SEGURIDAD®
EN AMÉRICA

Año 24 / No.141
Noviembre - Diciembre

www.seguridadenamerica.com.mx

Especial:
Seguridad en oficinas corporativas
Seguridad en la industria manufacturera

Reportaje: Seguridad en la industria energética

@MultiprosegOficial

@MULTIPROSEGOFICIAL

MULTIPROSEG OFICIAL

CONTAMOS CON COBERTURA EN TODOS LOS ESTADOS DE LA REPÚBLICA MEXICANA, CON LA ESTRUCTURA DE OFICINAS REGIONALES Y UN CORPORATIVO.

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

ALGUNOS DE NUESTROS CLIENTES

AUDI, TELCEL,BRASKEM IDESA, INNOPHOS, CEMEX, GRUPO COLLADO, CRYOINFRA, LACTALIS

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

CDMX
CIUDAD DE MÉXICO

CNS
COMISIÓN NACIONAL DE SEGURIDAD

redconocer
de prestadores de servicios
Entidad de Certificación y Evaluación

ISO

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE

ema
entidad mexicana de acreditación, a.c.

ANERPV
Asociación Nacional de Empresas de Rastreo y Protección Vehicular

COPARMEX

REPSE
Registro de Prestadoras de Servicios Especializados u Obras Especializadas

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

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

(55)7959 9598
(55)3455 4375

INFO@MULTIPROSEG.COM.MX

WWW.MULTIPROSEG.COM.MX

SEGURIDAD EN AMÉRICA

Año 24 / No. 141 / Noviembre - Diciembre / 2023

Portada:
SISSA DIGITAL

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

Seguridad en América es una publicación editada bimestralmente por Editorial Seguridad en América S.A. de C.V., marca protegida por el Ins-tituto de Derechos de Autor como consta en la Reserva de Derechos al Uso exclusivo del título número: 04-2005-040516315700- 102, así como en el Certificado de Licitud de Contenido número: 7833 y en el Certificado de Licitud de Título número: 11212 de la Secretaría de Gobernación. Editor responsable: Samuel Ortiz Coleman. Esta revista considera sus fuentes como confiables y verifica los datos que aparecen en su contenido en la medida de lo posible; sin embargo, puede haber errores o variantes en la exactitud de los mismos, por lo que los lectores utilizan esta información bajo su propia responsabilidad. Los colaboradores son responsables de sus ideas y opiniones expresadas, las cuales no reflejan necesariamente la posición oficial de esta casa editorial. Los espacios publicitarios constantes en esta revista son responsabilidad única y exclusiva de los anunciantes que oferten sus servicios o productos, razón por la cual, los editores, casa editorial, empleados, colaboradores o asesores de esta publicación periódica no asumen responsabilidad alguna al respecto. Porte pagado y autorizado por SEPOMEX con número de registro No. PP 15-5043 como publicación periódica. La presentación y disposición de **Seguridad en América** son propiedad autoral de Samuel Ortiz Coleman. Se imprimió en los talleres de Esténtor Impresos, Calle Virgen de Chiquinquira 706, Col. La Virgen, Ixtapaluca, Estado de México, C.P. 56530.

Apoyando a:

ASIS INTERNATIONAL · ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD · AMESP · Circulo Logistico · ANERPV

AppController

SISTEMA DE GESTIÓN DE SERVICIOS OPERATIVOS

Obtén información confiable, rápida y precisa sobre las operaciones realizadas en tu organización para el monitoreo y administración de tus activos.

DESARROLLO POR

SISSA DIGITAL

¿Qué puede hacer **AppController** en tu organización?

- Agiliza labores operativas y administrativas.
- Controla entradas, salidas y localización de artículos.
- Aumenta la seguridad de la información almacenada.
- Optimiza tiempos y mucho más.

Contáctanos y maximiza la gestión de todos los activos que ingresan, egresan y se utilizan en tu organización.

EDITORIAL

En el tercer Diálogo de Alto Nivel de Seguridad México-Estados Unidos, realizado el pasado 05 de octubre, se dieron a conocer los posicionamientos de cada integrante de las dos comitivas ante las problemáticas de narcotráfico, tráfico de armas y de personas entre ambos países. Y en el que resultaron los siguientes acuerdos: 1. Se creará un protocolo de seguimiento internacional de precursores de drogas, 2. Estados Unidos entregará a México un reporte mensual de flujo de armas y 3. La coordinación para el desmantelamiento de redes de tráfico de personas.

Al inicio de la reunión, la secretaria de Relaciones Exteriores (SRE), Alicia Bárcenas, afirmó que México mantiene su "firme compromiso" para combatir el tráfico de drogas sintéticas e indicó que el presidente Andrés Manuel López Obrador instruyó a su gabinete "brindar todo el apoyo y la colaboración" para atender el tema con "convicción humanista".

De acuerdo con Reuters, la canciller insistió en que invertir en la frontera compartida permite agilizar el tránsito de bienes y personas, pero también fortalecer la seguridad con proyectos de modernización, señalando que las secretarías de la Defensa Nacional y la Marina ya operan sistemas de revisión no intrusiva y rayos X en los puertos.

Por su parte, Antony Blinken, secretario de Estado de Estados Unidos, celebró que se realice un nuevo Diálogo de Seguridad desde 2021, al considerar que con ello se está avanzando con "la responsabilidad compartida, la cooperación, la colaboración y el respeto mutuo".

Afirmó que se buscará acordar una manera de redoblar esfuerzo "para detener el flujo ilícito de armas de Estados Unidos a México y de las drogas sintéticas de México a los Estados Unidos", reduciendo la demanda de fentanilo, metanfetaminas y otras sustancias ilegales, así como llevando ante la justicia a las redes criminales.

Coincidió en que ambos países son el principal socio comercial uno del otro, por lo que quieren asegurarse de que sus fronteras "sean seguras y estén protegidas"; no obstante, señaló que no lo pueden lograr por separado, por lo que hizo un llamado a tener enfoques compartidos.

En rueda de prensa tras, la reunión de Alto Nivel en Materia de Seguridad, el secretario de Seguridad Nacional de Estados Unidos, Alejandro Mayorkas, reiteró que el gobierno de su país no tiene planeado construir más muro en su frontera con México, sino que se reforzarán los 60 puertos de ingreso a ese país con tecnología de punta y anunció que como parte del compromiso de ese país para combatir el tráfico de armas hacia México, entregará mensualmente un reporte del flujo de armas hacia su frontera sur.

Estimado lector, ¿qué temas considera que hicieron falta tratar en esta reunión? ¿Qué acciones implementaría para el combate de estos y otros problemas de inseguridad que atañen a ambas naciones?

Seguridad en América *le desea felices fiestas y un próspero año nuevo 2024, lleno de abundancia y seguridad*

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 INTERNATIONAL CAPITULO MEXICO A.C.

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

RECONOCIMIENTO

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

En la presente edición, el director general de esta casa editorial, Samuel Ortiz Coleman, entregó un reconocimiento a Abraham Desantiago, presidente de ISRM Latam Chapter Chairman, quien en generosas ocasiones ha presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

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

Si desea conocer más del experto, consulte su currículo:

ENTREVISTA EXPRÉS CON

Cap. Víctor Aguirre,

director y fundador de VIP Protection

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

En mi opinión, uno de los grandes problemas que hemos tenido en México es la falta de capacitación de los cuerpos de seguridad pública llámese municipal, estatal o auxiliares, por lo que el pensar en sumar al sector privado para tareas del sector público no sería recomendable, ya que la capacitación también es uno de los aspectos que le falta reforzar a la seguridad privada. ■

TIMUR
Latinoamérica

GALEAM

NUESTRO VALOR, SU SEGURIDAD

CONSULTORÍA

GUARDIAS INTRAMUROS

PROTECCIÓN EJECUTIVA

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

info@galeam.mx | info@timurlatinoamerica.com

55 6840 1036 / 56 3048 9610 / 56 3700 0133

CERTIFICACIONES

CPP Certified Protection Professional
American Heart Association. Learn and Live
ALiCE

ÍNDICE

Noviembre - Diciembre 2023

ÍNDICE

Noviembre - Diciembre 2023

REPORTE

LA ENTREVISTA CENTRAL

ADMINISTRACIÓN DE LA SEGURIDAD

SEGURIDAD PÚBLICA

EL PROFESIONAL OPINA

CONOCE A TU ASOCIACIÓN

ENTREVISTA CON EL EXPERTO

FOROS Y EVENTOS

TIPS

LA GUERRA DE LOS DRONES,

UNA REVOLUCIÓN EN TECNOLOGÍA BÉLICA

Los drones de uso militar han originado una nueva etapa de conflictos armados con Inteligencia Artificial

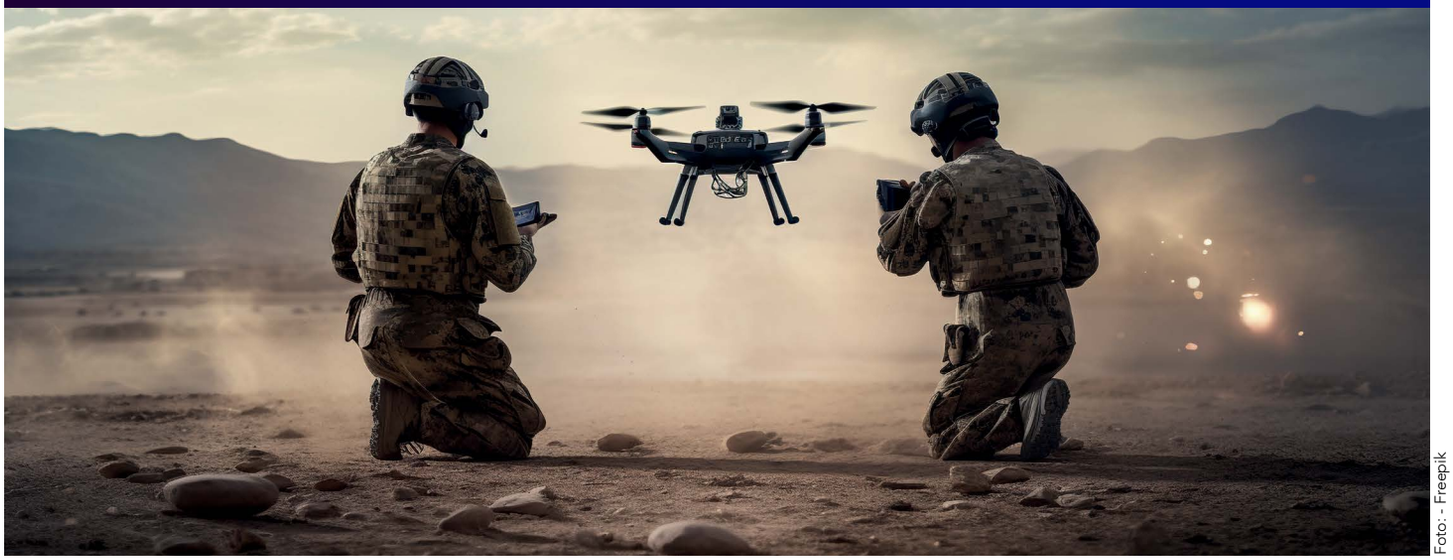


Foto: - Freepik

MÉXICO | **David Chong Chong**

En el campo de los conflictos bélicos, un factor crucial ha sido siempre el costo de los materiales de guerra, de tal suerte que cualquier ventaja para vencer y prevalecer, o al menos disuadir, corresponderá a quienes tengan la suficiente capacidad económica para financiar el desarrollo y disposición de recursos más sofisticados y funcionales, por lo regular las llamadas grandes potencias. En este contexto, la integración de los drones al acervo de materiales de guerra ha venido a cambiar el panorama de posibilidades tácticas y estratégicas, ya que se trata de recursos de bajo costo, pero con prestaciones funcionales similares a las de otros más sofisticados y por ende de alto costo, al alcance de potencias menores.

En la gama de recursos convencionales de materiales de guerra, podemos hablar del avión de reconocimiento Boeing RC-135, con un costo de 39 millones de dólares por unidad, 39 mil dólares por hora de vuelo, o el avión de ataque Fairchild Republic A-10 Thundrbolt II, con un costo de 12 millones de dólares por unidad y 22 mil dólares por hora de vuelo, así como el helicóptero Boeing AH-64 Apache con un costo de hasta 70 millones de dólares por unidad y cinco mil dólares por hora de vuelo.

En contraposición con el dron General Atomics MQ-9 Reaper, con un costo de 120 millones de dólares por unidad de combate (cuatro drones, estación de control y enlace satelital) y cuatro mil dólares por hora de vuelo, o incluso el dron Bayraktar TB2 fabricado por Turquía, con un costo de cinco millones de dólares por unidad y con mucho menos restricciones para su adquisición, sobre todo de índole política, como ha quedado demostrado en lo que bien se puede considerar como la primera "Guerra de los Drones", el conflicto entre Ucrania, una potencia menor, y Rusia, una supuesta gran potencia militar, y que sin embargo ha decidido adquirir drones de bajo costo desarrollados por una potencia relativamente menor, Irán.

En general un dron puede ser utilizado en misiones de "recolección" (*collect*) o "entrega" (*delivery*), reutilizables para el transporte de alguna carga útil, ya sea de uso, combate o rescate, o bien e misiones "sin retorno" (*no return*) o suicidas, de manera similar al BGM-198 Tomahawk con un costo de 1.5 millones de dólares por unidad más la carga explosiva que puede ser convencional o nuclear, con la ventaja de que un dron, cuando es operado de manera remota, puede abortar la misión para ser reutilizado nuevamente, mientras que un misil una vez lanzado ya no puede ser detenido, sólo destruido en vuelo o al impactar en su destino.

Por ello se puede considerar a los drones como un recurso "igualador" del potencial bélico entre grandes potencias y potencias menores, y el caso más ilustrativo de ellos es precisamente el de Ucrania, una potencia menor que ante la negativa de las potencias occidentales de la Organización del Tratado del Atlántico del Norte para suministrarle recursos militares más sofisticados como aviones

En México, con al menos dos grupos de la Delincuencia Organizada con la suficiente capacidad financiera, aunado a la corrupción que impera en algunas aduanas, existe la posibilidad de que adquieran drones incluso de grado militar de bajo costo, y los ingresen en partes junto con el personal técnico para ensamblarlos y operarlos

Un dron volando al menos con una velocidad de 10 metros por segundo y a menos de 50 metros de altura, no será detectado por los radares del CTA, y más aún si opera entre los edificios en un entorno urbano, y será capaz de superar cualquier despliegue convencional de protección en menos de un minuto

de combate y misiles, con la ayuda de, entre otros recursos, los drones de bajo costo suministrados por Turquía, ha logrado contener e incluso lograr un relativo equilibrio de fuerzas ante la agresión de una gran potencia como lo es Rusia, que a su vez tácitamente ha reconocido que los drones constituyen el recurso de combate más eficiente y conveniente en la actualidad y probablemente del futuro próximo.

HERRAMIENTA DE LA DELINCUENCIA ORGANIZADA

Sin embargo, el uso de estos recursos en aplicaciones bélicas no se limita a conflictos militares entre naciones, sino que también se abren oportunidades para cualquier grupo con la suficiente capacidad económica, no sólo para operar drones de grado militar, sino drones profesionales con un rango de costos entre 50 mil dólares y 150 mil dólares, e incluso de consumo o entretenimiento con costos en el rango de 400 a siete mil dólares, los primeros en todo tipo de misiones y los segundos, por nivel de costo, tal vez en misiones "sin retorno".

Grupos que pueden ser tanto opositores armados contra un gobierno, o terroristas, así como la delincuencia organizada que tiene la solvencia financiera no sólo para adquirir drones de cualquier grado, sino para contratar el personal técnico del más alto nivel para operarlos. Estos eventos ya han ocurrido en el marco de los conflictos en Medio Oriente por parte del autodenominado Estado Islámico, pero también en nuestro país por al menos un grupo de la delincuencia organizada en el Estado de Michoacán.

Y ante el "éxito" tanto aparentemente táctico como publicitario, existe la gran probabilidad de que estos eventos empiecen a proliferar. Asimismo, en el caso particular de México, con al menos dos grupos de la delincuencia organizada con la suficiente capacidad financiera, aunado a la corrupción que impera en algunas aduanas, existe la posibilidad de que adquieran drones incluso de grado militar de bajo costo, y los ingresen en partes junto con el personal técnico para ensamblarlos y operarlos dentro del territorio nacional.

El problema con estas posibilidades es que, en principio, la operación por lo regular clandestina de drones en operaciones antisociales, no se someterá a las regulaciones aeronáuticas en la materia, y no será posible identificarlos y ubicarlos por los medios normales de Control de Tráfico Aéreo (CTA), además de que, en manos de operadores técnicamente capacitados, tienen la aptitud de operarlos en condiciones furtivas no detectables por los medios actuales.

