio y su equipo.

9 **Participaré** activamente en todas las Políticas de Mejoras, de inclusión, así como en las de capacitación, en favor de mi persona, equipo, empresa y nación.

10 **Defenderé** puntualmente el Contrato de Prestación de Servicios, pues su cabal cumplimiento, es más que un contrato mercantil, es la relación social que beneficia a los involucrados. ■

Dante García Martínez, CPP, CPO, DSE, DSI, director general y abogado titular de Asistencia Legal a Empresas de Seguridad (ALES ABOGADOS).
Más sobre el autor:

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 · DNV · AMESP · Empresas GSI Grupo Seguridad Integral · BAC

Columna
EL TIGRE TIENE RAYAS

OMAR A. BALLESTEROS, DIRECTOR GENERAL Y CEO DE BALLESTEROS Y BARRERA SERVICIOS DE PROTECCIÓN.

Más sobre el autor:

SEGURIDAD PRIVADA: PRIORIDAD EN EL MUNDO EMPRESARIAL

Foto:-Freepik

"En México, la seguridad privada se ha desarrollado de manera sólida, alcanzando importante reputación y profesionalismo", Lic. Omar Ballesteros, presidente de la Asociación Nacional de Empresas de Seguridad Privada, A.C.

MÉXICO

Ante un panorama de esta dimensión, los números del posicionamiento de la seguridad privada a nivel mundial son impresionantes: De acuerdo con el presidente de la Asociación Nacional de Empresas de Seguridad Privada, A.C., Omar Ballesteros, el mercado global de estos servicios registró un valor estimado de 240 mil millones de dólares en 2020.

Esto supera el PIB (Producto Interno Bruto) de más de 100 países, incluidos Hungría y Marruecos. Sudáfrica, por ejemplo, cuenta con alrededor de 500 mil guardias de seguridad, el doble del total combinado de personal policial y militar del país. Las estimaciones sugieren que hay más de 20 millones de trabajadores de seguridad privada en todo el mundo, más que el número total de personas que viven en Chile o en los Países Bajos.

Señala, además, que la seguridad privada es una industria que crece cerca de un 6% anual, más rápido que la economía mundial en su conjunto. Es por eso que resulta esencial solicitar las credenciales y certificaciones que brinden certeza de su calidad y desempeño, al momento de contratar los servicios de una empresa de seguridad privada.

En México, la seguridad privada se ha desarrollado de manera sólida y ha alcanzado una gran reputación y profesionalismo. De hecho, esta industria da empleo a más de 600 mil trabajadores y representa el 2% del PIB anual.

EN EL MUNDO

Los elevados índices de violencia en Latinoamérica y la deficiente presencia de la autoridad de los respectivos estados en partes del territorio, han llevado a la proliferación de empresas privadas de seguridad en toda la región. Su número supera ya las 16 mil compañías, en una industria que involucra a más de 2.4 millones de personas. El sector afronta importantes retos, como legalidad imprecisa en muchos casos, déficit de experiencia, formas incompatibles con los derechos civiles y humanos en ciertos lugares y riesgo de escalada de arsenales.

La proliferación de las empresas de seguridad privada en América Latina va ligada a las estadísticas de criminalidad y violencia en la región. Se estima que 19 de cada 20 crímenes violentos que ocurren en el mundo tienen lugar en Latinoamérica, donde se encuentran 17 de las 20 ciudades más violentas del mundo y cuatro de los cinco países con mayor violencia.

La situación ha dado lugar a un "crecimiento explosivo" de la privatización de la seguridad en América Latina, como lo califica el informe "Seguridad a la venta" de Diálogo Interamericano. El aumento del número de Empresas de Defensa y Seguridad Privada (EMSP) se ha dado no sólo en países con acusados conflictos, como Colombia, donde en los últimos diez años se ha registrado un incremento del 126%, sino también en países de mayor paz social e institucionalidad como Chile, que en cinco años ha visto un incremento del 50%. El total de empresas dedicadas a esta función en Latinoamérica llegaba a 16 mil 174 en 2017, como precisaba entonces el Centro para el Control Democrático de las Fuerzas Armadas de Ginebra (DCAF).


Foto: Freepik

EL SECTOR DE LAS EMSP

El término EMSP incluye tanto las empresas se seguridad al uso en países desarrollados, dedicadas normalmente a labores de custodia de establecimientos o personas físicas, como también empresas de defensa que pueden llegar a sustituir funciones habitualmente reservadas al Estado. Estas últimas se desarrollaron tras el fin de la Guerra Fría y han llegado a ser un actor importante en las relaciones internacionales, con participación en conflictos de baja e incluso alta intensidad.

Esas empresas de defensa actúan en un marco de complicada legalidad, cuya regulación intentó estandarizarse en 2008 con el Documento de Montreaux, una compilación de obligaciones legales y buenas prácticas destinadas a garantizar la soberanía de los Estados y a proteger los Derechos Humanos. Si bien el texto se aplica más directamente a situaciones de conflicto armado, también aporta un marco regulatorio para las empresas de seguridad en general, dada la tenue frontera entre un tipo de empresas y otras, especialmente en Latinoamérica, donde la autoridad del Estado no alcanza muchas veces a todo el territorio nacional, algunos conflictos civiles son especialmente virulentos y ciertos usan a las Fuerzas Armadas en la lucha contra la violencia criminal y el mantenimiento del orden público.

MÁS GUARDIAS QUE POLICÍAS

Las más de 16 mil EMSP de América Latina emplean en torno a 2.4 millones de personas. Si bien los guardias de seguridad superan en número a los miembros de la policía en todo el mundo, en muchos países latinoamericanos se produce un especial desequilibrio entre el número de componentes de las fuerzas policiales y el de los agentes privados: en Colombia, Brasil y México la relación es de un policía por cuatro miembros de EMSP; en países de extrema violencia como Honduras y Guatemala la relación incluso llega a ser de uno a siete. También se da el caso de que muchos miembros de la policía recurren al pluriempleo, ejerciendo de policías durante el día y convirtiéndose en agentes de seguridad por la noche en algún vecindario, empresa o edificio.

Las mayores empresas son las que se dedican a la vigilancia y a la escolta de clientes VIP. Las más grandes son de origen europeo y estadounidense y están especializadas en una parte del sector, especialmente en la protección de la propiedad privada. En su mayoría actúan en ciudades o bien en centros de extracción de recursos naturales aislados de las zonas urbanas. En relación a las frecuentes críticas que reciben estas empresas, por supuesta suplantación de funciones propias de la autoridad legalmente constituida, es necesario destacar que el marco jurídico en el que las grandes empresas operan es estricto y se encuentra supervisado.

CARRERA DE ARMAMENTO

Se puede argumentar que la competencia entre los operadores ha generado una especie de carrera armamentística en la que cada empresa desea ofrecer servicios más eficaces. A su vez, al haber mayor número de agentes y además con armas más modernas, los criminales tienden igualmente a aumentar su potencia de fuego y sus capacidades para cumplir con sus objetivos, lo que consecuentemente lleva a las empresas a incrementar también el calibre de su armamento, en una espiral difícil de controlar. Las estadísticas muestran que Latinoamérica tiene la relación más alta de armas de fuego por guardia de seguridad del mundo fuera de aquellas áreas afectadas por conflictos. Esa relación es diez veces superior a la que existe sobre armas cortas en Europa.

Esto ha motivado que en el escenario latinoamericano en alguna ocasión se haya criticado a ciertas EMSP por haber contribuido, directa o indirectamente, al tráfico ilegal de armas y al aumento de las bandas armadas generando un círculo vicioso. Por ejemplo, en 2015 noventa personas fueron detenidas en San Francisco (algunas de ellas vinculadas a EMSP) por pertenecer a una red de tráfico de armas vinculada a la Mara Salvatrucha (MS-13). También se ha dado el caso de robo y extravío de armas importadas desde la región, tanto por parte de contratistas individuales de seguridad privada como por los propios militares; estas armas luego ingresan en el mercado negro. Así, más del 40% de las armas ilegales en El Salvador están vinculadas a unas 460 empresas privadas de seguridad, a pesar de la obligación de tener un registro oficial para su identificación.

RETOS

La reducción de los altos niveles de inseguridad es uno de los principales retos de muchos países latinoamericanos.

Las razones que explican la persistente violencia en sus sociedades son múltiples; entre ellas están la corrupción política y la desigualdad económica. Las clases más ricas pueden considerarse blanco de intentos de robo o secuestro, pero también las clases populares padecen las altas cifras de criminalidad, en su caso sin posibilidad de recurrir a la seguridad privada.

La seguridad privada en América Latina afronta dos importantes retos. Uno es ilegalidad de parte del sector: las empresas de corte ilegal crecen de forma más rápida que en el sector legal; en Brasil, por ejemplo, el número de guardias empleados informalmente supero a los formales.

El otro es la falta de entrenamiento o experiencia de cierto volumen de los guardias privados. Atender a la necesidad de mayor regulación legal, y de una regulación más ajustada a las especificidades nacionales, y a la conveniencia de mayor formación ayudará a reducir la zona gris en la que en muchos casos se opera y las violaciones de Derechos Humanos.

Texto basado en una aportación que el autor expuso en un Simposium de Criminología. ■

Columna de
Hermelindo Rodríguez Sánchez
hermers@hotmail.es

HERMELINDO RODRÍGUEZ SÁNCHEZ, CPO, CSSM, DSI, DES, CEO Y FUNDADOR DE LA CONSULTORÍA EN SEGURIDAD Y PROTECCIÓN INTEGRAL (COSEPRI).

Más sobre el autor:

IMPORTANCIA DE SER UN BUEN GUARDIA DE SEGURIDAD PRIVADA (PARTE I)

MÉXICO

Foto: Freepik

Es un trabajo que ofrece el crecimiento profesional, ya que se pueden cursar nuevas capacitaciones que te van a hacer escalar en el trabajo y por último el sueldo, ya que tendrás un horario fijo y una remuneración mensual, con prestaciones y seguro de vida

Si buscas un trabajo que sea *part-time*, no necesite experiencia y ni título universitario, si tienes mucho tiempo libre o si sólo quieres ganar dinero rápido, estable y bueno, pero que no tengas que volver a estudiar para trabajar, ¿alguna vez pensaste lo que hace un guardia de seguridad?

Sabemos que lo que quieres es trabajar rápido y que buscas algo sin requisito de título, mejor si es un trabajo *part-time* y sin experiencia en donde tengas un sueldo estable. Por lo que en esta guía te explicaremos todo lo necesario para que, ser guardia de seguridad privada, sea primera tu opción.

LO QUE SIGNIFICA GUARDIA DE SEGURIDAD

Es un profesional capacitado para ejercer funciones de protección de personas, infraestructuras, lugares y activos valiosos. Por lo general, cumplen funciones de:

- Resguardo de la integridad física de las personas de una organización.
- Vigilancia del cumplimiento de protocolos y servicios de instituciones.
- Monitoreo de recintos.
- El resguardo de bienes y activos.

Según la naturaleza o la necesidad del trabajo, el servicio de vigilancia, monitoreo, CCTV y protección puede ser más especializado, pero esto depende de las características y el riesgo del área.

LAS VENTAJAS Y LOS RIESGOS DE TRABAJAR DE GUARDIA DE SEGURIDAD

Ahora que ya sabemos lo que significa ser guardia de seguridad, explicaremos las ventajas que tiene el trabajar en esta área. Comencemos con que es un trabajo que siempre va a tener ofertas de empleo, ya que se están buscando personas para trabajar como guardia con frecuencia aún en tiempos de crisis y es un tra-

bajo que puede ser *part-time* y sobre todo es que es sin experiencia, sólo necesitas ser capaz, tener actitud positiva, buena visión, buen comportamiento, y ser socialmente respetuoso, este puede ser tu primer trabajo.

También es un trabajo que ofrece el crecimiento profesional, ya que se pueden cursar nuevas capacitaciones que te van a hacer escalar en el trabajo, y por último, el sueldo, ya que tendrás un horario fijo y una remuneración mensual, con prestaciones y seguro de vida. Se puede considerar un trabajo de medio tiempo, ya que con los turnos trabajas un par de días y luego descansas.

Es una oportunidad laboral para todas las personas, sin excepción, que el "no tengo título" no sea un límite. Aun así, debemos explicarle los riesgos que se pueden correr trabajando como guardia, en las tareas pueden ocurrir momentos que se vean violentados por personas o situaciones amenazantes, riesgos debido a la carga física, fatiga, carga emocional, sedentarismo en el caso de los que monitorean, y los riesgos en el recinto como caídas, golpes, atropellos, choques, atrapamientos, etc. Pero siempre contarás con equipos de seguridad personal y con elementos de protección, para evitar a toda costa estos riesgos.

UNIFORME DE UN GUARDIA DE SEGURIDAD

Según las normas y reglas del personal, estos deben vestir:

1) Gorra color negro, modelo militar, visera negra y barboquejo del mismo color.
2) Camisa color negra, confeccionada con tela gruesa o delgada, manga corta o larga abotonada, según la época del año.
3) Pantalón color negro, confeccionado con tela gruesa o delgada, según la época del año.
4) Calzado y calcetines negros.
5) Cinturón sin terciado, de cuero negro, con cartuchera del mismo color, para portar bastón retráctil, en caso que sea procedente.
6) Chaleco de alta visibilidad, color flúor o rojo, dependiendo de lo estipulado en uniforme declarado.
7) Chaquetón impermeable, con cierre o abotonado, para uso en la época del año que corresponda.

Un guardia siempre va a contar con elementos de protección personal.

¿TE ENCUENTRAS CAPACITADO PARA SER GUARDIA?

Seguramente crees que ser guardia es algo sencillo y que cualquiera puede hacerlo, pero no, estamos lejos de la realidad. Para ser guardia es necesario tener características psicológicas que te hagan poder cumplir con tu servicio.

Para ser guardia no basta con tener habilidades físicas, sino que también debes tener habilidades psicológicas que te hagan discernir, reaccionar, tolerar y solucionar situaciones de peligro, por ello en este artículo verás todas las características psicológicas que debe tener un guardia de seguridad.

Un guardia de seguridad debe poseer una serie de habilidades para desarrollar la importante labor

de seguridad, tanto en el aspecto físico como psicológico y el manejo de conflictos, por ello en esta guía te mostraremos las principales habilidades que debe tener un guardia para ejercer su labor.

Características psicológicas que debe tener un guardia de seguridad:

- Sentido de Pertenencia o Responsabilidad con lo que sucede en el entorno.
- La interacción con el entorno genera la necesidad del control consciente y el esfuerzo por lograr mantenerlo.
- Autoconsciencia o Nivel de Autoestima.
- En cada test psicológico de evaluación general, se debe indagar en el auto concepto, en el nivel de autoestima generado por la integración de la personalidad con la motivación de desempeñarse en el rol de guardia.

El rol en los servicios de seguridad:

Este rol debe ser establecido con claridad para así modelar la actitud y la conducta que asume el guardia de seguridad, esto va en los reglamentos y protocolos internos que permitan una adecuada selección de habilidades para su desempeño.

- **Tolerancia.** Algo muy importante es que el guardia sea tolerante, que logre dar respuestas adecuadas y proporcionadas frente a situaciones de frustración o conductas que evadan las reglas. Deben estar preparados para dar una respuesta persuasiva para reducir las actitudes negativas de respuesta.
- **Manejo de la agresión.** Dado que los guardias hacen frente a las situaciones de violencia, deben mantener la situación al margen siempre intentando buscar una solución al problema que sea. Deben exponer y buscar puntos de acuerdo de manera clara y objetiva, para así buscar la solución.
- **Control de Impulsos.** Un guardia de seguridad debe estar al tanto de los riesgos que se van a correr durante su jornada de trabajo, por ello, deben ser capaces de autorregularse, medirse y reprimir o reemplazar los impulsos frente a situaciones o provocaciones. Un factor importante para lograr esto es la experiencia ya que permite desarrollar la capacidad de ajustarse frente a cambios en el entorno. Esto se puede ver en un test psicológico.
- **La toma de decisiones.** Los actos de elección entre alternativas aun cuando implican incertidumbre siempre deben ser según los procedimientos estipulados y con actitud asertiva, deben apegarse a protocolos de forma racional y con equilibrio, con tolerancia y control de impulsos para la resolución de cualquier situación.
- **Solución de Conflictos.** La resolución de los conflictos debe estar basada en la empatía y la mediación, para contribuir a disuadir y evitar malos entendidos mediante el diálogo.

Por lo anterior, es importante que conozcas cuáles son las habilidades que tiene un guardia para ser el idóneo para la organización. ■

CONSULTORES EN SEGURIDAD INTEGRAL ®

40 AÑOS
Gracias a tu Confianza

CONSULTORES EN SEGURIDAD INTEGRAL: 40 AÑOS DE HONESTIDAD, LEALTAD Y MÍSTICA DE SERVICIO

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Conservar clientes de más de tres décadas, es resultado del profesionalismo y la atención personalizada que cada cliente requiere

Este año, la empresa Consultores en Seguridad Integral celebró cuatro décadas de brindar servicios bajo los mismos valores que la han caracterizado desde el principio: honestidad, integridad, lealtad y mística de servicio. Exactamente el 14 de mayo de 1984, inició el proyecto que, posteriormente, permitió que los C. Coroneles Miguel y Carlos González Zaragoza, encabezaran la Dirección de la primera empresa.

"El comienzo no fue fácil, a pesar de la enorme riqueza de conocimientos y experiencia de 25 y 20 años que cada uno de nosotros tenía a raíz de nuestro paso por la Policía Bancaria e Industrial, sin embargo, nos dimos cuenta de la gran oportunidad que teníamos, ya que, hasta ese momento, no existía una empresa de seguridad privada, y al ser pioneros en la industria, siempre buscamos brindar servicios de calidad, siendo honestos, íntegros y cuidando el salario y beneficios de nuestros colaboradores", comentó en entrevista el Cnel. Carlos González Zaragoza, director general de Consultores en Seguridad Integral.

Con tan sólo una máquina de escribir mecánica y una secretaria, en una oficina de 4x4 m, ubicada en el edificio Mallorca (CDMX), donde, por coincidencia, durante 20 años fue la Comandancia General de la P.B.I., la empresa comenzó a buscar clientes; "Segunda Mano" fue su primer servicio con tres elementos, en un horario de 12x24h, convirtiéndose en el amuleto de Consultores; después llegaron corporativos como Ingramex (35 años), Kimberly Clark (34 años), Procter and Gamble (32 años), Hospital ABC (26 años) y posteriormente se incorporaron otras empresas como IBM, Microsoft, Walmart, Smurfit Kappa, American Express, Grupo Peñafiel, entre otras, así como algunos condominios y zonas habitacionales.

Consultores en Seguridad Integral conserva clientes con más de 30 años de permanencia, resguardando y protegiendo sus bienes y capital humano. "La honestidad y el profesionalismo que adquirimos a lo largo de nuestra vida, nos ha llevado a ser los mejores, y así motivamos a cada uno de los integrantes de Consultores, siempre con mística del servicio para poder seguir creciendo. Además de nuestra experiencia en seguridad, desde un inicio nos destacamos por ofrecer un servicio personalizado, nosotros mismos íbamos y seguimos visitando a nuestros clientes", destacó el Coronel.

"Siempre buscamos brindar servicios de calidad, siendo honestos, íntegros y cuidando el salario y beneficios de nuestros colaboradores"

SEGURIDAD ESPECIALIZADA

Para el año 1992, la empresa estaba consolidada y el futuro se vislumbraba atractivo, pero al mismo tiempo difícil y retador, ya que en esos tiempos el auge de las empresas de seguridad privada fue notablemente intenso, así que gracias a los valores aprendidos: Integridad, Honestidad, Lealtad y Mística de Servicio, le agregaron un ingrediente extra que motivó a su personal a dar siempre el máximo de su esfuerzo.

"El secreto es mantener alta su moral, lograr que piensen menos en sí mismos y más en el Grupo, que la seguridad privada es tan útil y valiosa como la de las corporaciones, y que la ausencia de un arma de fuego, en ese año, debía superarse con tecnología e inteligencia, pero sobre todo con valor, destacándose, aunque reiterativo, por la Mística de Servicio".

A partir de Consultores en Seguridad Integral, surgen otras tres empresas debido al éxito y la demanda de servicios. La segunda, en 1991: Consultores en Protección Integral, quedando a cargo el Cnel. Miguel González Zaragoza; en 1992, nace Consultores Asociados en Protección Privada Empresarial, misma que comanda a la fecha el Cap. Salvador López Contreras.

Y para completar la escena de crecimiento se unió al Grupo en el año 1994, Consultores Internacionales de Seguridad Asociados, adición que coincidió con el arribo al grupo del recientemente retirado de la P.B.I. Superintendente José Luis Murillo Rincón quien, hasta el día de su fallecimiento, el 12 de octubre de 2024 (Q.E.P.D.), ocupó el cargo de Director General Adjunto, fue así que a la fecha las cuatro empresas siguen funcionando de forma eficaz y profesional.

"La seguridad es demandante, absorbente, y atractiva, por eso, desde un principio, le dedicamos todo nuestro esfuerzo y el Grupo se ha convertido en nuestra segunda familia, aquí convivimos todos por mucho tiempo. Y de nosotros dependen más de cuatro mil familias, eso nos genera una gran satisfacción y a la vez es una gran responsabilidad. Y así seguiremos, en honor también de nuestro compañero y amigo el Cnel. Murillo".

Desde el año 2012, el Grupo obtuvo los permisos de Portación de Armas que otorga la Secretaría de la Defensa Nacional (SEDENA) a nivel nacional, en sus tres modalidades: Intramuros, Traslado de Valores, y Seguridad a Personas.

"Iniciar una obra es una apariencia relativamente fácil, en ocasiones basta con tener recursos, un poco de reconocimientos y entusiasmo, pero perseverar en ella hasta ALCANZAR RECONOCIMIENTO, ESTABILIDAD Y PRESTIGIO, es algo diferente, ya que se requiere un esfuerzo continuo, RESPONSABILIDAD A TODA PRUEBA, mucho SACRIFICIO, PERO SOBRE TODO INTEGRIDAD Y RESPETO hacia los usuarios y a las otras empresas competidoras, bases sin las cuales no habría sido posible que Consultores en Seguridad Integral haya alcanzado la meta de 40 años brindando servicios de seguridad", finalizó el Cnel. Carlos González.

Dedicado con mucho cariño y respeto a la memoria del Cnel. José Luis Murillo Rincón (q.e.p.d.). ■

Fotos: Cortesía Consultores en Seguridad Integral

EL RETO DE ALIMENTAR AL MUNDO

Robo y vandalismo, fraude alimentario, contaminación intencional, interrupción en la cadena de suministro, son sólo algunos de los riesgos a los que está expuesta la industria alimentaria; además de la inseguridad que vive todo el país. ¿Será la tecnología su principal aliado?

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La industria alimentaria como tal tiene sus propias características que requieren de cuidados precisos para que los productos lleguen en perfecto estado a los consumidores, de hecho, su principal reto es garantizar la disponibilidad de alimentos seguros y nutritivos para toda la población, por ello es necesario mejorar las prácticas de producción, almacenamiento y distribución de alimentos para evitar la contaminación y garantizar la calidad.

Otro de los retos de este sector es la sostenibilidad, "el producir alimentos de manera sostenible, minimizando el impacto ambiental y promoviendo prácticas agrícolas y ganaderas responsables. Esto implica reducir el uso de agroquímicos, implementar técnicas de producción más eficientes y promover la conservación de los recursos naturales", así lo explicó Yovan Galico Wernicky, director de Seguridad Nestlé México, en entrevista para **Seguridad en América** (**SEA**).

El especialista en gestión de riesgos, también señaló como retos generales de la industria, el desarrollo rural, puesto que muchas zonas rurales en Latinoamérica enfrentan problemas de pobreza y falta de acceso a servicios básicos. "La industria alimentaria debe contribuir al desarrollo de estas comunidades, generando empleo y promoviendo la inclusión social", indicó. Y añadió a la innovación tecnológica, el cambio climático, la producción de una alimentación saludable, y el acceso a mercados internacionales para impulsar el crecimiento a través del cumplimiento de estándares de calidad y seguridad alimentaria exigidos por los países importadores.

El reto de alimentar al mundo es bastante complejo, y el área de Seguridad junto con sus vertientes, son primordiales para contrarrestar y superar los retos antes mencionados, es por ello, que además de entrevistar a Yovan Galico, **SEA** realizó una reunión con diversos especialistas en la materia para conocer los riesgos actuales de seguridad y cómo los están enfrentado.

RIESGOS DE SEGURIDAD

De acuerdo con datos de Overhaul, 31 por ciento de las mercancías robadas durante el primer semestre de 2024 fueron alimentos y bebidas, mientras que el nueve por ciento fueron productos misceláneos, además el informe publicado señaló, que, de esos robos de carga, el 84% se llevaron a cabo con algún tipo de violencia[1]. Alimentos y abarrotes son el blanco en carretera de la delincuencia organizada, estos productos llegan al mercado negro, en donde, una de las afectaciones más importante, es el impacto del costo en los alimentos.

"El riesgo de fraude en la industria alimentaria, donde se pueden adulterar o falsificar productos, puede comprometer la calidad y seguridad de los alimentos, así como dañar la reputación de las empresas", Yovan Galico

Nota: "Lo vertido en este artículo es a mi opinión personal y no representa la opinión ni posición de la empresa en la cual laboro"

Foto: Freepik

En agosto del presente año, decenas de limoneros suspendieron sus actividades de forma indefinida en huertas de los municipios de Apatzingán, Buenavista y Parácuaro, tierras que están dentro de la región llamada "Tierra Caliente" en el estado de Michoacán, según ellos, debido a que los cárteles aumentaron de dos a tres pesos el pago de un "impuesto criminal" por cada kilogramo que llega a las empacadoras.

"Eventos como desastres naturales, conflictos sociales, el robo de transporte de carga o los problemas logísticos pueden interrumpir la cadena de suministro de alimentos. Esto puede afectar la disponibilidad de productos, generar pérdidas económicas y dificultar el abastecimiento de alimentos a la población", explicó Yovan Galico.

El especialista agregó los siguientes riesgos de seguridad, de acuerdo con su análisis y experiencia:

- **Robo y vandalismo:** Las instalaciones de producción, almacenamiento, distribución y el transporte de alimentos son susceptibles a robos y actos de vandalismo. Esto puede resultar en pérdidas económicas significativas y afectar la continuidad de la cadena de suministro.
- **Fraude alimentario:** Existe el riesgo de fraude en la industria alimentaria, donde se pueden adulterar o falsificar productos alimentarios. Esto puede comprometer la calidad y seguridad de los alimentos, así como dañar la reputación de las empresas.
- **Contaminación intencional:** La industria alimentaria también enfrenta el riesgo de contaminación intencional de productos, ya sea por motivos económicos o por actos de sabotaje. Esto puede tener graves consecuencias para la salud de los consumidores y generar pérdidas económicas considerables.
- **Incendios y explosiones:** Las instalaciones de la industria alimentaria están expuestas al riesgo de incendios y explosiones, especialmente en áreas de producción y almacenamiento donde se manejan sustancias inflamables. Estos incidentes pueden causar daños materiales significativos y poner en peligro la vida de los trabajadores.
- **Ciberseguridad:** Con el aumento de la digitalización en la industria alimentaria, existe el riesgo de ciberataques que pueden comprometer la seguridad de los sistemas informáticos, las líneas de producción y la confidencialidad de la información. Esto puede afectar la operatividad de las empresas y poner en riesgo la integridad de los datos.

"Es importante que las empresas de la industria alimentaria en México implementen medidas de seguridad patrimonial adecuadas para mitigar estos riesgos, como sistemas de vigilancia, controles de acceso, protocolos de seguridad, capacitación del personal y planes de contingencia. Además, es fundamental contar con una cultura de seguridad y promover la colaboración con las autoridades competentes para prevenir y responder eficientemente a los riesgos de seguridad patrimonial", puntualizó.

ESTRATEGIA DE SEGURIDAD

La única constante que existe en el campo de la seguridad, es el cambio. Cada día los especialistas del área están en constantes foros de actualización, ya sea compartiendo sus experiencias y resultados, o bien aprendiendo los nuevos modus operandi de la delincuencia, y planteándose nuevas estrategias para combatir esos riesgos.

"Una de las estrategias con la que hemos tenido buenos resultados, es el monitoreo dedicado a través de las cámaras de videovigilancia y la supervisión efectiva para asegurar que se cumplan con los procesos y procedimientos. Respecto al robo de mercancía en tránsito, seguir los lineamientos de Seguridad para los transportistas, y el monitoreo dedicado en rutas peligrosas; así como la custodia en corredores y la afiliación a los programas de prevención de robos de la Guardia Nacional: LAICA, Cordillera Segura y Escalón", compartió Rodrigo Tinajero López, gerente nacional de Seguridad Patrimonial de Grupo Bafar.

Hasta el mes de agosto, la Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV) reportó 2 mil 294 vehículos robados, de los cuales, mil 135 corresponden a unidades de carga. Durante ese mes, el Estado de México, registró un incremento del 11.8%, Puebla del 17.6%, y Nuevo León, 160%, con respecto a los meses pasados[2].

Frente a esta situación, los especialistas se cuestionan si ha llegado el momento de blindar las unidades de carga. Oscar Torres, CPP, responsable de Seguridad Patrimonial en GEPP, considera que sí. "Sería

"Una de las estrategias con la que hemos tenido buenos resultados, es el monitoreo dedicado a través de las cámaras de videovigilancia y la supervisión efectiva para asegurar que se cumplan con los procesos y procedimientos", Rodrigo Tinajero

"Tenemos que seguir buscando y desarrollando más estrategias y herramientas que permitan minimizar el riesgo; el apoyo entre empresas y el intercambio de información resultan de vital importancia", Jorge Garcés Anaya

Foto:–Freepik

muy viable implementar el uso de blindaje en vehículos de carga primaria siempre y cuando se justifique el costo vs. beneficio dependiendo del valor de la carga, pero en el caso del negocio de bebidas esto incrementaría de manera muy importante los costos de operación no justificándose los mismos; en el caso de otros negocios de la industria posiblemente sí sea una alternativa a considerar, sobre todo por la integridad de los operadores".

Por su parte, Gerardo Ortega, director de Seguridad Integral de ROCA, compartió las siguientes estrategias:

- HACCP (Hazard Analysis and Crittical Control Pooints). Es un proceso sistemático preventivo, para garantizar la inocuidad alimentaria, de forma lógica y objetiva.
- Ley de modernización de la inocuidad alimentaria (FSMA) de USA.
- Capacitación constante de los colaboradores.
- Sistema de gestión de la inocuidad alimentaria.

"A lo largo de la cadena de suministro tenemos controles y sistemas que nos fortalecen, siendo sin duda el más fuerte, la capacitación y los canales de comunicación con el capital humano en cada etapa de nuestros procesos", indicó Ortega.

Uno de los riesgos que sigue presente en distintas industrias, es el robo hormiga, Jorge Garcés Anaya, director de Seguridad de Grupo Herdez, explicó que en su equipo se realizaron trabajos de campo con enfoques muy precisos para identificar y entender de manera más puntual cómo opera el robo hormiga, desde las líneas de producto terminado hasta su embalaje y trasportación a centros de distribución y después al cliente final.

"Una vez entendida la forma de operar, hicimos modificaciones sustantivas para tener certeza de la existencia de cada producto, se dotó de herramientas electrónicas a cada responsable de área que participa en las distintas etapas de la cadena productiva y logística, para auditar en cualquier momento la entrada, almacenamiento y entrega de productos al transportista para entrega al cliente final. Todo esto con el objetivo de tener áreas más ordenadas y con mejor visibilidad".

También redujeron el número de tarimas apiladas en toda la bodega, lo que permite al personal de Seguridad tener una mejor visión de lo que sucede entre líneas de circulación, y apoyado todo esto con circuito cerrado de televisión (CCTV), incluidas las puertas de embarque y patios de salida donde los conductores de los tráileres no conocen el contenido ni la caja que les será asignada.

La tecnología es una herramienta que hoy en día forma parte indispensable para la prevención, monitoreo y reacción de cualquier compañía, sin embargo y pese a los pronósticos con la llegada de la Inteligencia Artificial, el capital humano sigue siendo requerido para el control en esta área. "Definitivamente la seguridad privada seguirá siendo requerida en esta industria, podemos crear binomios con los guardias de seguridad y la tecnología, definiendo funciones y actividades claras, sin dejar nada a la interpretación", externó Rodrigo Tinajero, también Jorge Garcés la considera necesaria, tanto la seguridad privada como de la seguridad pública y las prestadoras de servicios de custodia. "En paralelo a la seguridad privada, nosotros tenemos que seguir buscando y desarrollando más estrategias y herramientas que permitan minimizar el riesgo; el apoyo entre empresas y el intercambio de información resultan de vital importancia", comentó el especialista.

TECNOLOGÍA EN SEGURIDAD

Uno de los especialistas invitado para hablar sobre la seguridad en la cadena de suministro y logística, fue David Bautista, *Chief Security Officer* en Detecta, quien habló sobre los beneficios de implemen-

tar plataformas de rastreo con Inteligencia Artificia para la mercancía en ruta.

Detecta es una es una compañía de tecnología enfocada en solucionar, proteger, y optimizar riesgos en la cadena logística, algunos de sus valores añadidos son: calidad de servicio, precio competitivo y altos niveles de eficiencia (siniestralidad y recuperación). Sus servicios se dividen en dos rubros:

1. Digital

Consiste en la implementación de soluciones de tecnología (rastreo satelital) con aplicaciones de telemetría, monitoreo según los más altos estándares de seguridad con protocolos de prevención y reacción, así como la coordinación con las autoridades en caso de siniestro para buscar su recuperación.

- *Checkmark.*
- Rastreo Satelital | GPS.
- Videovigilancia | CCTV.
- Candados | Retardadores.
- Monitoreo.
- Reacción.

2. Dedicado

Además de incluir los servicios de DETECTA DIGITAL, el dispositivo de seguridad se refuerza con patrullas físicas de custodia cuya función es garantizar el cumplimiento de las consignas de seguridad definidas.

- *Checkmark.*
- Rastreo Satelital | GPS.
- Videovigilancia | CCTV.
- Candados | Retardadores.
- Monitoreo.
- Reacción.
- Custodia Física.
- Informes de inteligencia.
- *Risk Assessment.*

David señaló que este tipo de reuniones les ayuda a conocer y comprender de viva voz, las necesidades que industrias, como la alimentaria, requieren específicamente para mitigar los riesgos actuales de seguridad en la cadena de suministro y logística.

TENDENCIAS PARA EL 2025

Estamos en el último bimestre del año, y después de haber enfrentado un periodo violento de campaña electoral, será el 2025 el año que empiece a definir el rumbo de la nueva mandataria, las reformas aprobadas, y en este caso, los estragos de seguridad y nuevos retos por enfrentar.

Para Oscar Torres, las tendencias en seguridad de la industria alimentaria, reflejarán la necesidad de proteger, tanto los activos físicos como la propiedad intelectual, en un entorno cada vez más digitalizado y globalizado. Integración de tecnologías avanzadas de vigilancia, ciberseguridad y protección de la infraestructura crítica, sistemas de control de acceso mejorados, gestión del riesgo interno, automatización de la seguridad, colaboración con las fuerzas de seguridad y comunidades, protección contra el sabotaje y la adulteración de productos y la gestión de crisis y continuidad del negocio, son algunas que el especialista mencionó.

Foto: Freepik

"Sería muy viable implementar el uso de blindaje en vehículos de carga primaria siempre y cuando se justifique el costo Vs. beneficio dependiendo del valor de la carga", Oscar Torres

"Las innovaciones tecnológicas, como la inteligencia artificial vienen a fortalecer y/o reemplazar métodos tradicionales para dar lugar a un producto más seguro y mejorar de forma sustancial la eficiencia en la producción y la gestión de la cadena de suministro", Gerardo Ortega

"Todas ellas, serán reflejo de un entorno cada vez más complejo y exigente, donde la tecnología y la sostenibilidad jugarán un papel fundamental siendo las más relevantes las tecnologías de rastreo y trazabilidad, el uso de IA y *Big Data* para predecir riesgos y optimizar procesos; respecto a la seguridad en la cadena de suministro, el enfoque estará puesto en la sostenibilidad y la cultura de seguridad promoviendo una mayor conciencia y formación en temas de seguridad dentro de las organizaciones", indicó.

También hizo la recomendación de continuar con la automatización de la seguridad para mejorar la eficiencia de los procesos y depender menos del factor y error humano, incluyendo el uso de robots de seguridad para patrullaje y monitoreo, así como la detección de intrusos y la respuesta a emergencias.

Por su parte, Gerardo Ortega añadió que esta industria muestra una clara tendencia hacia la valoración de la seguridad alimentaria y la sostenibilidad ambiental, derivado de que existe mayor conciencia sobre la salud, se quieren y requieren más productos con ingredientes naturales, considerados nutritivos y que tengan un valor agregado vs. otras alternativas, aunado a que el consumidor pide que las empresas muestren transparencia en sus etiquetados conforme a los ingredientes que constituyen sus productos.

"Las innovaciones tecnológicas, como la inteligencia artificial vienen a fortalecer y/o reemplazar métodos tradicionales para dar lugar a un producto más seguro y mejorar de forma sustancial la eficiencia en la producción y la gestión de la cadena de suministro. Como consecuencia se espera un menor impacto ambiental, de la mano del uso de certificaciones y auditorías de Responsabilidad Social que coadyuven a garantizar la seguridad alimentaria", añadió.

Debido a que las estadísticas muestran que el robo a transporte de carga, desafortunadamente, va en aumento, Jorge Garcés considera que el próximo año la implementación de tecnologías para el rastreo de productos, como el *blockchain* estarán más presentes.

"Veremos la integración de la Inteligencia Artificial, que hace posible analizar gran cantidad de datos que permitan identificar patrones y prever riesgos, tener una gestión efectiva y respuesta a posibles problemas, dicho de otra manera, el tener la capacidad de anticipar y prevenir problemas antes de que sucedan. La Robótica será otra tendencia que augura una mayor eficiencia en los procesos de envasado, empaquetado y palettizado".

La tecnología en la industria de los alimentos ha tenido un crecimiento importante, explicó Garcés, el uso de *software*, de aplicaciones y programas diseñados a medida los sistemas para el proceso de alimentos, la información en la cadena de suministro, la información de clientes y proveedores puede ser información vulnerable a ataques cibernéticos, lo que lleva a la organización a realizar acciones que permitan garantizar la protección de los sistemas de manera efectiva, por ende, una tendencia del 2025, será el robustecer las medidas de ciberseguridad de las compañías.

LAS 5 PARTICULARIDADES
QUE SEGURIDAD DEBE TOMAR EN CUENTA PARA LA CADENA DE SUMINISTRO, DE ACUERDO CON YOVAN GALICO

1) **Cadena de frío:** Los productos perecederos requieren condiciones específicas de temperatura para mantener su calidad y seguridad. El área de Seguridad Patrimonial debe asegurarse de que los sistemas de refrigeración y almacenamiento estén adecuadamente protegidos y funcionando correctamente.

2) **Manipulación de productos químicos:** Desinfectantes, pesticidas y aditivos alimentarios. El área de Seguridad Patrimonial debe garantizar que estos productos estén almacenados y manejados de manera segura, evitando su acceso no autorizado y minimizando el riesgo de contaminación o accidentes.

3) **Alta rotación de personal:** Esto es común y puede aumentar el riesgo de robos internos o la divulgación de información confidencial. Seguridad Patrimonial debe implementar medidas de control de acceso y realizar verificaciones de antecedentes para mitigar estos riesgos.

4) **Cumplimiento normativo:** La industria alimentaria está sujeta a una amplia gama de normativas y regulaciones, tanto a nivel nacional como internacional, relacionadas con la calidad, seguridad y etiquetado de los alimentos. Seguridad Patrimonial debe asegurarse de que la empresa cumpla con todas las normativas aplicables y mantener registros adecuados para demostrar el cumplimiento.

5) **Vulnerabilidad a la contaminación:** La industria alimentaria es especialmente vulnerable a la contaminación, ya sea por microorganismos, sustancias químicas o alérgenos. Seguridad Patrimonial debe implementar medidas de control y monitoreo para prevenir la contaminación de los alimentos, como la instalación de sistemas de filtración de aire, controles de plagas y protocolos de limpieza y desinfección rigurosos.

Referencias:
1 *"Alimentos y bebidas son el 31% de las mercancías robadas a transporte de carga: Overhaul". Sara Garcés, Milenio 19/08/2024. https://www.milenio.com/negocios/alimentos-bebidas-representan-31-ciento-mercancias-robadas*
2 *"Reporte de robo y recuperación de vehículos" Agosto, 2024. ANERPV.*

Fotos: Mónica Ramos / SEA

Agradecemos las facilidades otorgadas a Hacienda de Los Morales, para la realización de este reportaje.

Este reportaje se llevó a cabo gracias al patrocinio de Detecta.

VEHÍCULOS ELÉCTRICOS: EL NUEVO RETO DE LA INDUSTRIA AUTOMOTRIZ

Las industrias del mundo están cambiando su forma de producir, la sustentabilidad es ahora parte fundamental del desarrollo de un producto, ¿cómo se está adaptando la seguridad a este cambio?

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Las ventas de automóviles nuevos con algún grado de electrificación en México, crecieron 44.3% (73 mil 680 unidades), en 2023, de acuerdo con cifras del Instituto Nacional de Estadística y Geografía (INEGI), siendo un mercado que va al alza, aunque el proceso parezca lento. En ese mismo año, se comercializaron en México un total de un millón 361 mil 433 automóviles nuevos, la participación de mercado del segmento de coches electrificados fue de 5.4%, mostrando un incremento de 0.7 puntos respecto al año anterior (4.7%).

En el primer bimestre de este año, las ventas de vehículos híbridos y eléctricos en México crecieron 58% anual a 7 mil 248 unidades, se comercializaron 1,405 automóviles, de acuerdo a cifras del Registro Administrativo de la Industria Automotriz de Vehículos Ligeros (RAIAVL), emitido por el INEGI. Actualmente hay una oferta de 60 modelos de coches de este tipo en el mercado mexicano, y se espera que continúen importando y produciéndose más. Sin embargo, aún hay mucho desconocimiento respecto al uso correcto de estas unidades, el daño y reparación de alguna de sus partes, la prevención y reacción ante un incidente, y desinformación sobre qué sí y qué no ocurre con las baterías, principalmente.

La industria automotriz enfrenta diferentes retos de seguridad, además de aquellos que convergen dentro y fuera de ella, se suma la producción en aumento de estos vehículos, es por ello que realizamos una serie de entrevistas con especialistas en el tema para conocer los riesgos y mejores prácticas de seguridad de este sector.

PANORAMA MUNDIAL DE LA INDUSTRIA AUTOMOTRIZ

De acuerdo al análisis de los especialistas, este sector tiene puesta su atención en dos aspectos: uno, la electrificación de los vehículos; y dos, la comercialización en potencia de unidades de origen chino.

"La industria automotriz está pasando por varios cambios a nivel mundial. Uno de ellos es el aumento de inversión y producción de vehículos eléctricos o híbridos, sin embargo falta mucho para que estos puedan responder a las necesidades de sus usuarios, por ejemplo, los vehículos de carga o de transporte público pueden verse comprometidos, ya que recorren largas distancias y tendrían que pararse varias veces y por lapsos de tiempo prolongados, para poder recargar la batería y así poder continuar su recorrido, lo cual también significaría un tema de seguridad", explicó Guillermo Hassey, gerente de Seguridad Corporativa en Daimler Truck México.

Otro de los cambios que comentó el especialista, tiene que ver con la entrada de nuevos competidores, principalmente chinos, en este segmento de vehículos a nivel mundial, ofreciendo niveles de calidad muy similares a los de las marcas consolidadas en el mercado, pero su precio es significativamente más bajo, debido a que los costos de producción en China son muy bajos por el sistema de apoyos gubernamentales que tienen.

"Para hacerlos competitivos (los vehículos), el gobierno subsidia impactando en los costos de producción. Por lo tanto, en algunos mercados esto se ve como una práctica desleal y se están imponiendo altas tasas de aranceles para la comercialización en estos mercados. Estas dos perspectivas hacen que el panorama en la industria automotriz a nivel mundial sea muy retador y un tanto incierto", comentó.

Los vehículos eléctricos (VE) representan una innovación clave en el sector automotriz, pero también traen consigo nuevos desafíos de seguridad que deben abordarse con particular atención en México. Enrique Arellano, MBA, *Corp. Security Manager* en Mercedes-Benz México, hace las siguientes recomendaciones de seguridad:

1) **Infraestructura de carga segura.** Es fundamental que las estaciones de carga, tanto públicas como privadas, cuenten con certificaciones y estándares adecuados para evitar sobrecargas eléctricas, cortocircuitos o incendios. En México, es necesario garantizar que los puntos de carga cumplan con las normativas de seguridad eléctrica, especialmente en áreas donde la red eléctrica puede ser más inestable.
2) **Protección contra incendios en baterías.** Los vehículos eléctricos utilizan baterías de iones de litio, que, aunque son eficientes, presentan un riesgo de incendio si no se manejan correctamente. Las empresas automotrices deben asegurar que los vehículos cumplan con estándares internacionales de seguridad de baterías y que los consumidores sean educados sobre el mantenimiento adecuado para minimizar el riesgo de incidentes.
3) **Ciberseguridad.** Con el aumento de la conectividad en los vehículos eléctricos, surge una nueva dimensión de riesgos relacionados con la seguridad cibernética. Los sistemas digitales y *software* que gestionan algunas funciones tales como la navegación autónoma y segura, apertura y cierre de los autos, control de carga de la batería y/o las actualizaciones remotas, pueden ser vulnerables a ciberataques. Es crucial que los fabricantes implementen medidas robustas de ciberseguridad para proteger tanto a los vehículos como a los datos personales de los usuarios.
4) **Capacitación para emergencias.** En México, es esencial capacitar a los equipos de emergencia y rescate para que sepan cómo manejar incidentes que involucren vehículos eléctricos, ya que estos vehículos requieren un enfoque distinto en caso de accidentes, especialmente por la presencia de baterías de alto voltaje. La formación adecuada garantizará una respuesta rápida y segura en situaciones de emergencia.
5) **Normativas locales y estándares internacionales.** Es importante que México actualice y adopte regulaciones específicas para vehículos eléctricos, tomando como referencia estándares internacionales de seguridad, pero adaptándolos a las condiciones locales. Esto abarca desde la seguridad en la construcción de los vehículos hasta el transporte y disposición final de las baterías usadas, las cuales también representan un riesgo ambiental si no se gestionan de manera adecuada.
6) **Seguridad en la conducción.** Los vehículos eléctricos suelen ser más silenciosos que los convencionales, lo que puede representar un riesgo para peatones y ciclistas, especialmente en áreas urbanas densamente pobladas. Los fabricantes deben considerar la implementación de alertas sonoras para

"Los vehículos eléctricos de carga o de transporte público pueden verse comprometidos, ya que recorren largas distancias y tendrían que pararse varias veces y por lapsos de tiempo prolongados, lo que significaría un tema de seguridad", Guillermo Hassey

"Los sistemas digitales y software que gestionan algunas funciones tales como la navegación autónoma y segura, apertura y cierre de los autos, control de carga de la batería y/o las actualizaciones remotas, pueden ser vulnerables a ciberataques", Enrique Arellano

Foto: Freepik

los VE a bajas velocidades, de acuerdo con las regulaciones internacionales, para mejorar la seguridad vial.

PRINCIPALES RIESGOS

Los riesgos de la industria automotriz son una combinación de desafíos operativos, logísticos, tecnológicos y de seguridad pública. De acuerdo con el análisis de Guillermo Hassey, los principales son:

- **Riesgos de Seguridad Pública y crimen organizado.** El robo de camiones y vehículos en tránsito es uno de los mayores desafíos para la cadena de suministro automotriz en México. Los vehículos que transportan autopartes y materiales para la fabricación de automóviles son objetivos frecuentes de robos, especialmente en carreteras clave como la autopista México-Puebla, el corredor industrial del Bajío y el corredor exportador hacia Nuevo Laredo.
  La disrupción en la cadena de suministro, ya sea por bloqueos de carreteras, robos o retrasos en la entrega de insumos, representa un gran riesgo para la continuidad de las operaciones de las fábricas automotrices, este tipo de acciones del crimen organizado actualmente afecta la capacidad de las empresas para garantizar un transporte seguro de insumos y productos terminados.
- **Riesgos cibernéticos**: La industria automotriz, que depende cada vez más de tecnologías avanzadas, es un objetivo para los ataques cibernéticos. Los ciberataques dirigidos a sistemas de producción, diseño o almacenamiento de datos pueden causar interrupciones en la fabricación y exponer datos sensibles de la empresa. Muchos de estos ataques pueden estar focalizados en el robo de propiedad intelectual, como el diseño de vehículos, tecnologías de manufactura o datos de investigación y desarrollo, es una preocupación creciente, especialmente con la digitalización de las operaciones.
- **Riesgos de corrupción y cumplimiento regulatorio:** la corrupción en ciertos niveles de gobierno puede representar un riesgo significativo para las empresas automotrices, especialmente en la obtención de permisos y regulaciones para operar. La necesidad de cumplir con múltiples normativas locales, estatales y federales añade complejidad, y las empresas que no manejan bien estos riesgos podrían enfrentar sanciones o interrupciones en sus operaciones.

Por su parte, Enrique Arellano agregó que la industria también enfrenta el desafío de la contaminación y el robo de autopartes, factores que están provocando pérdidas millonarias en las líneas de producción y en la comercialización de posventa. Estas actividades no sólo afectan la estabilidad financiera del sector, sino que también deterioran la confianza en la cadena de suministro.

"El robo de vehículos terminados es un problema cada vez más visible debido a los sofisticados métodos que emplea el crimen organizado para apoderarse de los automóviles de manera ilegal. Este fenómeno no sólo representa un grave daño económico para la industria automotriz, sino que también impacta directamente a los clientes finales. En muchos casos, quienes esperaban la entrega de su vehículo se ven forzados a posponer su adquisición o, en situaciones extremas, cancelar la compra, lo que genera un efecto dominó en la economía local y nacional. Este escenario de inseguridad coloca a México en una posición desafiante, afectando tanto la percepción del país como su competitividad en el mercado global", destacó Arellano.

El área de seguridad debe visualizar y tener identificados esos riesgos, que no solamente implican a la industria, sino también su contexto social, demográfico, comercial, local. "La seguridad en la industria automotriz se debe de ver desde un punto de vista de socio de negocio, somos una parte fundamental en toda la cadena de producción, desde la seguridad de los empleados, material productivo, cadena de suministro, seguridad de instalaciones, coordinación con autoridades, uso de sistemas tecnológicos hasta el manejo de crisis y respuesta a emergencias", comentó Erik Navarro

García, *Head of Stellantis Mexico Security and Fire Prevention.*

El especialista agregó que, específicamente, la cadena de suministro se encuentra muy vulnerable hoy en día, y que aspectos como la impunidad, desatención de autoridades, falta de capacitación de operadores, presencia y control territorial de la delincuencia organizada, así como la falta de estado de derecho en algunas zonas del país, y la insuficiente infraestructura ferroviaria, colocan en riesgo el crecimiento y la inversión a este sector.

Por su parte, Alfonso S. Solleiro, *Security Director & LR Mexico* de Pirelli, señaló que, en el mercado de los neumáticos, es esencial evitar los mercados negros, tanto por la propia protección de la marca, como, la competencia ilegal y desleal que se genera, propiciando mermas importantes en las utilidades de las empresas dedicadas a la legal comercialización de estos productos, debido a que las llantas son un *commodity* de gran comercialización.

"Debemos desarrollar un sistema integral de gestión de seguridad para la cadena de suministro, en donde sean analizados y verificados todos y cada uno de los eslabones que la integran, como lo son: la infraestructura de todos los socios logísticos y esquemas de selección de personal, programas de capacitación, de mantenimiento a las unidades, centrales de monitoreo. También es importante un análisis profundo de nuestro producto final y materias primas; debemos darles un tratamiento de riesgos para que, con base en la administración de estos, podamos entender el potencial de abastecimiento a mercados negros a los que son susceptibles. Finalmente, los análisis de vulnerabilidad para nuestra propia operación y nuestras rutas de suministro son necesarias", detalló.

SOLUCIONES DE SEGURIDAD PARA LAS NUEVAS REFORMAS A LA LEY

Los especialistas resaltaron trabajar bajo procesos bien establecidos de seguridad, protocolos que conozca el personal, y compartieron algunas soluciones que les han funcionado, ya que actualmente, la seguridad privada requiere ser complementada con nuevas tecnologías, recordando, también, que el crimen organizado también muestra conocimiento de éstas, incluso de contrainteligencia.

Junto con los responsables de Seguridad, Alejandro Rojas, del equipo comercial de Convergint; Carlos Sánchez y Ricardo Riva Palacio, gerente regional de Ventas, y gerente de Ventas Verticales Enterprise de Genetec, respectivamente; así como Jorge Galán, gerente de Ventas de IDEMIA, compartieron algunas de las soluciones más innovadoras que han aplicado en este sector con gran éxito, y aquellas que se pueden adaptar como un "traje a la medida", de acuerdo con sus requerimientos.

"Convergint, junto con sus socios, tiene la capacidad de ofrecer proyectos integrales y personalizados que satisfagan estas necesidades. Nos especializamos en diseñar soluciones a la medida, adaptándose a las especificaciones y requerimientos únicos de cada cliente. Esto incluye la integración de sistemas avanzados de vigilancia, control de acceso y monitoreo en tiempo real, asegurando una protección completa y eficiente para la infraestructura y los activos de las empresas automotrices", comentó Alejandro Rojas.

En cuanto a soluciones de seguridad unificadas, Genetec proporciona una plataforma tecnológica que unifica video y analíticas, mapas, sensores, radares, entre otros. Esto permite a los departamentos de Seguridad detectar y prevenir eventos como robos en casetas de telecomunicaciones e intrusiones en sus propiedades, así como apoyar en tiempo real con visualización de lo

"Somos una parte fundamental en toda la cadena de producción, desde la seguridad de los empleados, material productivo, cadena de suministro… hasta el manejo de crisis y respuesta a emergencias", Erik Navarro

"Es importante un análisis profundo de nuestro producto final y materias primas; debemos darles un tratamiento de riesgos para que podamos entender el potencial de abastecimiento a mercados negros a los que son susceptibles", Alfonso S. Solleiro

Foto: Freepik

que sucede en los patios de maniobras, tanto con video como con posicionamiento en mapas y valores de sensores. Todos estos elementos, unificados bajo la plataforma *Security Center*, pueden ser complementados con la automatización y asistencia para la atención de incidentes que aporta el módulo de Mission Control.

"Genetec recomienda a los responsables de Seguridad tener amplio conocimiento de la infraestructura instalada en sus plantas y corporativos para validarlas en cuanto a compatibilidad y certificaciones internacionales, y conocer las políticas de la empresa respecto al uso de biométricos. Para 2025, Genetec presenta tendencias enfocadas en inteligencia artificial, analíticas y plataformas de seguridad que correlacionen los datos de manera óptima y auditable, fortaleciendo así la seguridad en el sector automotriz", detalló Carlos Sánchez.

Complementando esta ecuación, IDEMIA, uno de los líderes en controles de acceso biométricos, identificó retos claros en el sector automotriz como la optimización de procesos, la capacitación del personal operativo y la integración de infraestructura existente. De acuerdo con su análisis, recomienda fortalecer la seguridad de la cadena de suministro mediante la automatización de procesos con IA en video para el transporte y logística, procesos de ensamble y actividades inusuales o sospechosas. De igual forma, precisa incluir la automatización de controles de acceso en pagos de nóminas, reclutamiento de nuevo personal (interno y externo), y monitoreo de afluencia, asegurando que todo esté integrado.

"La tecnología de identidad de IDEMIA mejora significativamente la seguridad en plantas automotrices al asegurar que sólo las personas autorizadas accedan a áreas sensibles, protegiendo la confidencialidad y la integridad de los reportes de acceso. Optimiza la gestión de riesgos al reducir eventos fallidos, eliminar el riesgo de robo de identidad y accesos no autorizados, y rastrear accesos sospechosos. Además, mejora la productividad mediante la automatización de entradas y salidas, eliminando cuellos de botella y reduciendo la necesidad de recursos humanos. Ofrece máxima seguridad de información con archivos biométricos cifrados, un algoritmo propietario, cifrado punto a punto y configuraciones 'Security by Default' que cumplen con normas internacionales como GDPR", complementó Jorge Galán.

Uno de los aspectos que está presente en todas las industrias y que la automotriz ya está trabajando, tiene que ver con las nuevas Reformas a la Ley, por ello se presentó una solución para cumplir con la normatividad, y es la actualización del Sistema de Gestión de Talento en México, enfocándose en la regulación de las 40 horas semanales laborables.

Convergint y sus socios, pueden ayudar a las empresas a cumplir con esta normativa mediante la implementación de sistemas de control de acceso, videovigilancia y analítica avanzada. Estos sistemas registran la presencia del personal y generan evidencia visual y analítica para demostrar el cumplimiento legal. La adopción de estas tecnologías asegura que las empresas cumplan con las regulaciones oficiales, eviten sanciones y mejoren la seguridad laboral al monitorear y controlar el acceso a las instalaciones, protegiendo a empleados y activos.

La tecnología continuará evolucionando de acuerdo a las necesidades de cada sector y los retos que existen y aquellos que irán surgiendo, y ese es un reto que las marcas antes mencionadas tienen presente y los responsables de Seguridad.

"Referido a las tendencias tecnológicas, la convergencia en los sistemas

Foto: Freepik

"La seguridad digital, es decir, aquella responsable de proteger la parte tecnológica de nuestros autos, es uno de los desafíos a considerar con una mayor prioridad, al igual que el resguardo, manipulación y contención segura de los componentes químicos necesarios para la electromovilidad",

Alejandro G. Barrera, Security Chief en General Motors (GM)

de administración y control es lo que se vislumbra siga evolucionando hacia el futuro. En la medida que logramos integrar las soluciones de seguridad existentes de cualquier tipo: video, alarmas, accesos, evacuación, incendio, etc., mediante una arquitectura abierta que facilite el intercambio de datos a nivel lógico, alcanzaremos un nivel de maduración adecuado enfocado en la prevención y no sólo en la reacción", explicó Martín Calvo Etcheverry, director de Seguridad Corporativa en Volkswagen México.

Un ejemplo de esto es cuando se consigue vincular alarmas con apertura automática de barreras de accesos, cámaras de video y mapas en una sola interfaz visual hacia un operador de seguridad electrónica que permita tomar decisiones adecuadas antes del agravamiento de la situación planteada.

El especialista también agregó un reto tecnológico, y es la aplicación de la IA sobre los sistemas convergentes de seguridad mencionados precedentemente. Aplicar su capacidad predictiva sobre las fuentes de recolección de datos que son dichos sistemas, es de igual manera una de las tendencias más relevantes a tener en cuenta para los profesionales de seguridad.

RUMBO AL 2025

Definitivamente este año tuvo cambios drásticos en todo el país, nos encontramos en el cierre, y los especialistas en seguridad, ya tienen previsto lo que depara el 2025. "Desde mi punto de vista, tenemos grandes retos para el siguiente año, entre ellos, seguridad en la infraestructura ferroviaria, el fortalecimiento/debilitamiento del Estado de Derecho y de corporaciones de seguridad de los tres niveles de gobierno, impunidad y corrupción, certeza para el establecimiento de empresas proveedoras de la industria automotriz, y aquellos que convergen con el *nearshoring*", comentó Erik Navarro.

Sobre los retos, Martín Calvo sigue considerando a los vehículos electrificados puesto que estamos una trasformación histórica que modifica el paradigma, colocando a la sostenibilidad como prioridad en el nuevo modelo.

"En las tensiones habituales que toda transformación lleva implícita, y que por cierto está tomando más tiempo del que inicialmente se pensaba, la seguridad también se está adecuando a este nuevo escenario en el cual a los clásicos retos que vivimos a diario, se le agregan aquellos derivados de esta situación. La seguridad digital, es decir, aquella responsable de proteger la parte tecnológica de nuestros autos (cada vez más evolucionada), es uno de los desafíos a considerar con una mayor prioridad, al igual que el resguardo, manipulación y contención segura de los componentes químicos necesarios para la electromovilidad".

Poniendo sobre la mesa el uso de las baterías como componente indispensable de los nuevos vehículos, representando un gran reto para los especialistas en protección contra incendio para planificar, capacitar, prevenir y responder ante esta nueva amenaza a la seguridad personal.

Finalmente, y compartiendo el análisis de Martín Calvo, Alfonso S. Solleiro, agregó a la IA como una tendencia cada vez más revolucionaria. "Los algoritmos capaces de entender y alertar respecto a los mapas de calor serán esenciales en el desarrollo de estrategias de predicción y prevención para la protección, especialmente al transporte de carga, también sumaría los analíticos que conviertan la data de incidencia en información para la toma de decisiones", concluyó. ■

Agradecemos las facilidades otorgadas a Hacienda de Los Morales, para la realización de este reportaje.

convergint® Genetec IDEMIA

Este reportaje se llevó a cabo gracias al patrocinio de Convergint, Genetec e Idemia.

Fotos: Mónica Ramos / SEA

SEGURIDAD EN LA INDUSTRIA ENERGÉTICA: PETRÓLEO Y GAS LP

Actualmente se estima un robo de 60 mil toneladas mensuales de Gas LP a PEMEX, con una afectación económica de más de 20 millones de pesos anuales. ¿Cuáles son las estrategias que las empresas están implementando para proteger sus activos?

Foto: Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

En 2019, el gobierno del ex presidente Andrés Manuel López Obrador, inició una guerra contra el llamado "huachicoleo", el robo de combustible en ductos de Petróleos Mexicanos (PEMEX). Lo que parecía el fin, o al menos el inicio, de una iniciativa que favorecería al sector y a la economía mexicana, no dio los resultados esperados. Hasta ese momento, y a lo largo de varias décadas, el Estado Mexicano sufría pérdidas por 60 mil millones de pesos al año (poco más de tres mil millones de dólares).

El primer paso fue cerrar cuatro de los 13 oleoductos de PEMEX, lo que detonó, además, la falta de suministro a diferentes ciudades de los estados de México, Michoacán, Guanajuato, Aguascalientes, Jalisco, Querétaro y Tamaulipas. Durante varios días, decenas de autos se formaban para cargar el tanque de sus vehículos, trasladándose de una estación a otra, hasta encontrar el combustible. No es que la iniciativa fuera errónea, el robo a los ductos de la empresa nacional petrolera son un golpe fuerte a la economía del país, sin embargo, con el paso de los años, los empresarios tienen "otros datos" respecto a esta estrategia.

Uno de los sucesos que marcaron ese año respecto al "huachicoleo", fue precisamente el ocurrido el 18 de enero, en el municipio de Tlahuelilpan, Hidalgo. Una fuga de combustible en el ducto Tuxpan-Tula, producto de la imprudencia y delincuencia, provocó la explosión y muerte de 137 personas: 69 fallecieron en el lugar y de los 81 hospitalizados por quemaduras, perdieron la vida 68; sólo 13 fueron dados de alta con lesiones. De acuerdo con información de "El Financiero vía Transparencia", en enero de 2019 se detectaron mil 565 tomas clandestinas, y para mayo, esa cantidad bajó a mil 76 tomas.

Pero, ¿cuáles han sido las consecuencias de esta estrategia? Dos reconocidos especialistas en Seguridad Patrimonial, impartieron una conferencia magistral en uno de los *roadshows* organizados por **Seguridad en América**, de donde obtuvimos la siguiente información para realizar este reportaje especial.

FORTALECIMIENTO DE LA SEGURIDAD EN EL SECTOR DE HIDROCARBUROS

El sector de acero e hidrocarburos es el segundo más afectado en robo a transporte (24%), de acuerdo con cifras de la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital (AMESIS) reportadas en el primer semestre de 2024, en primer lugar, están los alimentos y abarrotes (32%); en tercer lugar, neumáticos (15%); le siguen materia prima (15%), herramientas (9%), y otras mercancías (7%).