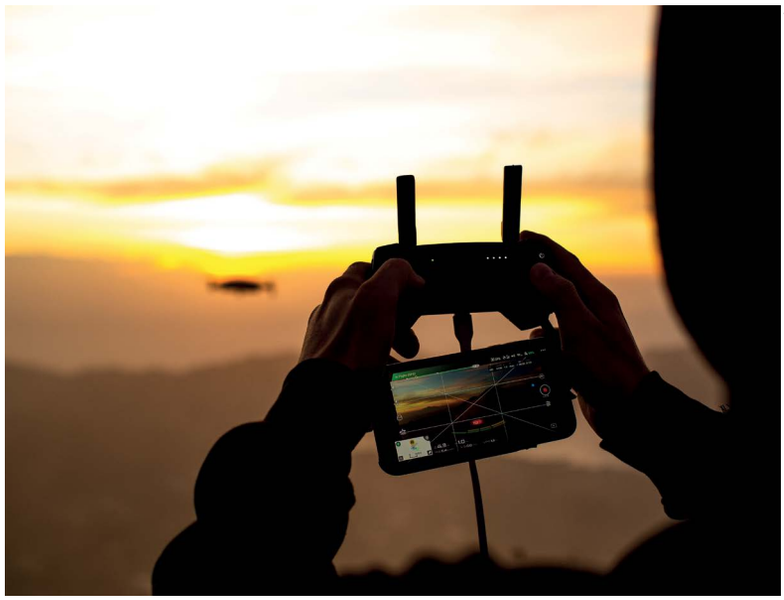


Foto: - Freepik

Por ejemplo, un dron volando al menos con una velocidad de 10 metros por segundo y a menos de 50 metros de altura, no será detectado por los radares del CTA, y más aún si opera entre los edificios en un entorno urbano, y será capaz de superar cualquier despliegue convencional de protección en menos de un minuto. Esto significa, en términos prácticos, que hoy por hoy no existe una forma de impedir un ataque con drones operado en las condiciones antes descritas, y que además pueden confundirse con otros drones operados con propósitos no hostiles, como vigilancia de seguridad o cobertura de medios de prensa.

La Guerra de los Drones ya es una realidad, porque esta revolución de la tecnología bélica ya esta aquí, incluso en nuestro país, y tenemos que enfrentarla, de inicio con los medios conocidos y disponibles, a la vez que se desarrollan otros más efectivos, aprendiendo de lo que ha ocurrido y previendo otros posibles escenarios inéditos, porque en el ámbito de la Seguridad, algo que ya ha ocurrido puede replicarse, y algo que nunca ha ocurrido, puede llegar a ocurrir, aunque parezca de fantasía o de ciencia ficción. ■

'Igitur qui desiderat pacem, praeparet bellum'
"Si realmente deseas la paz, prepárate para la guerra", Vegecio

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

LA FALACIA DE LA INTELIGENCIA ARTIFICIAL Y EL PODER DE LA ADMINISTRACIÓN POR EXCEPCIÓN

MÉXICO **Gonzalo Castillo Vite**

Imagen generada por wepik, una de las llamadas inteligencias artificiales

La Gestión por Excepción (o Management by Exception, MBE) establece que los directivos de las empresas deben dirigir su atención a aspectos o datos excepcionales (o que tiendan a ser excepcionales) que van apareciendo en el control de los diversos procesos de su organización

En la actualidad, nos encontramos inmersos en una era de transformación sin precedentes, impulsada por avances tecnológicos que están redefiniendo la manera en que vivimos, trabajamos y nos relacionamos con el mundo que nos rodea.

En el epicentro de esta revolución se encuentran las tecnologías de vanguardia, con un enfoque especial en las inteligencias artificiales (IA). Estas sofisticadas y cada vez más omnipresentes creaciones digitales han llegado a ser una fuerza motriz detrás de la transformación digital, alterando profundamente la forma en que las empresas operan, los gobiernos toman decisiones y las personas interactúan en su vida cotidiana.

Interesante introducción, ¿no crees? Clara, concreta, coherente y sin ningún error semántico ni de sintaxis. Pues déjame decirte que los dos primeros párrafos que acabas de leer no los redacté yo, Gonzalo Castillo, sino una de las tecnologías más populares del momento: Chat GPT.

MODELOS DE LENGUAJE VS. IA

Nadie puede negar el impacto y los beneficios que implica una tecnología como ésta en términos de transformación digital, siendo una herramienta útil y capaz de aportar valor en diversos campos; sin embargo, es importante tener claro que, aunque así se les ha nombrado de manera popular, tecnologías como Chat GPT no son inteligencias artificiales, sino modelos de lenguaje capaces de interactuar de forma conversacional, es decir, utilizando un lenguaje natural y ampliamente comprensible. Hoy día no existe un solo sistema que cuente con singularidad o que esté dotado de personalidad; cuando esto suceda, será considerado un verdadero hito en la historia de la humanidad.

LAS FÁBRICAS DE *SOFTWARE* Y LAS TECNOLOGÍAS DEL MAÑANA

Una de las industrias que más se han visto beneficiadas por el surgimiento de este tipo de tecnologías es la del desarrollo de *software*. Las fábricas de *software* son aquellas empresas dedicadas a desarrollar soluciones digitales o productos bajo demanda y con los más altos estándares de calidad para resolver las necesidades específicas de todo tipo de organizaciones, y para ello requieren una amplia gama de herramientas y modelos de vanguardia.

Por ejemplo, las fábricas de *software* aprovechan las bondades de motores de búsqueda como Elastic, y modelos semánticos como Chat GPT y Watson para automatizar y acelerar diversas operaciones que forman parte de sus procesos de desarrollo, desde la creación de código -incluyendo la identificación de vulnerabilidades y huecos en el mismo- hasta la ejecución de pruebas unitarias.

Sin embargo, aunque dichas herramientas son las que han causado mayor revuelo durante los últimos meses, existen otros conceptos que están revolucionando igual o en mayor medida las prácticas desarrolladas en las fábricas de *software* para impulsar la transformación y aceleración digital mediante la creación de soluciones cada vez más robustas, escalables, seguras y precisas. Tal es el caso de la administración por excepción.

ADMINISTRACIÓN POR EXCEPCIÓN: IMPULSANDO LA TRANSFORMACIÓN DIGITAL

La administración por excepción, gestión por excepción o Management by Exception (MBE) es un concepto, práctica, sistema, corriente o técnica de gestión que plantea la idea de que solamente es necesario intervenir o actuar en un proceso cuando suceden situaciones anormales o excepcionales que podrían representar una situación de riesgo o un problema para determinada organización.

Cuando una fábrica de software logra implementar un sistema basado en la administración por excepción que resuelve de manera efectiva las necesidades del cliente, significa que ésta comprendió profundamente la situación de la empresa, la problemática presentada y los objetivos que se buscaban alcanzar

Mediante la administración por excepción se pueden establecer reglas, indicadores clave de rendimiento (KPIs) y umbrales bien definidos para utilizarlos como puntos de referencia a partir de los cuales se determinará el momento en que una situación se sale de lo establecido como normal, es decir, cuando realmente requiere atención y una intervención oportuna. De esta manera, queda obsoleto el enfoque de monitoreo y control tradicional que se basa en la supervisión constante e ininterrumpida por parte de un monitorista de todo lo que ocurre en las instalaciones y equipos de una organización, lo que le permitirá enfocar su tiempo y recursos en aspectos verdaderamente críticos.

En otras palabras, podemos decir que con este enfoque se proporciona al personal información precisa y relevante para optimizar su toma de decisiones estratégica e inteligente, facilitando sus labores y evitando que el personal se sature o abrume con información intrascendente.

¿CÓMO CONFLUYE LA ADMINISTRACIÓN POR EXCEPCIÓN CON EL DESARROLLO DE *SOFTWARE*?

Para comprender mejor este concepto, tomemos como ejemplo VSS, plataforma de integración de sistemas de alta disponibilidad desarrollada por SISSA Digital. A partir de la administración por excepción, VSS tiene la capacidad de establecer un modelo de operación basado en reglas de negocio previamente definidas en conjunto con los clientes o usuarios finales, lo que le permite recibir alertas de las múltiples tecnologías monitoreadas (CCTV, control de acceso, inhibición de señal celular, etc.) únicamente cuando se presentan situaciones que hayan sido tipificadas como riesgosas o relevantes para la organización.

Por ejemplo, si una persona se acerca a un área previamente definida como no autorizada, se activará una alerta sonora y/o visual en la central de monitoreo, y la cámara más cercana al evento comenzará a transmitir lo que sucede en la pantalla del operador, todo de forma automática. Así, el operador o monitorista podrá tomar una decisión informada y activará los protocolos de respuesta adecuados sobre el evento ocurrido, como hacer un voceo o establecer comunicación inmediata con otras áreas para pedir apoyo.

Imagen generada por bluewillow, una de las llamadas inteligencias artificiales

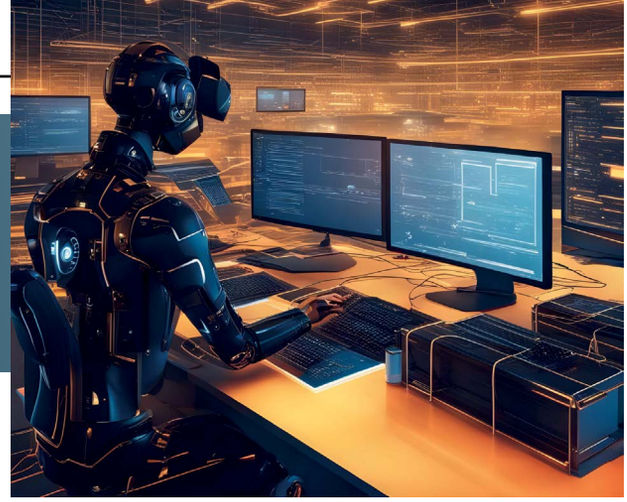


Imagen generada por bluewillow, una de las llamadas inteligencias artificiales

En IXMAKI, sistema de gestión de identidad de SISSA Digital, la administración por excepción ayuda a establecer reglas de negocio para el proceso de pase de lista. Por ejemplo, si en una organización o institución existen horarios que deben ser cubiertos por el personal, esta plataforma podrá generar reportes en caso de que una persona falte o ingrese después de la hora establecida, además de que se podría configurar para enviar de forma automática un aviso o recordatorio vía SMS a la persona que cometió la falta.

De igual forma, AppController, sistema de gestión de servicios operativos también desarrollado por SISSA Digital, al tener como principal función la administración de incidencias, utiliza la administración por excepción para categorizar por color el nivel de importancia de cada una de las incidencias y de las alertas emitidas, lo que facilitará a los operadores del sistema identificar rápidamente la relevancia de los eventos que se presenten y ponderar sus esfuerzos para la resolución de los mismos. Por ejemplo, cuando se abra la puerta del cuarto de lavado de una organización no emitirá el mismo tipo de alerta que cuando se abra la puerta de un área crítica, o no será el mismo tipo de alerta cuando los artículos de un almacén estén a punto de agotarse que cuando se presenten errores con alguna otra incidencia.

Algo que vale mucho la pena mencionar acerca de este concepto, es que cuando una fábrica de *software* logra implementar un sistema basado en la administración por excepción que resuelve de manera efectiva las necesidades del cliente, significa que ésta comprendió profundamente la situación de la empresa, la problemática presentada, los objetivos que se buscaban alcanzar y todas las variables que intervienen en un proceso de desarrollo e implementación de *software*.

EVOLUCIÓN DEL PERFIL DE DESARROLLADOR DE *SOFTWARE*

Hoy día, una de las diferencias más importantes entre un desarrollador *Sr.* y un desarrollador *Jr.* es que el primero cuenta con una amplia, nutrida y diversificada gama de librerías y herramientas en su portafolio, lo que, aunado a su amplia experiencia, le permite crear productos con altos niveles de escalabilidad y en cortos periodos de entrega.

Ahora bien, tenemos que ser muy conscientes de que el surgimiento de nuevas tecnologías de automatización también implica retos y desafíos importantes para el factor humano, especialmente para el desarrollador de *software*. Nunca había existido tanta urgencia por que los perfiles profesionales evolucionaran y se adaptaran en función de las nuevas tecnologías, los cuales deben ser cada vez más estratégicos y capaces para comprender, utilizar y aprovechar las ventajas que ofrecen estas nuevas herramientas en beneficio de las diferentes industrias.

En otras palabras, el nuevo perfil del desarrollador de *software* debe estar orientado en gran medida al perfil de un consultor; de esta manera, las fábricas de *software* podrán entender a profundidad las necesidades de sus clientes, seleccionar estratégicamente las herramientas más adecuadas para desarrollar soluciones específicas —comprendiendo sus ventajas y limitantes—, y así entregar productos de mejor calidad.

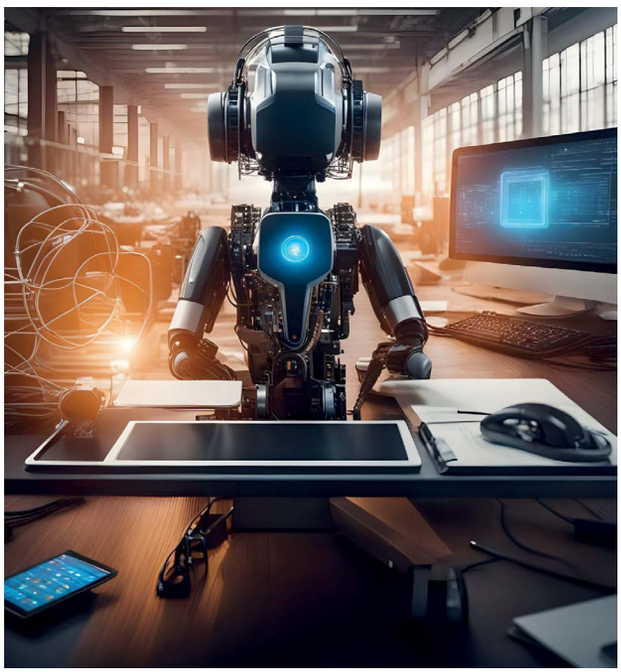


Imagen generada por bluewillow, una de las llamadas inteligencias artificiales

Gonzalo Castillo Vite, director de Desarrollo de *Software* en SISSA Digital. *Más sobre el autor:*

FÁBRICAS DE *SOFTWARE*: ALIADOS ESTRATÉGICOS IMPRESCINDIBLES

Las fábricas de *software* de la actualidad tienen la capacidad de crear soluciones de seguridad, automatización y control a partir de modelos de operación escalables y editables a fin de que las organizaciones puedan editar y adaptar sus sistemas en función de las demandas y necesidades cambiantes de su entorno.

Una de las principales ventajas de adquirir un servicio de consultoría, desarrollo e implementación de *software* a medida —y la que se hace evidente con mayor rapidez— es que las empresas toman consciencia sobre sus procesos, las problemáticas que estos tienen, y el alcance que pueden tener a corto, mediano y largo plazo, lo que resulta esencial para depurar sus áreas de oportunidad y comenzar a ganar mayor competitividad en sus industrias. Además, al solicitar los servicios de una fábrica de *software* de alto nivel y con amplia trayectoria, tienes la certeza de que ésta se ha enfrentado al menos en una ocasión a un problema similar al tuyo, por lo que al momento de brindarte sus servicios tendrá la experiencia y habilidad necesarias para ofrecerte una solución aún más precisa y eficiente.

Asimismo, este tipo de empresas cuentan con alianzas comerciales con las marcas más importantes del sector tecnológico y, por lo tanto, tienen acceso a certificaciones tecnológicas en diferentes campos, como el de la seguridad y la normatividad.

Por ésta y muchas otras razones más, hoy en día resulta fácil afirmar que quienes no se encuentran en un proceso de adopción de tecnologías y *software* de innovación, están en una clara desventaja frente a sus competidores; como dice aquella frase célebre y que toma más fuerza con el paso del tiempo: lo que no se mide, no se puede controlar (y por ende, mejorar).

EL PODER DEL FACTOR HUMANO

Para concluir, la recomendación que aquí se pretende dejar asentada es que todas las tecnologías desarrolladas hasta hoy en día deben ser comprendidas como elementos integrantes de una caja o set de herramientas, y no como soluciones definitivas que pueden operar a la perfección de manera autónoma. La tecnología es y siempre será un medio para que el factor humano, a partir de su inteligencia, capacidad estratégica, creatividad y preparación continua, proporcione soluciones robustas y eficaces para atender las problemáticas y necesidades de cualquier sector.

¿CUÁL ES LA VENTAJA DE SISSA DIGITAL?

SISSA Digital nació como una integradora de soluciones, por lo que nuestros especialistas están capacitados y orientados a evaluar y analizar las tecnologías que tienen implementadas nuestros clientes en sus instalaciones. De esta manera, los sistemas que sean compatibles y que cumplan los parámetros necesarios podrán integrarse con el *software* desarrollado.

Asimismo, en SISSA Digital estamos acostumbrados a ponernos en los zapatos de nuestros clientes, lo que nos ha permitido establecer relaciones de negocio sólidas y duraderas con las organizaciones que solicitan nuestros servicios.

Si te interesa obtener más información sobre nosotros, no dudes en contactarnos por cualquiera de los canales de comunicación de SISSA Digital. ■

Fotos: SISSA Digital

¡Paragon establece el estándar para el futuro!

Revolucionando la prevención de pérdidas.

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

ESCANEAR PARA MÁS INFORMACIÓN

PARAGON

Ambiscan

MADE IN THE USA

GARRETT

SISTEMA DE CONTROL DE ACCESO

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura

Foto: Freepick

COLOMBIA

Javier Nery Rojas Benjumea

El sistema de control de acceso es una parte del programa de seguridad física y está constituido por aquellas medidas (políticas, procedimientos e instructivos) y equipos (tecnología aplicada a la seguridad) cuya implantación permita en todo momento la identificación de personas y cosas que pretenden acceder (de entrada, o de salida) a una determinada área, controlando, facilitando o denegando el acceso, según un planteamiento o criterio preestablecido.

Dos son sus atributos principales: mantener un orden, y dejar un registro permanente, y es menester fundamental que estén diseñados de manera coherente con el sistema de barreras o cerramiento perimetral, el sistema de circuito cerrado de televisión y el sistema de alarmas de intrusión.

OBJETIVOS QUE SE PERSIGUEN AL IMPLANTAR UN SISTEMA DE CONTROL DE ACCESO:

- Identificar los intentos de acceso.
- Impedir los no autorizados.
- Controlar y gestionar ambos.
- Obtener información del tráfico resultante.
- Delimitar en detalle las autorizaciones de acceso.
- Definir el comportamiento de los distintos accesos.

ALGUNOS TIPOS DE SISTEMAS (TECNOLOGÍA):

- Tarjeta de infrarrojos.
- Tarjeta Wiegand.
- Tarjeta de elementos magnéticos aislados.
- Tarjeta de proximidad (pasiva o activa).
- Tarjeta banda magnética.
- Tarjeta chip.
- Por huellas dactilares.
- Lectores biométricos de mano.
- Lectura por infrarrojos del iris del ojo humano.
- Por reconocimiento de voz.
- Por firma, rasgos faciales, etc.

COMPOSICIÓN DE UN CONTROL DE ACCESO:

Elementos:

- Elemento de identificación.
- Lector o identificador.
- Unidad de control o toma de decisión.
- Transmisor de información.
- Control de paso (elemento físico).
- Gestor de información y programación.

Tipos de Elementos:

- Lectores autónomos.
- Lectores cableados.
- Programadores portátiles.
- Editor de tarjetas.
- Red de comunicaciones.

¿DÓNDE INSTALAR UN CONTROL DE ACCESO?

- Puertas de acceso principal, o de alto tráfico.
- Accesos a *parkings*, sótanos, pasillos de tránsito, etc.
- Almacenes de materiales, laboratorios, salas de ordenadores, etc.
- Oficinas, despachos, salas de conferencias o reunión, etc.

¿QUÉ APORTA Y CÓMO SE RENTABILIZA LA INVERSIÓN EN UN SISTEMA DE CONTROL DE ACCESO?

- Seguridad: personas, bienes y edificios.
- Póliza de seguros más barata.
- Ahorro en gastos de mantenimiento del edificio y ahorro en personal.
- Ahorro en el costeo de materiales robados o utilizaciones indebidas de equipos.
- Control del personal: registro de sus movimientos por el edificio.
- Ahorro en el costeo de las llaves y cambios de cerraduras cuando éstas se pierden.

¿CÓMO DEBERÍA SER SU SISTEMA DE CONTROL DE ACCESO?

- Permitir la combinación de elementos autónomos y cableados.
- Configuración versátil y expandible.
- Capacidad de integración.
- Facilidad de instalación.
- Estética.
- Buena relación prestaciones/precio.
- El sistema debería dar soluciones *online* donde se necesitan realmente, y permite utilizar elementos autónomos en más puntos con la misma o menor inversión.
- Un *software* y un *hardware* muy sencillos que proporcionen un control de acceso que permita mantener un orden y dejar un registro permanente de los eventos. ■

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

SISSA DIGITAL

www.sissadigital.com.mx

Vector SCADA System

PLATAFORMA DE Integración de Sistemas

Monitorea, automatiza, controla y gestiona todos tus sistemas tecnológicos.

Seguridad Electrónica

Telecomunicaciones y Cómputo

Infraestructura Crítica

¿Qué puede hacer **VSS en tu organización?**

- ✓ **Integra toda tu tecnología e infraestructura en un sólo lugar.**
- ✓ **Permite la detección en tiempo real de eventos de riesgo (administración por excepción).**
- ✓ **Genera reportes sobre el funcionamiento y operación de cada sistema.**

Contáctanos y adquiere una visión completa y detallada sobre la seguridad y gestión de tu organización.

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:

EL HOSPITAL Y SU SEGURIDAD CONTRA INCENDIOS

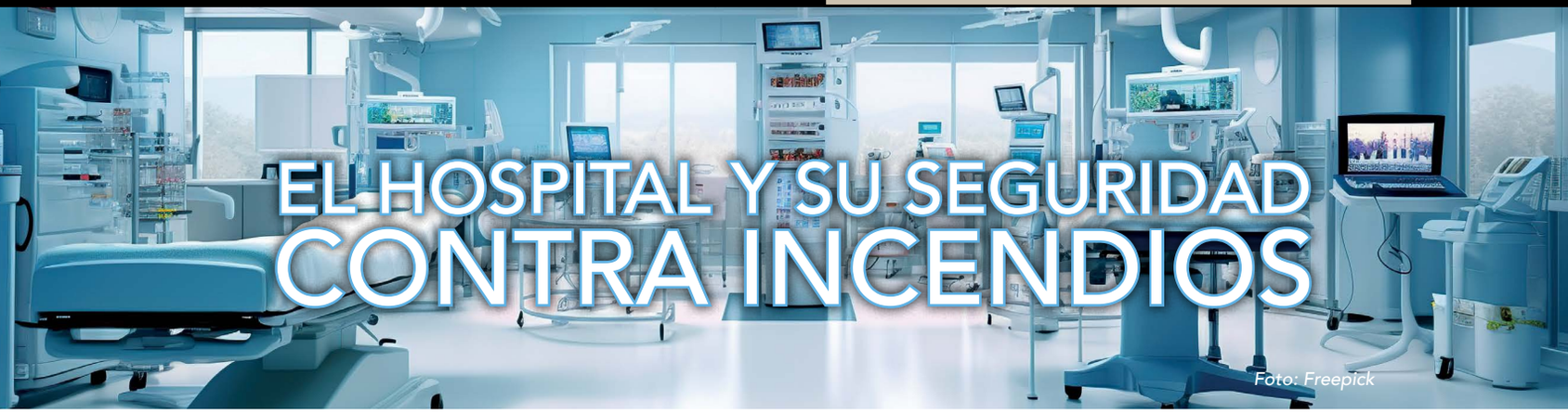


Foto: Freepick

EUA

Los hospitales tienen retos especiales para los que velan por la seguridad contra incendios de este tipo de ocupaciones, pues albergan a ocupantes que son incapaces de auto preservación debido a discapacidades físicas, mentales o por su edad. Aún en centros de atención médica ambulatoria, los pacientes pueden recibir anestesia general u otro tratamiento que los hace también incapaces de auto preservación. Esto quiere decir que muchos de los ocupantes de estos hospitales o centros ambulatorios son incapaces de evacuar por sí mismos, o si tienen movilidad, pueden no ser capaces de percibir una amenaza de incendio o tener una reacción racional.

NECESIDAD DE MÁS HOSPITALES

Se estima que el tamaño del mercado latinoamericano de camas de hospital estará aumentando a una tasa de crecimiento anual de casi el 5% hasta 2027. El aumento del gasto en hospitales por los gobiernos locales y una mayor población geriátrica está contribuyendo a este crecimiento. Se espera que para 2050, el número de personas de 65 años o más se duplique en Latinoamérica. Geográficamente, Brasil, seguido de México y Colombia, lideran el mercado latinoamericano de camas hospitalarias, con aproximadamente 330 mil, 170 mil y 85 mil camas de hospital respectivamente[1].

Sin embargo, la cultura de la protección contra incendios en hospitales, en países latinoamericanos, no se ha desarrollado tan rápidamente como la que, por ejemplo, se ha visto en edificios de oficinas de gran altura, hoteles, industrias y bodegas. Incendios recientes, como el trágico incendio del Hospital Badin en Río de Janeiro, Brasil, en septiembre de 2019, donde 11 pacientes perdieron la vida, o el del Hospital Calderón Guardia en San José de Costa Rica, donde 19 personas murieron en julio de 2005, colocan en relieve la necesidad de poner mayor atención en más modernos y efectivos métodos de seguridad contra incendios. Desde mi óptica, sólo hospitales financiados por el Banco Mundial u otras entidades financieras internacionales le están poniendo suficiente atención al impacto de un posible incendio.

NORMAS NFPA

NFPA 101, Código de Seguridad Humana y NFPA 99, Código de Instalaciones en Edificios de Cuidado de la Salud, son de requerido cumplimiento en los hospitales de los EUA y otras partes del mundo. Particularmente la NFPA 101 establece un método integral, conocido como el método de "defensa en su lugar", pues la emergencia menos deseada en un hospital es la que pueda requerir relocalización o evacuación de pacientes. Por consecuencia, NFPA 101 establece una estrategia que utiliza un enfoque llamado "concepto total", que requiere una variedad de características de seguridad contra incendios que se consideran necesarias para evitar la evacuación de los pacientes hacia el exterior durante un incendio. Este "concepto total" incluye los siguientes principios generales:

- Construcción resistente al fuego y subdivisión de cada piso, conocida como compartimentación, para evitar la propagación del humo así como protección de aberturas verticales.
- Limitación en el uso de materiales combustibles en acabados interiores.
- Protección por medio de rociadores automáticos.
- Dispositivos de notificación de incendios en todo el hospital y detección de humos en ciertas áreas con camas.
- Provisión de medios de salida adecuados y marcación e iluminación de salidas.
- Energía eléctrica de emergencia.
- Dependencia en personal debidamente capacitado y ejercitado que sean capaces de tomar medidas que protejan la vida de los pacientes como parte de la planificación de emergencias.

A continuación explico a mayor detalle varios aspectos importantes en la estrategia de seguridad contra incendios de un hospital:

¿CÓMO RESPONDER ANTE UN INCENDIO?

La acción del personal del hospital como doctores, enfermeras, camilleros, personal administrativo y de mantenimiento, entre otros, es parte integral de la estrategia de seguridad humana en un centro de atención médica. La respuesta adecuada de este personal en términos de disponibilidad, acciones y manejo de un incendio puede influir rápidamente en el resultado de una emergencia por incendio.

Este personal tiene la responsabilidad de preservar la seguridad de los pacientes a su cargo, ya sea que eso implique informar a los pacientes que no están en peligro por el incendio o ayudar a reubicar a los que sí lo están. Su capacitación debe ser parte integral y continua en la estrategia de seguridad contra incendio del hospital.

Reubicación de pacientes de la zona comprometida a otro compartimiento protegido contra el humo

RESISTENCIA AL FUEGO Y COMPARTIMENTACIÓN DEL EDIFICIO

En un hospital es importante la definición del tipo de construcción que debe tener el edificio, desde el punto de vista de su resistencia al fuego. Dependiendo si el hospital tiene o no protección con rociadores automáticos, NFPA 101 limita el número de pisos que puede tener el edificio dependiendo de su tipo de construcción.

Los tipos de construcción están definidos por la NFPA 220, Norma Sobre Tipos de Construcción de Edificios, y a razón de que este tema es incipiente en Latinoamérica por la falta de información sobre la resistencia al fuego de la mayoría de los métodos constructivos utilizados, requiere el apoyo de alguien familiarizado con ingeniería de protección contra incendios para poderlo resolver de una manera efectiva. Otro tema importante es la subdivisión de cada piso en por lo menos dos sectores, separados por barreras corta humo.

Compuerta corta humo en un ducto de aire traspasando una pared corta humo

ROCIADORES AUTOMÁTICOS

Todos los hospitales o edificios utilizados para propósitos de atención o tratamiento médico simultáneo a cuatro o más pacientes con internación, deben estar protegidos por un sistema de rociadores automáticos, incluyendo áreas de quirófano. Los edificios de cuidado ambulatorio de gran altura también requieren protección con rociadores. Éstos se deben instalar en todo el edificio, utilizando rociadores de respuesta rápida.

Las alas psiquiátricas deben estar protegidas con rociadores de tipo institucional, a prueba de golpes. Una unidad de control para cada sistema de rociadores debe ser instalada por cada piso del hospital, generalmente instalada dentro de la escalera de emergencia, que, con las conexiones para mangueras, son parte del montante de agua contra incendios.

Unidad de control de los rociadores, con conexión Clase I para mangueras dentro de la escalera

CONEXIONES PARA MANGUERAS

NFPA requiere también la instalación de "conexiones" para mangueras en lugar de "gabinetes equipados con mangueras" en hospitales que tengan tres o más pisos, la cual es llamada Columna de Agua Clase I. El Sistema Clase I provee una columna o montante en la escalera de evacuación, típicamente de 6 pulgadas (152 mm) de diámetro, cargada de agua a presión, con conexiones para mangueras de 2-½ pulgadas de diámetro (64 mm), con una reducción para manguera de 1-½ pulgadas (38 mm). Debe quedar claro que NFPA no requiere la instalación de gabinetes con mangueras en ningún hospital.

ALARMA Y DETECCIÓN

Todos los hospitales requieren un sistema de alarma a través de una alarma de tono o de voceo codificado. Se permite un retraso de hasta 180 segundos en la secuencia de alarma para permitir la investigación de la señal de alarma. Esto implica la iniciación de la alarma a través del interruptor de flujo de los rociadores automáticos o los pulsadores manuales instalados en puntos estratégicos del hospital, como en las estaciones de enfermeras. Especial énfasis se debe tener con la zonificación de la anunciación de la alarma.

NFPA 101 puede requerir detección de humo en las áreas donde existan camas con pacientes, así como sus corredores adyacentes, donde no exista una supervisión visual por parte de las enfermeras. La localización de estos detectores de humo requiere una evaluación más profunda de la NFPA 101. Fuera del área con camas, no se requiere detección de humo en un hospital, excepto en las unidades de manejo de aire o enfrente de los elevadores.

OTROS SISTEMAS DE EXTINCIÓN

NFPA reconoce la efectividad de los extintores manuales en incendios incipientes, y estos son de uso requerido en todos los hospitales. Las campanas de la cocina deben estar protegidas con un sistema de extinción a base de químicos húmedos, certificados de acuerdo con UL 300. El cuarto de IT/Computo, debe ser protegido con rociadores automáticos, aunque, normalmente en Latinoamérica estos cuartos se protegen con agentes limpios. Es importante que si un operador elige voluntariamente proteger este cuarto con agentes limpios, no se eliminen los rociadores automáticos del cuarto.

NFPA requiere que el hospital esté protegido por un sistema de iluminación de emergencia en los medios de evacuación y señalización de las salidas

El Plan Maestro tiene como propósito proveer un registro del proceso de decisiones durante la determinación de las protecciones a los riesgos de incendios presentes en el hospital, así como documentar cómo se ha cumplido la NFPA 101 y cómo se ha definido la estrategia de protección

EVACUACIÓN

La evacuación es un tema complejo, pues como se estableció anteriormente, la estrategia es la de "defensa en su lugar" y requiere un estudio específico del hospital. En este estudio se establece la filosofía de relocalización y los criterios específicos para el diseño de las vías de evacuación (localización, cantidad, ancho, distancia, sectorización y protección contra humo). NFPA requiere que el hospital esté protegido por un sistema de iluminación de emergencia en los medios de evacuación y señalización de las salidas. También se requieren sistemas de energía de emergencia conectada a equipos críticos para la seguridad humana y de autopreservación de los pacientes.

ESTRATEGIA DE PROTECCIÓN CONTRA INCENDIOS

Lo más temprano posible en el proceso de diseño de un hospital se deben establecer las bases de diseño de la seguridad contra incendios del edificio. Estas bases de diseño se llaman tradicionalmente el Plan Maestro de Seguridad Contra incendios. El Plan Maestro tiene como propósito proveer un registro del proceso de decisiones durante la determinación de las protecciones a los riesgos de incendios presentes en el hospital, así como documentar cómo se ha cumplido la NFPA 101 y cómo se ha definido la estrategia de protección.

Este documento no solamente se revisa, mejora y modifica a medida que se refina el diseño del hospital, sino que debe ser continuamente revisado y mantenido durante la vida de la instalación. Se ha vuelto más común que hospitales existentes en Latinoamérica elaboren también este tipo de documento para saber dónde están y qué deben hacer para mejorar sus niveles de protección. Él método más común para elaborar este Plan Maestro es a través de la contratación de firmas de ingeniería de protección contra incendios con experiencia en la utilización de la NFPA 101 en hospitales. ■

Referencias:

[1] *Report on Latin America Hospital Bed Market by Market Data Forecast, March 2023.*

Fotos: Cortesía IFSC

MAK MR
EXTINGUISHER

"Protege tu negocio y a tu personal con nuestros sistemas contra incendios. Seguridad completa para tu tranquilidad. ¡Contáctanos hoy!"

MAKSeguridad

Distribuidor mayorista
SIEMENS

www.makseguridad.com

RANSOMWARE Y SU EVOLUCIÓN: EL DILEMA DE PAGAR (PARTE II)

En esta segunda parte del artículo, nuestra autora invitada habla de que el objetivo final es proporcionar una seguridad más robusta, adaptativa y resistente frente a amenazas internas y externas en un entorno empresarial cada vez más distribuido y en evolución constante. Asimismo, lo invitamos a leer la primera parte del artículo en la página 40 de nuestra edición 140 (septiembre-octubre)

Foto: Freepick

MÉXICO **Gigi Agassini**

Hay cuatro acciones principales que el *ransomware* puede ejecutar: bloquear, cifrar, eliminar y robar. Estas cuatro acciones se identifican como LEDS (*Lock, Encrypt, Delete, Steal*). El *ransomware* puede bloquear el acceso a un activo, como bloquear la pantalla o el acceso a una aplicación en particular. Puede cifrar un activo, haciéndolo no disponible para el objetivo. Puede robar un activo, comprometiendo su disponibilidad y, al final, su confidencialidad. Por último, puede eliminar un activo y dejarlo permanentemente no disponible.

Identificar el uso de las acciones en los activos, permite identificar las capacidades del *ransomware* como se muestra en la siguiente tabla compartida por ENISA (European Union Agency for Cybersecurity) en su reporte "Panorama de amenazas para los ataques de *ransomware*" (*Threat Landscape for Ransomware Attacks*).

Capacidades del *ransomware* actual en términos de acciones que realizan y activos a los que apuntan

	Acciones			
Activos	Cerrar	Cifrar	Eliminar	Robar
Archivos	✗	✓	✓	✓
Memoria	✗	✓	✓	✓
Carpetas	✗	✓	✓	✓
Contenido de la base de datos	✗	✓	✓	✓
MFT	✓	✓	✓	✗
MBR	✓	✓	✓	✗
Nube	✗	✓	✓	✓
CMS	✗	✓	✓	✗
Pantalla	✓	✓	✓	✗

RANSOMWARE AS A SERVICE

Siguiendo con la evolución del *ransomware*, en la actualidad nos enfrentamos a RaaS (*Ransomware as a Service*), este es un modelo en el que los ciberdelincuentes ofrecen el acceso y uso de herramientas de *ransomware* a otros actores malintencionados a través de una plataforma o servicio en línea.