El robo o extracción de combustible sigue siendo un problema de gran impacto a esta industria y a la economía del país. Pese a que la "guerra contra el huachicoleo", tenía buenas intenciones, la realidad es que, más que dejar de existir las tomas clandestinas, la delincuencia ha encontrado otras maneras de obtener de forma ilegal el combustible y otros energéticos

Foto: Freepik

> *"Cuando hablamos del transporte de hidrocarburos no pensamos en que son seres humanos los que se arriesgan en la ruta, y deben ser el primer factor a cuidar",* Rogelio Medrano Tinoco

como el Gas LP (GLP). Hoy en día, ya no sólo se extrae directamente de los ductos, sino que se roban los autotanques, y extorsionan tanto a empresas legales del sector, como a los usuarios finales.

Ante esta situación, Rogelio Medrano Tinoco, gerente del área de Inteligencia y Seguridad Corporativa en Repsol México, compartió que el sector ha fortalecido sus estrategias priorizando la seguridad de las personas operativas, seguida de la protección a las instalaciones y productos, y en tercer lugar, pero no menos importante, la reputación de la marca.

"Cuando hablamos del transporte de hidrocarburos no pensamos en que son seres humanos los que se arriesgan en la ruta, y deben ser el primer factor a cuidar, por lo que usamos mecanismos preventivos para reducir, no sólo robo en carretera, intentos de extorsión, sino también el robo hormiga, que es de las principales afectaciones que tenemos", y agregó algunas de estas estrategias, como es la vinculación con las autoridades, mantener contacto con aquellas que se encargan de dar respuesta a incidentes de seguridad, la creación de Comités de Seguridad, y el fomentar la denuncia de los robos o delitos, para así bridar información, *data*, sobre las rutas con más robos, los modus operando de la delincuencia, etcétera.

"Es importante conocer todo el proceso de ciclo de carga de combustible, e identificar los puntos de dolor, es decir, las vulnerabilidades. Enfrentamos riesgos como la extracción de una parte del producto en carretera, en zonas de descarga o en paradas no autorizadas. Y aunque parezca una baja cantidad de robo de combustible, llamado robo hormiga, en realidad es una gran pérdida", agregó.

El sector energético no sólo se ve afectado por la delincuencia organizada, sino también por algunos operadores de autotanques que pueden estar coludidos con los primeros, así como con estaciones de carga o empresas que aceptan la compra de combustible robado. Respecto al robo hormiga del remanente de combustible en los autotanques, Rogelio Medrano señaló que los operadores pueden quedarse desde 200 hasta 600 litros de combustible que venden de forma ilegal.

MEDIDAS DE MITIGACIÓN

El especialista recomienda hacer auditorías de la carga de los autotanques con un proveedor externo para poner sellos en las válvulas y que no se pueda extraer fácilmente el producto, y a su vez hacerles revisiones constantes a estos proveedores.

"Para el robo en carretera, hemos establecido diferentes medidas de protección, empezando por establecer rutas de circulación con horarios estratégicos. Por ejemplo, el horario límite de circulación en alguna de las rutas es de 05:00 a 18:30 horas, debido a que, si existiera un robo en ese lapso, existen mejores posibilidades de que las autoridades estén presentes y brinden apoyo.

Otra estrategia que ha funcionado es la realización de un mapeo para monitorear la seguridad logística. Esta información es de gran utilidad, sobre todo si se tiene un centro de control, ya que sirve como una herramienta rápida y de fácil acceso para identificar todas las rutas del país. Con el mapeo, se puede saber cuáles son las rutas y terminales de abastecimiento que deben recorrer los autotanques, además de las estaciones y todas las paradas que se realizan en el recorrido.

Con el seguimiento discreto con custodia se puede revisar si cumplen con el traslado seguro del producto, o si realizan paradas no autorizadas, o si hay alguna extracción ilegal en el camino. También

"Los dos lugares donde se presenta el mayor robo de GLP son en el ducto y las estaciones de PEMEX. El gas es difícil de almacenar, por lo que se genera una distribución ilegal del combustible enfocándose en grandes centros de consumo del país, como lo es el área metropolitana", Benjamín Grajeda Regalado

Foto: Freepik

han optado por alquilar pensiones para los autotanques, así en caso de una retención en algún tramo carretero, un incidente o un posible robo, es mejor resguardar las unidades en estos lugares y esperar a que la ruta sea segura de nuevo.

De acuerdo a la información generada con estas estrategias, y al compartir información con otras empresas y autoridades, se tiene presente que Guanajuato es uno de los estados que presentan mayor robo de combustible; los municipios que presentan gran riesgo para circular son: Celaya, Apaseo El Grande, Apaseo El Alto, Salvatierra, Villagrán, Salamanca, Irapuato, Silao, León, San José Iturbide, y San Diego de La Paz.

LA SEGURIDAD EN EL TRANSPORTE Y COMERCIALIZACIÓN DE COMBUSTIBLE GAS LP

En México la mayor parte del Gas LP que se vende pertenece a PEMEX, el cual tiene seis refinerías y nueve Centros de Almacenamiento de gas; una vez que se produce se envía a las Plantas (33 terminales) a través de un ducto, ahí es donde se produce el robo de GLP. Continuando con la cadena de suministro, el siguiente paso es la transportación conformada 3 mil 336 semirremolques, cuatro ductos, ruta férrea.

Después están las mil 121 plantas de distribución a través de empresas legalmente establecidas, las cuales ponen el GLP de venta al público en 3 mil 623 estaciones de servicio, estaciones y bodegas de expendio. Por otra parte, están los 14 mil 335 vehículos de reparto, 17 mil 332 autotanques, de los que seis mil son comisionistas, los cuales no están muy bien regulados, pero que existen por la alta demanda del producto y porque ellos entran a zonas conflictivas. En total, se tienen contabilizados 27 millones de hogares que consumen Gas LP, y más de 100 millones de mexicanos. Es decir, el GLP es un combustible de alta demanda, esencial y que también está siendo afectado por la delincuencia.

"Distribuimos más de 720 mil toneladas mensuales de Gas LP en México, a través de 2.5 millones de tanques estacionarios, más de un millón de servicios diarios, y 18 millones de cilindros todos los días. Es una industria dinámica, fuerte y necesaria", explicó Benjamín Grajeda Regalado, director de Seguridad Patrimonial en PROGLP – SAE.

El especialista coincide con el análisis de Rogelio Medrano, los principales riesgos de seguridad de la industria petrolera en México son el robo o extracción de combustible, robo de autotanques y tanques portátiles, y agregó que, desafortunadamente, gran parte del producto robado se traslada a los grandes centros de consumo, contribuyendo a que esta mala práctica siga incrementándose.

"En esta industria enfrentamos diferentes riesgos, uno de ellos es que el gas que es extraído ilegalmente, se distribuye mediante autotanques robados o pertenecientes a empresas no autorizadas. Estos grupos de distribución ocupan tácticas de intimidación para evitar la venta por parte de empresas legalmente establecidas. Ya sea que arremetan contra las empresas para que compren el combustible sólo a ellos, o extorsionen directamente a los clientes finales. Además de los riesgos de Protección Civil en toda la cadena alterna e ilegal de suministro", puntualizó.

De acuerdo con información compartida por el especialista, el robo de gas LP a PEMEX está focalizado en seis estados: Veracruz, Puebla, Estado de México, Tlaxcala Oaxaca, y Tabasco. El primero, ha duplicado las tomas clandestinas, mientras que en el año 2021

presentaba 122 tomas de este tipo, en 2022, incrementaron a 541; para 2023, se localizaron mil 25 tomas. Los delincuentes siguen encontrando nuevas formas de robar sin verse afectados, evitando que suceda lo que en 2019 en Hidalgo.

"Los dos lugares donde se presenta el mayor robo de GLP son en el ducto y las estaciones de PEMEX. El gas es difícil de almacenar, por lo que se genera una distribución ilegal del combustible enfocándose en grandes centros de consumo del país, como lo es el área metropolitana (CDMX) y su zona conurbada. También se ha expandido la distribución a los estados de Puebla, Tlaxcala, Veracruz, Hidalgo y Estado de México. Se estima un robo de 60 mil toneladas mensuales, con una afectación económica a PEMEX de más de 20 millones de pesos anuales por el robo de GLP", sentenció el especialista.

Los principales canales de distribución del GLP robado son:

- Autotanques irregulares.
- Estaciones de carburación y expendios clandestinos.
- Algunas plantas de distribución que se prestan a estas prácticas ilegales.

EFECTOS DEL ROBO, TRANSPORTE Y COMERCIALIZACIÓN DE GAS DE PROCEDENCIA ILÍCITA

Con base en el análisis y experiencia de Benjamín Grajeda, algunas consecuencias del robo de GLP son:

- Riesgo de graves accidentes para la población.
- Participación creciente de grupos delictivos controlando zonas de reparto y desplazando a empresas formales.
- Se violenta el Estado de Derecho e incrementa la inseguridad.
- Se desincentivan las inversiones productivas.
- Se sustituye la actividad de una empresa legal que genera empleos formales y paga impuestos tomando su lugar la delincuencia organizada.
- Se pierden ingresos: IVA, ISPT, ISR, pago de derechos y costos regulatorios.
- Se pierden plazas de empleos formales, se dejan de pagar salarios y prestaciones laborales de Ley (IMSS, INFONAVIT, etc.).
- Se pierden inversiones indispensables para garantizar el abasto energético para el crecimiento y desarrollo del país.
- Con las empresas ilegales, se corre el riesgo de tanques estacionarios que explotan dentro de casas que los almacenan.

ESTRATEGIAS DE SEGURIDAD

Ante esta situación, los responsables de Seguridad de la industria energética, está desarrollando diferentes estrategias de seguridad para contrarrestarlos, algunas de ellas son:

- Unión de empresas a través de las asociaciones.
- Impulsar la creación de direcciones de Seguridad Patrimonial en las empresas.
- Fortalecimiento en la cadena de suministro de las empresas y de los protocolos de seguridad.


Foto: Freepik

- Creación del Comité de Seguridad y de la Asociación Mexicana de Distribuidores de Gas Licuado y Empresas Conexas, A.C. (AMEXGAS).
- Establecimiento de mesas de coordinación en los estados con mayor problemática a nivel estatal y federal.
- Capacitación a autoridades en relación con la reglamentación que regula a la industria.
- Colaboración con autoridades.
- Resultados:
- Comunicación coordinada con autoridades para atención a robos de unidades.
- Disminución de robo de unidades y aumento de unidades recuperadas.
- Operativos en estados de alta incidencia, teniendo muy buena respuesta en Hidalgo y Tlaxcala. ■

Referencias:

- *Fuentes consultadas: Centro Nacional de Prevención de Desastres. "A tres años de la explosión en Tlahuelilpan, Hidalgo". Gobierno de México, 18/01/2022*
- *Portal Asociación Mexicana de Distribuidores de Gas Licuado y Empresas Conexas A.C. (AMEXGAS).*

SEGURIDAD PARA LOS CENTROS DE DATOS EN MÉXICO

En 2024 el número de usuarios de Internet en el mundo alcanzó los 5 mil 450 millones de personas (67.1% de la población mundial); cada una en promedio genera 1,7 MB de datos por segundo. ¿México tiene la suficiente infraestructura para albergar la demanda de data centers?

Foto: Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Un Centro de Datos (*data center*) es una ubicación física que almacena máquinas de computación y sus equipos de *hardware* relacionados. Contiene la infraestructura que requieren los sistemas de Tecnologías de la Información (TI), como: servidores, unidades de almacenamiento de datos, y equipos de red. Los *data centers* han tomado gran relevancia en todo el mundo, dado que, ante imprevistos, crisis y emergencias, estos ayudan a la continuidad del negocio y, sobre todo, garantizan la seguridad de la información.

De acuerdo con declaraciones de la Asociación Mexicana de Centros de Datos (MEXDC), México es un país muy atractivo para esta industria, tanto por el creciente interés de empresas extranjeras (*nearshoring*), como por su relevancia en América Latina. Actualmente en el país operan 166 *data centers*, los cuales requieren de aproximadamente 305 MegaWatts hora (Mw/h) para su funcionamiento.

Y agregaron que, en los próximos cinco años se instalarán, al menos, 73 nuevos centros de datos para responder a las necesidades de servicios digitales en el país, lo que requerirá una inversión de 9 mil 192 millones de dólares, y aproximadamente, mil 492 MegaWatts hora, un 400% más de lo que se utiliza hoy en día[1].

Pero, ¿el país y los usuarios están conscientes de la importancia, relevancia y necesaria aplicación de los centros de datos?

PANORAMA DEL USO DE DATOS EN EL MUNDO

Quedó claro que la pandemia por COVID-19 cambió la vida de todas las personas, sus costumbres, rutinas, trabajos, y formas de consumo. Con ella el *e-commerce* y el uso de aplicaciones e Internet, tuvieron un crecimiento exponencial, México, es un claro ejemplo de esto.

De acuerdo con información de We are the social, agencia de *marketing* digital, el número de usuarios de Internet en el mundo alcanzó los 5 mil 450 millones de personas (67.1% de la población mundial); 167 millones de nuevos usuarios en comparación al 2023, un aumento de 3.2%[2].

Por su parte, el portal de estadísticas globales, Statista, posiciona a China como el país con mayor número de usuarios conectados a Internet con 1.090 millones; le sigue India con 751.5 millones, y México ocupa el octavo lugar con 107.3 millones.

Durante el *roadshow* titulado "Seguridad *en Data Centers*", organizado por **Seguridad en América** este año, José Guadalupe González García, CPP, director de Proyecto en Orion Innovation México, destacó que cada persona, de esos 5 mil 450 millones, en promedio genera 1.7 MB de datos por segundo, integrados no sólo por redes sociales. "Con base en datos publicados por Dell, cada minuto se envían 188 millones de correos electrónicos, se realizan alrededor de 4.5 millones de búsquedas en Google, y más de 200 mil llamadas en Skype", resaltó el especialista en infraestructura crítica.

TIPOS DE CENTROS DE DATOS

Es importante conocer los tipos de centro de datos por temas de eficiencia y seguridad:

- **Edificios específicos para *data centers.*** Proyecto y construcción de edificios exclusivos de misión crítica.
- **Edificio Multidisciplinario.** Edificios no exclusivos para misión crítica.
- **Adecuaciones.** Renovación de la infraestructura en un ambiente de misión crítica existente.
- **Contenedores prefabricados.** Centros de datos modulares prefabricados.

El especialista comentó que actualmente existen diversas instituciones que desarrollan mejores prácticas, así como empresas que, comercialmente, clasifican los *data centers* en Tiers (capas), por Nivel o Tipo del 1 al 4 o 5 dependiendo la institución o empresa, sin embargo, "lo que debemos tener en cuenta es que los centros de datos, no son un producto que puedes comprar y poner a funcionar. La realidad es que el tipo el servicio o *data center* que vas a adquirir, va a depender de las necesidades que tenga el cliente o las de tu propia empresa", indicó el también presidente del Comité Nacional Permanente de Peritos de *Data Center.*

RETOS DE LOS *DATA CENTERS*

Ante el incremento del uso de Internet y del consumo elevado de energía en el mundo, los *Data Centers* enfrentan diferentes retos, algunos de ellos:

- Generar soluciones sostenibles.
- Sustentabilidad/ Sostenibilidad.
- Necesidades del cliente.
- Cadena de suministro dada la inseguridad que se vive en el país.
- Fallas en las líneas de distribución energética.

NORMAS VS. ESTÁNDARES

José Guadalupe externó a los responsables de Seguridad y TI a entender que una norma no es un estándar. "Las normas locales, por país, son predominantes ante las internacionales, simplemente por el marco legal de cada uno, puesto que, ante una situación de controversia, ya sea económica o vital, la norma local es la que va a validar si se está dentro del cumplimiento legal para enfrentar la controversia o no", explicó.

También compartió normas que ayudan a entablar mejores prácticas, entre ellas:

- **ANSI/BICSI 002.** Es la norma base para el diseño de centros de datos alrededor del mundo, su misión es proporcionar requisitos, directrices y mejores prácticas aplicables a cualquier *data center.*
- **NFPA 72.** Proporciona las últimas disposiciones de seguridad para satisfacer las cambiantes demandas de la sociedad en materia de detección de incendios, señalización y comunicaciones de emergencia.
- **NFPA 75.** Establece los requisitos mínimos para la protección de equipos y áreas de computación contra daños causados por incendios o sus efectos asociados.
- **NFPA 255.** Es una prueba para proporcionar una medición que compara la propagación de la llama (incendio), por la superficie y la emisión de humo en ciertos materiales con las respectivas mediciones de un determinado tipo de roble rojo y planchas de cemento reforzado bajo condiciones específicas de exposición al fuego.

"Riesgo es todo evento o situación que puede evitar la correcta operación de un centro de datos. ¿Y cuál creen que es la principal causa de una falla de infraestructura de un Data Center? ¡Un error humano!", José Guadalupe González García, CPP, ATD, DCEP, DSI

Foto: Freepik


Foto: Freepik

- **NFPA 99.** Establece criterios para los niveles de los servicios o sistemas de cuidado de la salud basados en el riesgo para los pacientes, el personal o los visitantes de las instalaciones de cuidado de la salud para minimizar los peligros de incendio, explosión y electricidad.
- **ANSI/TIA 942.** Estándar concebido como una guía para los diseñadores e instaladores de centros de datos, que proporciona una serie de recomendaciones y directrices (*guidelines*) para la instalación de sus infraestructuras.
- **ICREA.** Asociación Internacional formada por ingenieros especializados en el diseño, construcción, operación, administración, mantenimiento, adquisición, instalación y auditoría de centros de cómputo.

Refiriéndose a las mejores prácticas locales, el Mtro. José Guadalupe, resaltó que, "la normativa nacional va a ir en función del negocio", y compartió tres normas para centro de datos en México, dependiendo de qué es lo que queremos con éste, no sólo en materia de construcción, arquitectura y diseño, sino también de procesos y riesgos.

- **NOM 001.** Norma Oficial Mexicana NOM-001-STPS-2008, edificios, locales, instalaciones y áreas en los centros de trabajo. Condiciones de seguridad.
- **NMX 489.** Norma mexicana establece los requisitos para el diseño, construcción y operación de las edificaciones sustentables y energéticamente eficientes denominadas centros de datos de alto desempeño (CDAD).
- **NOM-022-STPS-1999.** Norma Oficial Mexicana NOM-022-STPS-1999, Electricidad estática en los centros de trabajo-Condiciones de seguridad e higiene.

Algunas de las instituciones que se encargan de clasificar y certificar los DC, el especialista compartió las siguientes:

- **CEEDA (*Certified Energy Efficient Datacenter Award* o CEEDA®).** Es un programa de certificación global evaluado de forma independiente y diseñado para reconocer la aplicación de las mejores prácticas de eficiencia energética en los centros de datos.
- **ASHRAE.** Es la Sociedad Estadounidense de Ingenieros de Calefacción, Refrigeración y Aire Acondicionado, una asociación profesional estadounidense que busca avanzar en el diseño y la construcción de sistemas de calefacción, ventilación, aire acondicionado y refrigeración.
- **UP TIME.** Up Time Institute es una organización que ofrece diferentes certificaciones relacionadas con los centros de datos, como la certificación Tier y el programa AOS.

También recomendó certificarse en ISO (Organización Internacional de Normalización), y en IEC (Comisión Electrotécnica Internacional); así como en CPTED (metodología que busca reducir la delincuencia y el temor a través del diseño ambiental. Se basa en la idea de que las personas pueden prevenir la delincuencia a través del diseño de los espacios físicos), relacionada con la arquitectura y protección civil, aspectos relevantes en la construcción de los *data centers*.

ANÁLISIS DE RIESGOS

Para empezar la correcta instalación y uso de un centro de datos, es importante realizar un análisis de riesgos. "Riesgo es todo evento o situación que puede evitar la correcta operación de un centro de datos. ¿Y cuál creen que es la principal causa de una falla de infraestructura de un *Data Center*? ¡Un error humano!", explicó. Y como conclusión, dejó los siguientes tips para los responsables del área, hacia el personal:

- Profesionalización.
- Certificación.
- Desarrollo.
- Empoderamiento.
- Construcción de líderes y equipos multidisciplinarios.
- Construcción de planes de carrera.
- Integración de mujeres y jóvenes al equipo. ■

Referencias:

[1] *"Industria de Data Centers invertirá 9 mil 192 mdd en México para instalar 73 Centros de Datos", Christopher Calderón. El Financiero 04/17/2024 https://www.elfinanciero.com.mx/empresas/2024/04/17/industria-de-data-centers-invertira-9-mil-192-mdd-en-mexico-para-instalar-73-centros-de-datos/*

[2] *https://wearesocial.com/es/*

LA TECNOLOGÍA Y EL SOPORTE TÉCNICO APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA

SEGURIDAD ELECTRÓNICA:

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

REGISTRO FEDERAL DGSP/303-16/3302 PERMISO SSP PUEBLA

SSP/SUBCOP/DGSP/506-23/460

REPSE ARR3280/2024

ALAS Asociación Latinoamericana de Seguridad — 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

Alejandro Romero Vargas,

fundador y director general de Cyberpeace

1. ¿Cuáles son los sectores industriales en América Latina más vulnerables a ciberataques?

Principalmente los servicios financieros, tecnología, salud, y *retail*. Estos sectores manejan grandes volúmenes de datos sensibles, como información personal, financiera y de pago, que son altamente valiosos para los atacantes. El sector financiero es un objetivo frecuente debido al potencial económico que representa para los atacantes, mientras que en el sector salud, los ataques de *ransomware* pueden paralizar servicios críticos. En tecnología y *retail*, el enfoque suele estar en robar propiedad intelectual o datos de clientes, que luego se usan para extorsión o venta en el mercado negro.

Estas industrias son especialmente vulnerables por la falta de inversión en ciberseguridad en muchas organizaciones, así como por el uso de infraestructuras tecnológicas desactualizadas que no logran hacer frente a las amenazas avanzadas de hoy en día.

2. ¿Qué tipo de ciberataques son los más comunes en la región y cuáles son sus principales objetivos?

En América Latina, los ciberataques más comunes son *ransomware*, *phishing* y *exploits* de vulnerabilidades, y aunque estos ataques afectan a diversos sectores, los objetivos son bastante específicos. El *ransomware* es el más persistente y ha aumentado en frecuencia. Su objetivo principal es obtener ganancias financieras rápidas a través de la extorsión. Los atacantes interrumpen operaciones críticas para presionar a las empresas a pagar un rescate. En algunos casos, incluso buscan dañar la reputación de la organización si no cumplen con sus demandas.

Otro ataque muy común es el *phishing*, cuyo objetivo principal es el robo de identidad y el acceso no autorizado. Los delincuentes intentan obtener credenciales o datos personales y financieros que luego pueden usar para comprometer sistemas más grandes o vender en mercados ilícitos. Además, puede estar dirigido a manipular cuentas bancarias o acceder a información confidencial. Por último, están los *exploits* de vulnerabilidades, que buscan explotar fallos en la seguridad para obtener acceso privilegiado a sistemas críticos. Aquí los atacantes se enfocan en comprometer servidores, bases de datos y aplicaciones esenciales.

3. ¿Qué factores hacen que las industrias latinoamericanas sean un blanco atractivo para los ciberdelincuentes?

En primer lugar, muchas organizaciones de la región no invierten lo suficiente en ciberseguridad ya sea en personal, tecnologías o procesos, lo que las deja con sistemas más vulnerables. Esto se refleja en el uso de tecnologías heredadas, falta de parches de seguridad y soluciones de defensa menos avanzadas, lo que facilita que los atacantes encuentren vectores de manera más fácil y logren explotarlos sin mayor resistencia.

Además, la conciencia sobre ciberseguridad entre empleados y directivos tiende a ser más baja en comparación con otras regiones, lo que facilita ataques como el *phishing*, donde los delincuentes aprovechan la falta de conocimiento para obtener acceso a sistemas sensibles. Otro factor importante es la dependencia de terceros y proveedores externos, que a menudo no tienen los mismos niveles de protección, lo que abre la puerta a ataques en la cadena de suministro.

Por último, aunque la regulación en ciberseguridad está mejorando en la región, todavía no es tan estricta o madura como en Europa o Estados Unidos. Esto genera brechas normativas que los atacantes pueden aprovechar, sumado a la presión limitada sobre las empresas para cumplir con estándares de seguridad más altos. Todos estos factores combinados hacen que las industrias latinoamericanas sean un blanco muy atractivo para los ciberdelincuentes.

4. ¿Cuáles son las tácticas más comunes utilizadas por los ciberdelincuentes en ataques a empresas mexicanas?

Lo que hemos visto en los últimos años es que los ciberdelincuentes están utilizando una combinación de tácticas

y técnicas de ingeniería social cada vez más sofisticadas para comprometer a sus víctimas, una de las tácticas más comunes es el *phishing* dirigido o *spear phishing*, donde los atacantes envían correos electrónicos que parecen legítimos, pero están diseñados para engañar a los empleados y que estos descarguen *malware* o revelen credenciales de acceso. Este método ha sido muy efectivo en los ataques recientes.

Otra táctica clave es el uso de *ransomware* con doble extorsión. En este caso, los atacantes no sólo cifran los datos de la empresa, bloqueando sus operaciones, sino que también roban información sensible y amenazan con publicarla si no se paga el rescate. Esto pone a las empresas en una situación de alta presión, ya que no sólo enfrentan la paralización de sus sistemas, sino también posibles daños reputacionales.

Los ciberdelincuentes también están aprovechando vulnerabilidades en sistemas no actualizados, especialmente en servicios de acceso remoto como RDP o en *software* de transferencia de archivos. Este tipo de ataques ha sido muy común, particularmente en sectores críticos como la energía y la manufactura. Además, los ataques a la cadena de suministro han aumentado, donde los delincuentes comprometen a proveedores o socios comerciales para infiltrarse en redes corporativas.

5. ¿Qué tecnología o estrategias se deben implementar para impedir ataques cibernéticos tanto en pymes, empresas y sociedad?

Cuando hablamos de ciberseguridad, no se trata sólo de implementar tecnología avanzada. En realidad, debe ser un esfuerzo integral que involucre personas, procesos y tecnología. Desde la perspectiva empresarial, la clave es entender que la ciberseguridad no es una responsabilidad exclusiva del área de TI, sino que debe ser parte de la cultura de toda la organización. En este sentido, una estrategia efectiva no sólo protege, sino que también prepara a la empresa para responder de manera rápida y efectiva a cualquier amenaza.

En cuanto a las personas, es fundamental que todos los empleados, desde el nivel operativo hasta el C-level, estén capacitados para reconocer amenazas como el *phishing* o los intentos de ingeniería social. En cuanto a los procesos, es necesario que las organizaciones tengan un plan claro de respuesta ante incidentes cibernéticos.

Finalmente, la tecnología es el tercer pilar que refuerza esta estrategia. Aquí, las empresas deben adoptar soluciones como autenticación multifactor (MFA), cifrado de datos, monitorización continua y el modelo de Zero Trust, que se basa en verificar y validar constantemente todos los accesos dentro de la red. Además, las tecnologías de detección y respuesta extendida (XDR) permiten a las empresas detectar rápidamente comportamientos sospechosos y reaccionar de forma automática o semiautomática para contener posibles amenazas antes de que causen un daño significativo.

6. ¿Cuáles son los servicios que ofrece Cyberpeace?

Cyberpeace es una empresa con 25 años de experiencia en el campo de la ciberseguridad, especializada en la protección proactiva de infraestructuras críticas y activos digitales. Nuestra propuesta de valor se basa en ofrecer servicios agnósticos, es decir, completamente adaptables a cualquier plataforma o tecnología existente, lo que nos permite trabajar con cualquier infraestructura que el cliente tenga implementada.

Somos un proveedor de servicios MDR (Managed Detection and Response), lo que significa que no sólo prevenimos y detectamos amenazas, sino que también respondemos de manera inmediata a los incidentes, garantizando una cobertura 24/7 a través de nuestro equipo de especialistas. Además, contamos con un CSIRT (CPCSIRT), que forma parte de FIRST, un grupo global que nos permite colaborar a nivel internacional en la gestión de incidentes de seguridad.

Uno de nuestros mayores diferenciadores es nuestro enfoque en la ciberseguridad como servicio. En lugar de vender licencias o productos, ofrecemos una solución integral, gestionando todos los aspectos de la seguridad para que las empresas puedan concentrarse en su negocio sin preocuparse por los riesgos cibernéticos. Esto se complementa con nuestra estrategia de seguridad adaptable, que nos permite diseñar soluciones personalizadas según las necesidades específicas de cada cliente.

7. ¿Cuáles son las funcionalidades y beneficios de SOC360?

SOC360 es una aplicación que está diseñada para ofrecer seguridad gestionada 24/7 y permitir a las empresas delegar toda la responsabilidad de ciberseguridad a un equipo de expertos altamente capacitados. Uno de los mayores beneficios es que, al ser un servicio completamente agnóstico, SOC360 se adapta a cualquier tecnología o infraestructura que la empresa ya tenga, lo que significa que no es necesario realizar grandes cambios o inversiones en nuevas plataformas.

El enfoque de SOC360 no es sólo tecnológico, sino también estratégico y humano. Nos enfocamos en los procesos y las personas, asegurando que cada amenaza sea identificada y gestionada de manera proactiva, permitiendo a las organizaciones concentrarse en su negocio mientras nosotros nos ocupamos de la seguridad.

Nuestro equipo de expertos monitorea, responde y se mantiene actualizado en las últimas tendencias y técnicas de protección, además, al ser parte de FIRST, tenemos acceso a inteligencia global y colaboramos con otros expertos en ciberseguridad a nivel mundial, lo que nos permite anticipar amenazas y compartir mejores prácticas. Esto, combinado con nuestro compromiso de desarrollar talento mexicano especializado en ciberseguridad, refuerza nuestra capacidad para ofrecer un servicio de máxima calidad. ■

Fotos: Cortesía Cyberpeace

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

SOCIO DIRECTOR, ALTAIR, SECURITY CONSULTING & TRAINING.

Más sobre el autor:

TRANSFORMANDO LA CULTURA DE SEGURIDAD

LATINOAMÉRICA

En este tema apasionante del Cambio Cultural en las organizaciones, tratando desde la raíz, desde el fundamento y desde la parte más profunda de las personas, de sus hábitos y valores. Pero, ¿cómo lograrlo? Hay muchas formas efectivas, que integradas entre sí, a través de programas permanentes, potenciarán el resultado y serán cruciales para el éxito.

Si bien los esfuerzos aislados sirven de alguna forma, no son suficientes para permear la cultura en seguridad que pervalezca en el tiempo. Es necesario aspirar a una inmersión y capacitación continua e integral de todo el personal. Sólo así lograremos mantener a los empleados sensibilizados, informados sobre las amenazas presentes y las mejores prácticas de neutralización y prevención.

LA COMUNICACIÓN

Una herramienta muy valiosa es la comunicación efectiva en seguridad. La comunicación de la seguridad no es sólo un componente más de la gestión de riesgos; es una pieza clave que puede determinar el éxito o el parcial cumplimiento de nuestros proyectos de seguridad. En un mundo cada vez más turbulento y lleno de incertidumbre, necesitamos una estrategia de comunicación creativa, eficiente y efectiva para construir una cultura de seguridad sostenible. ¿Cómo lograrlo? Acá te dejo algunas ideas claras:

- **Campañas Permanentes:** Es fundamental realizar campañas continuas y permanentes, no sólo esfuerzos aislados. Sólo así podremos construir una mentalidad de seguridad que se refleje en los hábitos y la disciplina diaria de las personas.
- **Especialistas en Comunicación:** Contar con el apoyo de los especialistas en comunicación, nos ayudará a crear, desarrollar y transmitir mensajes claros y efectivos, utilizando un lenguaje sensible e inclusivo que llegue al corazón y a la mente de las personas, a través de los diversos canales de comunicación disponibles.
- **Educación y Formación:** La educación y formación son esenciales. Boletines, infografías, documentos, entre otros, son herramientas valiosas para compartir conocimientos, desarrollar habilidades, instaurar valores y normas de conducta, y comunicar las estrategias de seguridad en beneficio de todos.
- **Capacitación y Entrenamiento:** A través de seminarios, cursos, talleres, pláticas, lecciones aprendidas, casos de éxito y otras herramientas en seguridad es crucial para integrar la cultura de seguridad en el ADN de tu organización. Sensibilizando sobre los riesgos y promoviendo medidas preventivas y reactivas, en los diferentes entornos de las personas, no sólo fortaleceremos la seguridad en el entorno laboral, sino también en los ámbitos social y familiar, así como los movimientos entre estos ambientes.
- **Actualización Constante:** Hoy más que nunca, debemos estar actualizados y preparados para adaptarnos a los cambios. Los riesgos son dinámicos, por lo que nuestras estrategias de seguridad, información y conocimientos también deben serlo. Mantener a las personas informadas sobre los nuevos retos y cómo enfrentarlos eficientemente, a fin de mantener condiciones tranquilas y seguras, es crucial para estar siempre un paso adelante.