Bajo este modelo, los "afiliados" pueden obtener y personalizar variantes de *ransomware*, utilizar paneles de control para administrar sus campañas y recibir una parte de los pagos de rescates generados.

Algunos aspectos sobre *Ransomware as a Service* que se ofrecen a los "afiliados", es el acceso a herramientas previamente desarrolladas, lo que permite lanzar ataques de *ransomware* sin tener que crear su propio código malicioso desde cero. Pueden personalizarlo también, es decir que pueden agregar sus propias instrucciones de rescate, estableciendo monto y definir los activos objetivo. Proporcionan infraestructura de comando y control para la administración de campañas y monitoreo del estado de las infecciones, así como creación de reportes.

Los beneficios financieros generados por estos ataques se comparten entre el operador del RaaS y los afiliados, lo que incentiva a estos últimos a lanzar más ataques y aumentar la rentabilidad. El RaaS ha contribuido a una mayor disponibilidad y accesibilidad del *ransomware*, lo que ha reducido la barrera de entrada para los atacantes menos sofisticados o con menos experiencia técnica.

Es importante destacar que el *Ransomware as a Service* ha aumentado la proliferación del *ransomware* y ha facilitado a los actores malintencionados llevar a cabo ataques en gran escala. Este modelo ha impulsado el crecimiento de la industria del *ransomware* y ha llevado a un aumento significativo en el número de ataques en los últimos años.

ETAPAS DE UN ATAQUE DE *RANSOMWARE*

El ciclo de vida del *ransomware* se mantuvo sin cambios hasta alrededor de 2018, cuando el *ransomware* comenzó a agregar más funciones y las técnicas de chantaje maduraron, por lo que hoy podemos identificar cinco etapas de un ataque de *ransomware*:

1. Acceso inicial, es la primera etapa para acceder al objetivo.
2. Ejecución, estudian el objetivo, se mueven lateral a otras computadoras y emplean las técnicas de ataque.
3. Acción sobre objetivos, es aquí donde se aplican las técnicas LEDS, estas pueden tomar semanas después de la infección inicial del sistema.
4. Chantaje, una vez que los objetivos están comprometidos, el delincuente procede a comunicarse con la víctima, amenazando y demandando el pago.
5. Negociación de rescate, normalmente la comunicación es privada entre la víctima y los delincuentes y sólo hay dos opciones en la negociación, la víctima paga el rescate o no paga.

Y aunque estas etapas no son estrictamente secuenciales, ya que pueden variar, es importante destacar que son las más identificables, por lo que si ya fuiste víctima o quieres protegerte de serlo, es importante que las conozcas.

El promedio para identificar y contener un *ransomware* o ataque destructivo es significativamente

En la actualidad nos enfrentamos a RaaS (Ransomware as a Service), esto es un modelo en el que los ciberdelincuentes ofrecen el acceso y uso de herramientas de ransomware a otros actores malintencionados a través de una plataforma o servicio en línea

Foto: Freepick

alto, ya que un ataque de *ransomware* en promedio toma 237 días identificarlo, 89 días para contenerlo, lo que nos da un total en el ciclo de vida de 326 días. Un ataque destructivo toma en promedio 233 días para identificarlo y 91 días para contenerlo lo que nos da un ciclo de vida total de 324 días, según el reporte "Cost of Data Breach Report 2022" de IBM.

Hay diferentes opiniones por agencias públicas y privadas con relación a pagar o no pagar un *ransomware*, pero la gran mayoría menciona que pagar nunca es recomendado, principalmente porque no garantiza la solución al problema.

Cuando se habla "teóricamente", la mayoría de las agencias de aplicación de la ley te instan a no pagar a los atacantes de *ransomware*, con la lógica de que hacerlo sólo alienta a los delincuentes a crear más *ransomware*.

Sin embargo, muchas organizaciones que se ven afectadas por el *malware* rápidamente dejan de pensar en términos del "bien común" y comienzan a hacer un análisis de costo-beneficio, sopesando el precio del rescate contra el valor de los datos cifrados. Según una investigación de Trend Micro, mientras que el 66% de las empresas dice que nunca pagaría un rescate como principio, en la práctica el 65% paga el rescate cuando recibe un golpe.

Desafortunadamente, es extremadamente difícil cuantificar quién pagó o no el rescate y en qué casos se acordó un rescate menor. Esta información normalmente no se pone a disposición del público. A menudo, hay reportes en los que se informan las ganancias totales de los actores de la amenaza, pero no a nivel individual. También hay actores de amenazas que, después de un pago exitoso, eliminan el nombre de destino comprometido de su sitio web público. Sin embargo, no es seguro generalizar y asumir que todos los objetivos que ya no están en la página web pagaron una tarifa de rescate, ya que en muchos casos los sitios web de *ransomware* tienen errores y son inestables, basar las evaluaciones en las afirmaciones de los ciberdelincuentes definitivamente, no es una fuente confiable.

Después de analizar la cronología evolutiva del *ransomware* y las posiciones de agencias públicas y privadas sobre si pagar o no, podrás darte cuenta que una vez que tú o tu organización están frente al vector de ataque se requiere de muchos factores de evaluación para tomar decisión tan sensible, lo más importante es tener herramientas, y un plan de respuesta a incidentes basados en marcos

de referencia y estándares de la industria para poder minimizar el riesgo pero sobre todo, reaccionar ante un ataque de *ransomware*.

PLAN DE RESPUESTA A INCIDENTES

Como referencia te puedo compartir el Plan de Respuesta a Incidentes, según el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), que consta de cuatro pasos:

1) Preparación:
- Establecer una política de respuesta a incidentes y definir los roles y responsabilidades del equipo de respuesta.
- Identificar los activos críticos de la organización y realizar una evaluación de riesgos.
- Desarrollar y mantener un plan de respuesta a incidentes que incluya los procedimientos y las acciones a seguir en caso de un incidente de seguridad.
- Proporcionar capacitación y concienciación sobre seguridad a los empleados.
- Establecer acuerdos de colaboración con socios externos, como proveedores de servicios de seguridad o agencias de aplicación de la ley.

2) Detección y análisis:
- Implementar soluciones y controles de seguridad que permitan la detección temprana de incidentes.
- Monitorear de forma continua los sistemas y redes en busca de eventos o actividades sospechosas.
- Analizar los indicios y las alertas para determinar si se trata de un incidente de seguridad real.
- Recopilar y preservar la evidencia relevante para futuras investigaciones.

3) Contención, erradicación y recuperación:
- Tomar medidas inmediatas para contener el incidente y evitar su propagación.
- Identificar la causa raíz y eliminar el acceso no autorizado o los puntos de entrada del atacante.
- Restaurar los sistemas y los servicios afectados a un estado operativo normal.
- Aplicar parches de seguridad, actualizaciones y mejoras en los sistemas para evitar futuros incidentes similares.

4) Lecciones aprendidas y revisión:
- Analizar el incidente y evaluar la respuesta y los procedimientos implementados.
- Identificar las lecciones aprendidas y las áreas de mejora en el plan de respuesta a incidentes.
- Realizar cambios y actualizaciones en el plan, las políticas y los controles de seguridad con base en las lecciones aprendidas.
- Documentar y comunicar los resultados de la revisión a los interesados pertinentes.

Foto: Freepick

ZERO TRUST

Otra alternativa es aplicar *Zero Trust*, que es un enfoque de seguridad cibernética que se basa en la premisa de no confiar en ningún usuario o dispositivo, tanto dentro como fuera de una red corporativa. En lugar de confiar en la tradicional estrategia de seguridad basada en perímetros, *Zero Trust* se centra en la verificación continua y la autenticación exhaustiva de todos los usuarios, dispositivos y recursos, sin importar su ubicación.

Este modelo se basa principalmente en verificación continua, identidad centrada, menor privilegio, seguridad basada en contexto, seguridad centrada en aplicaciones de datos, monitoreo y análisis continuos. La implementación de *Zero Trust* implica la adopción de tecnologías como autenticación multifactor (MFA), microsegmentación de red, cifrado, controles de acceso basados en políticas y análisis de comportamiento de usuarios y dispositivos. El objetivo final es proporcionar una seguridad más robusta, adaptativa y resistente frente a amenazas internas y externas en un entorno empresarial cada vez más distribuido y en evolución constante.

Si llegaste hasta aquí, notaste que el tema es tan extenso que nos da aún para mucho y podríamos seguir y seguir sin llegar a una conclusión o respuesta acotada a la pregunta ¿pagar o no pagar? Lo que quiero dejarte con este artículo es más información de lo que es *ransomware* y su evolución, los riesgos a su alrededor por la madurez a la que ha llegado es que cada vez es más difícil poderlo detectar y por consecuencia recuperarse de ello.

Por lo anterior es fundamental desarrollar una cultura interna, el uso de herramientas, pero sobre todo la implementación de procesos y políticas respaldados por estándares internacionales y marcos de referencia, recordando que siempre la inversión en la prevención será mucho menor que esperar a que nos ocurra pensando que si esto pasa, seguramente no tendrá el impacto del que tanto se habla.

Tu empresa hoy probablemente ya fue víctima de *ransomware* o está siendo y aún no lo sabes. Dime, ¿pagarías? ■

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

MONTERREY / CANCÚN / VERACRUZ / / COATZACOALCOS / VILLAHERMOSA

GORAT SEGURIDAD PRIVADA

ALARMAS

GPS

CCTV

GUARDIAS

ESCOLTAS

CUSTODIA DE TRANSPORTE

SERVICIOS INTEGRALES DE SEGURIDAD

800 00 46728 / www.tecuidamos.mx

OFICINA C4 RIVIERA / +52 229 193 5519

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

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

RIESGO CIBERNÉTICO: ¿UN RIESGO OCULTO EN LA DINÁMICA SOCIAL?

Una nueva evolución del riesgo cibernético podría estarse gestando de forma velada en medio de la dinámica del mundo actual

COLOMBIA
Jeimy Cano

Foto: Freepick

Los eventos internacionales y las noticias alrededor de los ataques cibernéticos y sus impactos parece generar un efecto amplificador del riesgo cibernético que permite tanto a la sociedad como a las organizaciones mantener un nivel de atención importante sobre la dinámica de este riesgo y la relevancia del mismo para el desarrollo de sus negocios.

Considerando los elementos de amplificación del riesgo como son (Kasperson *et al.*, 1988):

- Filtrado de señales (sólo se procesa una fracción de toda la información entrante).
- Decodificación y reformulación de las señales.
- Procesamiento de la información sobre riesgos (por ejemplo, inferencias); atribución de valores sociales a la información como base para extraer implicaciones para la gestión y la política.
- El cambio de comportamiento de individuos e instituciones.

Éstos establecen la base sobre la cual las comunicaciones que alrededor de los ciberataques se generan a nivel internacional, para mantener una tensión consistente y concreta sobre la importancia que se le debe dar a dichos eventos.

No obstante, pueden existir ciertos eventos que los especialistas pueden estimar de bajo impacto y ganar toda la atención de la sociedad, y viceversa, aquellos que los expertos establecen con graves consecuencias, y la dinámica social le ofrece menos atención.

En este sentido, es posible que eventos de interés particularmente en el escenario cibernético se puedan estar atenuando y creando una zona de opacidad e inestabilidad que pueda sorprender tanto a las organizaciones como los Estados, en la gestión y atención del riesgo cibernético. Basado en lo anterior, los académicos Kasperson (Kasperson & Kasperson, 1991) establecen los fundamentos de los "riesgos ocultos" como aquellos con una extrema atenuación de ciertos sucesos de riesgo, de modo que, a pesar de sus graves consecuencias para los causantes del riesgo y la sociedad en general, pasan prácticamente desapercibidos y desatendidos, y a menudo siguen aumentando sus efectos hasta alcanzar proporciones de catástrofe.

Estos riesgos ocultos terminan configurando sorpresas predecibles (Bazerman & Watkins, 2004) que son aquellas donde:

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

Las cuales crean crisis institucionales o nacionales cuando dichos riesgos se materializan, y las organizaciones y Estados sólo reaccionan, sabiendo que se pudo haber anticipado o preparado considerando la información y detalles sobre las tendencias, señales débiles, anomalías o inciertos propios de la dinámica de su negocio o del contexto de la nación.

TIPOS DE PELIGRO

Los Kasperson (1991) establecen cinco elementos que impulsan la atenuación de los riesgos, los cuales se detallan a continuación:

1) **Los peligros elusivos globales** implican una serie de problemas complejos (interacciones regionales, acumulación lenta, largos desfases temporales, efectos difusos). Su incidencia en un mundo políticamente fragmentado y desigual tiende a silenciar su poder de señalización en muchas sociedades.
2) **Los peligros ideológicos** permanecen ocultos sobre todo porque están integrados en una red social de valores y supuestos que atenúa las consecuencias, eleva los beneficios asociados o idealiza ciertas creencias.
3) **Los peligros marginales** afectan a las personas que ocupan los bordes de las culturas, sociedades o economías, donde están expuestas a peligros alejados y ocultos por los que se encuentran en el centro o en la corriente dominante. Muchos de los que se encuentran en estas situaciones marginales ya están debilitados o son muy vulnerables, mientras que disfrutan de un acceso limitado a los derechos y pocos medios alternativos para hacer frente a la situación.
4) **Los peligros amplificados** tienen efectos que eluden los tipos convencionales de evaluación de riesgos y análisis de impacto ambiental, por lo que a menudo se permite que sus consecuencias secundarias crezcan antes de que se produzca una intervención social.
5) **Y, por último, los peligros que amenazan los valores** alteran las instituciones humanas, los estilos de vida y los valores básicos, pero como el ritmo del cambio tecnológico supera la capacidad de respuesta y adaptación de las instituciones sociales, la falta de armonía en los propósitos, la voluntad política y los esfuerzos dirigidos impiden respuestas eficaces y los peligros crecen.

Basado en esta propuesta conceptual una nueva evolución del riesgo cibernético podría estarse gestando de forma velada en medio de la dinámica del mundo actual. Una posible lectura de este avance se detalla a reglón seguido por cada uno de los elementos mencionados previamente:

- **Peligros elusivos globales.** En un mundo fragmentado, desigual y polarizado la dinámica digital de las naciones crea entornos con microcomunidades, tribus y necesidades de comunicación que se traducen en movimientos activistas digitalmente correctos (asociados con demandas legítimas de las personas) e incorrectos (con acciones de hecho afectando las infraestructuras tecnológicas) que tienen la capacidad de crear inestabilidad e incierto por cuenta de acciones coordinadas que afecten no sólo a empresas, sino a naciones. Estos grupos son un escenario natural para potenciar acciones de intereses nacionales o de operaciones cognitivas de otros Estados para crear escenarios inéditos poco perceptibles y eficaces en el tiempo, que pueden terminar con la implosión de un país.
- **Peligros ideológicos.** En línea con lo anterior, la expansión del poder político y el uso de las redes sociales como medio de conexión ágil y eficiente, confirma una manera de comunicar y fortalecer una posición, que mantiene un imaginario que da cuenta de la agenda de un mandatario, disminuyendo aquellos eventos que puedan oscurecer su postura frente a las personas. La persuasión y amplificación de mensajes usando *influencers* o mecanismos como *bots* (ahora potenciados con inteligencia artificial generativa) crea un espectro de expansión y control que puede pasar desapercibido con efectos adversos a largo plazo.
- **Peligros marginales.** El discurso de los "nadies", de "los que no tienen voz", del "pueblo" ahora situado a través del uso de tecnologías móviles y exacerbado por las dinámicas sociales, crea mayores fisuras y menos escenarios de conciliación. Por tanto, los mensajes no harán énfasis en el 80% que ha tenido y logrado beneficios, sino en el 20% que no logró recibir los beneficios, estableciendo y profundizando el concepto de los "ricos" y "pobres" que crea división y establece una ruta asistencialista que marca la agenda de las naciones en vía de desarrollo, y debilita el aparato productivo de los países en el largo plazo.
- **Peligros amplificados.** Las noticias más relevantes sobre los ciberataques hacen énfasis en las técnicas, tácticas y procedimientos de los atacantes, creando una sensación de especialidad y complejidad que genera un "estatus" a los adversarios, ocultando la dinámica real alrededor de sus prácticas internas que los hacen más efectivos, como son el compartir, el experimentar, el probar y tomar riesgos para lograr sus objetivos. De esta forma, se crea un imaginario en los analistas que busca equiparar sus competencias con su adversario y seguir la vía tradicional de la gestión de riesgos, en lugar de concretar escenarios no convencionales que trate de sorprenderlos en su propio terreno creando mayor incierto en sus acciones y obligándolos a revisar su propio análisis de riesgo.
- **Peligros que amenazan los valores.** Los ciberataques cada vez más van a generar situaciones que amplifiquen las tensiones y los miedos tanto en las personas como las organizaciones y las naciones. La connotación de un estado sitio cibernético o la experiencia de un estado de excepción por crisis cibernética, estarán planteadas por los adversarios. De esta forma, debilitar la institucionalidad y la capacidad de protección del Estado a sus conciudadanos, tendrá una profunda huella en los imaginarios humanos y por tanto, la sensación de indefensión será una nueva estrategia para degradar y comprometer la experiencia social de las naciones y las organizaciones.

Estas posibilidades advierten de una rápida evolución del riesgo cibernético ahora situado y desarrollado en la dinámica social, como un elemento que articula agendas políticas, sociales y económicas, que apalancado en una mayor democratización tecnológica de iniciativas digitales y estrategias de desinformación, logra pasar desapercibido en los más detallados análisis de riesgos, los cuales sitúan este riesgo en la esfera tecnológica exclusivamente, ignorando su esencia sistémica que genera efectos inesperados por su alto acoplamiento con las dinámicas sociales y activa interacción a través de dispositivos tecnológicos.

En este contexto, el riesgo cibernético se advierte como un riesgo oculto, que maximizando su visibilidad sensacionalista de los efectos en las infraestructuras, logra mimetizarse rápidamente en medio de los escenarios sociales, políticos y económicos, para pasar desapercibido y crear condiciones de inestabilidad, incierto y caos, que terminen atribuidas a eventos conocidos y naturales de la sociedad, cuando desde la perspectiva cibernética son otras las dinámicas y las agendas que se plantean para crear los contextos de incertidumbre y ambigüedad que terminan afectando la forma como las personas perciben y entienden la realidad.

Si las organizaciones y naciones mantienen su foco de atención al riesgo cibernético sólo en sus efectos tecnológicos, es probable que no tengan margen en el futuro para defender la institucionalidad y gobernabilidad de sus propios dominios de operación, pues estarán completamente infiltrados y manejados por agendas que se han instalado de forma silenciosa y eficiente, donde un tercero ha logrado su misión y prepara la puesta en marcha de la siguiente parte de su plan: confundir al propio objetivo y reafirmar la apuesta de una sociedad con una lectura influenciada y manipulada, y así, perpetuar su influencia en el discurso e imaginario social.

Defender la integridad cognitiva de la sociedad deberá ser un nuevo imperativo digital. Este debe ser abordado con precisión quirúrgica, vocación democrática y estrategias de defensa híbrida para motivar las transformaciones sociales y la innovación empresarial que habilite la prosperidad social y económica de las naciones que ahora hacen parte de la economía digital global. ■

Referencias:

- *Bazerman, M. & Watkins, M. (2004). Predictable surprises. The disasters you should have seen coming and how to prevent them. Boston, MA. USA: Harvard Business School Press.*
- *Kasperson, R. E. & Kasperson, J. X. (1991). Hidden hazards. En D. G. Mayo & R. D. Hollander (eds.) Acceptable Evidence: Science and Values in Risk Management. New York: Oxford University Press, pp. 9-28.*
- *Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. & Ratick, S. (1988). The Social Amplification of Risk: A Conceptual Framework. Risk Analysis, 8(2), 177–187. doi:10.1111/j.1539-6924.1988.tb01168.x*

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:*

¿QUÉ ES LA CIBERCRIMINOLOGÍA?

"La cibercriminología es la ciencia que busca estudiar las causas, factores y escenarios que permiten la materialización del cibercrimen o los delitos informáticos", Dr. Kyung-Shick Choi

MÉXICO | **Julio César García Luna**

Foto: Freepick

En la historia del desarrollo científico, los teóricos y prácticos suelen tener profundas discrepancias en aspectos básicos, que van desde la terminología, el glosario, el campo de acción y hasta los conductos morales de las ciencias a desarrollar. Este dilema suele intensificarse cuando un área de estudio requiere de la intervención de especialistas en materias distantes, lo que hace aún más complejo un consenso interdisciplinario.

Es en esta circunstancia donde la Cibercriminología encuentra un escenario similar, al existir aún discrepancias sobre sus definiciones más populares y las nuevas propuestas conceptuales que surgen con cada especialista que busca desarrollar su propio concepto. Teniendo igualmente la mencionada característica, de una intervención de áreas tan divergentes como las ingenierías, la Informática, el Derecho, la Psicología, la Sociología de forma complementaria; y la propia Criminología, siendo esta última la base epistemológica y su especialización donde nace la Cibercriminología.

La Cibercriminología ya cuenta con algunas propuestas de definiciones, como la que señala Abel González (2012) en la descripción de la asignatura por la universidad de UDIMA: "La Cibercriminología es una parte de la Criminología que tiene como objeto el estudio de la delincuencia y la conducta antisocial en el ciberespacio y sus implicaciones en el espacio real".

En un tenor similar el Dr. Daniel Peña Labrin afirma que: "La Cibercriminología es una ciencia multidisciplinaria encargada del estudio del crimen, su origen, causas y la prevención del delito a través de medios informáticos".

Si bien estas definiciones propuestas por sus autores pueden emplear términos distintos, así como objetos de estudio; existe una coincidencia estructural sobre el espacio de interés para los investigadores. También se puede observar que, aunque no existe una coincidencia mayoritaria sobre la aproximación disciplinar, tampoco se consideran aspectos que se refuten entre ellos.

Finalmente revisemos la definición propuesta por el Dr. Kyung-Shick Choi (2017), quien es considerado una de las principales autoridades de Cibercriminología a nivel mundial, quien la identifica como: "La ciencia que busca estudiar las causas, factores y escenarios que permiten la materialización del cibercrimen o los delitos informáticos. De esta manera el fin que persigue la cibercriminología es prevenir los delitos que se cometen en el ciberespacio o con acción de las tecnologías de la información y la comunicación".

En este punto es importante mencionar que existen otros autores que consideran el término de "Cibercriminología" como inexacto o insuficiente para el estudio de la cibercriminalidad y se han inclinado por plantear términos como "Criminología Informática", "Criminología *Cyborg*", "Criminología de las TIC's" o "Criminología Tecnológica", si bien se respeta cada una de estas sugerencias, el autor del presente artículo sostiene que Cibercriminología es la concepción adecuada, ya que la derivación de ciberespacio, el cual emana directamente de la ciencia de la "cibernética" por consiguiente, el estudio de los sistemas de control y comunicación basados en retroalimentación.

Con el debido contexto presentado, también se planteará una definición basada en el conocimiento y experiencia propio como investigador en Cibercriminología: "La Cibercriminología es el área de especialización de la Criminología, que estudia en un enfoque tripartito al cibercrimen, el cibercriminal y la cibercriminalidad, en sus diversas modalidades y áreas de acción. Con el propósito de identificar, diagnosticar, prevenir, intervenir y disminuir las incidencias dentro o a través del ciberespacio".

Si bien esta propuesta puede encontrar similitudes con los ejemplos ya mencionados, se hace énfasis en aquellos elementos que se consideran más pertinentes para el conocimiento público, ya que los objetivos del estudio cibercriminológico se aclaran, así como quedan cubiertos en su campo de acción, estableciendo que los cibercrímenes pueden tener como fin o como medio al ciberespacio. Finalmente, los verbos de acción se mencionan hacía el interés primario de reducir la altísima cantidad de víctimas que se generan diariamente, ya sea a través de la prevención o directamente hacía la intervención.

No obstante, el propósito del artículo abarca mucho más allá de comparar definiciones y proponer otra más al abanico de opciones que ya están disponibles. También se busca, ofrecer una idea concreta sobre la utilidad y contribuciones que la Cibercriminología realiza para impactar positivamente en la seguridad en línea y a través de dispositivos digitales.

PRINCIPALES DIFERENCIAS CON LAS ÁREAS TRADICIONALES

A diferencia de las áreas tradicionales asociadas a la ciberseguridad, la Cibercriminología ofrece algunas ventajas proporcionando conocimientos innovadores y generando nuevas metodologías que en conjunto arrojen mejores resultados, entre las que se encuentran:

- **Perfilación del cibercriminal:** Uno de los mayores provechos que pueden obtenerse del cibercriminólogo, es su capacidad metodológica en la realización de perfiles. En este contexto extendidos al ciberespacio.
- **Estudio de las subculturas criminales:** En la misma tesitura del análisis del cibercriminal, se pueden realizar análisis a una diferente escala; ahora enfocándose en los grupos cibercriminales y su comportamiento
- **Identificación de la criminalidad en el plano físico y digital:** El conocimiento de la criminalidad en el mundo físico es vital en el estudio de la cibercriminalidad, en consideración que existen agrupaciones que han transicionado de la delincuencia clásica hacia las nuevas opciones que ofrecen las TICs.
- **Predicción y prevención a través del comportamiento:** A partir de la perfilación del cibercriminal, también se pueden realizar predicciones basadas en probabilidad y en el comportamiento de éstos, con el propósito de tomar medidas que impidan o disminuyan el impacto de un ciberataque.

CONCLUSIONES

Es de esta forma en como la Cibercriminología puede realizar invaluables contribuciones en la prevención de potenciales víctimas en el ciberespacio, así como precisar que los objetivos profesionales de sus especialistas no buscan sustituir a otros trabajadores en el sector, sino que se buscan crear sólidos equipos de trabajo multidisciplinarios que generen resultados más completos y de alcances que de manera individual no se podrían obtener. ■

Julio César García Luna, criminólogo e investigador en Cibercriminología bajo el seudónimo "*Meibomius Livrea*", conferencista y capacitador en temas de prevención de la cibercriminalidad.
Más sobre el autor:

CIBERSEGURIDAD EN TELETRABAJO

Retos, amenazas y riesgos derivados de la nueva realidad del trabajo desde casa

Foto: Freepick

MÉXICO

Luis Fernando Heimpel Boyoli

"El hardware es fácil de proteger: encerrarlo en una habitación, encadenarlo a un escritorio o comprar uno de repuesto. La información plantea más un problema. Puede existir en más de un lugar; ser transportado a la mitad del planeta en segundos; y ser robado sin su conocimiento", Bruce Schneier

El confinamiento y la imposibilidad de poder asistir de manera presencial a muchas actividades como las laborales y educativas durante la pasada pandemia nos dejaron como secuela un importante uso de las tecnologías de la información y las comunicaciones, de modo que no solamente podemos trabajar sino también adquirir mercancías y estudiar desde la comodidad de nuestra casa o simplemente asistir a un café en el que tengamos acceso libre y gratuito a Internet para poder disfrutar nuestra bebida favorita y terminar los pendientes de la oficina del día anterior.

Si bien estas herramientas generan una flexibilidad impresionante permitiendo a las personas ahora comunicarse sin necesidad de desplazarse o encontrarse todas en el mismo lugar, también plantean una serie de retos interesantes que van más allá de la simple negociación entre patrón y empleado sobre el pago tanto del servicio de Internet como de la energía eléctrica que se consume al estar trabajando desde casa, comenzando por el hecho de que estamos permitiendo que información confidencial o sensible salga de la empresa y se procese en equipos de cómputo que en muchas ocasiones no tenemos la menor idea de cómo están configurados.

Poder comprar productos y servicios sin salir de casa e inclusive recibirlos en algunas horas o minutos en la comodidad de nuestro hogar, el contar con la flexibilidad de poder estudiar en el tiempo y forma que mejor nos acomode o que se ajuste a nuestras otras actividades como el trabajo o responsabilidades del hogar, son herramientas que se impulsaron mucho y nos brindan algunas comodidades con ciertos riesgos menores como el uso de nuestra tarjeta de crédito y la información personal que damos a los proveedores para que puedan brindarnos el servicio o entregar el producto adquirido.

Pero, ¿resulta el mismo beneficio a un riesgo tan bajo el ocupar a las personas en casa para trabajar y permitir que tengan información de la empresa? La respuesta no es simple ni se puede tomar a la ligera, se han utilizado ya varias alternativas para garantizar la configuración correcta del equipo como el que la empresa provea el mismo al empleado, además forzando a que la información "vuelva" a la empresa cuando el empleado deje de laborar ahí o sea reemplazado el equipo por uno de mejor desempeño; pero no podemos estar seguros de que este tipo de iniciativas serán suficientes para garantizar la seguridad de nuestra información como empresa, ni la seguridad de nuestros empleados.

RECOMENDACIONES

Una regla no escrita en la seguridad informática es que la gran mayoría de los ataques que se logran concretar en contra de cualquier tipo de organismo (hablamos de un 75% aproximadamente y en promedio) tienen éxito derivado del factor humano, ya sea utilizando técnicas de ingeniería social o simplemente pidiendo las cosas "por favor", muchas empresas han visto transgredidos los sistemas de seguridad más complejos y en capas que se han instalado, manteniendo todavía la concientización del personal como el tema más importante de la estrategia de seguridad informática para las organizaciones.

Foto: Freepick

Si bien cuando nos encontrábamos todos en un ambiente presencial resultaba complejo lograr capacitar y mantener actualizado al personal en temas de seguridad de la información, con el trabajo en casa se incrementó exponencialmente la situación derivado de la imposibilidad de reunir al personal o garantizar que todas las personas involucradas tomen la capacitación, porque ¿quién nos garantiza que el empleado no está prestando la computadora a sus hijos para tomar la clase o hacer la tarea? Y cada persona que tenga acceso al equipo puede poner en riesgo la información que se encuentra ahí, terminando por ampliar el problema y los requerimientos de capacitación inclusive fuera del alcance y recursos de la propia empresa, la pregunta es si esto es realmente necesario y desde mi opinión sí, al menos en hacerle saber y conocer al empleado que no puede prestar el equipo de cómputo a un tercero.

El utilizar una plataforma de enseñanza virtual pudiera solucionar en parte el problema al entregar el contenido de los cursos de capacitación a cualquier persona que requiera recibirla incluyendo a los familiares de los empleados, cubriendo así en mejor medida varios de los puntos de riesgo que se tienen ya sea con el propio empleado o su familia inmediata quienes podrían tener acceso al equipo, además de garantizar la disponibilidad de acceso al material por lo menos dos veces al año para mantenerse actualizado; es responsabilidad de la empresa mantener dicho material y conocimientos actualizados, de modo que al tomarlo la segunda ocasión en el año pueda ver el empleado realmente alguna actualización y contenido nuevo que le confirme la necesidad de volver a tomar el curso.

Adicionalmente este tipo de alternativa nos permitirá generar capacitación para la instalación y configuración de otros niveles de protección y seguridad en los equipos que no sean propiedad de la empresa, incluyendo la eliminación correcta de la información a la que se hubiera tenido acceso una vez que el equipo ya no sea destinado para el uso de trabajo o se retire al empleado del servicio, pudiendo inclusive instalar algún tipo de *software* que nos permita remover todas las licencias y la información que corresponden a la empresa.

Es también recomendable el contemplar la instalación de *software* especializado para proteger el equipo de infecciones de virus y otro tipo de *malware* que pueda dañar no solamente el sistema operativo y los programas, sino también comprometer la información de la empresa y la propia infraestructura de la misma, al generarse un foco de infección que pudiera llegar a contaminar a otros empleados o inclusive los centros de datos de la empresa. Si los equipos son propiedad de la empresa se pueden instalar antes de entregarla al empleado, pero si el empleado utilizará su propio equipo se debe considerar poner a disposición una capacitación para poder instalar y configurar dichos programas en su computadora.

Por último, es necesario que se contemple dentro de las capas de seguridad para proteger a la empresa, tanto la comunicación con ella desde la casa del empleado como el acceso a los centros de datos y el equipo de procesamiento y almacenamiento que ahí se encuentra, siempre privilegiando el habilitar al negocio para no detener o mermar la operación pero cuidando de que la seguridad sea la necesaria para poder mantener la información de la empresa segura y disponible para habilitar a las áreas de negocio.

Me permito respetuosamente recordarles que las infecciones que mayor número de víctimas han tenido en cuestión de seguridad electrónica han sido por instalación directa del usuario al abrir archivos comprimidos o supuestas fotografías o videos de contenido regularmente sexual supuestamente, y que terminaron por no mostrar lo que el usuario esperaba observar u obtener y por el contrario tomaron control de su equipo o información e hicieron modificaciones o eliminaciones no deseadas que en muchos casos causaron costos graves a las empresas que los padecieron.

Asegurar el canal de comunicación finalmente se puede concretar con la instalación de un *Firewall* y un posible túnel en el que la comunicación se encripte (hay varias opciones en el mercado que ofrecen el túnel ya incluido o por un pago adicional de licencia del *software*, pero existe la posibilidad con el propio equipo) y evite así vigilancia no deseada en sus comunicaciones, además de evitar que un visitante no deseado pueda hacerse de direcciones de sus servidores o almacenamiento interno para que no pueda obtener información de la empresa sin previo consentimiento.

Finalmente mencionar que el proporcionar equipos a los empleados pone un reto al levantamiento de inventario, esto se puede solventar con la instalación de *software* que nos permita la toma de inventarios de manera remota y directamente sobre los equipos, apoyando al área técnica en conocer el estado y modificaciones hechas al equipo, sin tener que visitar al empleado o interrumpir sus labores o descansos para poder conocer el estado del equipo y garantizar su buen funcionamiento; algunas de estas soluciones inclusive contienen una forma de acceder de manera remota al equipo para poder darle soporte al usuario, lo que simplifica el trabajo de las áreas de tecnología y soporte técnico en particular. ■

Luis Fernando Heimpel Boyoli,
propietario de Comercializadora PIEC (Proveedora Integral de Equipos y Consumibles). *Más sobre el autor:*

GORAT SEGURIDAD: EMPRESA 100% MEXICANA

Conformada por un grupo de especialistas con más de 35 años de experiencia al servicio de nuestro país en diferentes áreas operativas y estratégicas de la Marina Armada, Ejército, Fuerza Aérea y Policía Federal

MÉXICO

GORAT surge hace diez años con la firme idea de crear una corporación con los más altos estándares de calidad para proporcionar herramientas efectivas y medibles que se adapten a las necesidades de cada situación. Nuestras operaciones comenzaron en la ciudad de Coatzacoalcos, Veracruz, siendo integrada en ese momento por diez elementos operativos.

Para el año 2022, esperamos alcanzar la cifra de mil colaboradores directos en las distintas áreas que conforman el grupo, manteniendo la dinámica de desarrollo profesional de nuestro personal, invirtiendo en su capacitación integral y proporcionando los mejores salarios del mercado.