La seguridad no sólo es un departamento, es un compromiso y un comportamiento diario de cada persona con nuestra organización y con nosotros mismos. Formemos parte activa esencial crear métodos accesibles, interesantes y motivadores para fomentar la seguridad, involucrar activamente a los colaboradores y asegurar la retención de conocimientos y habilidades, utilizando situaciones y experiencias reales como base, así como una comunicación constante sobre el tema.

¿En tu organización se vive una Cultura de Seguridad? ¿Tienes una estrategia cohesiva en tu organización para crear una cultura de seguridad? ¡Platícamela!

¿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 Padilla

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

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

Grupo de Ejecutivos en Manejo GEMARC de Riesgos Corporativos A.C.

Columna de
GEMARC

joseluisdse@gmail.com

JOSÉ LUIS SÁNCHEZ GUTIÉRREZ, DIRECTOR DE SEGURIDAD PATRIMONIAL EN LA INDUSTRIA CÁRNICA.

Más sobre el autor:

DECÁLOGO DE CARACTERÍSTICAS QUE DEBE TENER UN DIRECTOR DE SEGURIDAD CORPORATIVA

Foto: Freepik

MÉXICO

Como es habitual, estimados lectores, realmente muy agradecido por su acostumbrada preferencia; y en esta ocasión tocaremos el tema de: ¿Cuáles son esas 10 características que debe tener un director de Seguridad Corporativa? Que te ayudará a transformarte de ejecutivo especialista a líder de Seguridad Corporativa.

Siempre debemos tomar en cuenta que, en el mundo de los negocios, donde las empresas enfrentan riesgos cada vez más complejos y globalizados, la seguridad corporativa ha evolucionado de una función operativa a un pilar estratégico para la sostenibilidad y crecimiento de las empresas.

Para aquellos ejecutivos especialistas que buscan mejorar, ascender y convertirse en directores de Seguridad Corporativa, el camino no sólo implica una mayor responsabilidad, sino una transformación completa en sus competencias, mentalidad y liderazgo. A continuación, te presento un decálogo que todo profesional debe seguir para hacer esta transición con éxito, basada en mi experiencia.

1. DESARROLLA UNA VISIÓN ESTRATÉGICA INTEGRAL

Un buen especialista en seguridad conoce los detalles operativos; sin embargo, un director de Seguridad Corporativa ve el panorama completo. La seguridad ya no es sólo sobre "control de acceso" o "gestión de riesgos". Hoy, está profundamente integrada en la estrategia corporativa. Debes aprender a vincular la seguridad con la visión empresarial, y comunicar su valor en términos de retorno sobre la inversión, resiliencia y ventaja competitiva.

Punto clave: Pregúntate siempre, ¿cómo contribuye la seguridad a los objetivos estratégicos de la empresa?

2. CONVIÉRTETE EN UN MAESTRO DE LA GESTIÓN DE RIESGOS GLOBALES

El entorno de riesgos está en constante cambio. Desde ciberataques y amenazas físicas, hasta pandemias y crisis económicas. Como futuro DSC, debes no sólo entender estos riesgos, sino anticiparlos y adaptarte rápidamente. Desarrolla competencias en análisis de riesgos y crea escenarios preventivos.

Punto clave: Haz del análisis predictivo una herramienta básica. Asegúrate de que cada decisión de seguridad esté respaldada por hechos datos duros, y evaluaciones de riesgos.

3. ADOPTA LA TECNOLOGÍA Y LIDERA LA INNOVACIÓN

La seguridad corporativa está siendo transformada por la tecnología: desde la Inteligencia Artificial y la automatización, hasta la vigilancia basada en *big data* y los análisis predictivos. El futuro DSC debe ser tecnológicamente competente, entender cómo estas herramientas optimizan las operaciones y conocer sus implicaciones legales y éticas.

Punto clave: Invierte tiempo en capacitarte en las tecnologías emergentes y cómo aplicarlas a la seguridad, siempre priorizando la seguridad cibernética y física de la empresa.

4. DOMINA LAS HABILIDADES DE COMUNICACIÓN Y NEGOCIACIÓN

No basta con ser un técnico excelente; debes ser capaz de comunicarte con la alta dirección, empleados, clientes y socios. Ser claro, directo y persuasivo en la explicación de riesgos y necesidades es esencial. Un DSC debe influir en la cultura organizacional para que la seguridad sea una prioridad compartida por todos.

Punto clave: Mejora tu habilidad para traducir términos técnicos en un lenguaje que todos comprendan, y en liderar con empatía y autoridad.

5. CONSTRUYE ALIANZAS CON OTROS DEPARTAMENTOS

La seguridad corporativa no opera en un silo. Debes colaborar estrechamente con Recursos Humanos, Finanzas, Operaciones, TI y *Marketing*. La seguridad debe ser parte integral de todas las funciones de la empresa.

Punto clave: Participa activamente en reuniones interdepartamentales. Demuestra cómo las decisiones de seguridad afectan directamente el éxito de otras áreas y viceversa.

6. CREA UNA CULTURA DE RESILIENCIA ORGANIZACIONAL

En lugar de ver la seguridad como una serie de controles que evitan eventos negativos, ve la seguridad como la capacidad de recuperarse rápidamente de las crisis. Los DSC exitosos no sólo evitan problemas, sino que aseguran que la empresa pueda continuar operando después de una interrupción.

Punto clave: Implementa planes de continuidad de negocio robustos. Asegúrate de que toda la organización esté preparada para responder a cualquier crisis.

7. LIDERA Y DESARROLLA UN EQUIPO DE EXCELENCIA

Ningún director de Seguridad Corporativa puede hacerlo solo. Tu equipo será tu mayor activo. Invierte en su desarrollo profesional, fomenta una cultura de aprendizaje continuo y construye una estructura de trabajo colaborativa donde cada miembro entienda su rol crítico en la protección del negocio.

Punto clave: Implementa programas de capacitación continuos y reconoce el talento dentro de tu equipo. El éxito del equipo será tu éxito.

8. OPTIMIZA LA GESTIÓN DE PRESUPUESTOS Y RECURSOS

La seguridad es costosa, y en tiempos de recortes, será tu responsabilidad justificar cada peso/dólar. Un DSC debe tener habilidades financieras sólidas, saber cómo optimizar recursos y demostrar cómo la seguridad agrega valor financiero a la empresa.

Punto clave: Aprende a elaborar presupuestos detallados que alineen los gastos en seguridad con los objetivos empresariales. Haz del retorno de inversión en seguridad una parte central de tus informes.


Foto: Freepik

9. SÉ PROACTIVO Y ANTICIPA EL FUTURO

El peor error que puede cometer un ejecutivo es esperar a que suceda una crisis para actuar. Los mejores DSC son proactivos, siempre buscando formas de mejorar la seguridad antes de que surjan problemas. Esto implica estar constantemente informado sobre nuevas amenazas y oportunidades.

Punto clave: Mantente actualizado sobre las tendencias globales de seguridad, participa en conferencias, seminarios y talleres. Utiliza herramientas de análisis predictivo. Estar a la vanguardia es lo que te diferenciará de los demás.

10. ABRAZA LA ÉTICA Y LA TRANSPARENCIA

Finalmente, la seguridad corporativa no es sólo un asunto de prevención; también es un tema ético. A medida que avances en tu carrera, serás responsable de proteger los datos, la privacidad y el bienestar de miles de personas. Actúa siempre con integridad y transparencia.

Punto clave: Promueve una cultura ética dentro de tu equipo y en toda la empresa. Asegúrate de que la seguridad sea percibida no sólo como una necesidad empresarial, sino como un compromiso moral con todos los involucrados.

Desde mi observador te comparto que puede haber más características que te hagan exitoso como director de Seguridad Corporativa; pero lo que, si te garantizo, es que, si te enfocas y aplicas las 10 características comentadas, te aseguro que será un camino lleno de logros. Reitero mi agradecimiento por permitirme compartirte esta columna y que sea de tu interés, tanto la lectura y su aplicación; buscando realmente generar en ti un valor agregado, mil gracias. ■

VIOLENCIA EN EL TRABAJO: PREVENCIÓN Y ABORDAJE EN EL SECTOR SALUD

En estas situaciones es fundamental estar alerta, evitar responder las amenazas con amenazas, procurar no dar órdenes en ese momento, y sobre todo trabajar mucho en cómo responder de una manera empática con especial atención en reconocer los sentimientos de las personas


Foto: Freepik

MÉXICO | **Francisco Javier Villegas Barbosa**

Los hospitales y centros de salud son lugares que fueron creados para procurar el bienestar y salud de las personas, mantenerlas sanas, sin dolor y prolongar la vida el mayor tiempo posible. Con esto, podría pensarse que en todo momento se respira un ambiente de tranquilidad y serenidad en los pasillos de los nosocomios, sin embargo, la realidad es que son lugares en los que se presentan una mezcla de sentimientos y emociones que pueden desencadenar comportamientos violentos. La incertidumbre ante el estado de salud de un ser querido, el estrés económico asociado a los tratamientos médicos y la frustración ante demoras o errores pueden generar tensión y agresividad.

En el sector salud, existen además factores de riesgo que pueden promover la violencia en los hospitales, como lo son sus ubicaciones, su tamaño, el tipo de asistencia médica que proveen, así como pacientes volubles, bajo la influencia de drogas o alcohol, o personas con un historial psicótico.

Actualmente, en el mundo se ha destacado a la violencia en el sistema hospitalario como una pandemia que afectará en el futuro la atención de la salud. La Organización Mundial de la Salud (OMS) menciona que los trabajadores sanitarios representan el 73% de todas las lesiones y enfermedades no mortales en el lugar de trabajo debido a la violencia, se estima que el 38% de los trabajadores sanitarios sufren violencia física en un momento determinado de su carrera. Al mismo tiempo muchos más están expuestos o son amenazados con agresiones verbales, la mayoría de los casos violentos son cometidos por familiares o amigos de los pacientes y seguidos por los propios pacientes.

Esto se empeora cuando existen crisis, emergencias o desastres que involucran grandes grupos de personas que están aún más abrumadas, con ataques de pánico, conmoción, incertidumbre, miedos y preocupaciones por las condiciones de ellos o sus familiares.

AGRESIONES AL PERSONAL DE SALUD

Las agresiones al personal de salud deben estar en la agenda de riesgos de las organizaciones y deben abordarse de una manera integral involucrando a todos los niveles, haciendo énfasis en el compromiso, la garantía y la definición de políticas claras y procedimientos de actuación.

De la misma manera, el colaborador debe tomar conciencia y conocimiento sobre la violencia en su lugar del trabajo y como erradicarla.

Para minimizar el riesgo de violencia en los hospitales es de suma importancia que se desarrollen programas de seguridad; los responsables de la Seguridad y Protección en conjunto con enfermería y otros líderes de los hospitales deben de identificar estrategias de desescaladas exitosas.

Partiendo por identificar los factores que puedan escalar a una situación de violencia en cada una de las posiciones de trabajo, principalmente aquellas con interacción con el paciente o familiares. Una vez detectados estos factores, debe definirse un procedimiento para buscar una solución de prevención, de control y una manera de como reportarlo que anticipe cualquier acto de violencia. Aún y cuando los hospitales o clínicas sean diferentes en tamaño, ubicación o especialidades, existen comportamientos esenciales que pueden ser detectables.

Adicionalmente, se debe capacitar al personal para que sean capaces de detectar un lenguaje no verbal o microexpresiones que muestren rasgos de ira y frustración (ya sea verbal o físico), así como todos aquellos gestos amenazadores, además de saber identificar a una persona que está bajo la influencia del alcohol o alguna droga. Con la misma importancia, deben ser entrenados en inteligencia emocional para que puedan gestionar con mayor estabilidad este tipo de situaciones.

Existen tres motivos principales por lo que las personas pueden molestarse y comenzar una situación de violencia:

1) **Tiempo de Espera:** El hacer esperar una persona más del tiempo establecido es motivo suficiente para que exista una molestia.
2) **Mala calidad y/o altas expectativas del servicio:** Experimentar un servicio deficiente o simplemente por debajo de la expectativa de la persona.
3) **Económico:** Cuentas no claras, cargos inesperados o lo más común, la molestia de que su seguro de gastos médicos no cubra la cuenta por múltiples razones.

En estas situaciones es fundamental estar alerta, evitar responder las amenazas con amenazas, procurar no dar órdenes en ese momento, y sobre todo trabajar mucho en cómo responder de una manera empática con especial atención en reconocer los sentimientos de las personas.

Para gestionarlas y que no escalen, es indispensable considerar lo siguiente:

- Hoy en día una de las cosas más importantes para las empresas es la experiencia del consumidor, una buena experiencia desde el momento que ingresa al hospital nos ayudará mucho en el comportamiento de nuestros consumidores, adoptar una actitud de empatía, servicio, tranquilidad y bondad, ante todo.
- Identifica las áreas que son más comunes en las que se pudieran presentar molestias como urgencias, laboratorio, imagenología, cajas, por mencionar algunas.


Foto:-Freepik

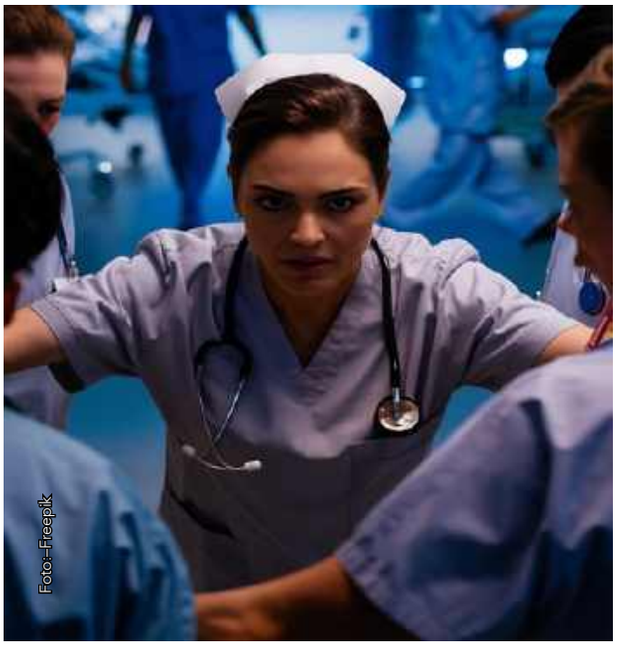


Foto:-Freepik

- Desarrolla un procedimiento específico sobre cómo abordar a las personas que pueden molestarse e iniciar una situación de violencia. Este abordaje se hará con el fin de ayudarlos, orientarlos y que se sientan atendidos, ya que, en muchos de los casos, las personas sólo desean ser escuchadas. Es preciso actuar de manera anticipada ante reclamaciones, establecer un diálogo que provea soluciones e incluso que se pueda ofrecer cortesías o descuentos de ser necesario. Toma en cuenta también estas recomendaciones:
  - ⊙ Cuando entres en una sala o empieces a tratar con un paciente o visitante, evalúa la posibilidad de que se pueda presentar un acto de agresión.
  - ⊙ Mantente alerta durante el encuentro.
  - ⊙ No te quedes a solas con una persona que pudiera tornarse violenta.
  - ⊙ Siempre mantén un camino abierto para salir. No permitas que la persona que pueda tornarse violenta se ponga entre tú y la puerta.
  - ⊙ No realices movimientos rápidos que pudieran confundirse como agresiones.
  - ⊙ Modera tu tono de voz.
  - ⊙ Toma tu distancia, evita invadir el espacio personal, no te acerques demasiado.
  - ⊙ Evita tocar a la persona en esos momentos.
  - ⊙ Si la situación se complica: aléjate de inmediato, llama y pida ayuda, y reporta cualquier incidente violento. ■

Francisco Javier Villegas Barbosa, subdirector de Protección Patrimonial del Sistema Hospitalario Christus Muguerza. *Más sobre el autor:*

ACTIVE SHOOTER, UNA AMENAZA REAL EN LAS ESCUELAS EN ESTADOS UNIDOS

Las medidas de seguridad en centros educativos son una prioridad social y de Estado

Foto: Freepik

VENEZUELA | **Fabián E. Girón Pérez**

"*Active Shooter, Active Shooter, Active Shooter*", es quizás la frase más aterradora que se puede escuchar en la radio o estaciones de televisión de los Estados Unidos.

Parkland, Florida, en febrero en 2018; Uvalde, Texas, en mayo de 2022; y Nashville, Tennessee, en marzo de 2023, son algunas de las fechas y lugares que quedarán en la memoria como días trágicos, cubiertos en sangre de niños y adultos inocentes a manos de personas perturbadas. El debate con respecto al control de armas continúa sin dar ningún tipo de fruto.

¿Es verdad que el control de armas puede servir para algo? Aún no podemos responder esa pregunta con propiedad, lo que sí podemos hacer es tomar las medidas de prevención y protección adecuadas para minimizar los daños que este tipo de ataques llevan consigo. El conteo de cuerpos no es un indicador que queramos continuar reconociendo.

La vida de miles, sino millones de niños que acuden día a día a los colegios en todo el territorio estadounidense, siguen estando en riesgo si no se toman las medidas necesarias y está en las manos de los distritos escolares, cumplir con estas medidas, pero es papel de los gobiernos regionales, estatales y federales, disponer los recursos económicos necesarios para que esto se vuelva una realidad.

MEDIDAS FÍSICAS SIGNIFICATIVAS

Son varios los análisis de riesgo que se han llevado a cabo en distintas escuelas, se han escrito varios protocolos de actuación, los cuales son puestos a prueba por medio de simulacros. Sin embargo, existen medidas físicas significativas que pueden aplicarse y que he evidenciado yo mismo que aún no se han puesto en práctica.

Podríamos nombrar algunas de estas medidas, aunque no se limitan a:

- Puertas metálicas con una sola ventana en el lado opuesto a la cerradura.
- Cerraduras de un solo sentido (con llave desde afuera y libres desde adentro).
- Sistemas de videovigilancia instaladas con criterio lógico y respaldada por los resultados y recomendaciones arrojadas del análisis de riesgo.
- Personal calificado que realice CCTV de manera constante al sistema de videovigilancia.
- Personal de seguridad entrenado para responder este tipo de crisis y comenzar un *lock down* y/o evacuación en caso de que este tipo de situaciones ocurra.

Y quizás una de las medidas más importantes, simulacros. La participación debe incluir a los cuerpos de respuesta a emergencias (policías y bomberos) personal educativo y administrativo de los colegios y por supuesto a la población estudiantil.

Varios cuerpos policiales en los condados de Miami-Dade y Broward en el sur de la Florida, han puesto manos a la obra en realizar simulacros a gran escala con el fin de no repetir la trágica y vergonzosa actuación de los cuerpos policiales de Uvalde, Texas, donde la falta de coordinación y comunicación propicio el trágico desenlace que todos conocemos.

En conclusión, las medidas de seguridad en centros educativos son una prioridad social y de Estado, son los recursos en los que padres y representantes confían para dejar a sus hijos al cuidado de los docentes, es la garantía donde se soporta la confianza de las familias de los maestros y personal administrativo, que sus seres queridos regresaran a casa sanos y salvos. ■

Fabián E. Girón Pérez, *Assistant Security Officer* en New Face MD, Miami. *Más sobre el autor:*

amesis MR

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

SIAMES C5

Uso exclusivo de la plataforma, para comunicación con las autoridades

TOTAL ACCESO

Consulta a reportes de estadísticas de robos

24/365 DÍAS

Atención personalizada de nuestro centro de monitoreo

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

SOCIOS ACTIVOS

Con acceso a plataforma SIAMES C5 y P.U.C.(Punto Único de Contacto)

Tracking Systems · sitel · Holkan · skyguardian · skymeduza · ADS LOGIC · SECURE WITNESS · INFO TRAX · TECNO LOGISTIK · RALNDE · SEGURIPAC.com · ATLANTIDA · TTC · ISIS · geotrucks · GRUPO ALFIL · SOLUCIONES · GPSMonitor · PRYSE · DUMAX · PROTECZONE · Triskelion

SOCIOS ADHERENTES

Sin acceso a servicio de recuperación

GPS TRACKER MX · SATECH · TSNISION · RCU · GEOTRACKING · MAGNI Tracking

¡Síguenos en nuestras redes!

c.administrativa@amesis.org.mx

amesis.org.mx

COMUNÍCATE

55 3334 4707

¿CÓMO LOGRAR EL INVOLUCRAMIENTO SIN APOYO GERENCIAL?

Recomendaciones de nuestro colaborador para lograr que los altos mandos se involucren en la gestión de la seguridad

Foto: Freepik

PERÚ

Herbert Calderón

Constantemente los profesionales de diferentes rubros en sus labores en empresas privadas y públicas, se sienten desprotegidos, desmoralizados y hasta decepcionados cuando en muchas oportunidades no logran el apoyo, involucramiento y comprensión necesaria para cumplir con los objetivos trazados o metas personales.

La mejor solución tal vez sería renuncia, desmoralización, ejecución al pie de la letra la debilidad del sistema, buscar nuevas oportunidades en donde podamos ser considerados, escuchados, apoyados y así lograr los resultados deseados.

En lo personal pienso que estamos para solucionar inconvenientes y mejorar el desarrollo de las funciones asignadas, sería como un paralelo del médico que renuncia al paciente por las dificultades encontradas.

Lo recomendable es trabajar desde los mandos inferiores a los mandos superiores, vale decir, comenzar a transmitir buenas prácticas, recomendaciones, con mucha estrategia de comunicación de forma de construir una completa pirámide de escucha y respuesta.

Muchas veces los directores no prestan la atención a los profesionales que vienen con muy buenas estrategias de desarrollo, porque simplemente no saben escuchar, si en primera instancia se generan estrategias de comunicación, participación, como talleres, grupos de trabajo, etc.

En resumen, los sistemas de comunicación son ascendentes o descendentes, lo ideal es hacer descendentes, sin embargo, dada la problemática que nos aborda debemos hacerlo descendente.

En la práctica, ¿qué significa esto? Muy sencillo, conversar con el personal de toda la organización:

- Hacer amistad con todos.
- Acercarse a ellos en horas de relajo, eventos sociales.
- Ofrecer charlas o talleres de máxima participación de ellos.
- Coordinar la estrategia con toda nuestra área.
- Participar en eventos deportivos internos.
- Participar en los comités de seguridad y salud.
- Ofrecerse voluntariamente a cualquier requerimiento interno extra curricular o ajeno a nuestro trabajo.
- Participar en la organización de eventos sociales, navideños, etc.
- Compartir horas de almuerzo, refrigerio con nuestro personal de reporte directo, para ejemplarizar esta buena práctica.
- Lo esperado de toda esta estrategia es la siguiente:
- Acercamiento de los empleados a las gerencias.
- Satisfacción de necesidades relacionadas con los procesos en general de la organización.
- Mejora de las condiciones de trabajo, seguridad, clima laboral.
- Mejora del proceso productivo en general.
- Reducción de pérdidas generadas por los propios empleados ante la ausencia de comunicación y apoyo.

RESULTADOS

Finalmente, los esperado, ante la mejora de los indicadores comentados líneas arriba, la alta gerencia percibirá los resultados en los siguientes aspectos:

- Indicadores generales de producción.
- Mejora del clima laboral.
- Menor rotación de empleados.
- Fidelización de los colaboradores.
- Involucramiento en manejo de crisis, y respuesta a emergencias.

Adecuación y alineamiento de la alta gerencia a los objetivos de nuestra área. ■

Herbert Calderón, CPP, PCI, PSP, CSMP, CFE, gerente corporativo de Seguridad Integral de Grupo Gloria. *Más sobre el autor:*

RENTA DE BLINDADOS

COLEMAN

Tel.: 557672.4992

krauda@seguridadenamerica.com.mx

www.rentadeblindados.com.mx

CULTURA DE MEDICIÓN EN SEGURIDAD

Si la curva o nivel de madurez de medición en la organización es bajo, el profesional encargado de gestionar la seguridad, se enfrentará a un desafío significativo, donde debe superar barreras y sesgos de los colaboradores e incluso propios

Foto: Freepik

VENEZUELA | **Leonardo Taly**

La cultura de una organización es el conjunto de costumbres, principios y valores, que de una forma u otra caracterizan el comportamiento de las personas que la integran, identificando la manera de ser o de cómo hacen las cosas.

Para que una organización logre alcanzar una cultura de medición se requiere del compromiso de sus líderes en todos los niveles, de esta manera, identificar y gestionar el cambio de los paradigmas que puedan existir con relación a medir los resultados obtenidos, tales como: esto es imposible medirlo–no hay tiempo para medir–es mejor hacer que medir–medir pueden ser contraproducente.

¿POR QUÉ Y PARA QUÉ MEDIMOS?

Uno de los procesos de la administración en la teoría de Henry Fayol es "controlar" y, de acuerdo con el postulado de Peter Drucker, que "medir y evaluar" es una de las funciones gerenciales, resulta de vital importancia definir e implementar indicadores de gestión o *Key Performance Indicator* (KPI), que nos permitan identificar un punto de partida y observar la dirección que están llevando nuestros planes de acción en relación a los objetivos propuestos, aumentando notoriamente la eficiencia, agregando valor a los procesos, abaratando costos y mejorando la calidad de nuestros productos servicios prestados.

"Lo que no está definido, no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, siempre se degrada", William Thomson Kelvin.

¿QUÉ ES UN INDICADOR DE GESTIÓN O KPI?

Son parámetros cuantitativos y/o cualitativos definidos, que nos sirven de apoyo en la toma de decisiones informadas, analizando los datos, valores obtenidos, monitoreando patrones y tendencias del negocio, por consiguiente, es una herramienta clave para alcanzar la eficiencia y la mejora continua en nuestra unidad de negocio u organización.

"Un indicador es una magnitud que expresa el comportamiento o desempeño de un proceso, que al compararse con un nivel de referencia permite detectar desviaciones exclusivamente negativas", Luis Mora García, 2012.

Existen una gran variedad de indicadores que podemos utilizar para medir nuestro desempeño, sin embargo, debemos definir los factores claves que contribuyen a las metas que queremos conseguir y, sobre todo, que estén alineados a los objetivos estratégicos de la organización.

Los indicadores de acuerdo con lo que monitorizan, se clasifican en tres niveles: estratégico (impacto de la estrategia), táctico (resultados de los procesos), operacionales (planes de acción).

Ahora bien, cuando definimos nuestros objetivos podemos emplear los criterios del método **SMART:**

***S**pecific*: específicos.
***M**easurable*: medibles.
***A**chievable*: alcanzables.
***R**ealistic*: realistas.
***T**ime-bound*: tiempo límite.

El profesional de seguridad está obligado a conocer la actividad principal del negocio o core business, para poder alinear su estrategia a la misión de la empresa u organización, en donde, presta su servicio, ya que, su producto terminado no es seguridad per se

Luego de definir los objetivos, debemos establecer nuestros indicadores claves, se recomienda utilizar la regla **R.I.M.O:**

Relevante, para el negocio.
Inequívoco, que sea preciso.
Medible, su valor o expresión.
Objetiva, su fuente.

Por otra parte, es importante nombrar un responsable por los indicadores, fijando periodos para su actualización, frecuencia de control, quien realice el seguimiento y registro correspondiente en el tablero de control (TC) – *dashboard* o en su defecto ficha o matriz de indicadores, su rendición de cuenta y especialmente la manera de graficarlos o representarlos, para una adecuada comunicación y comprensión para la alta dirección.

¿QUÉ ES UN TABLERO DE CONTROL (TC)?

Es una herramienta de gestión visual que nos permite registrar y monitorear todos los indicadores claves y los planes de acción que contribuirán a logros de nuestras metas, generando alertas tempranas en desviaciones para las oportunidades de mejoras que afecten en los resultados de dichas acciones, de esta manera, acercarnos al cumplimiento de nuestros objetivos. Es recomendable utilizar colores o semaforización en nuestros TC, mejorando la visualización de los cumplimientos o desviaciones.

No obstante, si la curva o nivel de madurez de medición en la organización es bajo, el profesional encargado de gestionar la seguridad, se enfrentará a un desafío significativo, donde debe superar barreras y sesgos de los colaboradores e incluso propios. Así, poder implementar estrategias para desarrollar una cultura de medición de seguridad en toda la organización, ya que, esta práctica no es tan habitual.

En el establecimiento de un proyecto de seguridad, es necesario comprender que los indicadores poseen un ciclo de vida, ya que, al ir alcanzando los objetivos planteados, estos dejan de tener utilidad y es necesario ajustar los factores claves que se requieran mantener bajo control, para evaluar el comportamiento de nuevas variables que surjan en el proyecto de seguridad.

El profesional de seguridad está obligado a conocer la actividad principal del negocio o *core business*, para poder alinear su estrategia a la misión de la empresa u organización, en donde, presta su servicio, ya que, su producto terminado no es seguridad *per se*.

Fotos: Freepik

Existen una gran variedad de indicadores que podemos utilizar para medir nuestro desempeño, sin embargo, debemos definir los factores claves que contribuyen a las metas que queremos conseguir y, sobre todo, que estén alineados a los objetivos estratégicos de la organización

Por consiguiente, puede encontrarse gestionando seguridad física, seguridad en la cadena de suministro, seguridad de la información, etc. Por tal motivo, debe tener la flexibilidad para adaptarse a las necesidades y requerimientos que les demanden las unidades de negocio o clientes internos.

En este sentido, es de fundamental importancia poseer los conocimientos y habilidades que le permitan comprender la trasversalidad y relación que pueden existir entre los objetivos, de esta manera, poder identificar y establecer los diferentes elementos o variables relevantes para sus indicadores y planes de acción, que lo llevarán a la consecución de sus objetivos propiciando e impulsando desde su gestión una cultura de medición en seguridad para toda la organización. ■

Leonardo Taly, profesional del área de Seguridad con estudios realizados en Ciencias y Artes Militares. *Más sobre el autor:*

ENTENDIENDO LAS MATRICES DE RIESGO CUALITATIVAS Y CUANTITATIVAS:

UNA CUESTIÓN DE ESTRATEGIA Y RECURSOS DISPONIBLES

El autor hace un análisis profundo sobre los métodos de evaluación de riesgos en las empresas

Foto: Freepik

BRASIL **Tácito Augusto Silva Leite**

Este artículo analiza el documento *A Comparison of Risk Assessment Techniques from Qualitative to Quantitative*, elaborado por Thomas J. Altenbach en 1995, con el objetivo de arrojar luz sobre el tema de las matrices de riesgos, explorando tanto metodologías cualitativas como cuantitativas en su aplicación.

Curiosamente, a pesar del avance tecnológico y el desarrollo de nuevas metodologías a lo largo de casi 30 años, las preocupaciones fundamentales asociadas a la cuantificación de riesgos permanecen notablemente consistentes. La sección dedicada a los diez principales motivos para no cuantificar una evaluación de riesgo revela una persistencia de desafíos y cuestionamientos que atraviesan el tiempo, reflejando tanto los límites como las consideraciones prácticas que rodean el proceso de cuantificación en evaluaciones de riesgo.

Este artículo no sólo revisita estas cuestiones fundamentales, sino que también proporciona una reflexión sobre cómo, a pesar de las evoluciones en herramientas y enfoques, ciertas dudas y dilemas en la cuantificación de riesgos se mantienen pertinentes. Al explorar estas continuidades y cambios, el texto ofrece una perspectiva valiosa para profesionales y estudiosos del área, destacando la importancia de abordar la evaluación de riesgos con un equilibrio cuidadoso entre métodos cuantitativos y cualitativos, siempre atentos a las lecciones aprendidas a lo largo del tiempo.

El documento *A Comparison of Risk Assessment Techniques from Qualitative to Quantitative*, disponible en su totalidad en *https://www.osti.gov/biblio/67753*, presenta una discusión profunda sobre las diversas técnicas de evaluación de riesgo, variando de métodos puramente cualitativos a cuantitativos. El autor destaca las limitaciones y problemas de cada técnica, comparándolas entre sí, y ofrece una perspectiva sobre las implicaciones prácticas de estas metodologías en el campo de la evaluación de riesgos.

El texto aborda conceptos fundamentales de evaluaciones cualitativas y cuantitativas, discutiendo cómo cada enfoque impacta la interpretación y la comunicación de los riesgos. El documento también introduce matrices de riesgo cualitativas y semi-cuantitativas, explicando cómo estas herramientas se utilizan para categorizar y evaluar riesgos. Altenbach explora las limitaciones de estas matrices y sugiere que la falta de una base lógica consistente puede comprometer su eficacia.

¿CUÁNDO USAR UNA MATRIZ CUALITATIVA O CUANTITATIVA? BENEFICIOS Y LIMITACIONES

El artículo de T.J. Altenbach proporciona un análisis profundo de las matrices de riesgo, concentrándose en las diferencias fundamentales entre los enfoques cualitativos y cuantitativos, así como en sus respectivos beneficios y limitaciones.

Las matrices cualitativas, según describe el autor, se basan en descripciones y clasificaciones que no utilizan números para evaluar la frecuencia y las consecuencias de los riesgos. Estas matrices son particularmente útiles en contextos donde la información es limitada o cuando la evaluación debe realizarse rápidamente y sin la necesidad de datos detallados.

El beneficio de este enfoque es su simplicidad y la capacidad de proporcionar una visión general inmediata de los riesgos. Sin embargo, las limitaciones son notables: el enfoque cualitativo puede ser muy subjetivo, y la falta de cuantificación puede llevar a interpretaciones ambiguas y potencialmente a decisiones menos informadas.

Por otro lado, las matrices cuantitativas emplean métodos numéricos para definir tanto la frecuencia como las consecuencias de los riesgos, proporcionando una evaluación más precisa y objetiva. La utilización de la teoría de utilidad multiatributo para equilibrar diferentes tipos de riesgos de una misma operación es un ejemplo de la complejidad que este enfoque puede abarcar.

Los beneficios de esta técnica incluyen la capacidad de realizar comparaciones más precisas y basadas en datos, facilitando decisiones más fundamentadas y estratégicas. Sin embargo, las limitaciones de las matrices cuantitativas incluyen la necesidad de datos extensivos y confiables, además del riesgo de confiar excesivamente en números sin considerar el contexto cualitativo, lo que puede llevar a una percepción distorsionada de los riesgos.

Altenbach resalta que, mientras las matrices cualitativas son adecuadas para una visión rápida y generalista, care-

cen de la precisión y profundidad de los análisis cuantitativos. No obstante, la aplicación de matrices cuantitativas requiere recursos sustanciales y una comprensión profunda de los métodos estadísticos, pudiendo no ser siempre la elección más viable o necesaria. En última instancia, la elección entre una matriz cualitativa o cuantitativa debe estar guiada por el contexto específico de la evaluación de riesgo, considerando los recursos disponibles, la naturaleza de los datos y el objetivo del análisis.

CASI 30 AÑOS DESPUÉS Y LOS MISMOS 10 MOTIVOS PARA NO REALIZAR UNA EVALUACIÓN DE RIESGOS CUANTITATIVA

En un segmento interesante, el autor enumera los diez principales motivos para no cuantificar una evaluación de riesgo, donde aborda de manera un tanto jocosa los desafíos y las trampas de la cuantificación de riesgos. Esta sección destaca el escepticismo con relación a la cuantificación y sugiere una reflexión sobre cuándo y cómo los métodos cuantitativos deben ser aplicados en la evaluación de riesgos.

En el contexto más amplio, el documento enfatiza la necesidad de un enfoque equilibrado e informado en la evaluación de riesgos, reconociendo tanto los méritos como las limitaciones de cada técnica. Altenbach anima a los profesionales a considerar cuidadosamente la elección de las metodologías, basando sus decisiones en el contexto específico y en los objetivos de la evaluación de riesgo.

En el documento analizado, el autor Thomas J. Altenbach presenta una sección humorística e instructiva titulada los diez principales motivos para no cuantificar una evaluación de riesgo. A continuación, se presenta un resumen de los puntos destacados de esta sección del estudio:

Exposición a la crítica: Cuando los analistas proporcionan números específicos en sus evaluaciones, se convierten en blancos fáciles para críticas y escrutinios, pudiendo ser desafiados a defender cada dato utilizado en la cuantificación.

Pérdida de visión sistémica: Existe el riesgo de que los números generados en una evaluación cuantitativa se utilicen fuera de contexto, oscureciendo la comprensión más amplia del sistema evaluado.

Desafíos de la cuantificación: Los números son concretos y, por lo tanto, más fácilmente impugnables que los conceptos cualitativos, que por su naturaleza son más abiertos a interpretaciones.

Recursos y costo: Realizar un análisis cuantitativo detallado puede ser extremadamente costoso y consumir significativos recursos de tiempo y financieros.

Incertidumbre: Los análisis cuantitativos traen consigo incertidumbres inherentes, y el enfoque a menudo recae sobre estimaciones puntuales, ignorando la distribución de la incertidumbre.

Necesidad de formación especializada: La cuantificación requiere habilidades específicas en modelado, estadística y uso de *software* especializado, demandando una inversión significativa en formación.

Dependencia de datos: Las evaluaciones cuantitativas necesitan datos, que a menudo son escasos, imprecisos o de calidad cuestionable.

Miedo a lo desconocido: El análisis cuantitativo puede revelar riesgos inesperados o incómodos, llevando a resistencias basadas en el temor de lo que puede ser descubierto.

Suficiencia cualitativa: Puede existir la percepción de que los resultados cualitativos son "suficientemente buenos", evitando así la complejidad y el esfuerzo adicionales de la cuantificación.

Comprensión de la probabilidad: El concepto de probabilidad es a menudo mal interpretado o mal comprendido, lo que puede complicar la comunicación y la eficacia del análisis de riesgo cuantitativo.

Estos puntos resaltan la complejidad y los desafíos asociados a la cuantificación de evaluaciones de riesgo, sugiriendo que, aunque la cuantificación puede ofrecer *insights* detallados, viene acompañada de varias consideraciones importantes que deben ser cuidadosamente evaluadas.

CONCLUSIÓN

La exploración detallada de las matrices de riesgo por T.J. Altenbach nos ofrece un panorama esclarecedor sobre las matices y consideraciones cruciales en la elección entre enfoques cualitativos y cuantitativos en la evaluación de riesgos. Conforme delineado en el artículo, mientras las matrices cualitativas proporcionan una manera rápida e intuitiva de categorizar y priorizar riesgos, pueden carecer de la precisión y profundidad necesarias para un análisis más detallado y basado en datos.

Por otro lado, las matrices cuantitativas, aunque ofrecen un nivel de detalle y objetividad superior, demandan una inversión significativa en términos de recolección de datos, análisis y experiencia, lo que puede no ser justificable o viable en todas las situaciones.

La elección entre emplear una matriz cualitativa o cuantitativa no debe verse como una decisión binaria, sino como una consideración estratégica que tenga en cuenta el contexto específico de la evaluación, los recursos disponibles y los objetivos del análisis de riesgos. La comprensión de estas herramientas y la capacidad de aplicarlas adecuadamente son fundamentales para la gestión de riesgos eficaz e informada. Así, al avanzar hacia una práctica más matizada y consciente en la evaluación de riesgos, se vuelve esencial equilibrar la simplicidad y accesibilidad de los enfoques cualitativos con la precisión y profundidad de las metodologías cuantitativas, buscando siempre la aproximación más alineada con las necesidades específicas y el contexto del análisis.

¡Es con un espíritu entusiasta que anticipamos el futuro de las matrices de riesgo! Si hay algo que el artículo de Altenbach nos enseña, es que las discusiones sobre las mejores prácticas en evaluación de riesgos tienen el potencial de permanecer vibrantes y pertinentes, ya sea en los próximos 30 o, quién sabe, en los próximos 300 años. Esta continua evolución no se trata sólo de buscar la máxima eficiencia, sino de adaptar los recursos disponibles a la estrategia ideal, manteniendo los enfoques de evaluación de riesgos alineados con las demandas de cada era. Así, celebramos la incesante jornada de aprendizaje y adaptación en el campo de las matrices de riesgo, anticipando con alegría las innovaciones y debates que moldearán su futuro. ■

Tácito Augusto Silva Leite, CEO de la Plataforma t-Risk. *Más sobre el autor:*

AS3 DRIVER TRAINING SE UNE AL FESTEJO DE LOS **25 AÑOS DE SEA**

Especialistas en Seguridad se reunieron en las instalaciones de Off Road México, para realizar un curso de manejo evasivo y de prevención

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Como una de las actividades que conmemoran el 25 aniversario de **Seguridad en América**, AS3 Driver Training llevó a cabo un curso exclusivo de manejo evasivo y prevención de accidentes con diferentes responsables de Seguridad del país. Durante ocho horas, los especialistas pudieron llevar a la práctica los conocimientos brindados durante la capacitación teórica del curso, entre ellos: control y pérdida de control, velocidad, prevención de delitos o secuestro, maniobras evasivas, mitos de la seguridad, entre otros. El curso fue impartido el pasado 05 de septiembre en las instalaciones de Off Road México, ubicadas en Ocoyoacac, Estado de México.

De acuerdo con información del Instituto Nacional de Estadística y Geografía (INEGI), durante el 2023 se registraron 377 mil 231 accidentes, de los cuales, 229 mil 940 fueron colisión con vehículo; 11 mil 066 fueron colisión con peatón; 10 mil 911 fueron volcaduras; 10 mil 857 salieron del camino; y 4 mil 048 fueron colisión con ciclistas, de ahí la importancia de aprender, no sólo a reaccionar ante un posible accidente vehicular o asalto, sino desde los aspectos básicos de manejo: posición del asiento, presión en las llantas, posición al volante, uso de frenos, entre otros.

Las pruebas que se realizaron fueron cuatro diferentes, poniendo a prueba el 80% de las funcionalidades de los vehículos y la capacidad de reacción de los conductores frente a una situación fuera de su zona de confort, una de ellas fue el frenado en seco a 60 km por hora, otra, el control del volante y la dirección, en un circuito en el que no se podían utilizar los frenos. También se puso a prueba la evasión ante un intento de robo,

Los ejercicios de AS3 Driver Training, se basan 100% en técnicas de entrenamiento respaldadas por ciencia, utilizando instrumentos tecnológicos de medición que garanticen que se generen habilidades reales, para aplicaciones reales

manejando en forma de "y". Todos los participantes realizaron las cuatro pruebas aplicando los conceptos antes vistos, y corrigiendo diferentes aspectos.

El ejercicio final los posicionó en una situación en la que el estrés y los nervios pueden ser los peores enemigos para un conductor, una, que lamentablemente sucede con más frecuencia de la que pensamos, y es la intercepción de un vehículo. Todas las pruebas se realizan siempre bajo el cuidado y la dirección de los instructores de manejo de AS3 quienes tienen más de 10 años siendo profesionales capacitados en la materia.

AS3 DRIVER TRAINING

Durante la parte teórica, Pablo Ortiz-Monasterio, *co-founder & CEO* de AS3 Driver Training, comentó que este tipo de cursos demuestran con teoría y práctica cómo las personas consideran ser "buenos" conductores, hasta que se les pone a prueba frente a situaciones que alteran su seguridad y la estabilidad del vehículo, y cómo es importante conocer y verificar la situación del vehículo, sus partes y el mantenimiento que se le tiene que dar.

La compañía, que tiene más de 20 años especializada en manejo y seguridad, cuenta con las herramientas, estrategias e instructores altamente capacitados. Los ejercicios se basan 100% en técnicas de entrenamiento respaldadas por ciencia, utilizando instrumentos tecnológicos de medición que garanticen que se generen habilidades reales, para aplicaciones reales.

Actualmente, AS3 ofrece cursos dirigidos a escoltas y choferes ejecutivos, y ejecutivos y familias. Sin lugar a dudas, es una experiencia con grandes aprendizajes y, sobre todo, pensando en cómo prevenir, actuar, reaccionar, para conservar la vida e integridad de las personas. Al finalizar el curso, se otorgaron diplomas a los asistentes y la premiación para los mejores tres tiempos del circuito final. Samuel Ortiz Coleman, director general de **SEA**, brindó unas palabras en agradecimiento a los asistentes.

"Estamos muy agradecidos con AS3 Driver Training, con Pablo y todo su *staff* por formar parte de este gran aniversario, ya que 25 años se dicen fácil, pero han sido años de esfuerzo y dedicación para que ustedes siempre tengan la mejor información, y nos convirtamos en lo que hoy ya somos, que es una fuente de conocimiento y actualización". ■

Fotos: Mónica Ramos / SEA

"Han sido años de esfuerzo y dedicación para que ustedes siempre tengan la mejor información, y nos convirtamos en lo que hoy ya somos, que es una fuente de conocimiento y actualización", Samuel Ortiz Coleman

LOS EVENTOS MÁS IMPORTANTES QUE MARCARON EL AÑO 2024

Elecciones, reformas, guerras, desastres naturales, celebraciones y todos los acontecimientos más importantes que marcaron el rumbo de 2024

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

El año 2024 será recordado por los intensos conflictos político-sociales que enfrentaron varios países, pero también por los Juegos de la XXXIII Olimpiada en París, una de las ciudades más emblemáticas del mundo, la cual estuvo llena de emociones, drama, polémica, nuevos héroes e historias de vida dignas de admiración. Sin embargo, México, dentro de todo ese fervor deportivo, que además fue incendiado por la victoria de los medallistas paralímpicos, atravesó meses de violencia por las elecciones de 20 mil 708 cargos públicos en todo el país.

A continuación, se enlistan algunos de los sucesos más importantes que ocurrieron en 2024 —hasta el momento del cierre de esta edición—, los cuales impactaron en gran medida y, en algunos casos, tuvieron repercusiones en todo el mundo.

ENERO

01 de enero: Un terremoto de magnitud 7.6 sacudió la península de Noto, en la prefectura de Ishikawa (Japón), provocando un temblor de nivel 7 en la escala de intensidad sísmica en el pueblo de Shika, más de 200 personas perdieron la vida.

02 de enero: Se reportó una balacera entre presuntos extorsionadores y policías en la alcaldía de Iztacalco, Ciudad de México, dentro de un mercado de la colonia Agrícola Oriental, dejando dos fallecidos y siete heridos.

05 de enero: Siete ataques simultáneos de criminales fueron reportados en Villahermosa, Tabasco. Una serie de asaltos, quema de vehículos y la aparición de ponchallantas, provocaron pánico e incertidumbre entre la población.

07 de enero: Adolfo Macías, alias "Fito", se fugó de la cárcel del Litoral de Guayaquil (Ecuador) en la que estaba pagando una condena de 34 años desde el 2011 por delincuencia organizada, narcotráfico y asesinato.

09 de enero: Grupos criminales perpetraron secuestros de policías, colocaron explosivos en distintas ciudades de Ecuador e irrumpieron una transmisión en vivo del canal TC de Guayaquil. Unidades especializadas de la policía ecuatoriana llegaron a las instalaciones, lograron entrar, detener a 13 de los implicados y evacuar a las víctimas.

14 de enero: La activista trans y precandidata de Morena al Senado por la Ciudad de México, Samantha Carolina Gomes Fonseca, fue asesinada a balazos afuera del Reclusorio Preventivo Varonil Sur, en la alcaldía Xochimilco (CDMX).

17 de enero: El fiscal ecuatoriano, César Suárez, fue asesinado a tiros en la ciudad de Guayaquil. Suárez era uno de los fiscales que investigaba el asalto armado al canal TC de Guayaquil y grandes casos de corrupción.

25 de enero: El Fiscal General de Justicia del Estado de México, José Luis Cervantes, sufrió un intento de asesinato.

FEBRERO

10 de febrero: El aspirante a diputado federal de Morena, Yair Martín Romero Segura, fue asesinado junto con su hermano en Ecatepec, Estado de México.

20 de febrero: Se aprobó en el Senado de La República la "Ley Silla", que busca reducir los riesgos a la salud de todos los trabajadores cuya labor requiere que pasen lapsos prolongados de tiempo, de pie.

28 de febrero: Andrés Manuel López Obrador (presidente de México en ese momento) inauguró el "Gran Museo de Chichén Itzá", como parte de las obras complementarias del Tren Maya. El recinto cuenta con más de 400 piezas originales en 2,800 metros cuadrados de espacios de exhibición.

29 de febrero: El ejército disparó contra una multitud de personas que trataba de recoger alimentos de un convoy de camiones en Gaza. En el incidente murieron 112 personas y más de 700 resultaron heridas.

MARZO

06 de marzo: Dos trabajadoras de la Universidad Tecnológica de Guadalajara (UTEG) fueros asesinadas por arma blanca en manos de un hombre de 20 años, quien horas antes también asesinó a una joven de 22 años dentro de un motel, el sujeto fue detenido por las autoridades.

08 de marzo: Más de 180 mil mujeres, en su mayoría vestidas de color morado en protesta por la violencia de género, participaron en la marcha conmemorativa del "Día Internacional de la Mujer" en el Centro de la CDMX.

10 de marzo: La cinta de Christopher Nolan, 'Oppenheimer', ganó siete estatuillas en la 96ª edición de los Premios Óscar, incluidas: mejor director, actor principal y secundario. Mientras que el reconocimiento a "Mejor actriz", se lo llevó Emma Stone por su papel en "Pobres criaturas".

ABRIL

01 de abril: La candidata de Morena a la alcaldía de Celaya, Guanajuato, Bertha Gisela Gaytán, fue asesinada recién iniciaron las campañas electorales en la entidad. El atentado ocurrió cuando la morenista recorría las calles del centro de la comunidad de San Miguel Octopan.

08 de abril: Desde Mazatlán, México, hasta Indianápolis, EEUU, pudo observarse uno de los fenómenos astronómicos más extraordinarios del mundo: un eclipse total del sol.

30 de abril: Cinco pipas de gas LP explotaron en la gasera Mega Gas, ubicada en Tlahuelilpan, Hidalgo, sin que se reportaran personas heridas o fallecidas.

liminares (PREP), mostró la ventaja de la candidata Claudia Sheinbaum con el 59.4% de los votos, mientras que Xóchitl Gálvez (PAN-PRI-PRD), 27.9%, y Jorge Álvarez Máynez (MC), 10.4%.

02 y 03 de junio: Se suscitan diferentes actos vandálicos y violentos en varias partes de México, debido a las elecciones. Entre ellos: Grupos de choque, supuestamente, asociados a Morena atacaron y quemaron urnas en donde los resultados no les favorecían en Zumpango, Estado de México.

La coalición "Fuerza y Corazón por México", denunció el intento de secuestro de un simpatizante, justo afuera de una de las casillas ubicada en Huatabampo, Sonora.

Después del cierre de las urnas, personas armadas dispararon contra los funcionarios de la casilla 1020 instalada en el ejido de Carrizal, en el municipio de Paraíso.

18 de marzo: Joaquín Martínez López, alcalde de Chahuites, Oaxaca (Partido Verde Ecologista de México- PVEM), se convirtió en el candidato número 25 que fue asesinado en el proceso electoral. Aspiraba a reelegirse o una diputación.

22 de marzo: Sesenta y seis personas fueron privadas de su libertad en Culiacán, Sinaloa.

25 de marzo: Fueron encontradas con vida 58 personas de las 66 que fueron secuestradas en Culiacán, ninguna levantó una denuncia o quiso revelar lo que vivió.

26 de marzo: Aparecieron varias 'narcomantas' presuntamente firmadas por Iván Archivaldo Guzmán Salazar, identificado como el líder de 'Los Chapitos', en las que se leía: "Esto le va a pasar a todos los rateros de Sinaloa para que sientan lo que sienten las familias cuando se meten a robarle sus casas a invadir su privacidad. Familiares de personas que anden en esos delitos eviten pasar un mal rato y denuncien cualquier acto de esa índole".

MAYO

10 de mayo: Habitantes de las localidades de Lázaro Cárdenas y Nueva Morelia (Chiapas) reportaron la presencia de sujetos armados y el corte de la energía eléctrica como resultado de los conflictos entre el Cártel de Sinaloa y el Cártel Jalisco Nueva Generación (CJNG).

13 de mayo: Un comando de sicarios irrumpió en el ejido Nueva Morelia y masacró a 11 personas, de las cuales cinco son mujeres y seis son hombres. Uno de los asesinados era Ignacio López, un catequista de 52 años que aspiraba a ser pastor y se habría negado a trabajar para criminales con presencia en la región.

JUNIO

02 de junio: En México se llevó a cabo la elección más grande de la historia, por el número de cargos a elegir, 20 mil 708 en todo el país. El Programa de Resultados Electorales Pre-

06 de junio: El Instituto Nacional Electoral (INE) confirmó la victoria contundente de Claudia Sheinbaum con 35,923,984 votos (59.76% de los votos totales).

07 de junio: Más de cuatro mil indígenas choles fueron desplazados por la violencia que azota a la localidad de Tila, Chiapas, debido a la presencia de un grupo armado denominado Los Autónomos, quienes también son reconocidos como 'karma' y la 'Fuerza Armada de Tila.

JULIO

13 de julio: El ex presidente Donald Trump, sufrió un atentado en un mitin en Butler, Pensilvania (EEUU), Thomas Matthew Crooks, de 20 años, efectuó varios disparos, incluido uno que, según Trump, le rozó la oreja. Al menos tres asistentes al mitin recibieron disparos, uno de los cuales murió.

19 de julio: Apagón informático causado por CrowdStrike provocó el colapso de bancos, hospitales, aerolíneas y oficinas gubernamentales a nivel mundial.

26 de julio: Se inauguran los Juegos de la XXXIII Olimpiada en París, Francia.

28 de julio: Se llevaron a cabo las elecciones presidenciales en Venezuela, resultando como presidente electo, Nicolás Maduro, quien será presidente por los siguientes seis años. Maduro fue declarado ganador de los comicios por parte del Consejo Nacional Electoral (CNE) venezolano, con 51.20% de los votos con 80% de las mesas escrutadas, aunque ciudadanos y la oposición consideran fraude y manipulación del ejecutivo.

AGOSTO

11 de agosto: La ciudad de la luz se despide de los JJOO, México obtuvo cinco medallas: tres platas y dos bronces, que se conquistaron en las disciplinas de clavados, boxeo, judo y tiro con arco.

28 de agosto: Dan inicio los Juegos Paralímpicos en París.

SEPTIEMBRE

08 de septiembre: Concluye los Juegos Paralímpicos en París, Francia. México fue bien representado por estos atletas, de donde se obtuvieron un total de 17 medallas: tres de oro, seis de plata y ocho de bronce.

11 de septiembre: Fue aprobada la reforma al Poder Judicial en México. El punto más polémico de la ley radica en la elección popular de más de 1,600 cargos judiciales, entre ministros de la Suprema Corte, consejeros del Consejo de la Judicatura Federal, magistrados del Tribunal Electoral Federal, magistrados de circuito y jueces de distrito.

15 de septiembre: Ryan Wesley Routh, de 58 años, y con antecedentes penales, fue detenido por un aparente intento de asesinato a Donald Trump en el Trump International Golf Club de West Palm Beach, Florida, al ser descubierto por agentes del Servicio Secreto con un rifle asomándose en los arbustos cerca del ex presidente de Estados Unidos.

22 de septiembre: El Pacífico mexicano recibió a la Tormenta Tropical "John", la cual con el paso de los días se intensificó hasta formarse un huracán que pasó de categoría 3 a 1. Las principales zonas afectadas fueron en el estado de Guerrero, así como Oaxaca y Michoacán.

26 de septiembre: El Huracán "Helene" tocó tierra en Florida, Estados Unidos como categoría 4, y el cual cobró la vida de siete personas en ese estado, 15 en Georgia y otras 17 en Carolina del Sur, dos de ellas bomberos, hasta ese momento. "Helene" dejó a 4.3 millones de personas sin electricidad.

27 de septiembre: Al menos 11 personas perdieron la vida debido a las afectaciones por el Huracán "John". Las autoridades informaron que las precipitaciones acumuladas del 22 al 27 de septiembre fueron de 949.2 mm, "lo que significa que en cuatro días llovió el 80% de lo que llueve en un año".

28 de septiembre: **Seguridad en América**, fuente de actualización y conocimiento, cumple sus primeros 25 años de existencia en el mercado.

OCTUBRE

01 de octubre: Claudia Sheinbaum asume oficialmente el cargo de (la primera mujer) presidente de México.

02 de octubre: Marcha en la Ciudad de México por la conmemoración de los 56 años de la masacre de Tlatelolco.

02 de octubre: Eclipse solar anular, también conocido como el "Anillo de Fuego", el cual pudo verse en algunos lugares de Baja California, Baja California Sur, Colima y Jalisco, entre las 9:48 a las 11:17 de la mañana.

08 de octubre: Asesinan y decapitan a Alejandro Arcos Catalán, presidente municipal de Chilpancingo, Guerrero, quien acababa de cumplir 43 años y apenas hacía seis días que había asumido el cargo.

11 de octubre: El presidente Joe Biden declaró que el huracán "Milton" causó daños estimados en 50 mil millones de dólares en Florida, además de costar la muerte de al menos 16 personas, hasta ese momento.

16 de octubre: Muere Liam Payne, ex cantante de One Direction, tras caer del tercer piso de un hotel en Buenos Aires, Argentina. El incidente ocurrió aparentemente tras estar bajo los efectos de drogas o alcohol.

16 de octubre: Dan sentencia por 38 años a Genaro García Luna, ex secretario de Seguridad en el sexenio del panista Felipe Calderón Hinojosa, por los cargos de narcotráfico, delincuencia organizada y falsedad documental.

NOVIEMBRE

05 de noviembre: Celebración de las sexagésimas elecciones presidenciales en Estados Unidos.

19 de noviembre: Se cumplieron 40 años de la tragedia de San Juanico (explosión de la terminal de almacenamiento de Petróleos Mexicanos en San Juan Ixhuatepec, Estado de México, 1984), en la que se estimó la pérdida de entre 500 y 600 personas, mil heridos, y la evacuación de 60 mil personas por los daños en un área de hasta un kilómetro de la planta siniestrada.

DICIEMBRE

24 de diciembre: Celebración de Navidad (religión católica).

31 de diciembre: Celebración de fin de año. ■

Fuentes consultadas:

- *https://www.infobae.com/america/mundo/2024/01/11/japon-declaro-el-terremoto-de-ano-nuevo-como-un-desastre-de-gravedad-extrema-y-elevo-a-mas-de-210-los-muertos/*
- *https://cnnespanol.cnn.com/2024/06/01/politicos-asesinados-campana-mexico-orix*
- *https://www.infobae.com/mexico/2024/01/15/quien-es-samantha-gomes-fonseca-activista-trans-que-fue-asesinada-al-salir-de-una-visita-en-el-reclusorio-sur/*
- *https://www.bbc.com/mundo/articles/c51z74dz79zo*
- *https://elpais.com/mexico/2024-02-20/el-senado-aprueba-la-ley-silla-para-regular-el-trabajo-de-pie-durante-largas-jornadas.html*
- *https://www.jornada.com.mx/2024/02/29/cultura/a05n1cul*
- *https://elpais.com/hemeroteca/2024-02-29/1/*
- *https://www.bbc.com/mundo/articles/c970y3my60jo*
- *https://www.eleconomista.com.mx/politica/Asesinan-a-Bertha-Gisela-Gaytan-candidata-a-la-alcaldia-de-Celaya-20240401-0112.html*
- *https://www.infobae.com/mexico/2024/03/26/esta-es-la-razon-detras-del-secuestro-masivo-en-culiacan-segun-narcomanta-firmada-por-el-chapito/*
- *https://www.infobae.com/mexico/2024/05/16/masacre-en-chicomuselo-confirman-que-hay-miembros-de-la-iglesia-entre-las-11-victimas/*
- *https://www.milenio.com/estados/estiman-10-mil-desplazados-tila-violencia-chiapas*
- *https://elpais.com/mexico/elecciones-mexicanas/2024-06-07/asi-quedaron-los-computos-distritales-que-otorgan-la-victoria-a-claudia-sheinbaum.html*
- *https://mvsnoticias.com/nacional/estados/2021/11/19/explosion-de-san-juanico-una-tragedia-que-no-se-olvida-37-anos-474914.html*
- *https://www.razon.com.mx/mexico/que-eventos-astronomicos-habra-octubre-2024-cometa-del-siglo-lunas-de-otono-594821*

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

LÍDERES EN SOLUCIONES DE

RASTREO SATELITAL

24/365 DÍAS Monitoreo de equipos

Desarrollo de WEB y APP

Telemetría e Inteligencia Artificial (IA)

Tecnología 3G/4G/Satelital

Contamos con puntos estratégicos en todo el país

amazon web services

Azure

Infraestructura sustentada por AWS y Azure

gmesis · AMESP · ANTP · ASIS · CANACAR · COPARMEX · ConaLog

Más Información:

Contáctanos

55·5374·9320

¡Síguenos en nuestras redes!

trackingsystems.mx

+ de 52,500 Equipos Instalados

24/7 Rastreo Satelital

Recuperación 98.5% Aviso en menos de 30 minutos*

IA

VALIDACIÓN DE IDENTIDAD CON IA

REVISIÓN A NIVEL MUNDIAL EN MÁS DE 1,100 LISTAS RFL

ANÁLISIS POR FRECUENCIA DE VOZ

TRUST ID

VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL

LA FORMA MÁS RÁPIDA Y PODEROSA DE CERTIFICAR A TU PERSONAL

UNA SOLUCIÓN DE Grupo UDA · Tracking Systems

¡Síguenos en nuestras redes!

TRUSTID.MX

Contáctanos

55·4447·0231 · 5374·9320 · EXT 159

atencionaclientes@trustid.mx

Más Información:

Foto: Freepik

CONDUCTOR PREVENTIVO

Un conductor preventivo es aquel que analiza constantemente su entorno y anticipa posibles riesgos para evitar que se conviertan en problemas. Este tipo de conducción se basa en la capacidad de identificar riesgos potenciales y tomar medidas rápidas para evitarlos

VENEZUELA **Henry Carracedo**

El presente trabajo fue realizado con el objetivo de ampliar y conocer algunas técnicas de la conducción preventiva, en pro de disminuir la cantidad de accidentes de tránsito.

Cuando nos referimos a seguridad vehicular el proceso está centrado en el concepto: manejo defensivo y ofensivo. Recopilando información actualizada y en búsqueda de la prevención vehicular fortalecida, nace el concepto conductor preventivo (espacio operacional). El conductor preventivo tiene su espíritu en evitar y evadir los peligros existentes en las carreteras.

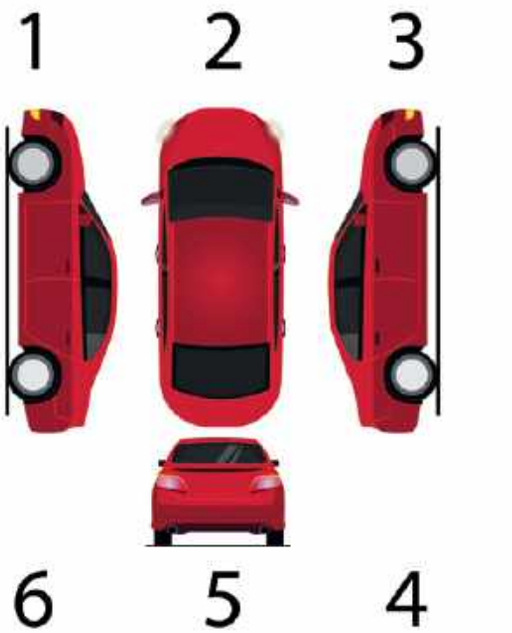
Mi preocupación se inicia cuando nos reportan estadísticas donde identifican a Venezuela entre los 26 países con fallecidos en accidentes de tránsito, quinta causa de muerte, y en un 90% por fallas/error humano. En la actualidad más del 80% de los accidentes de tránsito están involucrados motorizados, con una alta tasa de lesionados y fallecidos.