FORMACIÓN PROFESIONAL

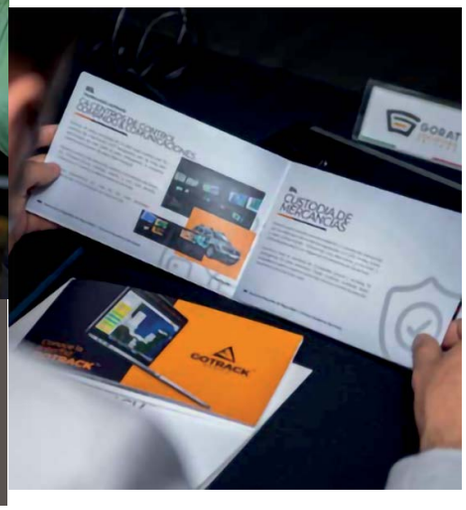
Con la más exigente y alta formación profesional, nuestros mandos operativos mantienen siempre presente, la responsabilidad de proporcionar servicios y productos de calidad en cualquier lugar y momento, con la misma lealtad, honor y disciplina con que se desempeñaron en su trayectoria en el activo.

En GORAT nos esforzamos todos los días por mantener los más áltos estándares de calidad, así como en cumplir con toda la reglamentación de nuestro sector, por lo que estamos debidamente registrados ante las autoridades estatales y federales, cumpliendo con todos los permisos necesarios de operación, certificaciones nacionales e internacionales en constante actualización.

La profesionalización del sector y la implementación de las mejores prácticas comerciales es un imperativo en nuestra organización, es por ello que con mucho orgullo estamos afiliados a la Asociación Mexicana de Empresas de Seguridad Privada, A.C. (AMESP), misma que agrupa a las 245 empresas más importantes, capaces y cumplidas del sector a nivel nacional e internacional, lo que representa un sello de calidad y tranquilidad para los clientes.

En GORAT contamos con varias divisiones operativas para proporcionar un servicio integral 360°, entre los cuales destacan:

Nuestro principal diferenciador es la atención personalizada que se brinda a cada uno de los prospectos y clientes, con procesos bien definidos, sistemas de gestión de calidad y una capacidad de respuesta inmediata que no tiene competencia



En GORAT nos esforzamos todos los días por mantener los más altos estándares de calidad, así como en cumplir con toda la reglamentación de nuestro sector, por lo que estamos debidamente registrados ante las autoridades estatales y federales

GORAT PROTECT:
- Guardias intramuros.
- Oficiales de custodia carretera.
- Oficiales de protección ejecutiva.
- Oficiales para control de accesos.
- Centros de control, comando y comunicación.
- Análisis y gestión de riesgo.
- Batallón de patrullas para vigilancia.
- Custodia de mercancías.
- Binomios caninos.
- Vigilancia aérea no tripulada.
- Transportación ejecutiva blindada y convencional.

GOTRACK:
- Sistemas de videovigilancia de última generación.
- Sistemas de geolocalización para personas, bienes y vehículos de todo tipo.
- Controles biométricos de acceso.
- Sistemas de radiocomunicación encriptada.

GORAT 911:
- Ambulancias de terapia intensiva 24/7 para prestar servicios al público en general.
- Agrupamiento potros de paramédicos motorizados.
- Agrupamiento de rescate carretero.
- Contención de crisis, emergencias, desastres naturales y primeros respondientes.

GORATRAINING:
- Capacitación en distintos niveles para el manejo de armas de fuego.
- Capacitación en distintos niveles para el manejo defensivo táctico de vehículos convencionales y blindados.
- Capacitación en primeros auxilios y esquemas de protección.

Actualmente tenemos presencia en México, en las ciudades de Cancún (Quintana Roo), Coatzacoalcos (Veracruz), Villahermosa (Tabasco), Veracruz, Boca del Río y Xalapa (Veracruz), Ciudad de México, San Pedro Garza (Nuevo León) y la ciudad de Dallas, Texas, en Estados Unidos.

Nuestro principal diferenciador es la atención personalizada que se brinda a cada uno de los prospectos y clientes, con procesos bien definidos, sistemas de gestión de calidad y una capacidad de respuesta inmediata que no tiene competencia.

Si deseas una seguridad eficiente, de alto valor agregado, permítenos asesorarte para conseguir los mejores resultados. Nuestro equipo comercial está disponible 24 horas para atenderte.

GORAT es para todos, pero no para cualquiera, ya que contamos con un proceso de evaluación de nuestros clientes muy detallado, que nos permite mantener un estándar de calidad óptimo para sólo trabajar con los mejores.

Encuéntranos a través de nuestras diferentes formas de contacto y de inmediato te atenderemos. ■

Fuente y fotos: GORAT Seguridad

IFPO – ISRM, ALIANZA PARA LATINOAMÉRICA

Uniendo esfuerzos

VENEZUELA

Abraham Desantiago

Como presidente de ISRM Latam Chapter (Institute of Strategic Risk Management), estoy encantado de anunciar la emocionante asociación entre IFPO Hispanoamérica (Fundación Internacional para Oficiales de Protección) e ISRM Latam. El 28 de julio del presente año, estas dos estimadas organizaciones unieron sus fuerzas para fortalecer la formación en gestión de riesgos de seguridad y el desarrollo profesional de todos nuestros miembros.

Esta colaboración marca un hito importante hacia la creación de profesionales más seguros y capacitados. Con la experiencia combinada de IFPO e ISRM, los profesionales de LATAM pueden esperar recibir una formación en seguridad de primera categoría que cumpla las normas internacionales. La asociación no sólo mejorará la calidad de la formación en seguridad, sino que también ofrecerá amplias oportunidades de promoción profesional. Al ofrecer programas y certificaciones integrales, la IFPO y la ISRM pretenden dotar a las personas de las habilidades y los conocimientos necesarios para triunfar en diversos sectores.

Juntos, imaginamos un futuro en el que todos los profesionales de LATAM tengan acceso a una formación en seguridad de primer nivel que pueda impulsar sus carreras. Estamos entusiasmados con este esfuerzo de colaboración y esperamos tener un impacto positivo en la fuerza laboral de la región.

El ISRM Latam Chapter se lanzó en mayo de 2022 y celebró su evento *webinar* en diciembre de 2022 con Kevin Palacios, sobre los beneficios del ESRM. El ISRM es una organización de rápido crecimiento de manera global y esta alianza con IFPO es un ejemplo. ■

Abraham Desantiago, presidente de ISRM Latam Chapter Chairman.
Más sobre el autor:

ESPECIALISTAS EN

TRASLADOS VIP

Y PROTECCIÓN EJECUTIVA

NUESTROS SERVICIOS:

GRIPERS
ESPECIALISTAS EN
SEGURIDAD INTRAMUROS

AUDITORÍA Y
CONSULTORÍA

ANÁLISIS DE RIESGOS

ESTUDIOS
DE CONFIANZA

VIGILANCIA Y DETECCIÓN
DE VIGILANCIA Y CONTRAVIGILANCIA

CAPACITACIÓN EN
ARMAS DE FUEGO

grip®
global risk prevention

CONTÁCTANOS

55 1391 6570

comercial@grip.mx

SÍGUENOS EN REDES SOCIALES

www.grip.mx

RECONTEXTUALIZANDO LA POLIGRAFÍA

El polígrafo, una herramienta de evaluación técnica-científica de la credibilidad para el apoyo a la toma de decisiones

MÉXICO

Carlos Alberto Orozco Victoria y Rodolfo Prado

Foto: Freepick

Si se pidiera opinión a algunos miembros de la sociedad, empresas o medios de comunicación acerca de su percepción u opinión de lo que es una prueba poligráfica, muy probablemente se encontrarían opiniones favorables, pero se espera que una parte importante exprese sus dudas acerca de la precisión de los resultados que genera este tipo de prueba, o se cuestione el estilo de entrevista inquisitivo utilizado por los poligrafistas.

Como en cualquier profesión, las malas prácticas de evaluadores no actualizados, o que fueron certificados por instituciones apócrifas generan pruebas poligráficas en evidente desapego a los procedimientos validados, tanto en el trato de los evaluados, como en la aplicación de procedimientos.

Todo lo anterior influye significativamente en la opinión de la sociedad con respecto a la poligrafía.

El presente artículo pretende explicar el quehacer de la poligrafía desde la perspectiva de las mejores prácticas y con sustento en estudios recientes relacionados con técnicas poligráficas y sistemas de calificación validadas por la ciencia.

La evaluación para la Detección Psicofisiológica del Engaño (PDD, por sus siglas en inglés) es una prueba que se basa en la misma premisa básica de muchas pruebas conocida como Estímulo-Respuesta. El estímulo de la prueba es una pregunta que describe la conducta o comportamiento investigado y la respuesta son los cambios fisiológicos involuntarios correlacionados con este estímulo, estos cambios son registrados para poder ser analizados.

Ya que se busca consistencia en el tipo de respuestas obtenidas, los estímulos se presentan en múltiples ocasiones para obtener múltiples respuestas que se convierten en datos de prueba que finalmente serán convertidos en un puntaje que será comparado con un modelo de referencia probabilístico (Nelson, 2016). Un ejemplo sería medir y pesar a un niño en repetidas ocasiones para obtener datos que compararemos con un modelo estadístico (tabla) que permitirá conocer el estado de desarrollo del menor.

Aunque al polígrafo se le conoce como detector de mentiras, lo que realmente hace el instrumento es amplificar las reacciones fisiológicas del evaluado ante diferentes tipos de preguntas dentro de la misma prueba. Algunas de las preguntas son estímulos ante los que se sabe con certeza que la persona está hablando con la verdad (¿estamos en el año 2023?), preguntas en las que se sabe que está mintiendo y las preguntas relacionadas con el asunto bajo investigación. Estas preguntas permiten realizar una comparación *ipsativa*, lo que significa que se comparan las reacciones del individuo ante estos diferentes tipos de preguntas con el mismo evaluado.

La mentira no es algo que podamos ver, que tenga materia o peso, y es lo que se conoce como un fenómeno intangible. Como la mentira no puede ser medida u observada de manera directa, la poligrafía utiliza variables *"proxy"* (de manera similar a todas las pruebas que evalúan fenómenos intangibles como por ejemplo la inteligencia), las cuales tienen una relación estadística con lo que sucede en el organismo cuando un ser humano miente.

¿QUÉ REACCIONES FISIOLÓGICAS ESTÁN RELACIONADAS CON LA MENTIRA?

Los cambios en la actividad cardiaca como el volumen y presión sanguínea, cambios electrodérmicos provocados por la sudoración en la piel, y cambios en los músculos intercostales y diafragmáticos son ejemplos de respuestas fisiológicas relacionadas (correlacionadas) estadísticamente con la mentira o el engaño. Todos estos cambios están controlados por el sistema nervioso autónomo, es decir, la parte de nuestro organismo que no podemos controlar a voluntad.

Durante la prueba se conectan sensores que amplifican estos cambios fisiológicos y los presentan en forma de trazos de gráfica que el poligrafista podrá comparar en su fase de análisis.

Ateniéndonos a los conceptos de hipótesis, teorías y leyes científicas, la prueba poligráfica se considera una evaluación científica de la credibilidad porque sus procedimientos se basan en evidencia, se han replicado en diversas investigaciones y se ha encontrado consistencia en sus resultados. Raymon Nelson (2016) escribió que "la teoría analítica de la prueba poligráfica es, que los mayores cambios en la actividad fisiológica se cargan ante los diferentes tipos de estímulo de prueba en función del engaño y veracidad, en respuesta al estímulo relevante objetivo".

En resumen, se presentan diferentes estímulos durante la prueba que son las diferentes preguntas de prueba, se extraen los datos fisiológicos provocados por estos estímulos y a estas reacciones se les asignan puntajes numéricos. El puntaje final obtenido se compara finalmente con datos de referencia estadística (tablas) para ubicar al sujeto dentro de una clasificación en particular que podría ser de mentira o veracidad.

Las tablas de las que se hace mención, son una referencia de lo que en múltiples estudios se ha encontrado como puntajes típicos de las personas cuando dicen la verdad o cuando mienten. Esto significa que si el puntaje obtenido en la prueba se asemeja a los puntajes reportados por los estudios estadísticos previos, se reporta un resultado estadísticamente significativo de veracidad o mentira y se reportan además las probabilidades de veracidad o engaño según sea el caso. Antes de que se aplique una prueba poligráfica, las probabilidades de verdad

o engaño son como lanzar una moneda al aire, es decir 50/50, no hay certeza, después de una prueba, los puntajes estadísticos nos dan luz con respecto a las probabilidades posteriores.

Ninguna prueba científica es perfecta y por lo tanto no se espera que la poligrafía lo sea, pero proporciona resultados altamente precisos.

Una prueba poligráfica basada en evidencia (y en estándares Daubert), presenta un resultado solamente cuando la probabilidad de error es menor al 5% (alfa a .05), o cuando el nivel de confianza de ese resultado es de al menos el 95%.

Muchos evaluados, empresas y comunidad en general piensan que los resultados se ven seriamente afectados por el nivel de estrés o nerviosismo del entrevistado al tiempo de la prueba. La respuesta sencilla es que la prueba poligráfica no es un detector de nerviosismo y por lo tanto no busca variables relacionadas con el estrés. Aunado a lo anterior sabemos que mucha gente acostumbrada a mentir o engañar no se siente nerviosa y muchas personas honestas y veraces se sienten tensas.

El detonador psicológico de la mentira o el engaño no es el nerviosismo, es lo que se conoce como "carga cognitiva". Se asume que una persona que miente realiza un esfuerzo mental más intenso al crear y construir respuestas y una historia, en comparación con quien simplemente reporta un recuerdo.

De acuerdo con la Asociación Americana de Poligrafía (2011), las examinaciones poligráficas constan de tres fases: 1) entrevista de *pre-test,* 2) una fase *in-test* o de recolección de datos de prueba, y 3) análisis de datos de prueba.

En la fase de *pre-test* se le explica al evaluado el procedimiento que se llevará a cabo, se le explica qué sensores se utilizarán en la prueba y se detalla que ninguno genera daño al cuerpo. Se presenta de manera clara el propósito de la prueba y sólo entonces se pide la autorización por escrito para comenzar con la evaluación.

La entrevista sigue un procedimiento como entrevista semiestructurada que requiere el establecimiento de "rapport" que permita establecer una relación de trabajo para que el entrevistado pueda comentar toda la información que le permitirá obtener un buen resultado y a su vez que quien esté mintiendo genere un esfuerzo mayor al construir respuestas que tienen la intención de convencer al entrevistador de que lo que está diciendo es verdad. Dicho esfuerzo provocará mayores cambios en su actividad fisiológica involuntaria al tiempo de la prueba.

Cuando la entrevista utiliza un procedimiento coercitivo, intimidatorio o agresivo, el entrevistador y el ambiente incómodo de entrevista será la razón del por qué la persona presentará reacciones fisiológicas en la prueba y no por el proceso mental de estar mintiendo.

Un poligrafista-entrevistador eficiente, además de ser un receptor de información, cuestiona, genera retos y desafíos que permiten que el veraz otorgue toda la información que posee para liberar dudas de su mente y tener un buen resultado, pero esta misma estrategia provocará que un sujeto con intenciones de engaño incremente su esfuerzo mental y tenga un resultado no aprobatorio.

Dos ideas antiguas y sin fundamento que, por desgracia se siguen enseñando en las escuelas de criminología, son que "…los sospechosos casi nunca confiesan espontáneamente, sino prácticamente siempre en respuesta a la presión policial" (Leo, 2008, p. 162) y "las confesiones, especialmente de delitos graves, rara vez se hacen de forma espontánea. Más bien se obtiene activamente… normalmente tras una presión psicológica sostenida" (Leo, 2008, p. 162), estas ideas erróneas generan tres problemas: falsas confesiones de inocentes, reactancia entre los culpables y negación del delito.

Reportado por múltiples estudios, cualquier entrevista logra altos niveles de efectividad no cuando se presiona emocionalmente al entrevistado, sino cuando se realizan las siguientes actividades:

- Tener claro el objetivo y propósito de la entrevista.
- Analizar todas las pruebas e información disponible.
- Planear la entrevista.
- Ir de lo general a lo particular.
- Plantear retos y desafíos.
- Elementos de cooperación.
- Mostrar signos de escucha activa.

Otra idea errónea es que el poligrafista estará pendiente del lenguaje no verbal del entrevistado para obtener indicios de falta de veracidad. En un meta análisis realizado en 2020, Denault et al. encontraron que "…el uso de conceptos dudosos con respecto a la comunicación no verbal puede tener como resultado (i) fallos en la detección de amenazas reales y la identificación errónea de personas culpables como inocentes, (ii) identificar erróneamente a personas inocentes como culpables (iii) pérdida de tiempo", y este es sólo un ejemplo de conclusiones sobre los peligros de usar el lenguaje no verbal para la toma de decisiones.

En la fase 2 y 3 de la prueba poligráfica se recolectan los datos de prueba mediante instrumentos que se colocan en el cuerpo de la persona (por encima de su ropa) y que son registrados y grabados por un *software* que amplifica los cambios presentados ante la presentación de los estímulos (preguntas) de prueba. Como principio básico de la medición y la evaluación, se toman de tres a cinco muestras por cada pregunta de interés, con el objetivo de arrojar una conclusión o clasificación, y calcular y comunicar una estimación realista del nivel de confianza o margen de incertidumbre asociado con esa conclusión.

DOS USOS DE LA PRUEBA POLIGRÁFICA

En pruebas de investigación o de eventos conocidos ya sea por alguna evidencia (faltante de mercancía, por ejemplo) o por una denuncia o acusación directa, la prueba poligráfica indaga si la persona evaluada responde o no con la verdad con respecto a las conductas relacionadas con este evento (si lo robó, se quedó, dio información) que son conductas de participación directa o de participación secundaria (si ayudó, si se benefició del robo, etc.).

En pruebas de ingreso o de permanencia en una posición de trabajo, se analiza la posibilidad de ocurrencia de comportamientos no deseados en contextos laborales. Estudios de evaluación de riesgos consistentemente concluyen que la mejor manera de pronosticar conductas futuras es mediante la evaluación de conductas pasadas y por lo tanto las preguntas poligráficas describen conductas no deseadas por parte del sujeto examinado, adicción a drogas por ejemplo, o vinculación con grupos delictivos.

Las conductas de trabajo contraproducentes o *counterproductive work behaviour* (CWB, por sus siglas en inglés) son comportamientos voluntarios que dañan o afectan negativamente el bienestar de las organizaciones y/o personas en las organizaciones, estos comportamientos pueden ser recolectados y evaluados poligráficamente para que el solicitante pueda tomar una decisión sobre si contratar o no a los candidatos.

¿CÓMO SÉ SI UN POLIGRAFISTA ESTÁ CALIFICADO PARA TOMAR DECISIONES QUE PODRÍAN AFECTAR PERSONAS O INSTITUCIONES?

Perfil del poligrafista:

- Haber tomado entrenamiento básico presencial de al menos 400 horas con una escuela acreditada por APA (no en escuela nocturna, sabatina o en línea).
- Deberán cumplir con un mínimo de 30 horas de educación continua cada dos años, validada por APA.
- Preferentemente con formación universitaria.
- Que no realice presentaciones públicas en espectáculos que denigran la razón real de la prueba.

Examinaciones:

- Las pruebas no pueden durar menos de 90 minutos y con un promedio máximo de tres horas.
- No se deben aplicar más de cuatro preguntas de investigación por prueba.
- El poligrafista debe realizar máximo cinco exámenes en un día.
- Deberá realizar esfuerzos necesarios para determinar que el examinado es un candidato idóneo para la prueba poligráfica.
- Deberán utilizar instrumentación funcional que registre, por lo menos, dos patrones respiratorios, una actividad electrodérmica, una actividad cardiovascular y un sensor de actividad de asiento.
- El ambiente de evaluación deberá estar razonablemente libre de distracciones.
- Deberá obtener el consentimiento informado del examinado antes de la prueba.
- Deberá realizar prueba de familiarización a cada evaluado.
- Deberá utilizar técnicas de entrevista basadas en evidencia para obtener la mayor cantidad de información posible, así como avocar y detectar mentiras.
- Deberá revisar todas las preguntas de prueba antes de registrar las respuestas fisiológicas del examinado.
- Deberá utilizar técnicas poligráficas validadas y basadas en evidencia.
- Deberá tener disponible la grabación de audio y video de todas las fases del examen (siguiendo protocolos de confidencialidad).
- Deberá realizar la entrevista de manera no acusatoria.
- Deberá revisar minuciosamente los asuntos de interés para garantizar la comprensión del examinado antes de comenzar la prueba.
- En la sala de evaluación sólo debe estar presente el evaluado y el poligrafista. Se considera invalida la prueba en la que existan más de dos personas en la sala.
- No es válido desarrollar alguna de las etapas de la evaluación poligráfica en grupo, la evaluación poligráfica con todas sus fases es un proceso individual.

Emisión de resultados:

- Las conclusiones y opiniones del examinador deberán basarse en métodos de calificación y reglas de decisión validados.
- Deberá reportar tipo de técnica poligráfica, método de calificación utilizado, resultado y conclusiones que incluyan probabilidad de error de prueba.

Reporte del examinador:

- Deberá incluir ficha de identidad del examinado incluyendo fotografía.
- Deberá reportar propósito de prueba.
- Deberá presentar reporte de idoneidad médico/psicológica del evaluado al tiempo de la prueba.
- Deberá incluir toda la información obtenida durante la entrevista.
- Presentará todas las preguntas relevantes aplicadas al tiempo de la prueba.
- Resultados.
- Conclusiones que incluyan tipo de sistema de calificación utilizado, puntaje obtenido y probabilidad de error de prueba o nivel de confianza en el resultado.
- Calidad de la *Data* y Comportamiento del evaluado.

En conclusión, el polígrafo aplicado bajo los mejores estándares de práctica tiene entre sus múltiples ventajas, resultados con un alto porcentaje de precisión y obtención de información para coadyuvar a la toma de decisiones.

Aunque se le conoce popularmente como detector de mentiras, lo que realmente hace es amplificar las reacciones fisiológicas correlacionadas con la mentira, reacciones provocadas por la carga cognitiva y no por el nerviosismo o el estrés.

Las malas prácticas de poligrafistas no actualizados, que utilizan técnicas en desuso o acreditados por escuelas apócrifas, han dejado en mal el concepto de evaluación poligráfica y hace que un grupo importante de la población cuestione los resultados y la calidad de estos.

La poligrafía es un procedimiento técnico-científico que se apega a principios de validez, utiliza tecnología apropiada para registrar lo que se pretende registrar (actividad proxy correlacionada con la mentira), registra lo que dice que registra y pasa por procesos de control de calidad.

Por todo lo anterior se puede afirmar que la prueba poligráfica per se no detecta mentiras y no es funcional sin un poligrafista experto en técnicas de entrevista, que genere carga cognitiva, que se apegue a procedimientos validados, que utilice métodos de calificación y reglas de decisión validados. ■

Bibliografía:

- *B. Baker-Eck, R. Bull & D. Walsh. (2021). Investigative Empathy: Five Types of Cognitive Empathy in A Field Study of Investigative Interviews with Suspects of Sexual Offences. II:RP 11 (1) 27-37.*
- *Denault, et al. (2019). The analysis of nonverbal communication: The dangers of pseudoscience in security and justice contexts. Anuario de Psicología Jurídica, 30, (1) 12. https://doi.org/10.5093/apj2019a9*
- *Nelson, R. (2016). Teoría Científica (Analítica) de la Prueba Poligráfica. APA Magazine, 49 (5).*
- *Nelson, R (2018). Bases Científicas de la Examinación Poligráfica. APA Magazine. American Polygraph Association.*
- *Nelson, R. (2019) ¿Que mide el polígrafo? (en 600 palabras o menos). APA Magazine. American Polygraph Association*
- *Nelson et al. (2019). How To: A Step-by-Step Worksheet for the Multinomial ESS. Polygraph & Forensic Credibility Assessment. 48 (1) 72-74.*
- *R. Bull & R. Beker-Ec (2022). Effects of empathy and question types on suspects' provision of information in investigative interviews. International Journal of Police Science & Management 0 (0) 1-11.*

Carlos Alberto Orozco Victoria, director del área de Operaciones en International Polygraph Studies.
Más sobre el autor:

Rodolfo Prado Pelayo, CEO de International Polygraph Studies.
Más sobre el autor:

Tu seguridad, nuestra prioridad *con excelencia*

OSAO

Seguridad Electrónica

SERVICIOS OSAO

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

55 679 834 90

55 2430 8253

Info@osao.com.mx

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

LA TRANSICIÓN DE SERVICIOS ENTRE EMPRESAS DE SEGURIDAD (PARTE 1 DE 2)

Entrevista al Lic. Alejandro Liberman, CPP

Foto: Freepick

ARGENTINA

Ari Yacianci

Alejandro Liberman, CPP, es *partner* en SINDELARS SRL, una empresa pequeña que brinda servicios de seguridad privada con guardias en la Ciudad de Buenos Aires, Argentina. Tiene más de 100 guardias, y se especializan en servicios en edificios de vivienda y oficinas VIP.

Ari: Cuando se contratan los servicios de un proveedor de seguridad privada, frecuentemente el cliente ya contaba con otra empresa cubriendo el servicio. ¿Cómo suele ser esa transición?

Alejandro: Esas transiciones no son nada fáciles. En la empresa entrante surgen muchas dudas e imprevistos, el cliente normalmente resiste el cambio y las caras nuevas, y la empresa saliente suele "barrer cosas bajo la alfombra". Es la etapa de mayor fricción.

Ari: ¿Cómo podría mejorarse esto?

Alejandro: Es evidente que si ambas empresas de seguridad colaboraran varios días antes del cambio formal, se podría suavizar el traspaso. Pero durante ese período el cliente no quiere estar pagando a ambas empresas en simultáneo, ni la empresa entrante quiere pagarle esos días adicionales a sus vigilantes.

Si con anticipación se analizaran las particularidades del servicio, se conocieran a fondo las instalaciones del objetivo, y se escribieran los procedimientos, todo sería más fácil. Y si la empresa entrante pudiera hacer actividades con los diferentes habitantes del edificio, se podría reducir mucho la fricción con el cliente. Pero por lo general, la empresa saliente va a sentirse muy incómoda con esto.

Ari: Este es un tema del que se habla poco públicamente. ¿Por qué?

Alejandro: Porque significa que tanto la empresa saliente como la entrante hicieron algo mal y colaboraron a regañadientes. Nadie quiere ser "el maldito que sale" ni "el maldito que entra". No les gusta admitir que su empresa toma un servicio y le va mal porque se preparó poco, o demostrar que su empresa deja un servicio en malas condiciones por miserabilidad.

Ari: ¿Qué consecuencias tienen las malas transiciones?

Alejandro: Es muy habitual que, en los primeros días de trabajo, la empresa nueva se encuentre con faltantes, registros, listados, agenda de eventos o personas autorizadas, algunas herramientas de trabajo, claves de los sistemas, alguna llave… Esto produce tensiones con los interlocutores, ya sea en una empresa o habitantes de un condominio, porque normalmente tienen una expectativa de continuidad absoluta que a veces resulta irrealizable.

Alejandro Liberman, CPP, *partner* en SINDELARS SRL

Es muy habitual que, en los primeros días de trabajo, la empresa nueva se encuentre con faltantes, registros, listados, agenda de eventos o personas autorizadas, algunas herramientas de trabajo, claves de los sistemas, alguna llave, lo cual produce tensiones con los interlocutores

En algunos casos más difíciles, la empresa saliente manifiesta, a veces siendo cierto y a veces no, que debe retirar cosas de su propiedad afectadas al servicio. El cliente muchas veces lo desconoce, y si la conversación de transición no fue saludable, puede producir indisponibilidades inaceptables.

Ari: ¿Cuáles podrían ser algunos ejemplos de estas situaciones?

Alejandro: Estos son algunos ejemplos de la vida real.

- Una empresa se llevó los conos plásticos viales para ordenar la circulación interna, obligándonos a salir en el día a reemplazarlos, para mantener una "normalidad" y no parecer un servicio inferior al anterior.
- Un consorcio debió "comprar" un sistema de videoseguridad instalado por la empresa sin buena documentación, gastando dinero en una instalación obsoleta, con el fin de no quedarse sin capacidad de visualización de un día para el otro.
- Nosotros vendimos a un consorcio una TV utilizada para el monitoreo, se documentó su ingreso al servicio y se informó al condominio y a la empresa antes de realizar la transición, a manera de darles alternativas para que decidan qué hacer con ella.
- En una oportunidad, los guardias del servicio anterior, de los cuales ninguno realizaría la transición, al ver que nuestros guardias tomaban servicio de 12 horas antes del traspaso entre empresas, se retiraron del servicio varias horas antes del fin de turno y traspaso formal, ya que el servicio "se encontraba cubierto". Vale aclarar que decidieron facturar el servicio completo.

Ari: ¿Cómo se abordan los puestos de empleo de los guardias de seguridad durante las transiciones?

Alejandro: Es un asunto complejo. Entran en juego varios factores, como la continuidad de los puestos de trabajo. Si bien la empresa de seguridad no es una ONG, hay una intención de sostener el ingreso de las familias, cuando esto sea posible.

También hay que considerar la solicitud del cliente de mantener o dar continuidad a ciertos guardias del equipo. Eso en sí no es malo, pero requiere una consideración de parte de la empresa entrante respecto a las concesiones y riesgos asumidos, al incorporar una persona, reconocerle la antigüedad (riesgo laboralista) y mantener ciertos beneficios, que incluso quizás sean diferentes a los que tienen los guardias recién incorporados o incluso su estructura indirecta (supervisores, gerentes).

Ari: En el caso de que se sorteen esos desafíos, ¿qué más hay que tener en cuenta al incorporar personal de seguridad de otra empresa para el servicio?

Alejandro: El siguiente aspecto es el "*cultural fit*". La nueva empresa puede tener una forma de gestionar diferente a la que la precede, y el guardia incorporado por solicitud del cliente a veces se siente con cierto "poder" de establecer condiciones.

Si el vínculo se administra incorrectamente, ese guardia puede actuar como un agente de influencia negativa con personas relevantes de la organización. Del mismo modo, si el "cultural *fit*" se gestiona bien, se apreciarán la experiencia y capacidad de las personas históricas, pero también se fijarán condiciones y pautas claras de trabajo, por lo que habitualmente esos guardias serán agentes de difusión de las cualidades positivas que ha traído la nueva empresa.

En la parte 2 de esta entrevista, Alejandro nos comenta los desafíos relacionados con la renovación de los procedimientos y las tecnologías de seguridad durante las transiciones de servicios, y nos compartirá consejos prácticos para sortearlos. ■

Ari Yacianci, SRMP, profesional en gestión de riesgos y seguridad de Argentina. *Más sobre el autor:*

REUNIÓN DE ASIS CAPÍTULO PUEBLA-SURESTE

Desde el Casino Naval del Puerto de Veracruz y la Heroica Escuela Naval Militar

MÉXICO

El pasado 08 de junio, se llevó a cabo la Reunión de ASIS Capítulo Puebla-Sureste en el Casino Naval del Puerto de Veracruz, en el que los con 95 asistentes en total (en formato híbrido) disfrutaron de un desayuno típico del estado, para posteriormente escuchar dos conferencias muy interesantes sobre "Inteligencia de fuentes abiertas", a cargo de Noé Salvador Cuervo Carballo, director de Operaciones en DrCuervo Consultores, y "El poder marítimo de México en el ámbito hemisférico", con nuestro socio Iván Montiel, director general de NASS.

Dentro de los acuerdos realizados, se trabajará en conjunto con los socios de ASIS basados en Veracruz para crear una "Comunidad de Seguridad marítima" que apoye a los objetivos de sus actividades diarias dentro del sector.

MÁGICO RECORRIDO

Al término de la reunión, nos trasladamos a la Heroica Escuela Naval Militar, creada por decreto presidencial el 1° de julio de 1897 ubicada en el polígono naval de Anton Lizardo, Veracruz, con el propósito de formar oficiales líderes navales y futuros comandantes de la Armada de México.

Desde nuestra llegada fue mágico, mientras nos estacionábamos escuchábamos melodías en vivo, interpretadas por la banda de música de la H. Escuela Naval Militar, conformada por capitanes, oficiales, clases y marinería del servicio de músicos navales, mientras caminamos hacia la entrada principal del edificio de gobierno que alberga entre otras salas, la dirección de este heroico plantel, donde nos esperaba el C. Vicealmirante IM. DEM José Manuel Salinas Pérez, director de esta H. Escuela, para darnos la bienvenida e invitarnos a conocer las instalaciones.

En todo momento nos hicieron sentir únicos, cada uno de los invitados estábamos acompañados de un caballero y señorita cadete de quinto año, el último grado de sus estudios de las tres carreras que cursan en el plantel, que nos guiaron durante todo nuestro recorrido, detalle que lo hizo totalmente personalizado, ya que respondían las preguntas de interés de cada uno, brindándonos en todo momento un trato cálido y siempre con una sonrisa.

Así fuimos recorriendo algunos espacios de la H. Escuela Naval como el museo, donde pudimos apreciar la historia de nuestra armada mexicana, el paso del tiempo de los navíos que han forma-

"Tuvimos el honor de recibir de manos del director de la H. Escuela Naval Militar una pequeña réplica de la placa de este heroico plantel, que es un texto que define la mística del cadete naval, siendo una tradición que todo aquel que ingrese como cadete debe tenerla presente en su vida como cadete y en su futuro como oficial naval"

"Presenciamos el desfile militar que realizan como un acto de gallardía y disciplina para ingresar de manera marcial a los comedores de cadetes, algo que por más que quisiéramos explicar con palabras se quedaría corto con lo que te hace sentir, al presenciar esta actividad con cerca de 500 cadetes"

do parte de la flota naval de nuestro país, y un acervo ilimitado de la historia naval de México. Posteriormente visitamos la sala de banderas, siempre custodiada por un centinela en total posición de firmes y alerta con su arma M16, como símbolo de respeto por la patria.

REVISTA DE CADETES Y DESFILE MILITAR

Enseguida fuimos invitados al patio de honor, sitio estratégico de la Escuela, donde tuvimos la oportunidad de presenciar la revista de cadetes (que se hace tres veces por día antes de cada alimento) para verificar la presencia de todo el persona, así como la correcta portación del uniforme y aseo, con una parte de novedades de los cadetes más antiguos a cargo de sus compañías a los altos mandos directivos.

Enseguida presenciamos el desfile militar que realizan como un acto de gallardía y disciplina para ingresar de manera marcial a los comedores de cadetes, algo que por más que quisiéramos explicar con palabras se quedaría corto con lo que te hace sentir, al presenciar esta actividad con cerca de 500 cadetes (el número total de cadetes es de más de 900, pero el resto se encontraban en viajes de prácticas como complemento de sus estudios), quienes portaban su uniforme de faena color caqui en formación de sus compañías y que con gran gallardía desfilaban acompañados con marchas interpretadas por las bandas de guerra y de música de la Escuela Naval, el ambiente marcial se sentía en todas partes.

Claro que a todos los invitados que no tenemos educación militar / naval, todo esto se nos hace increíble y generaba más preguntas que respuestas que tienen que ver en casi todos los puntos con el orden, disciplina, constancia y respeto (a las personas, a los horarios, etc).