Analizando cifras publicadas por el Observatorio de Seguridad Vial, los accidentes de tránsito aumentaron en este año 2024, sólo en el mes de enero: 303 siniestros de vehículos, con 520 lesionados. Reportan más de 100 fallecidos en accidentes viales, por lo que convierte en un tema de salud pública.

Comparando las causas de los accidentes de tránsito a nivel internacional y en el territorio venezolano, se identifican las siguientes:

1) Alta velocidad.
2) Consumo de alcohol y drogas.
3) Distracción, en especial por manipulación del teléfono celular. El 94 %.
4) Falta de iluminación de los vehículos y de las carreteras.
5) Condiciones meteorológicas.
6) Vehículos en malas condiciones, cauchos vencidos, entre otros.

El espacio operacional, son las áreas circundantes al vehículo y que ayudan a la seguridad, limitando la posibilidad de probables accidentes. Este espacio tiene siete zonas, extendiéndose hasta lo que alcanza la vista del conductor: 1, 2 y 3 (180 grados) frente al vehículo. 4, 5 y 6 (180 grados) detrás del vehículo. 3 y 4 carril derecho del vehículo. 1 y 6 carril Izquierdo. La zona 7 son las áreas ciegas alrededor de su vehículo (lo que no se alcanza a visualizar por los retrovisores).



Vista del conductor

Sumando los sistemas y métodos de prevención para conductores conocidos como: SMITH, IPDE y BEE, se fortalece el concepto de conductor preventivo (espacio operacional).


Foto: Freepik

Más del 80% de los accidentes de tránsito están involucrados motorizados, con una alta tasa de lesionados y fallecidos

MÉTODO SMITH PARA REDUCIR ACCIDENTES DE TRÁFICO:

1) Ver siempre hacia adelante. Lo ideal es que no tenga ningún tipo de obstáculos visuales. Esto se llama espacio operativo abierto (condiciones ideales para conducir).

2) Identificar peligros en los 360 grados, siempre utilizando los retrovisores cada cinco a ocho segundos, alerta en los puntos ciegos y evitando las barreras en la visión delantera.

Existen varios métodos para calcular la distancia del vehículo delantero en movimiento, el más efectivo es el siguiente: se multiplica el primer número de tu velocidad, ejemplo:

80 Kp/h. 8 x 8: 64 metros. Estos 64 metros es la distancia mínima segura entre carros.

Existe otro método que es la regla de los tres segundos: comience a contar cuando el parachoques trasero del vehículo que esta adelante pase por un objeto, contar un millón, dos y tres millones, el parachoques delantero de su carro no debe pasar el objeto en referencia, sino después de contar los tres millones.

Si está en baja velocidad, calcule la distancia con el vehículo de delante de la siguiente forma: el ras de su capot o tablero con los cauchos traseros del vehículo que está adelante. Este espacio preventivo le permite salir en caso de emergencia.

3) Mantenga sus ojos en continuo movimiento. Visión periférica 180 grados.

4) Siempre mantenga una ruta de salida para casos de emergencia. Si pierde su espacio de maniobra, busque recuperarlo inmediatamente, esta distancia segura es más o menos cinco metros de distancia al vehículo más próximo. Una técnica rápida es observar los cauchos traseros del vehículo que se encuentra adelante.

Frene con anticipación, esta técnica activa la alerta de conductor que le sigue.

5) Asegúrese que los otros conductores lo vean y escuchen, es decir, buenas luces, triángulo o cono de seguridad (este es el ideal). Se deben colocar a una distancia de 50 metros.

SISTEMA IPDE (IDENTIFICAR, PREDECIR, DECIDIR Y EJECUTAR):

1) Identifique los posibles riesgos.

2) Prediga lo que pudiera ocurrir. Nunca descienda del vehículo. Reporte al 911 o Bomberos de la localidad. Si por razones de emergencia toma la decisión de salir del vehículo: no toque o pise los cables, brinque en un solo pie hasta salir del área (no coloque en el piso de forma simultánea los dos pies).

3) Decida cuáles son las probables alternativas. Elija la mejor acción.

4) Ejecute la acción. Siga o se retorna con precaución.

SISTEMA BEE (ESPACIO LIBRE EFICAZ):

1) Buscar/identificar los peligros potenciales y cambios de las condiciones de la carretera o el tráfico.

2) Evaluar qué acciones debe realizar para evitarlos. Opción más segura.

3) Ejecutar la acción más segura para evitar los peligros potenciales y que no se conviertan en amenazas. Maniobras preventivas y evasivas.

Recuerde siempre contar con un espacio seguro alrededor de su vehículo, siempre tendrá más opciones de cómo reaccionar para evitar un accidente. ■


Foto: Freepik

Analizando cifras publicadas por el Observatorio de Seguridad Vial, los accidentes de tránsito aumentaron en este año 2024, sólo en el mes de enero: 303 siniestros de vehículos, con 520 lesionados. Reportan más de 100 fallecidos en accidentes viales, por lo que convierte en un tema de salud pública

Henry Carracedo, especialista en Seguridad y Protección Integral y Seguridad Ciudadana, Técnico Prehospitalario y Materiales Peligrosos, Bombero Voluntario y facilitador en técnicas de seguridad.
Más sobre el autor:

OBJETIVO DE DESARROLLO SOSTENIBLE 11

Foto: Freepik

El Objetivo de Desarrollo Sostenible 11 (ODS 11) de la Agenda 2030 de las Naciones Unidas busca que las ciudades y comunidades sean sostenibles, inclusivas, seguras y resilientes

MÉXICO **Rafael E. Vera**

En un mundo cada vez más consciente de la necesidad de cuidar nuestro medio ambiente, la Responsabilidad Social Empresarial se ha convertido en un componente crucial para las empresas que buscan no sólo generar ganancias, sino también contribuir positivamente a la sociedad y el entorno. Un área en la que la RSE puede tener un impacto significativo es la reducción de emisiones de dióxido de carbono (CO_2), un objetivo alineado con el Objetivo de Desarrollo Sostenible 11 de la Agenda 2030 de las Naciones Unidas. En particular, la industria de la seguridad privada tiene una oportunidad única de liderar este cambio mediante la adopción de vehículos eléctricos en sus operaciones.

RESPONSABILIDAD SOCIAL EMPRESARIAL Y SOSTENIBILIDAD URBANA

La RSE implica que las empresas adopten prácticas que favorezcan el desarrollo sostenible y mejoren la calidad de vida de las comunidades en las que operan. En el contexto de las ciudades, el ODS 1[1] busca hacer que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles. Esto incluye, entre otros aspectos, la mejora de la calidad del aire y la reducción de la huella de carbono.

Las ciudades son responsables de una parte significativa de las emisiones globales de CO_2 debido al tráfico vehicular. En este sentido, la industria de la seguridad privada, que opera con una flota considerable de vehículos, puede desempeñar un papel fundamental en la reducción de estas emisiones mediante la transición a vehículos eléctricos.

REDUCCIÓN DE CO_2 A TRAVÉS DE VEHÍCULOS ELÉCTRICOS

Los vehículos eléctricos son una alternativa ecológica a los vehículos de combustión interna tradicionales, ya que producen cero emisiones directas de CO_2. La adopción de estos vehículos por parte de las empresas de seguridad privada no sólo contribuirá a la mejora de la calidad del aire urbano, sino que también alineará a estas empresas con las mejores prácticas de RSE y los objetivos globales de sostenibilidad.

La reducción de emisiones de CO_2 tiene múltiples beneficios. Además de mitigar el cambio climático, también se mejora la salud pública al disminuir los contaminantes del aire que pueden causar enfermedades respiratorias y cardiovasculares. Las empresas de seguridad privada, al optar por vehículos eléctricos, pueden posicionarse como líderes en sostenibilidad dentro de su sector y generar un impacto positivo tanto en el medio ambiente como en la salud de las comunidades en las que operan.

DIVERSIDAD DE VEHÍCULOS ELÉCTRICOS Y SU IMPLEMENTACIÓN EN LA SEGURIDAD PRIVADA

La variedad de vehículos eléctricos disponibles en el mercado ofrece múltiples opciones para su implementación en los diferentes servicios de la seguridad privada. A continuación, se describen algunos de estos vehículos y su posible uso en el sector:

1) ***Scooters* Eléctricos:** Ideales para patrullas en áreas urbanas densas y centros comerciales. Son fáciles de manejar y permiten una rápida movilidad en espacios reducidos.
2) **Monopatines Eléctricos:** Útiles para recorridos

cortos en parques industriales y campus universitarios. Su tamaño compacto facilita su uso en interiores y exteriores.

3) **Bicicletas Eléctricas:** Perfectas para patrullajes en parques, zonas residenciales y áreas donde se requiera una mayor cobertura. Proporcionan una buena velocidad y alcance, además de ser ecológicas y silenciosas.
4) **Automóviles Eléctricos:** Esenciales para patrullajes de largo alcance y transporte de personal y equipos en grandes áreas metropolitanas. Ofrecen mayor comodidad y capacidad de carga.

COMPARATIVO DE COSTOS: VEHÍCULOS DE COMBUSTIÓN VS. VEHÍCULOS ELÉCTRICOS

La transición a vehículos eléctricos no sólo tiene beneficios ambientales, sino también económicos. A continuación, se presenta un comparativo del gasto en pesos mexicanos entre vehículos de combustión interna y vehículos eléctricos:

Concepto	Vehículo de Combustión	Vehículo Eléctrico
Costo por litro de gasolina	$24 MXN	
Costo por kWh de electricidad		$1.8 MXN
Consumo promedio por 100 km	8 litros	18 kWh
Costo por 100 km	$192 MXN	$32.4 MXN
Mantenimiento anual	$10,000 MXN	$4,000 MXN

culo eléctrico es significativamente menor que el de un vehículo de combustión interna. La diferencia en el costo de combustible por cada 100 km recorridos es considerable, con los vehículos eléctricos presentando un ahorro del 83%. Además, los vehículos eléctricos requieren menos mantenimiento, lo que se traduce en menores costos anuales.


Foto: Freepik

La industria de la seguridad privada, que opera con una flota considerable de vehículos, puede desempeñar un papel fundamental en la reducción de estas emisiones mediante la transición a vehículos eléctricos

CASOS DE ÉXITO Y BENEFICIOS ECONÓMICOS

Varias empresas de seguridad privada en todo el mundo ya han comenzado a incorporar vehículos eléctricos en sus flotas. Estos casos de éxito demuestran no sólo la viabilidad de esta transición, sino también los beneficios económicos a largo plazo. Los vehículos eléctricos tienden a tener menores costos operativos y de mantenimiento en comparación con los vehículos de combustión interna, lo que puede resultar en ahorros significativos para las empresas.

Además, el uso de vehículos eléctricos puede mejorar la reputación corporativa y fortalecer la relación con los clientes que valoran la sostenibilidad y la responsabilidad ambiental. En un mercado cada vez más competitivo, ser reconocido como una empresa comprometida con la reducción de la huella de carbono puede ser un diferenciador clave.

La adopción de vehículos eléctricos en la industria de la seguridad privada representa una oportunidad significativa para avanzar en la agenda de la Responsabilidad Social Empresarial y contribuir al cumplimiento del ODS 11. Al reducir las emisiones de CO_2 y mejorar la calidad del aire urbano, las empresas de seguridad privada no sólo protegen a las comunidades a las que sirven, sino que también protegen el medio ambiente y promueven un futuro más sostenible. La transición a vehículos eléctricos es una inversión en el bienestar de las generaciones futuras y un paso importante hacia la construcción de ciudades más verdes y saludables. ■


Foto: Freepik

Rafael E. Vera, director general de Misiones Regionales de Seguridad, A.C. (MRS).
Más sobre el autor:

SABÍA DEMASIADO... ¿CONFIAR O NO CONFIAR? ESE ES EL DILEMA

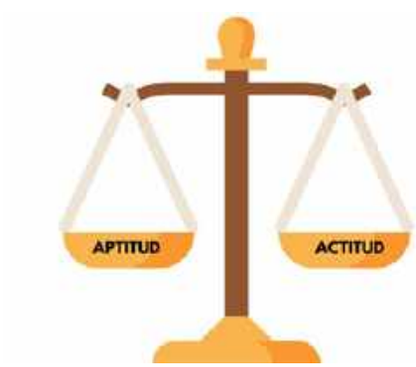
Aptitud y actitud en el ámbito de la seguridad

Foto: Freepik

MÉXICO **David Chong Chong**

Por una condición básica del ejercicio profesional, un elemento de Seguridad conoce lo que se considera como las grietas de seguridad (debilidades, vulnerabilidades, grado de exposición) del objetivo que pretende proteger, el cual pueden ser personas, instalaciones o transportes. Información muy sensible y de gran valor para un potencial agresor que puede ser un adversario personal, un competidor de negocio… o un delincuente, y que está en poder de ese elemento de Seguridad.

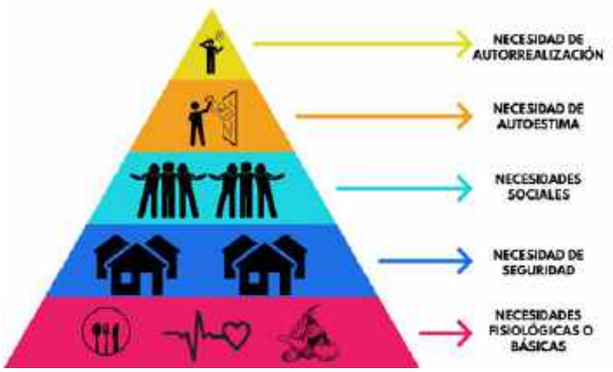
En general, el personal constituye el componente de eficacia (para hacer lo que se debe hacer de alguna manera), indispensable en cualquier campo de actividad, y la efectividad del desempeño en cualquier ámbito laboral se sustenta en un equilibrio entre dos atributos, la Aptitud (capacidad para hacer) y la Actitud (disposición anímica o voluntad para hacer). En este contexto se tiene que la Aptitud comprende lo que corresponde básicamente a las competencias laborales, que son el saber (conocimientos), el saber hacer (destrezas, habilidades, hábitos) y el saber qué hacer (criterios para tomar decisiones), que se adquieren, conservan y desarrollan por medio de procesos de capacitación, instrucción y adiestramiento.



Por su parte, la Actitud es una cuestión más subjetiva, determinada por la medida en que las perspectivas de certidumbre y estabilidad laboral, así como de suficiencia individual de las retribuciones y beneficios, cubran sus expectativas de bienestar (satisfactores para las necesidades) y prosperidad (oportunidades para las aspiraciones) personal, familiar y social, de tal suerte que este atributo es el de mayor influencia en este equilibrio.

En el ámbito de la Seguridad, la Aptitud es muy importante, pero la Actitud es crucial por el riesgo inherente de vida asociado el ejercicio profesional, lo que induce un efecto de incertidumbre en las perspectivas, más allá de sólo el bienestar y prosperidad, sino a la misma existencia e integridad física (el profesional de la Seguridad sale todos los días de si casa, sin saber si regresará o cómo regresará).

Esta relevancia y mayor influencia de la Actitud en este equilibrio con la Aptitud, proviene de los principios de la Teoría de las Jerarquías de Maslow, ya que, por las condiciones inherentes de riesgo de vida del ejercicio profesional en este ámbito, por atender a la necesidad de mayor prioridad, la Subsistencia para mantener la vida, se soslaya o "sacrifica" la atención a la necesidad de menor prioridad relativa, la Seguridad para mantener la vida, lo que resulta de alguna manera paradójico, a que por procurar la seguridad a otros, que en muchas ocasiones ni sólo lo ignoran y no lo agradecen, sino lo desprecian y lo hacen blanco de denostaciones, arriesga no sólo su propia seguridad, sino también la de su familia (el profesional de la Seguridad es el que da el paso al frente cuando los demás retroceden).



En el ámbito de la Seguridad las condiciones laborales antes descritas, tanto en lo personal como para la familia, proyectan un perfil mínimo de expectativas en cuanto que la magnitud de las retribuciones y beneficios recibidos, así como el marco de perspectivas de certidumbre y estabilidad laboral, correspondan o excedan las posibles consecuencias de los riesgos asumidos, tanto en lo individual como en lo familiar.

Y esto repercute en la conformación de un atributo particular y fundamental para este ámbito, la confiabilidad, proyectada en dos vertientes de efectividad, en el desempeño para el cumplimiento de las funciones a pesar de los riesgos que implica, y en la tutela de la confidencialidad de la información sensible del objetivo que se pretende proteger, en particular de sus grietas de seguridad, ante ofrecimientos de beneficios ilegales o al menos antiéticos para compartirla con agresores potenciales. Por ello, las condiciones laborales constituyen una cuestión de relevancia crucial para los Servicios de Seguridad.

SECTOR PÚBLICO

En el Sector Público, principalmente con el personal de las corporaciones de policía, las limitaciones a las condiciones laborales suelen estar "justificadas" por malentendidas medidas de "austeridad y economía" presupuestal, en un supuesto "beneficio de la ciudadanía", que en realidad sólo benefician a la imagen y "popularidad" de los personajes políticos a cargo de las instituciones, y que sólo perjudican a la propia ciudadanía. Esto aunado a un manejo arbitrario y discrecional de órdenes ilegítimas e incluso ilegales de abuso de autoridad, recompensas, reconocimientos, canonjías y privilegios, y extorsión a los subordinados por los mandos, que provocan no sólo un efecto dominó, sino multiplicador a expensas de la ciudadanía (si tengo que extorsionar por 200 para darle 100 al jefe, lo mismo da extorsionar por 300, 400 o más) por una permisividad implícita, una virtual "patente de corso" para extorsionar.

Adicionalmente en este sector concurren dos factores "ambientales". Por un lado, por parte de la propia ciudadanía, que en principio exige una aplicación estricta en las leyes, pero al encontrarse en situaciones sancionables, demanda un trato de excepción de lo que se podría describir, con cierta ironía, como "designios divinos selectivos" (¡Hágase la voluntad de Dios! En la yunta de mi comadre, no en la mía), lo que sólo contribuye a propiciar y fortalecer las prácticas de extorsión a la propia ciudadanía.

Por otro lado, la exposición personal y familiar de los elementos en su vivienda, aislados y sin protección, que los hace vulnerables a las exacciones y presiones con las prácticas descritas como "plata o plomo" de los grupos delictivos que actúan con superioridad numérica y de fuerza.

Fotos: Freepik

SECTOR PRIVADO

Por su parte, en el Sector Privado las limitaciones a las condiciones laborales que comprenden, entre otras, salarios y beneficios laborales, así como apoyos logísticos restringidos, jornadas extenuantes aunadas a una "multifuncionalidad" (el mismo elemento en diferentes tareas sólo con una preparación genérica no especializada), incertidumbre en la continuidad laboral, e incluso extorsiones y exacciones por los mandos operativos, se imponen por motivos de índole financiera, derivado de una visión empresarial de la Seguridad como un "gasto improductivo", de tal suerte que se proyecta una perspectiva de inestabilidad laboral en las prestadoras de estos servicios.

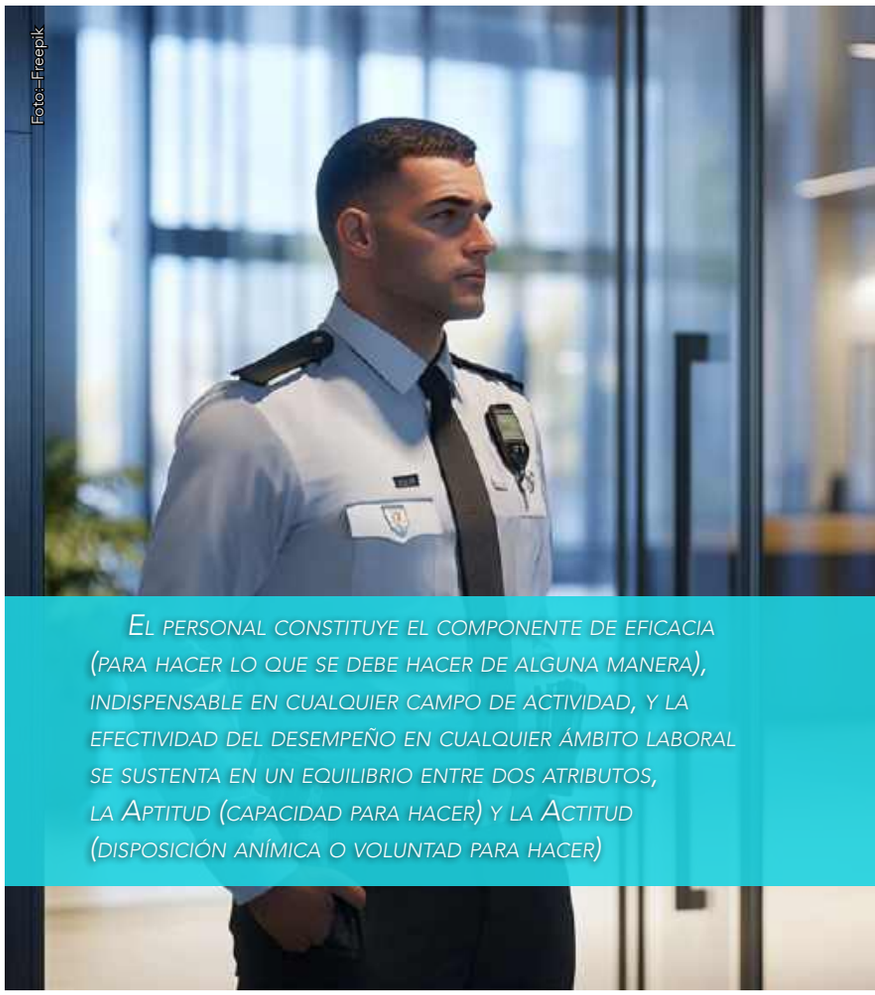
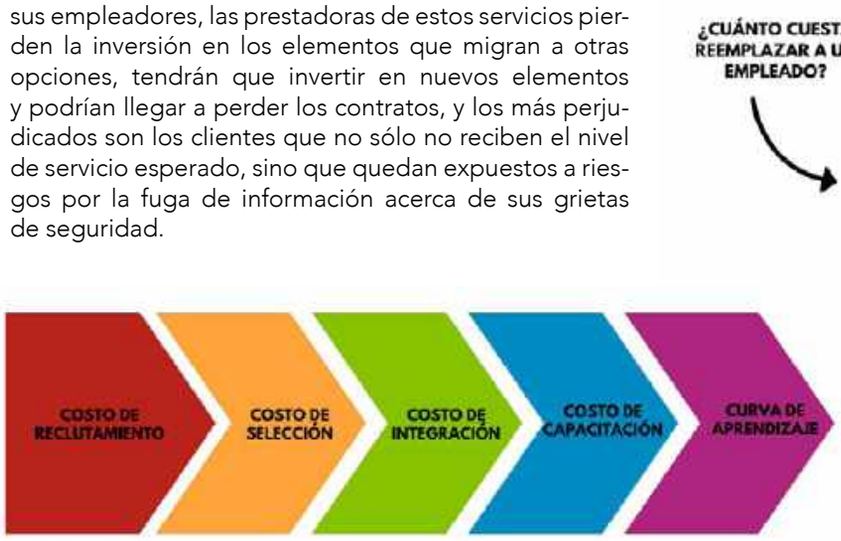


Foto: Freepik

El personal constituye el componente de eficacia (para hacer lo que se debe hacer de alguna manera), indispensable en cualquier campo de actividad, y la efectividad del desempeño en cualquier ámbito laboral se sustenta en un equilibrio entre dos atributos, la Aptitud (capacidad para hacer) y la Actitud (disposición anímica o voluntad para hacer)

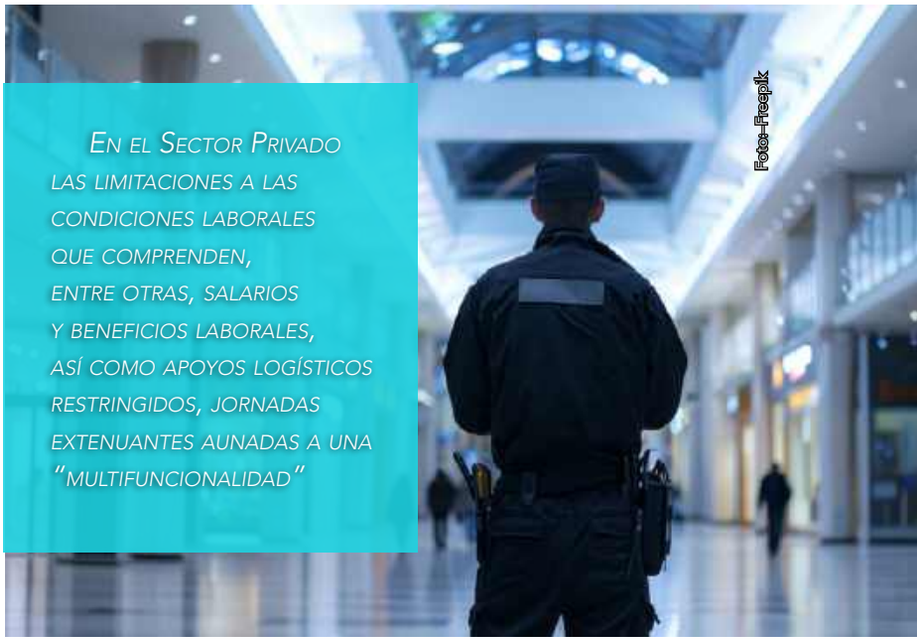
Y esta es una situación en la que nadie gana y todos pierden, porque los elementos no reciben lo que esperan y en ocasiones refieren buscar otras opciones, sus empleadores, las prestadoras de estos servicios pierden la inversión en los elementos que migran a otras opciones, tendrán que invertir en nuevos elementos y podrían llegar a perder los contratos, y los más perjudicados son los clientes que no sólo no reciben el nivel de servicio esperado, sino que quedan expuestos a riesgos por la fuga de información acerca de sus grietas de seguridad.



Las condiciones laborales constituyen el factor de mayor impacto en el atributo de Actitud, de tal suerte que cuando son o se perciben como precarias, insuficientes e insatisfactorias pueden comprometer la confiabilidad del personal operativo, ya sea degradando la efectividad de su desempeño, por desinterés, descontento, distracciones (al buscar opciones para cubrir sus carencias) y/o resentimientos, o bien, lo más crítico, quebrantar la confidencialidad de la información sensible que posee acerca de las grietas de seguridad de los clientes de los servicios, que puede ser de gran valor para potenciales agresores, ya sea adversarios personales, competidores de negocio… o la delincuencia.

En este contexto es que el problema de fondo son los elementos de Seguridad descontentos, insatisfechos o resentidos, que si permanecen en el servicio se pueden convertir en informantes, y si deciden separarse o son separados, muy probablemente no guardarán ninguna consideración o lealtad hacia sus antiguos empleadores y usuarios, pero se llevará consigo información sensible que podría poner a disposición de cualquier interesado, ya que es alguien que sabía demasiado. Por ello, la cuestión crucial no es tanto si se puede confiar o no confiar, sino hasta dónde se puede confiar, o mejor aún, considerando cuánto vale lo que se quiere proteger, la cuestión sería cuánto cuesta poder confiar en que tendrá la mejor protección posible.

En Seguridad, lo barato puede salir caro… muy caro. Puede consultar una versión ampliada de este artículo en este enlace: https://www.ceasmexico.org.mx/beta/data/art/Art00000249.pdf ■



En el Sector Privado las limitaciones a las condiciones laborales que comprenden, entre otras, salarios y beneficios laborales, así como apoyos logísticos restringidos, jornadas extenuantes aunadas a una "multifuncionalidad"

Foto: Freepik

David Chong Chong, secretario general para México de la Corporación Euro Americana de Seguridad (CEAS) México.
Más sobre el autor:

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

Cel: +52 477 828 1291

SEGURIDAD EN EL SECTOR PETROLERO

Elementos para una estrategia de seguridad integral

Foto: Freepik

COLOMBIA | **John Mario Pérez Morales**

En el sector petrolero, la seguridad de los empleados y la protección de los activos críticos son fundamentales para garantizar la continuidad del negocio. Las operaciones, tanto en tierra como en el fondo marino, requieren equipos especializados y una ingeniería precisa para identificar, evaluar y mitigar los riesgos asociados.

Cada complejo petrolero cuenta con servicios especializados que respaldan la explotación y producción, haciendo indispensable el soporte continuo de un departamento de Seguridad que se integre de manera transversal en todas las actividades.

La minimización de riesgos es una tarea esencial que involucra múltiples áreas, destacando especialmente la seguridad. Eventos como fugas de gas, incendios, explosiones, derrames de crudo o lesiones por aplastamiento deben ser documentados y comunicados a toda la compañía. Además, se debe capacitar y entrenar a brigadas para la atención de emergencias, realizando simulacros de preparación, como la evacuación médica, que puede requerir transporte aéreo dependiendo de la gravedad de las lesiones.

Entender el mapa de gestión de riesgos permitirá orientar los esfuerzos en materia de inversión tecnológica o humana, mejorando los controles establecidos, aprendiendo de las buenas prácticas y lecciones aprendidas del sector.

Las operaciones en el sector petrolero frecuentemente se llevan a cabo en áreas remotas y a menudo enfrentan desafíos adicionales como la presencia de actores ilegales, condiciones climáticas extremas y entornos de trabajo peligrosos. En este contexto, es crucial contar con una estrategia de seguridad integral que abarque desde políticas hasta procedimientos específicos para las actividades en campo.

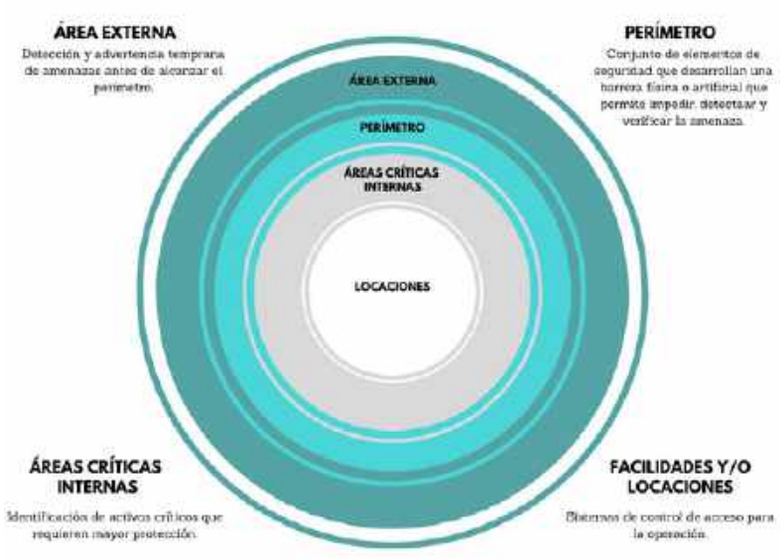
Establecer objetivos y metas claras, junto con métricas de evaluación frecuente, es esencial para garantizar el éxito y la eficacia de las

operaciones. Esta actividad comienza con la definición de estrategias que deben alinearse con la misión corporativa, lo que implica comprender a fondo el negocio y sus objetivos a largo plazo.

Al elaborar un plan de acción, es fundamental describir detalladamente cada una de las metas establecidas, así como las estrategias específicas que se implementarán para alcanzarlas. Cada meta debe ir acompañada de un indicador de gestión, que permita monitorear el progreso y evaluar el cumplimiento de manera efectiva. Además, es importante designar claramente a los responsables de cada tarea y establecer plazos realistas para su cumplimiento.

En resumen, la elaboración de una estrategia de seguridad efectiva en el sector petrolero requiere un enfoque meticuloso y bien estructurado, que considere un enfoque transversal que brinde soporte a todas las áreas del negocio.

NIVELES DE CRITICIDAD EN CAMPO



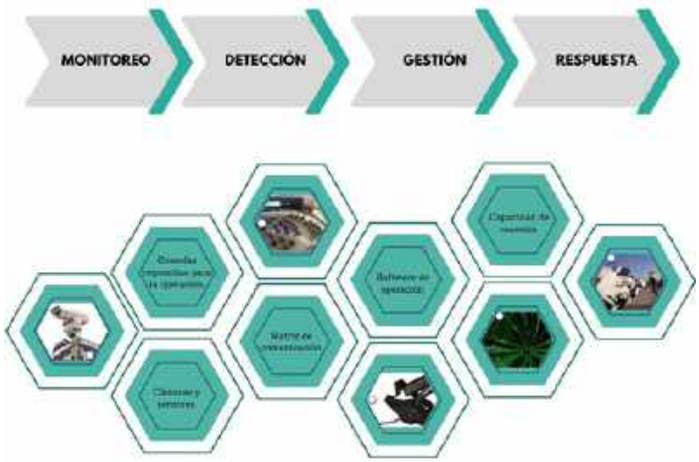
CARACTERÍSTICAS DE SEGURIDAD

En el sector petrolero, algunas de las características de seguridad más importantes son:

- **Cumplimiento normativo:** Adherirse a las regulaciones y estándares gubernamentales y de la industria para garantizar un entorno de trabajo seguro y la protección del medio ambiente.
- **Gestión de riesgos:** Identificar, evaluar y mitigar los riesgos asociados con las operaciones petroleras, desde la exploración y producción hasta el transporte y refinación.
- **Cultura de seguridad:** Fomentar una cultura organizacional donde la seguridad sea una prioridad en todas las actividades y en todos los niveles de la empresa.
- **Capacitación y entrenamiento:** Proporcionar programas de formación exhaustivos para garantizar que los empleados estén capacitados para realizar sus tareas de manera segura y responder efectivamente a situaciones de emergencia.
- **Protección de la salud:** Implementar medidas para proteger la salud física y mental de los trabajadores, incluyendo controles de exposición a sustancias químicas y programas de salud ocupacional.
- **Gestión de crisis:** Establecer protocolos claros y procedimientos de respuesta para manejar emergencias como derrames de petróleo, incendios y accidentes.
- **Tecnología y equipos de seguridad:** Utilizar tecnologías avanzadas y equipos de seguridad especializados para minimizar los riesgos en las operaciones y proteger a los trabajadores.
- **Comunicación y colaboración:** Fomentar una comunicación abierta y efectiva entre todos los empleados, contratistas y partes interesadas para compartir información sobre seguridad y mejorar la colaboración en la identificación y mitigación de riesgos.

Estas características son fundamentales para garantizar la seguridad y el bienestar de los trabajadores y el medio ambiente en el sector petrolero.

En materia de seguridad física conservando la premisa de la prevención, detección, retardo y respuesta, los esquemas de seguridad deberán contener un factor humano que de la mano de herramientas tecnológicas controle el acceso a las diferentes locaciones. Una seguridad tecnológica que brindará el soporte necesario a toda la operación, funcionará como el cerebro, donde se concentrará toda la información vital y operativa necesaria para la articulación operacional.



Los fenómenos criminales presentes en las áreas de operación petrolera, sean estos eventos delictivos o contravencionales deberán ser atendidos, con el apoyo de la fuerza pública, un área de control de pérdidas podrá apoyar todas las áreas para evitar acciones que alimenten o propicien desviaciones que terminen en la materialización de delitos.

- **Acercamientos con la Comunidad.** Es el apoyo permanente que debemos brindar a los equipos de responsabilidad social, y hacen parte de la anticipación de posibles eventos de protesta social, que imposibiliten el acceso a una locación interrumpiendo así las operaciones. Conocer las dificultades del día a día de la comunidad pueden mitigar necesidades puntuales que eviten acciones de hecho.

- **Relaciones con las autoridades.** El apoyo institucional es vital para el éxito operacional, algunas empresas manejan convenios que permiten contar con apoyos adicionales que sin desdibujar la misionalidad enfocan sus esfuerzos de forma más específica en el área de interés. Participar en los comités regionales de la industria, permiten conocer de primera mano las acciones que puedan afectar el normal desarrollo de las operaciones, y lograr una anticipación. La gestión de la información y su adecuado tratamiento permite a la alta dirección la acertada toma de decisiones.

En el desarrollo de los planes de seguridad antes de iniciar cualquier actividad del sector, requieren entender la dinámica de actividades de grupos ilegales, así como su referenciación, cercanías al proyecto, dinámica de la criminalidad urbana y rural, si es posible con análisis detallado de fenómenos delictivos y contravencionales, es decir entender el por qué se genera dicha conducta, la conflictividad social, en especial intereses de las comunidades, presencias de cabildos indígenas, áreas protegidas.

OBSERVACIONES	Confinamiento armado	Desplazamiento armado	Desaparición forzada	Atentados contra FP	Terrorismo armado	Secuestro	Extorsión	Homicidio selectivo	Minería criminal	Microtráfico	Narcotráfico	ACTIVIDADES / ORGANIZACIONES
GAO Entorno rural												
GAO Entorno urbano												

IMPACTO	ALTO	MEDIO	BAJO	NULO	SIN INFORMACIÓN

La identificación de riesgos, así como su evaluación, nos permitirá acertar en los controles que requiere el mantenimiento de la operación.

La construcción de una estrategia integral de seguridad para el sector petrolero es una labor prioritaria para cualquier compañía, contar con una estructura de seguridad con esquemas definidos podrá facilitar el control y soporte a las diferentes actividades que se desarrollen, así como la inmediatez y diligencia que generalmente requieren este tipo de actividades, Seguridad era entonces el aliado estratégico que se sume al mantenimiento de la continuidad del negocio.

ESTRATEGIA INTEGRAL DE SEGURIDAD

Una estrategia integral de seguridad petrolera debe incluir una serie de elementos clave para abordar los riesgos y proteger tanto a los empleados como al medio ambiente. Algunos componentes importantes de esta estrategia son:

- **Evaluación de riesgos:** Identificación y evaluación de los riesgos específicos asociados con las operaciones petroleras, desde la exploración hasta la producción y el transporte.
- **Políticas y procedimientos:** Desarrollo e implementación de políticas y procedimientos de seguridad claros y exhaustivos que establezcan estándares para todas las actividades y operaciones.
- **Capacitación y entrenamiento:** Provisión de programas de capacitación y entrenamiento continuos para garantizar que los empleados estén preparados para realizar sus tareas de manera segura y para responder efectivamente a situaciones de emergencia.

El apoyo institucional es vital para el éxito operacional, algunas empresas manejan convenios que permiten contar con apoyos adicionales que sin desdibujar la misionalidad enfocan sus esfuerzos de forma más específica en el área de interés

Foto: Freepik

- **Tecnología y equipos de seguridad:** Utilización de tecnologías avanzadas y equipos de seguridad especializados para minimizar los riesgos en las operaciones y proteger a los trabajadores.
- **Monitoreo y cumplimiento:** Implementación de sistemas de monitoreo y evaluación para verificar el cumplimiento de las políticas y procedimientos de seguridad, y tomar medidas correctivas cuando sea necesario.
- **Gestión de crisis:** Desarrollo de protocolos claros y procedimientos de respuesta para manejar situaciones de emergencia, como derrames de petróleo, incendios y accidentes.
- **Colaboración y comunicación:** Fomento de una cultura de seguridad que promueva la comunicación abierta y la colaboración entre todos los empleados, contratistas y partes interesadas.
- **Mejora continua:** Establecimiento de un proceso de mejora continua para revisar y actualizar regularmente la estrategia de seguridad en función de la evolución de los riesgos y las mejores prácticas de la industria.

Al integrar estos elementos en una estrategia integral, las empresas petroleras pueden mitigar los riesgos, proteger a su personal y minimizar el impacto ambiental y de riesgo público de sus operaciones. ■

John Mario Pérez Morales,
oficial en uso de buen retiro de la Policía Nacional y especialista en seguridad. *Más sobre el autor:*

LA CAPACITACIÓN ADECUADA ES LA CLAVE PARA LOGRAR UN SISTEMA DE GESTIÓN SÓLIDO

Fabiola Carrascal Carrillo
Coordinación de Capacitaciones
7 años trabajando en BASC

"La digitalización ha facilitado el aprendizaje y ayudado a las empresas a estar preparadas para enfrentar los desafíos del futuro con mayor confianza y capacidad de respuesta."

Durante el tiempo que llevo formando parte del Capítulo BASC México en el área de capacitaciones, he sido testigo de los desafíos que hemos enfrentado en los últimos años, cuando el mundo se detuvo. Esto nos llevó a plantear una nueva perspectiva sobre cómo avanzar frente a las adversidades tanto personales como laborales.

Considero que las capacitaciones desempeñan un rol crucial en el desarrollo de un sistema de gestión efectivo, que haga a las empresas más seguras y eficientes, en conjunto con el compromiso de la Alta Dirección. En BASC, nuestro objetivo es ofrecer a nuestros socios capacitaciones que proporcionen los conocimientos adecuados para implementar de manera eficaz y exitosa el sistema de gestión en control y seguridad.

He observado el compromiso de nuestros asociados, reflejado en la continua capacitación de sus colaboradores en los temas que ofrece el Capítulo. Por este motivo, trabajo junto a nuestros instructores para asegurar que los colaboradores comprendan los requisitos de la Norma y Estándares BASC y sepan cómo aplicarlos en su trabajo diario, logrando así un sistema de gestión maduro.

Vivimos en un mundo más digital, donde las capacitaciones han evolucionado para adaptarse a las necesidades de las empresas, siendo más accesibles para un mayor número de personas. La digitalización ha facilitado el aprendizaje y ha ayudado a las empresas a estar mejor preparadas para enfrentar los desafíos del futuro con mayor confianza y capacidad de respuesta. Esto nos llevó a rediseñar cursos y capacitaciones para ofrecerlos de manera virtual, permitiendo una mayor participación de nuestras empresas en el proceso de formación continua.

El compromiso del Capítulo, junto con el servicio y la atención que brindamos en el área de capacitaciones, son fundamentales para que las empresas sigan creciendo y estén preparadas para enfrentar los cambios del comercio global. Un sistema de gestión sólido es el resultado de un esfuerzo conjunto, y la capacitación adecuada es la clave para lograrlo. En lo personal, es gratificante acompañar a nuestros socios en cada etapa de la implementación del sistema de gestión.

En un entorno empresarial cada vez más desafiante y globalizado, la formación continua y adecuada se convierte en el pilar fundamental para garantizar un sistema de gestión en control y seguridad robusto. A través del esfuerzo conjunto entre las empresas y el equipo de BASC, hemos sido testigos del crecimiento y evolución de nuestros socios, quienes enfrentan con mayor confianza los retos del comercio global. La digitalización ha permitido que la capacitación sea más accesible y efectiva, asegurando que las empresas estén preparadas para el futuro. Como siempre, en BASC seguimos comprometidos con la excelencia en el servicio y el acompañamiento a nuestros socios, ayudándoles a construir sistemas de gestión sólidos y sostenibles.

BASC OCCIDENTE DE MÉXICO

BASC MÉXICO
www.bascoccidente.com.mx
BASCOccidenteMexico
basc_mexico
basc-occidente-méxico

ILUMINACIÓN DE SEGURIDAD

Cada tipo de luz tiene características especiales que la hacen recomendable para específicas aplicaciones y ofrecen diferentes efectos sobre los colores naturales

Foto: Freepik

COLOMBIA | **Javier Nery Rojas Benjumea**

GENERALIDADES

La selección de los medios de iluminación está determinada por la naturaleza o tipo de instalación y las operaciones que en ella se desarrollen. En todo caso su propósito es producir suficiente luz para crear un efecto disuasivo psicológico para la intrusión y permitir a la fuerza de seguridad o a otros medios electrónicos, la detección virtualmente cierta de cualquier anomalía.

El sistema debe proveer un nivel específico de iluminación para disuadir intrusos y evitar molestias o luces peligrosas, en especial cuando la instalación está adyacente a áreas residenciales o pobladas, calles, avenidas o vías navegables.

Un sistema de iluminación debe ser de fácil mantenimiento y debe estar protegido contra ataques o sabotajes. Para eso se debe determinar el grado de hermeticidad.

El sistema debe ser confiable por su capacidad de operación y por el cumplimiento de los estándares adecuados y estar diseñado de manera que el haz de luz o huella de iluminación quede traslapado para evitar que haya áreas desprotegidas en el evento de que una luminaria individualmente falle.

Todo sistema debe poseer una fuente de energía auxiliar de respaldo para el caso en que, por una emergencia o incidente, se produzcan en la instalación unas fallas de energía.

Los postes deben estar dentro del perímetro o barrera de la instalación, con el fin de mantener su seguridad. Las limas o cableado de la energía deben estar enterradas y las cajas de los *switches* y controles deben poseer un adecuado nivel de seguridad física.

La iluminación suplementaria, incluyendo luces de rastreo (reflectores) y lámparas portátiles también deben ser parte del sistema general de iluminación proyectiva. Estas luces se proveen para situaciones de emergencia y aunque no sean usadas con regularidad deben estar disponibles para las fuerzas de seguridad (*search lights, flood lights, fresnel lens*).

El sistema debe operar automáticamente (encenderse y apagarse) mediante fotoceldas que respondan a la cantidad de luz del crepúsculo y el amanecer. El sistema puede encender lámparas individuales o el sistema total. También existen y pueden ser usados controles temporizados o un sistema de operación manual.

La iluminación perimetral debe estar dirigida hacia abajo y afuera del área protegida y no hacia el frente, especialmente cerca de vías o áreas pobladas, para evitar encandilar peatones, residentes o conductores. También debe cuidarse de evitar el deslumbramiento de los guardias de seguridad y dirigirla preferiblemente para iluminar a quien se acerque desde afuera a la barrera o al sitio de recepción.

Como regla general, los elementos de iluminación cercanos a las barreras perimetrales deben estar alrededor de 30 pies dentro del perímetro, a una distancia aproximada de 150 pies y a una altura de 30 pies sobre el suelo.

En áreas aisladas o semi-aisladas del perímetro se usan reflectores de lente Fresnel o luz de inundación, donde se requiere deslumbramiento. No se deben usar estos reflectores enfrentados a avenidas, calles o en áreas pobladas. Si el área es semi-aislada, estos pueden ubicarse alrededor de 20 pies del cerramiento. Si el área es aislada se pueden ubicar a 250 pies del cerramiento.

Cuando el edificio está cerca del perímetro, las luces pueden ser montadas sobre el mismo edificio. Las entradas de estos edificios deben ser iluminadas individualmente para evitar sombras causadas por la otra iluminación.

En áreas donde la lima de propiedad limita con un cuerpo de agua, la iluminación debe estar diseñada para eliminar áreas sombreadas en especial en muelles y limas de marea. Cualquier plan de iluminación protectiva en la vecindad de aguas navegables debe ser consultado con el Servicio de Guardacostas.

GLOSARIO DE TÉRMINOS CLAVES

- ***Foot candle.*** Es una unidad de medida de la intensidad de la iluminación. Es la distribución uniforme de un lumen de luz en un pie cuadrado de área, esto es, la cantidad de luz que provee una vela sobre un pie cuadrado de espacio.
- **Lumen (*candle*).** Es el término técnico usado para medir el flujo luminoso emitido dentro del espectro visible o sea la cantidad de luz de una fuente luminosa. El Lumen por *Watt* es una medida de eficiencia o relación entre el flujo luminoso y la potencia absorbida por la fuente de luz. Es decir, que tanta luz es producida por el vatio de electricidad requerido para operar la fuente lumínica o bombilla.
- **Lux.** Es una unidad internacional de iluminación que significa la distribución de un lumen de luz sobre un metro cuadrado de superficie. Es la medida de un flujo luminoso sobre un área determinada. Equivale a un Lumen por metro cuadrado. Un *Foot Candle* es igual a 10.76 Lux. Algunos medidores de luz dan sus lecturas en Lux. Muchas cámaras de videovigilancia establecen sus estándares de desempeño en condiciones de baja luminosidad o sensibilidad, en términos de Lux.
  El ojo humano detecta objetos que reflejan 0.05 lux y las mejores cámaras de videovigilancia -sin IR- (día y noche), tienen una sensibilidad de 0.01 Lux. Una cámara BN CCD estándar tiene una sensibilidad de 0.03 Lux y una cámara a color para interiores estándar tiene sensibilidad de 0.1 Lux.
- ***Color Rendering Index* (CRI).** Es el efecto de la luz sobre el color aparente de los objetos. Es medido por el Índice de Desempeño del Color CRI. Una luz con un bajo CRI hace aparecer los colores menos naturales. Los rangos van de 0 a 100, teniendo la luz del sol un valor de 100 y la iluminación de LPS (*Low Pressure Sodium*) que es monocromática un valor de 0.
- **Reflector.** Este dispositivo redirecciona la luz a través de un proceso de reflexión. Es el "espejo" que está alrededor del bombillo en una linterna.
- **Refractor.** Es una lámina de vidrio, plástico o policarbonato diseñado para controlar la dirección de la luz a través del uso de prismas. El diseño del refractor junto con el uso del reflector ayuda a dirigir y distribuir la luz disponible.
- **Luminaria.** Es el dispositivo iluminador en conjunto y podría incluir: la fuente de luz, el reflector, el refractor y la cubierta o *housing* y el conjunto eléctrico. El poste y el brazo donde está la luminaria son considerados partes separadas.
- **Balasto.** Todas las fuentes de luz de HID requieren alguna forma de balasto, porque requieren un voltaje de encendido más alto que el voltaje de la línea. El balasto provee un voltaje transformado permitiendo el uso de diferentes voltajes de línea. Como para propósitos prácticos la bombilla se inicia como un corto circuito, el balasto limita y controla la forma de esa onda de corriente a través de la bombilla, por eso, escoger un mejor balasto es fundamental para obtener el mejor rendimiento y desempeño de la bombilla, aunque esto pudiera resultar en un costo inicial más alto. Hay otros componentes del llamado conjunto eléctrico, tales como: condensadores y arrancadores.

TIPOS DE FUENTES DE LUZ

- Incandescentes.
- Fluorescentes.
- *High Intensity Discharge* (HID).
- *Metal Halide*.
- Vapor de Mercurio.
- Vapor de sodio (alta presión).
- Vapor de sodio.
- Electroluminiscentes.
- Cuarzo
- *Light Emiting Diodes* (LED).

Cada tipo tiene características especiales que la hacen recomendable para específicas aplicaciones y ofrecen diferentes efectos sobre los colores naturales.

Las siguientes variables deben ser revisadas cuando se considere una instalación de iluminación para propósitos de seguridad:

- Vatiaje de la luminaria.
- Altura del montaje de la luminaria.
- Distancia entre las luminarias.
- Eficiencia de la luminaria.

Después de que se ha seleccionado la fuente de luz, la siguiente consideración es escoger la ubicación más adecuada de la luminaria. Para esto se debe entender los siguientes factores visuales:

- Tamaño de los objetos.
- Brillo o reflejo de las superficies.
- Contraste entre objetos.
- Tiempo de detección.
- Deslumbramiento.

RECOMENDACIONES PARA LA ILUMINACIÓN DE SEGURIDAD

- Iluminar entradas, salidas de emergencia, etc. con una luz brillante blanca.
- Los parqueaderos deben ser iluminados con luz brillante blanca que permita la uniformidad (sin dejar áreas oscuras).
- Tener un plan de Mantenimiento.
- Los parqueaderos deben ser iluminados de manera que se pueda distinguir una cara humana a 10 metros de distancia (tres *foot candles* verticalmente sobre la superficie).
- Deben usarse protectores de alambre o lentes resistentes para proteger las lámparas del vandalismo.
- Ubicar las lámparas evitando puntos ciegos.
- La regla general en la instalación de iluminación en parqueaderos es que la altura de la fuente de luz multiplicada por cuatro dará la distancia a la cual los postes debería estar alejados
- La regla general en la iluminación de muros aledaños al edificio es que la altura del muro multiplicada por seis dará la distancia a la cual los postes deberían estar alejados. ■


Foto: Freepik

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

ISO 22344:

LA NUEVA NORMA ISO DE LA PREVENCIÓN DEL DELITO MEDIANTE EL DISEÑO AMBIENTAL (CPTED)

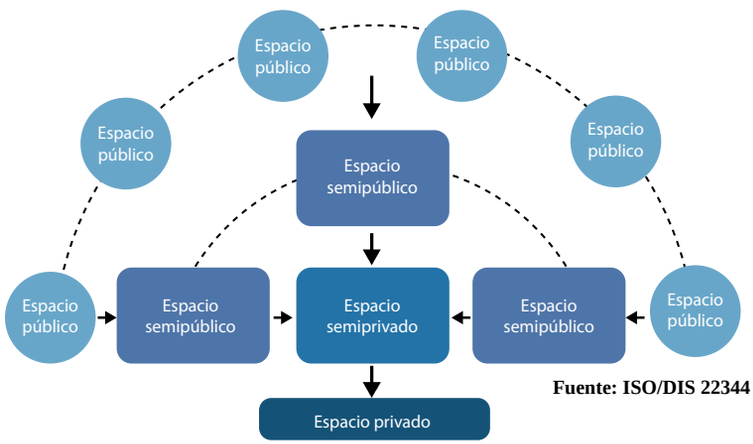
El objetivo no es sólo proteger las propiedades contra robos, sino también evitar el acceso de visitantes no deseados, la apropiación ilegal de espacios, la degradación del medio ambiente y mitigar el miedo a la delincuencia

Foto: Freepik

MÉXICO **Mercedes Escudero Carmona**

La Norma ISO/DIS 22344 *Security and resilience — Protective security — Guidelines for Crime Prevention Through Environmental Design for Residential Facilities,* salió publicada en mayo del 2024. Esta Norma nos hace comprender que los delitos y los riesgos de seguridad en las instalaciones residenciales tienen una naturaleza y un tipo de delito específicos, como el robo en el hogar (intrusión).

Tiene como objetivo proporcionar una guía para la prevención del delito mediante el diseño ambiental (CPTED, por sus siglas en inglés) con el fin de reducir las oportunidades de delincuencia y el miedo a la delincuencia, creando entornos residenciales seguros y sostenibles. Además, sigue el proceso y los principios generales que se describen en la norma ISO 22341 CPTED publicada en el 2021. Asimismo, establece de forma muy clara la jerarquía de los espacios para el correcto diseño de las estrategias.



Fuente: ISO/DIS 22344

La ISO 22341 define a CPTED como: el proceso para analizar y evaluar los riesgos de delincuencia y seguridad, para orientar el desarrollo, el diseño urbano, la gestión del sitio, el uso del medio ambiente construido con el fin de prevenir y reducir la delincuencia, el miedo a la delincuencia, y para promover y mejorar la salud pública, la calidad de vida y la sostenibilidad.

NORMAS ISO PARA INTERVENCIONES SOCIO URBANAS

Para realizar intervenciones socio urbanas con las dos normas ISO CPTED (22341 y 22344) debemos de considerar su transversalidad y seguir los lineamientos que establecen las siguientes normas:

- **ISO 9001:** fija los requisitos mínimos para un Sistema de Gestión de Calidad (SGC) en cualquier organización.
- **ISO 18091: Sistema de Gestión de Calidad para el Gobierno Local.** Es el primer estándar internacional que ofrece innovación, eficiencia y calidad en la gestión pública de los servicios municipales basada en la ISO 9001 con el objetivo de trabajar en la mejora continua y en la optimización de las políticas públicas para buscar la satisfacción del cliente/ciudadano.
- **ISO 22301: Gestión de la Continuidad del Negocio.** Especifica los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, el mantenimiento y la mejora continua de un sistema de gestión documentado.
- **ISO18788: Sistema de Gestión de Operaciones de Seguridad Privada.** Proporciona un marco de referencia para la gestión empresarial y del riesgo para las organizaciones que realizan o contratan operaciones de seguridad
- **ISO 14001: Sistemas de gestión ambiental.** Proporcionar a las organizaciones un marco de referencia para proteger el medio ambiente y responder a las condiciones ambientales cambiantes, en equilibrio con las necesidades socioeconómicas. Esta norma especifica requisitos que permitan que una organización logre los resultados previstos que ha establecido para su sistema de gestión ambiental.
- **ISO 27001: Sistema de Gestión de Seguridad de la Información.** Establece la política y los ob-

jetivos de gestión de la seguridad de la información y a comprender cómo se pueden gestionar los aspectos importantes, aplicar los controles necesarios y establecer objetivos claros para mejorar la seguridad de la información.

- **ISO 39001: Sistema de Gestión de la Seguridad Vial.** Ayuda a las organizaciones a reducir, y en última instancia, eliminar la incidencia y riesgo de las muertes y heridas graves derivadas de los accidentes de tráfico.
- **ISO 28000: Sistemas de Gestión de la Seguridad para la Cadena de Suministro**. Detalla temas potenciales de seguridad en todas las fases del proceso de suministro, centrándose especialmente en las áreas de logística. También, se concentra en mitigar los efectos de los incidentes de seguridad.
- **ISO 37120: Ciudades y comunidades sostenibles —Indicadores de servicios urbanos y calidad de vida.** Esta norma incluye un total de 100 indicadores que cubren una amplia gama de aspectos relacionados con la sostenibilidad urbana. Estos indicadores están agrupados en 17 categorías, que abarcan desde la planificación urbana y el medio ambiente hasta la educación y la salud.
- **ISO 37122: Indicadores para ciudades inteligentes.** Especifica y establece definiciones y metodologías para un conjunto de indicadores para ciudades inteligentes.
- **ISO 37123: Indicadores para ciudades resilientes**. Define y establece definiciones y metodologías para un conjunto de indicadores sobre resiliencia en las ciudades.

Las organizaciones que realicen las intervenciones deben evaluar las amenazas, vulnerabilidades y el alcance de las medidas para reducirlas al diseñar medidas de seguridad destinadas a reducir el delito, el comportamiento antisocial y el miedo de las personas a ser víctimas de un delito en las áreas residenciales. Existen muchos factores de riesgo que pueden influir en la comisión o no de un delito. Se pueden considerar factores como la distribución del vecindario y el diseño del edificio junto con una referencia específica a las medidas de endurecimiento de los objetivos.

El allanamiento de morada es uno de los delitos más temidos por los ciudadanos. Esta Norma nos marca los lineamientos para dar tratamiento a este riesgo y se requiere de un nivel proporcionado de CPTED y medidas de seguridad. La mayoría de los delitos se cometen porque los perpetradores han detectado las vulnerabilidades que se convierten en oportunidades para ellos, como: el fácil acceso, escondites, ausencia de demarcación entre el espacio público y privado, mala iluminación y/o paisajismo favorable para el delincuente.

Asimismo, la norma 22344 establece que se debe comprender el riesgo potencial de delincuencia y seguridad en las viviendas a través del proceso de evaluación de riesgos (identificación, análisis y evaluación de riesgos) y contrarrestarlo con medidas de seguridad física específicas y combinadas con elementos de diseño reales o simbólicos.

En las zonas residenciales con viviendas individuales o bloques residenciales, el objetivo no es sólo proteger las propiedades contra robos, sino también evitar el acceso de visitantes no deseados, la apropiación ilegal de espacios, la degradación del medio ambiente y mitigar el miedo a la delincuencia.

La organización debe considerar el diseño del entorno construido, que también puede influir en las percepciones individuales del miedo a la delincuencia, que comúnmente superan el nivel de riesgo real y debe exigir utilizar los lineamientos de CPTED como un componente de la norma de diseño como parte de un proceso de mejora continua para la seguridad, la protección y la calidad de vida de las comunidades, los sitios y las construcciones de las instalaciones residenciales.

Las organizaciones que trabajen con las normas ISO CPTED, deben implementar un proceso que involucre a todas las partes interesadas relevantes siguiendo el marco de gestión de riesgos que se proporciona en la Norma ISO 31000 para integrar la gestión de riesgos en las actividades de CPTED para las instalaciones residenciales.

Cualquier actividad humana se realiza en alguna instalación y/o espacio que se encuentra ubicado en un territorio. Con las Normas ISO 22341 y 22344 de CPTED lo hacemos diagnóstico de un territorio, buscamos hacer "Un Mapa Real del Espacio" y vamos más allá del diseño y recuperación física del espacio; ya que al recuperar calles, zonas, colonias y barrios con murales; limpiar y pintar mobiliario urbano, así como instalaciones y calles, ayuda disminuir factores de riesgo, pero si no se atienden las causas de la violencia y el delito o si sólo participa un número reducido de ciudadanos y servidores públicos que no dan seguimiento a los programas, solamente será una solución temporal. Por ello, las intervenciones CPTED son integrales y cuenta con tres generaciones:

- **CPTED 1ª. Generación:** CPTED Físico que incluye los pirncipios de Control de Acceso Natural, Vigilancia Natural, Imagen/ Gestión/Mantenimiento; Refuerzo Territorial, Apoyo a la Actividad y Endurecimiento del Sitio.
- **CPTED 2ª. Generación:** CPTED Social incluye los principios de Cohesión Social, Cultura Comunitaria, Capacidad de Umbral y Conectividad Social.
- **CPTED 3ª. Generación:** que incluye principios de Salud Social y Sustentabilidad.

Nuestra misión es ir más allá de la obra física, haciendo alianza con la comunidad creando un compromiso para mantener los espacios en buen estado y que se atiendan las causas de las violencias. Con ello, gobiernos, iniciativa privada y la comunidad hará de cada calle un espacio seguro con convivencia armónica y no tendrán temor de salir a caminarlas, estableciendo obras de confianza social y una mejor cultura de seguridad. ■

Mercedes Escudero Carmona, presidenta de la International Crime Prevention Through Environmental Design (CPTED) Chapter México. *Más sobre la autora:*

TODO ACERCA DE LA SEGURIDAD EN LA INDUSTRIA ALIMENTARIA

Estrategia integral de seguridad para la industria de alimentos

Fotos: Freepik

MÉXICO **José Luis Sánchez Gutiérrez**

Nuevamente estimados lectores, muy agradecido por su acostumbrada preferencia; y en esta ocasión tocaremos el tema de la Seguridad en la Industria Alimentaria.

Todo profesional de seguridad en la industria alimentaria sabe que está en una constante evolución; que requiere de una visión estratégica, y una capacidad de adaptación para enfrentar los desafíos actuales. Si bien existen barreras y retos, las oportunidades de mejorar y asegurar la cadena de suministro alimentaria son amplias.

Las empresas que invierten en estas áreas, no sólo protegerán a sus consumidores, sino que también se posicionarán como líderes en un mercado competitivo y cada vez más consciente de la seguridad y la sostenibilidad; por lo cual, desde mi punto de vista, te comparto lo que considero son los siete conceptos clave en la Seguridad Alimentaria (desde el acostumbrado análisis —*novelty* "novedad", *feasibility* "factibilidad, *specificity* "especificidad", *impact* "impacto" y *workability* "aplicabilidad"—):

1) Trazabilidad en la Cadena de Suministro Alimentaria.
2) Gestión de Riesgos y Control de Puntos Críticos (HACCP).
3) Ciberseguridad en Sistemas Alimentarios.
4) Controles de Calidad y Seguridad en la Cadena de Producción.
5) Sostenibilidad y Seguridad Alimentaria.
6) Cumplimiento Normativo Global.
7) Innovación en el Envasado de Alimentos.

1.- TRAZABILIDAD EN LA CADENA DE SUMINISTRO ALIMENTARIA

- ***Novelty:*** La trazabilidad es un concepto bien establecido, pero siempre debemos tomar en cuenta la implementación de tecnologías avanzadas como el *blockchain* para mejorar la transparencia y seguridad de forma innovadora.
- ***Feasibility*:** La tecnología *blockchain* es factible para grandes empresas, aunque su adopción masiva, aún enfrenta barreras tecnológicas y económicas en diferentes países.
- ***Specificity*:** Aplica específicamente a la capacidad de rastrear un producto alimentario desde su origen hasta el consumidor final (su total trazabilidad).
- ***Impact*:** Tiene un impacto significativo al reducir el riesgo de contaminación, fraude alimentario y garantizar el cumplimiento normativo.
- ***Workability*:** Requiere una integración sólida de sistemas y una colaboración transversal en todas las etapas en la cadena de suministro.

2.- GESTIÓN DE RIESGOS Y CONTROL DE PUNTOS CRÍTICOS HACCP (*HAZARD ANALYSIS AND CRITICAL CONTROL POINTS*)

- ***Novelty:*** El enfoque HACCP no es nuevo, pero su adaptación a nuevas amenazas emergentes, como lo son patógenos resistentes y la biotecnología, es central para poder administrar y gestionar los riesgos en la inocuidad alimentaria.

- ***Feasibility:*** Muy factible, ya que es un estándar globalmente reconocido y adoptado en la industria Alimentaria.
- ***Specificity:*** Se centra en identificar y controlar los puntos críticos en el proceso de producción alimentaria en cada empresa.
- ***Impact:*** Es primordial para prevenir la contaminación y garantizar la seguridad del producto final que llega a nuestros consumidores.
- ***Workability:*** Exige capacitación continua y una vigilancia constante para ser efectivo y aplicable.

3.- CIBERSEGURIDAD EN SISTEMAS ALIMENTARIOS

- ***Novelty:*** La ciberseguridad en sistemas de gestión de alimentos es un campo en expansión permanente, impulsado por la constante digitalización de la industria.
- ***Feasibility:*** Desplegar ciberseguridad es factible, aunque requiere inversiones significativas en infraestructuras y formación.
- ***Specificity:*** Específico para proteger datos sensibles, sistemas de control industrial y la integridad de las operaciones.
- ***Impact:*** Su impacto es crítico; un ciberataque podría paralizar la cadena de suministro y comprometer la seguridad alimentaria en la empresa.
- ***Workability:*** Funciona bien si se combina con estrategias de seguridad física y protocolos de respuesta inmediata a incidentes.

4.- CONTROLES DE CALIDAD Y SEGURIDAD EN LA CADENA DE PRODUCCIÓN

- ***Novelty:*** Aunque los controles de calidad son tradicionales, la incorporación de inteligencia artificial (IA) para mejorar la detección de anomalías es una tendencia emergente, la cual va mejorando de manera sustancial en el día a día.
- ***Feasibility:*** La inteligencia artificial (IA) es cada vez más accesible en todos los campos, lo que hace que su implementación sea factible para mejorar los controles de calidad.
- ***Specificity:*** Convenientemente útil para la monitorización en tiempo real de procesos productivos y la identificación temprana de problemas.
- ***Impact:*** Aumenta significativamente la seguridad y reduce el desperdicio de productos (hace más rentable el negocio desde la producción).
- ***Workability:*** Altamente funcional, si se integra con sistemas existentes y se entrena y certifica al personal adecuadamente en todo el proceso.

5.- SOSTENIBILIDAD Y SEGURIDAD ALIMENTARIA

- ***Novelty:*** La integración de la sostenibilidad con la seguridad alimentaria es una tendencia novedosa que responde a las exigencias de los consumidores y reguladores globales.
- ***Feasibility:*** Es factible mediante la adopción de prácticas agrícolas sostenibles y la reducción del uso de químicos (que son tendencias en las diferentes latitudes).

- ***Specificity:*** Específico para la producción y distribución de alimentos que minimicen el impacto ambiental sin comprometer la seguridad.
- ***Impact:*** Impacta positivamente en la salud pública y en la real preservación del medio ambiente.
- ***Workability:*** Funciona cuando hay un compromiso firme, que lleva un "cascadeo" desde la alta dirección y una cadena de suministro comprometida.

6.- CUMPLIMIENTO NORMATIVO GLOBAL

- ***Novelty:*** La necesidad de cumplir con normativas globales es un desafío constante, pero la armonización y las herramientas de *compliance* están en desarrollo en todo el mundo.
- ***Feasibility:*** Factible para empresas con recursos, aunque desafiante para pequeñas y medianas empresas.
- ***Specificity:*** Específico para asegurar que los productos cumplan con regulaciones locales e internacionales.
- ***Impact:*** El incumplimiento puede resultar en sanciones severas y pérdida de mercado.
- ***Workability:*** Requiere sistemas de gestión de calidad robustos y una vigilancia y cumplimiento permanente.

7.- INNOVACIÓN EN EL ENVASADO DE ALIMENTOS

- ***Novelty:*** La innovación en el envasado, como el uso de materiales biodegradables y envases inteligentes, es una tendencia emergente.
- ***Feasibility:*** Es factible, aunque puede implicar al iniciar con elevados costos y ajustes en la producción.
- ***Specificity:*** Específico para mejorar la conservación, seguridad y la comunicación de información al consumidor.
- ***Impact:*** Reduce el desperdicio, mejora la seguridad y responde a las preocupaciones medioambientales.
- ***Workability:*** Altamente efectivo cuando se adopta de manera coherente con las políticas de sostenibilidad.

Otra manera de observar la Seguridad en la industria alimentaria es cuando la analizamos e identificamos cuáles son los principales pros y contras que la envuelven:

PROS EN LA SEGURIDAD EN LA INDUSTRIA ALIMENTARIA:

- **Protección de la salud pública:** La seguridad alimentaria previene enfermedades transmitidas por alimentos y asegura que los productos consumidos sean totalmente seguros.
- **Cumplimiento normativo:** Ayuda a cumplir con las leyes y regulaciones, evitando cualquier tipo de sanciones legales.
- **Confianza del consumidor:** Mantiene y fortalece la confianza de los consumidores en los productos alimentarios que producimos.
- **Innovación tecnológica:** La adopción de nuevas tecnologías mejora la eficiencia y la seguridad en la gestión, producción y distribución de los alimentos.

CONTRAS EN LA SEGURIDAD EN LA INDUSTRIA ALIMENTARIA:

- **Costos elevados:** Las inversiones en seguridad alimentaria pueden ser significativas, especialmente para la implementación de nuevas tecnologías y la capacitación actualizada al personal involucrado.
- **Complejidad regulatoria:** Cumplir con las normativas en múltiples jurisdicciones es complicado y en ocasiones muy costoso para las pequeñas empresas.
- **Resistencia al cambio:** La adopción de nuevas prácticas y tecnologías puede encontrar resistencia dentro de la organización.
- **Riesgos de ciberseguridad:** La creciente digitalización aumenta la vulnerabilidad a ciberataques que podrían comprometer la seguridad alimentaria en cualquiera de sus fases.

LO QUE CONSIDERO SON LAS PRINCIPALES ÁREAS DE OPORTUNIDAD QUE NOS ENCONTRAMOS EN EL FUTURO A CORTO PLAZO SON:

- **Digitalización y Automatización:** La expansión de la automatización en los procesos productivos y de distribución puede aumentar la eficiencia y seguridad. La integración del IoT (Internet de la Cosas), IA y *machine learning*, nos permitirá un monitoreo más preciso y una respuesta rápida a cualquier tipo incidentes que se llegarán a presentar.
- **Sistemas de Alerta Temprana:** Desarrollar sistemas de alerta temprana más sofisticados, basados en el análisis de grandes volúmenes de datos (incluyendo poderosos motores analíticos), podría anticipar y mitigar riesgos antes de que se conviertan en problemas mayores.
- **Nuevas Tecnologías de Envasado:** La investigación y desarrollo en materiales inteligentes y biodegradables pueden revolucionar la manera en que protegemos y conservamos los alimentos, reduciendo al mismo tiempo el impacto ambiental y con ello lograr una producción menor en cantidad de basura.
- **Fortalecimiento de la Ciberseguridad:** Con la creciente digitalización de las cadenas de suministro, se requiere un enfoque más robusto y proactivo en ciberseguridad para proteger los sistemas críticos de la industria alimentaria.
- **Educación y Capacitación Continua:** Invertir en la formación continua del personal en las nuevas tecnologías, normativas y mejores prácticas de seguridad, será "vital" para mantener la seguridad alimentaria a la vanguardia.

Nuevamente muchísimas gracias por permitirme compartir contigo este artículo, esperando sea de tu interés y nos leemos en la siguiente edición. ■

José Luis Sánchez Gutiérrez, director de Seguridad Patrimonial en la industria Cárnica. *Más sobre el autor:*

COLEMAN

Jetlife

EL PODER DE VOLAR

RENTA DE AVIONES PRIVADOS Y HELICÓPTEROS

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

Powered by:
SEGURIDAD EN AMERICA

IS-BAO

REGISTERED OPERATOR
verify with wyvern

AEROPUERTO INTERNACIONAL DE TOLUCA

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

Tel. 55.7672.4992

SEGURIDAD GLOBAL: CULTURA Y PROTECCIÓN

Foto:-Freepik

Debemos ser conscientes de que en el mundo actual se están produciendo cambios profundos, no eventuales, y que es necesario contribuir de una forma más eficaz y realista a la mejora de la seguridad global

ESPAÑA **Manuel Sánchez Gómez-Merelo**

Una vez más, hemos de recordar que la inseguridad y la violencia están globalizadas y reflejan una organización social también en crisis, que involucra a individuos y a instituciones, donde los ciudadanos han de buscar los referentes para hallar las soluciones a los problemas más comunes, porque la seguridad no está globalizada.

Así, hemos de pensar en global como instituciones y ciudadanos del mundo, pero, hemos de actuar en local, en nuestra dimensión ciudadana. La fragilidad y las vulnerabilidades se ponen cada vez más de manifiesto y potencialmente con más violencia.

NUEVAS EXIGENCIAS Y RETOS PARA LA SEGURIDAD

Vivimos un panorama globalizado de nuevas amenazas, mayores riesgos en las actividades sociales, industriales y comerciales que ratifican nuevas demandas y exigencias de la sociedad con nuevos retos para la protección de sus actividades con plenas garantías para su seguridad.

Continuas señales de alarma, las más que percepciones de inseguridad, nos llegan por todos los frentes, provocando una sensación generalizada de múltiples inquietudes, problemas globales e inseguridades.

Así, si hablamos de Seguridad hemos de tener en cuenta esa clara existencia de una "seguridad objetiva" y, sobre todo, de la otra, la "seguridad subjetiva", que puede generar alarma social.

CULTURA INTEGRAL DE SEGURIDAD NACIONAL

Una Seguridad Objetiva, que es la que puede medirse cualitativa y cuantitativamente y es resultante de las acciones proactivas y reactivas programadas y realizadas por el Gobierno y sus Fuerzas y Cuerpos de Seguridad.

Y una Seguridad Subjetiva, que es aquella que realmente es percibida por el ciudadano en su propia vivencia y estado de ánimo y es más importante que los resultados de las frías estadísticas y estudios comparativos.

La idea de Seguridad Nacional está relacionada con la forma en la que vivimos a nivel geopolítico y, en la actualidad, el enemigo ha cambiado y los retos se han incrementado.

Así, disponemos de un Plan Integral de Cultura de Seguridad Nacional, un espacio de colaboración público-privada para desarrollar actividades e iniciativas dirigidas a incrementar la conciencia sobre la trascendencia de la seguridad nacional, así como la corresponsabilidad de todos en su salvaguarda.

Este Plan Integral de Cultura de Seguridad Nacional ha sido elaborado y aprobado en España por Acuerdo del Consejo de Ministros de 25 de mayo de 2021 con la participación de los veintidós Ministerios de la XIV Legislatura, la Secretaría de Estado de Comunicación y el Centro Nacional de Inteligencia.

Plan Integral de Cultura de Seguridad Nacional que ha de servir de catalizador para la implantación progresiva de una cultura de Seguridad Nacional inclusiva, participativa y colaborativa, todo ello con el fin de reforzar el Sistema de Seguridad Nacional, mejorar la coordinación y eficacia de la acción del Estado y la participación de la sociedad.

Los ámbitos de actuación y líneas de acción para el desarrollo del Plan, establece cuatro ámbitos de actuación:

- Formación, Comunicación pública y divulgación, Relevancia en el exterior y Participación, en los que se fomentará la colaboración y cooperación entre las comunidades de referencia.
- Formación para lograr una percepción correcta y fundamentada sobre la Seguridad Nacional, su trascendencia para garantizar la vida cotidiana y los esfuerzos que requiere su salvaguarda.
- Divulgación y comunicación pública para fortalecer una opinión pública consciente del carácter imprescindible e irrenunciable de nuestra seguridad a través de los medios y las plataformas de comunicación.
- Relevancia en el exterior, para mejorar la imagen de España como país íntegro, seguro y comprometido con el mantenimiento de la paz y la estabilidad internacionales.
- Participación, de la ciudadanía y de las organizaciones de la sociedad civil en las actividades de fomento de la cultura de Seguridad Nacional.

Igualmente, la Seguridad Nacional y las Infraestructuras Críticas y Estratégicas, pueden considerarse un problema global que se ha de abordar a nivel institucional, siguiendo políticas nacionales y un enfoque internacional.

Por las múltiples amenazas y los nuevos retos y desafíos para la Seguridad, el Esquema Nacional de Seguridad (ENS), en su capítulo de "Objetivos generales y líneas de acción de la Seguridad Nacional", identifica

cinco objetivos generales: "Avanzar en un modelo integral de gestión del riesgo y de crisis, promover una cultura de Seguridad Nacional, favorecer el buen uso de los espacios comunes globales, impulsar la dimensión de seguridad en el desarrollo tecnológico y fortalecer la proyección internacional de España".

SEGURIDAD GLOBAL, PLAN INTEGRAL E INTEGRADO

El orden global y el paradigma socioeconómico liberal se encuentran en un periodo de cambio, sin que aún se haya definido claramente el nuevo panorama del sistema internacional. Los principales vectores de transformación son: el contexto geopolítico, el entorno socioeconómico, la transformación digital y la transición ecológica.

El planteamiento de la Seguridad Global algo más que un concepto. En este mundo global de retos colectivos y futuro incierto, nos ayudará a entender las nuevas dinámicas sociales, económicas, energéticas y tecnológicas el desarrollo de ese amplio concepto que es la seguridad global que va a definir el presente y futuro del mundo.

Debemos ser conscientes de que en el mundo actual se están produciendo cambios profundos, no eventuales, y que es necesario contribuir de una forma más eficaz y realista a la mejora de la seguridad global. Desde esta perspectiva de la seguridad hemos de ayudar a instituciones y organizaciones a rediseñar nuevas estrategias en el mundo globalizado.

Para ello, hemos de estudiar las grandes tendencias que vivimos, definir los nuevos riesgos económicos, políticos y sociales que nos acechan y esquematizar un escenario de futuro en el que un modelo de gobernanza y seguridad global sea capaz de responder a los nuevos retos colectivos que nos amenazan.

Uno de los proyectos estrella de estos últimos años es el análisis de riesgos, con un matiz importante, que sea global-convergente-integral. Un análisis que evalúe todos los riesgos que puedan afectar a los procesos críticos de nuestras organizaciones.

Debemos invertir en gestionar el riesgo para prevenirlo y garantizar en todo lo posible superar las crisis siendo especialmente resilientes.

Una Seguridad Global, base para el nuevo estudio y análisis integral de los riesgos y las amenazas globales existentes hoy, como el cibercrimen, la inmigración, los cambios climáticos, el terrorismo, el crimen organizado trasnacional, la desinformación, los servicios de inteligencia, etc.

Las amenazas tienen muchos tamaños y formas, como la inestabilidad geopolítica, la delincuencia, las catástrofes naturales y, más recientemente, las pandemias mundiales.

Hemos de establecer un Plan de Seguridad Integral e Integrado basado en objetivos e, igualmente, implementar una gestión integral de los riesgos y las seguridades, con el esquema básico siguiente: Análisis de Riesgos, Amenazas y Vulnerabilidades; Implementación de los Medios de Seguridad Pasiva, Activa y de Ciberseguridad; Organización de las Medidas y los Medios Humanos de Seguridad; Planes Estratégicos y Operativos y Plan de Formación continua.

PLANES DE SEGURIDAD. PREVENCIÓN + PROTECCIÓN

Para una adecuada política de protección se han de establecer los diferentes Planes de Seguridad teniendo en cuenta los siguientes aspectos fundamentales, como:

- Política de Seguridad de las Organizaciones y la protección de los servicios esenciales.
- La Gestión Estratégica de la seguridad alineada con la política de riesgos y amenazas.
- La Estructura Organizativa y de responsabilidades en materia de seguridad integral e integrada.
- La Responsabilidad, compromiso y participación de todo el personal interno y externo de la organización.
- La Formación Especializada y concienciación de los recursos humanos adscritos a la prevención y protección.
- El Desarrollo y Gestión de capacidades para la prevención, detección, protección, respuesta, resiliencia y recuperación.
- La Colaboración con las Fuerzas y Cuerpos de Seguridad y establecimiento de planes de contingencia.
- El Cumplimiento Normativo, aplicación de buenas prácticas y la mejora continua de los procesos de seguridad implementados.

Sólo una seguridad integral e integrada y una cultura de seguridad, garantiza una protección eficiente frente a amenazas globales y supone una aplicación globalizada de la seguridad, en la que se tienen en cuenta los aspectos humanos, legales, sociales, económicos y técnicos de todos los riesgos, amenazas y vulnerabilidades que pueden afectar a las personas y bienes integrantes en la actividad de una organización.

Finalmente, hay que tener en cuenta que el concepto de Seguridad Global es especialmente importante en el ámbito de las Infraestructuras Críticas y Estratégicas.

RECOMENDACIONES

Hoy hay que dar una respuesta con una Seguridad Global, Única con mayúscula, integral e integrada, pública y privada.

Fomentar una Cultura de Seguridad, identificando las oportunidades y debilidades de los diferentes actores que abarcan el espectro: global, nacional, local de seguridad pública y privada.

La actual sociedad y sus inseguridades requiere de un punto de vista nuevo y diferenciador, ha de ser creativo, intuitivo e inclusivo y servir para romper nuestros hábitos, modelos mentales y paradigmas ya obsoletos, todo hacia un pensamiento cuántico.

La necesidad de cambiar de paradigma es real e imprescindible para acometer nuevos retos y exigencias en la sociedad a través de un pensamiento cuántico y holístico que unifique, contemple y relacione todos los datos e integre los procesos del pensamiento en serie y asociativo.

Ahora, más que nunca, es tan importante la imaginación como el conocimiento y la inteligencia.

Con todo ello, y como recomendaciones finales, debemos potenciar una nueva Cultura de Seguridad con visión común sobre la base de amenazas complejas e incrementar los recursos de análisis para desarrollar un nuevo esquema de Seguridad Global, integral e integrada, pública y privada. ■

Manuel Sánchez Gómez-Merelo,
consultor internacional de Seguridad.
Más sobre el autor:

JOSÉ LUIS ALVARADO *(BUSINESSMAN)*: DE LA LOGÍSTICA A LA SEGURIDAD

Con más de dos décadas de trayectoria en el sector, el especialista cierra el año como presidente de ASIS Capítulo México, para emprender una nueva aventura

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La industria de la seguridad se ha enriquecido con profesionales de distintas ramas académicas, uno de ellos, Ingeniero Industrial por parte de UPIICSA (IPN), es José Luis Alvarado, quien este año, representó a una de las asociaciones internacionales más importantes del sector, liderando al tercer capítulo más grande a nivel mundial, y el cual obtuvo la sede para el "Congreso ASIS Latinoamérica 2025" durante la realización de "The Global Security Exchange" (GSX), en Orlando, Estados Unidos, realizado en septiembre de este año, estamos hablando de ASIS Capítulo México, con más de 500 afiliados.

José Luis, con su característica sonrisa, su amabilidad y *expertise* en la Logística, proviene de una familia tradicional conformada por un maestro panificador (panadero) y una clásica ama de casa de los años 70, de quienes aprendió valores y recibió la atención y amor que todo hijo necesita. Nació en la zona centro de la Ciudad de México, y cuenta, además, con una Maestría en Administración y Dirección de Empresas (MBA), por la Unidad de Posgrado del IPN (Instituto Politécnico Nacional), y dos especialidades, una en Estrategia Comercial por parte del ITAM (Instituto Tecnológico Autónomo de México), y otra en Dirección de Servicios por el IPADE (Instituto Panamericano de Alta Dirección de Empresa).

Este 2024 también celebró los 30 años del Capítulo que encabeza, durante la ceremonia del aniversario, José Luis se mostró agradecido y orgulloso de pertenecer a la seguridad y de haber realizado una gran trayectoria en donde, como varios, nunca se había imaginado que terminaría.

DE LA LOGÍSTICA A LA SEGURIDAD

¿Cómo es que un ingeniero industrial se convierte en el socio director comercial de una reconocida empresa de seguridad privada?

"Yo era un ejecutivo de alto nivel en el ramo de la logística, siendo mi alma máter Colgate Palmolive; en el año 2000 formé parte de la dirección de Transporte en Dimalsa Logistics, como me reportaban 400 líneas de transporte y 20 empresas de seguridad privada, recibí una gran oferta de una empresa especializada en seguridad logística, así que no lo dudé y me integré a este gran gremio de la seguridad en el año 2001, considero que fue y sigue siendo, mi mejor decisión", externó José Luis (JL).

Y aunque el especialista ya tenía experiencia y conocimientos dada su relación con las empresas de seguridad, enfrentó algunos retos en la transición de áreas. Por ejemplo, el cambio cultural, "pasé de un mundo muy snob a la industria de la seguridad donde no existe área de confort, mi mayor reto fue adaptarme a un mundo diferente con desafíos diferentes cada día, y lejos de mi área donde me sentía estable y confiado".

A lo largo de estas dos décadas, JL ha conocido a diferentes representantes del sector, ha coincidido con ellos en diferentes foros de networking *roadshows*, y congresos; ha compartido paneles de opinión sobre los temas más relevantes que aquejan a esta industria y Encuentros donde se buscan las soluciones a estos. Pero también ha conocido personajes de la seguridad de los cuales ha aprendido más, no sólo en materia de seguridad, sino también como persona.

"Dentro de mis 24 años en Seguridad he tenido diferentes referencias y grandes ejemplos a seguir, sin embargo, una persona que ha sido un ejemplo de vida personal y profesional, es el Cap. Salvador López Contreras, quien ha sido una persona ejemplar y disciplinada a la cual le aprendo infinidad de cosas, resaltando la vocación de ayudar a los demás, la disciplina financiera y sobre todo los valores universales".

Más allá de la seguridad

Pasatiempo favorito:	Jugar billar.
Grupo de música o cantante favorito:	Patrick Cowley (High Energy).
Programa o serie de TV favorito:	Banshee.
Película favorita:	El Padrino 1 y 2.
Libro favorito:	*100 años de soledad.*
Destino favorito de vacaciones:	Buenos Aires, Argentina.
Bebida favorita:	Brandy Cardenal Mendoza.
Comida favorita:	Italiana.
Actor favorito:	Kevin Spacey y Al Pacino.
Personaje favorito:	Ultra Seven y Ultraman.

Asociación de palabras

México:	Esperanza.
Seguridad:	Mi pasión.
Presidenta:	Buena expectativa.
Gobierno:	Circo Político.
Policía:	Justicia.
Familia:	Mi razón de ser y existir.
Amigos:	Alimento de mi alma.
Galeam:	Mi gran futuro






Del sector se aprende mucho, y la mayoría de los que hemos tenido el honor de entrevistar en esta sección, coinciden en que no es simplemente un trabajo, es una gran responsabilidad que los apasiona. "Mi mayor aprendizaje en esta industria, ha sido la humildad y la capacidad de reinventarme, así como el manejo de las Relaciones Públicas y la política dentro de un esquema de desarrollo de ventas de alta gama y continuidad de negocio con empresas nacionales y globales", puntualizó.

ASIS CAPÍTULO MÉXICO

Cada mes, el primer o segundo martes, ASIS Capítulo México lleva a cabo sus Reuniones Mensuales, en las que más de 150 afiliados e invitados asisten para conocer los avances de dicho capítulo, pero también para aprender y conocer la situación de seguridad en México, principalmente, y Latinoamérica; esto gracias a las ponencias que cada presidente y su Consejo Directivo eligen para sus miembros. Cada mes, José Luis presenta los avances de su presidencia, y durante su gestión ha tenido logros que involucran a todos los integrantes del capítulo.




"Ser presidente de ASIS México ha sido un parteaguas en mi vida, me ha marcado para siempre, ya que me ha demandado desarrollar mis soft y hard skills, pero, sobre todo, la necesidad de aplicar mis habilidades políticas y de trabajo con equipos de alto nivel como son mi staff y mi consejo directivo. Sin lugar a dudas, ha sido de las mejores experiencias en mi vida, me siento muy afortunado".

GALEAM SECURITY SERVICES

Actualmente, José Luis es socio director comercial en Galeam Security Services, empresa encabezada por Francisco de Lago, y como director de Consultoría, Gerardo de Lago, vicepresidente de ASIS Capítulo México, y quien, al igual que José Luis, son piezas claves en la profesionalización del sector. "La seguridad privada en el país es un estilo de vida empresarial, nada se puede hacer sin seguridad, ya que el core business de las empresas no podría ser, ni existir, sin un ambiente seguro y de calidad; la seguridad privada en el país participa activamente en el Producto Interno Bruto y es artífice de la economía", comentó JL.

José Luis nos compartió que se integró a Galeam este año, porque llegó su tiempo de ser empresario, y le agradece "infinitamente" a Gerardo de Lago Acosta, por la oportunidad de ser socio director en su "brillante grupo empresarial", y en donde se encuentran en constante innovación para mejorar los procesos, protocolos, y capacitaciones de los elementos de seguridad, pues son una empresa donde el principal valor activo, son las personas.

A lo largo de estas dos décadas, JL ha participado en diferentes foros de *networking, roadshows,* y congresos; compartiendo paneles de opinión sobre los temas más relevantes que aquejan a esta industria y Encuentros donde se buscan las soluciones a estos. También ha conocido personajes de la seguridad de los cuales ha aprendido, no sólo en materia de seguridad, sino también como persona.

"Dentro de mis 24 años en Seguridad he tenido diferentes referencias y grandes ejemplos a seguir, entre ellos, y a quienes agradezco todo su apoyo y mentoría, están Gabriel Bernal y Rubén Fajardo; y en especial a una persona que ha sido un ejemplo de vida personal y profesional, es el Cap. Salvador López Contreras, quien ha sido una persona ejemplar y disciplinada a la cual le aprendo infinidad de cosas, resaltando la vocación de ayudar a los demás, la disciplina financiera y sobre todo los valores universales". ■

Fotos: Cortesía José Luis Alvarado

SEGURIDAD EN LA VÍA PÚBLICA (PARTE II)

Casi seis de cada 10 habitantes de más de 18 años consideran inseguro vivir en su ciudad, de acuerdo con la Encuesta Nacional de Seguridad Pública Urbana (ENSU) del segundo trimestre del 2024, que publicó el Instituto Nacional de Estadística y Geografía (Inegi). La ciudad mexicana con mayor percepción de inseguridad fue Fresnillo (Zacatecas), donde 94.7% de sus habitantes reportaron este sentimiento en medio de las masacres que ahí comete el crimen organizado. Le siguen Naucalpan (89.2%), Uruapan (86.8%), Irapuato (84.8%), Tapachula (84.7%) y Zacatecas (84.7%).

Las y los ciudadanos que reportaron haber visto delitos cerca de su vivienda, se relacionaron con consumo de alcohol en las calles (60.3%), robos o asaltos (47.8%), vandalismo (39.9%), venta o consumo de drogas (39.5%), disparos de armas (36.4%) y bandas violentas o pandillerismo (15.1%). De ahí la importancia de tener en cuenta los siguientes tips extraídos del Blog "Manual de Seguridad" de David Lee, para lograr una colonia segura.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Establecimiento de un sistema de comunicación e identificación vecinal.** Intercambiando teléfonos, correos electrónicos y haciendo un registro de los vehículos de cada familia, colocando en ellos distintivos que los acrediten como miembros de la comunidad.
2) **Elaboración de un análisis de riesgos.** Es importante detectar los elementos de vulnerabilidad y riesgo en la comunidad y en cada uno de los hogares de las distintas familias.
3) **Instalación de un método de alerta vecinal.** De acuerdo con las características de la comunidad y en función al presupuesto, se debe determinar la forma en la que se debe alertar a la comunidad, respecto de personas o situaciones sospechosas en el entorno, o bien a la policía ante casos de franca emergencia.
4) **Elaboración de planes de seguridad.** Es itinerante plantear y dar a conocer las estrategias de respuesta y actuación ante una persona sospechosa o un suceso que afecta la seguridad de los colonos.
5) **Establecimiento y seguimiento del programa de seguridad vecinal.** Es importante difundir, entre los vecinos, información que los estimule a adoptar hábitos que permitan reforzar las acciones de prevención y seguridad que se están implementando. ■


Foto: Freepik

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

¡Afíliate AHORA!

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

30 AÑOS PROFESIONALIZANDO

Conoce y disfruta de nuestros BENEFICIOS

- 12 REUNIONES MENSUALES PRESENCIALES SIN COSTO, CON CONFERENCISTAS DE PRIMER NIVEL QUE SUMAN A TU PROCESO DE PROFESIONALIZACIÓN.
- WEBINARS SIN COSTO.
- INSTRUCTORES CERTIFICADOS.
- CURSOS ESPECIALIZADOS EN LOS DIVERSOS CAMPOS DE LA SEGURIDAD, LOS CUALES OTORGAN CPE'S PARA TU RECERTIFICACIÓN.
- ESTAREMOS PRESENTES COMO CAPÍTULO EN LOS MEJORES EVENTOS DE SEGURIDAD DE MÉXICO.
- CONVENIOS DE DESCUENTO PARA DIVERSOS PRODUCTOS Y SERVICIOS.
- BOLSA DE TRABAJO.
- COMUNIDADES TEMÁTICAS.
- NEWSLETTER SEMANAL.
- CHAT PRIVADO DE SOCIOS ACTIVOS.
- ACCESO A LAS GUÍAS & ESTÁNDARES DE ASIS INTERNACIONAL.
- ACCESO A LA BASE DE DATOS DE MÁS DE 34 MIL PROFESIONALES DE SEGURIDAD ALREDEDOR DEL MUNDO.
- COSTO PREFERENCIAL EN CURSOS Y EVENTOS.
- ACCESO A LAS GRABACIONES DE LAS WEBINARS.

Linktree

MAYOR INFORMACIÓN

55 1321 1289

socios@asis.org.mx

ASIS MÉXICO 217
$5,650 MXN

ASIS INTERNACIONAL
$125 USD

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	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en Banco Barnorte, SEA MEDIA GROUP, S. de R. L. de C. V. Cuenta: 1095 5437 37

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe: 0721 8001 0955 4373 78

_____
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 2024

ALLIED UNIVERSAL
SECURITY SERVICES
There for you.

ENHANCED PROTECTION SERVICES

Descubra soluciones de seguridad incomparables que fusionan nuestra vasta experiencia con la tecnología de vanguardia. Proteja sus activos de manera eficiente y garantice la seguridad integral de sus instalaciones mediante nuestros servicios personalizados y adaptados a sus necesidades.

- Respuesta ante catástrofes y emergencias
- Seguridad K9
- Protección ejecutiva
- Inteligencia como servicio
- Investigaciones
- Consultoría de riesgos y vulnerabilidades
- GSOC como servicio
- Alarmas

SEGURIDAD PARA EVENTOS

Ofrecemos seguridad integral para eventos, gestión eficiente de multitudes y servicios para invitados, adaptados a las características del evento y del lugar. Contamos con diferentes coberturas para todo tipo de eventos, desde deportes y entretenimiento, hasta convenciones, eventos corporativos y de alto perfil.

- Gestión de multitudes
- Personal de seguridad para eventos
- Servicios especiales para eventos
- Centro de mando unificado para eventos
- Videovigilancia temporal
- Eventos corporativos

Contáctanos **https://ausecurity.mx/es** **(+52) 55 5337 0444**

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.

"Juntos construimos el mejor lugar para crecer"

Great Place To Work.®

Certificada 2024

México ™

Guardias, guardias armados, custodias,
custodias blindadas y custodias armadas.

Cobertura a nivel nacional.

www.sepsisa.com.mx comercial@sepsisa.com.mx 55 5351 0402