COMIDA Y ENTREGA DE RECONOCIMIENTO

Al término de la revista, nos invitaron a comer, donde también fue un espacio que nos hizo aprender a cada momento, la importancia del acomodo de mesas, donde cadetes de distintos grados comían (cabe

> *"Recibimos del director, una moneda conmemorativa que ente muchas cosas simboliza y representa la amistad, fraternidad y espiritualidad del que entrega para el que la recibe. Es una muestra de fraternidad y respeto y una tradición de las fuerzas armadas del mundo"*

mencionar que sólo tienen 20 minutos para esta actividad). Enseguida de los alimentos tuvimos el honor de recibir de manos del director de la H. Escuela Naval Militar una pequeña réplica de la placa de este heroico plantel, que es un texto que define la mística del cadete naval, siendo una tradición que todo aquel que ingrese como cadete debe tenerla presente en su vida como cadete y en su futuro como oficial naval, siendo menester aprenderla de memoria todos los que pasaron por esta Alma Máter (incluyendo a los que ya no están en activo).

Además, recibimos del director, una moneda conmemorativa que ente muchas cosas simboliza y representa la amistad, fraternidad y espiritualidad del que entrega para el que la recibe. Es una muestra de fraternidad y respeto y una tradición de las fuerzas armadas del mundo.

De la misma forma, ASIS Capítulo Puebla-Sureste, en manos de nuestro tesorero, Cap. Jesús Guerrero, nuestro vicepresidente ejecutivo, Héctor Romero, y nuestro socio Iván Montiel, le entregaron al director de la Heroica Escuela Naval un reconocimiento por permitirnos conocer las instalaciones de este gran plantel.

Al término de la comida, estuvimos un rato en la cafetería del cuerpo de cadetes (que debemos aceptar es muy bonita), donde pueden estudiar, tener un rato de esparcimiento si su rutina se los permite o simplemente tomarse un descanso.

Posteriormente a los simuladores de navegación marítima y de navegación aérea, aprendiendo un poco de su formación educativa, los idiomas obligados y mucho más que aprenden durante los cinco años que dura el programa para desempeñarse eficazmente en las unidades de superficie, aéreas, de infantería y cualquier posición estratégica donde deban cumplir su misión para servir a México.

No queríamos irnos, y la realidad es que la visita normalmente dura más de cinco horas para conocer cada espacio de la H. Escuela Naval, sin embargo, hasta el último momento fue por demás emotivo cuando al término estaba otra vez la banda de música para despedirnos con más melodías que hicieron nuevamente un cierre mágico.

Agradecemos a nuestros socios Iván Montiel y el Cap. Jesús Guerrero por haber gestionado esta gran visita, así como a Carlos Ponce y todo su equipo que estuvo en todo momento al pendiente de nosotros, realmente para los visitantes foráneos que acompañaron al capítulo en su evento, estamos seguros de que fue una experiencia inolvidable, además del invaluable apoyo del Cap. Corb. IM Miguel Ángel Ortiz Roux para coordinar lo necesario para nuestra participación. ■

Fuente y fotos: ASIS Capítulo Puebla-Sureste

¿Cómo hacer un análisis del contexto interno para sistemas de gestión?

Jorge Hutt
Auditor Internacional BASC

Desde la publicación en el año 2015 de las estructuras de alto nivel aplicadas a las normas internacionales de gestión, he intentado contribuir con las empresas para desarrollar un análisis concreto, funcional y práctico de los elementos o factores que comprende el análisis del contexto y que realmente aporte valor.

La metodología que propongo considera ***cinco*** dimensiones:

1- Recursos estratégicos.
En el análisis de esta dimensión, se propone que la organización considere los aspectos específicos en relación a su estrategia empresarial, tales como: ¿Es la empresa una empresa familiar? ¿La empresa cuenta con una junta directiva conformada por empleados, familiares, o es contratada externamente? ¿Cuenta la empresa con una planificación estratégica formal? ¿Cuenta la empresa con una misión, visión, valores y principios documentados? ¿Se despliega la estrategia y sus elementos? Estas y otras preguntas similares pueden fácilmente guiar la identificación de factores internos en esta dimensión.

2- Recursos humanos.
En esta dimensión se podría analizar la composición de su fuerza laboral, la diversidad los diferentes tipos de colaboradores, el conocimiento y las competencias críticas para el negocio, la transferencia de conocimientos, clima organizacional, beneficios laborales y similares.

3- Recursos tecnológicos.
En esta dimensión sugiero dividir el análisis en dos principales elementos: Tecnología y Manejo de la Información.

4- Recursos tangibles.
Se refiere a los elementos cuantificables y/o tangibles de la empresa tales como capital de trabajo, edificios, vehículos, activos, maquinaria e inventarios.

5- Recursos intangibles.
En esta dimensión de la empresa debe considerar los recursos que no sean claramente cuantificables tales como: competencias críticas, prestigio, influencia política y nivel de confianza desarrollada en el mercado.

Artículo completo en LINKEDIN

Una vez que la empresa, aplicando el análisis de las cinco dimensiones, ha identificado los factores de su contexto interno, sugiero establecer un método de priorización cuantitativo, basado en criterios claros, establecidos y documentados, para determinar la relevancia de estos elementos.

Alvaro Reyes

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE
OCCIDENTE DE MÉXICO

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

Socio Director,

Altair *Security*

Consulting & Training.

Más sobre el autor:

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

(SEGUNDA PARTE)

LATINOAMÉRICA

Realizar campañas permanentes apoyadas en los especialistas en comunicación, te podrá llevar por el camino de la construcción de una mentalidad de seguridad, que impregne en sus hábitos y como parte de su disciplina diaria

Continuando con nuestra entrega anterior sobre el apasionante tema de la Cultura de Seguridad y su implantación en las organizaciones, donde hablamos del papel fundamental del liderazgo, la importancia de una cultura de seguridad colectiva y la trascendencia de la educación y formación continua, expondré ahora el complemento de una de las rutas que se pueden seguir para lograr el éxito en este proyecto.

LA COMUNICACIÓN DE SEGURIDAD

Una estrategia de comunicación creativa, eficiente y efectiva, puede ser tan importante como la diferencia entre el éxito o el fracaso del proyecto. Si se llevan a cabo esfuerzos aislados, ayudará pero sin duda no será suficiente para permear una cultura de seguridad que permanezca en el tiempo. Realizar campañas permanentes apoyadas en los especialistas en comunicación, te podrá llevar por el camino de la construcción de una mentalidad de seguridad, que impregne en sus hábitos y como parte de su disciplina diaria.

La educación y formación que comenté en el número pasado será fundamental para lograrlo. Boletines, infografías y otros documentos, cursos y seminarios, lecciones aprendidas y casos de otras instituciones o sociedades que lo han logrado, que refuercen los conocimientos y alcances de seguridad a través de ideas claras y lenguaje sensible e inclusivo. A través de ello podrás actualizar a las personas sobre los nuevos retos de seguridad y cómo hacerles frente, recordando que los riesgos son dinámicos y así tienen que ser estrategias de seguridad, más en un mundo turbulento y con alta incertidumbre como al que nos estamos enfrentando. Hoy más que nunca hay que estar actualizados.

DETECCIÓN, REPORTE Y RETROALIMENTACIÓN EFICIENTE

Centremos el desarrollo en la motivación y el compromiso. Las métricas e indicadores de desempeño siempre serán fundamentales para evaluar el avance y la efectividad de las estrategias de seguridad, así también para hacer los ajustes necesarios. La detección temprana tiene sus frutos. La retroalimentación constante y constructiva, así como las medidas correctivas y ajustes necesarios que refuercen los comportamientos de seguridad. Un código de ética y conducta será imperativo como base de ello, ya que la práctica ética en las empresas es fundamental para su correcto desarrollo y para garantizar su crecimiento y éxito.

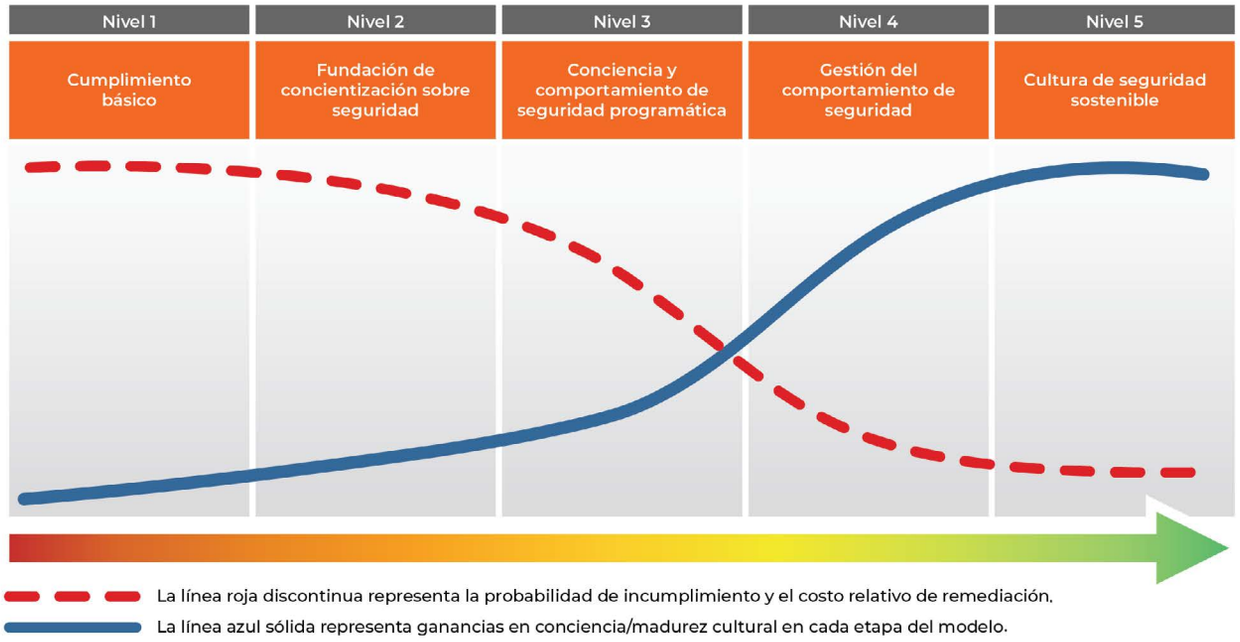
Considerando el principio que "nadie conoce mejor lo que sucede que quienes se encuentran donde sucede", sugerimos que la principal fuente de información requerida para prevenir los daños causados por prácticas faltas de ética de nuestros colaboradores, proveedores y/o clientes, sean por éstos mismos.

Además, siempre será importante tener una vía de desahogo para las personas. Implementar un eficiente proceso de reporte de amenazas, como vía de desfogue rendirá sus frutos. Sistemas de gestión de denuncias, las mediciones de *compliance* y auditoría, las campañas de simulacros de ataques y respuesta para medir la respuesta de los colaboradores, todo ello es de gran valía. Disponer de un servicio de correo electrónico, teléfono y/o página web a los cuales comunicarse las 24 horas del día los 365 días del año en caso de que los colaboradores quieran participar, será indispensable, así como garantizar el anonimato del participante y/o denunciante.

Considerando el principio que "nadie conoce mejor lo que sucede que quienes se encuentran donde sucede", sugerimos que la principal fuente de información requerida para prevenir los daños causados por prácticas faltas de ética de nuestros colaboradores, proveedores y/o clientes, sean por estos mismos

El modelo de madurez de la cultura de seguridad

El modelo de madurez de la cultura de seguridad basado en datos y evidencia, desarrollado por KnowBe4 Research, es el primer modelo de madurez de la industria específicamente diseñado para medir la cultura de seguridad. El modelo está impulsado por el enorme conjunto de datos culturales, de comportamiento y de concienciación sobre seguridad de KnowBe4.



Fuente: KnowBe4

EMPODERANDO A LOS EQUIPOS

Empoderar a las personas potenciará y acelerará los resultados en el proceso, por supuesto con el valioso apoyo y compromiso del C-Suite. Cuando a los colaboradores se les sensibiliza y se les concientiza de la importancia de mantener entornos seguros, se les enseña cómo hacerlo desde la prevención y de los beneficios que tiene para ellos mismos, sin duda derivará en acciones que ellos propongan para mejorar los sistemas y que sean sustentables en el tiempo.

Desde comenzar con los básicos de civilidad como el orden y la limpieza, la tolerancia y el respeto, la solidaridad y la honradez, guiarse con coherencia y responsabilidad agregará mucho valor al proyecto y permanecerá en el tiempo. Si ellos son quienes detectan las áreas de mejora y pueden evolucionar, resolverlas e incrementar los niveles de seguridad, fomentaremos un sentido de propiedad y responsabilidad.

Las acciones individuales tienen trascendencia social, pero sin duda los equipos unidos impulsan este cometido. Que ellos se involucren en los cambios y que vivan las mieles de los cambios. La seguridad en la compañía es fundamental y es responsabilidad compartida. Todos luchamos por mejorar y aprendemos de nuestros fracasos de equipo.

Como leerán, el cambio cultural es fundamental para cualquier transformación, ya que trata con los valores y la cultura de las personas. Al invertir en educación y estrategias bien orquestadas, las personas estarán tan comprometidas que serán siempre la mejor línea de prevención y defensa. Imaginen el poder de una mentalidad conciente de seguridad. El reto será nuestra capacidad de adaptación. Si requieres apoyo en ello no dudes en contactarnos. ■

¿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

TRUST GROUP

FESTEJA SU VIGÉSIMO ANIVERSARIO

MÉXICO

No existe una ruta exacta para alcanzar el éxito, pero sin duda hay complementos que abren camino como lo son la perseverancia, la disciplina y en el caso particular de Trust Group, su apuesta desde un inicio por la capacitación de calidad a sus integrantes

Una de las empresas de seguridad privada más reconocidas en el sector, suma ya veinte años de trayectoria brindando soluciones integrales de seguridad a personas, corporativos y gobierno.

Trust Group es un referente en el mercado como una empresa de calidad y confianza que cuenta con los permisos de la Secretaría de Seguridad y Protección Ciudadana, así como de la Secretaría de la Defensa Nacional en todas las modalidades para la portación de armas de fuego en todo el territorio nacional que establece su más alto compromiso con sus clientes brindando servicios de excelencia y manteniendo estrictos estándares de calidad, lo que les ha permitido llevar a cabo estrategias adecuadas y procesos operativos específicos y adecuados para cada uno de sus clientes, pues su experiencia les ha mostrado que no existe una solución única para cada segmento del mercado.

Hoy sus líderes reconocen que han sido años de constante labor, adaptación y sobre todo visión, lo que los ha proyectado y preparado para anunciar hoy en este importante aniversario número veinte, su expansión de servicios a través del relanzamiento de su empresa: **Incident Prevention and Response Private Security – IPR.**

Este hecho, permitirá ofrecer operaciones y servicios de alto impacto a clientes específicos que requieran este tipo de cobertura. Asimismo, **Incident Prevention and Response Private Security – IPR**, contará también con las licencias de portación de armamento en todas sus modalidades, siendo así la tercera empresa del grupo en contar con dichas licencias y de esta manera Trust Group se sigue adaptando a nuevos retos enriqueciendo y fortaleciendo cada línea de negocio que ofrece:

- **Agentes de Protección Ejecutiva:** Servicio de protección cercana a personas ejecutivos y personalidades, mediante agentes armados, especializados y certificados con los más rigurosos estándares de selección y entrenamiento.
- **Guardias de Seguridad Física:** Servicio compuesto de elementos armados y/o desarmados para el resguardo de instalaciones públicas o privadas, con la finalidad de salvaguardar y proteger a personas, bienes y valores.
- **Seguridad Logística:** Custodia al transporte de carga en toda la república mexicana, a través de agentes de protección en la modalidad de custodios armados, a bordo de unidades de tránsito y/o vehículos de seguimiento, responsables del resguardo de la cadena de distribución punto a punto.
- **Capacitación y Entrenamiento:** Brindado a directivos, fuerzas del orden, equipos de seguridad y protección con los mejores instructores capacitados, experimentados y certificados a nivel nacional e internacional, así como la impartición de seminarios, talleres y conferencias.
- **Traslado de Valores:** Un servicio complementario del sector financiero que permite trasladar dinero y objetos de valor mediante mecanismos especializados, custodios armados, dispositivos tecnológicos y procedimientos específicos.
- **Administración de Crisis:** Consultoría y asistencia de emergencia ante eventos de riesgo y situaciones de crisis, que por sus efectos inmediatos pongan en grave peligro la estabilidad personal o institucional, así como sus recursos.
- **Estudios de Integridad:** Aplicación de estudios necesarios para determinar la integridad, personalidad y confianza de los evaluados con las diferentes herramientas de medición conductuales.
- **Proyectos Integrales de Seguridad:** Elaboración de análisis de riesgos y vulnerabilidad, políticas y procedimientos, diseños de proyectos de seguridad electrónica, asistencia profesional desde la definición, hasta su conclusión.

Hoy sus líderes reconocen que han sido años de constante labor, adaptación y sobre todo visión, lo que los ha proyectado y preparado para anunciar hoy en este importante aniversario número veinte, su expansión de servicios a través del relanzamiento de su empresa: Incident Prevention and Response Private Security – IPR

No existe una ruta exacta para alcanzar el éxito, pero sin duda hay complementos que abren camino como lo son la perseverancia, la disciplina y en el caso particular de Trust Group, su apuesta desde un inicio por la capacitación de calidad a sus integrantes, lo cual se ha forjado como base de su cultura laboral y lo que ha fomentado el desarrollo y compromiso de sus colaboradores.

Y es que ante un escenario de constantes cambios, donde las condiciones del país son variables, es meritorio mencionar que actualmente Trust Group cuenta con cerca de mil colaboradores a nivel operativo y administrativo, con lo que garantizan y refuerzan su dominio en temas de seguridad nacional, pública y privada sobresaliendo con éxito en un entorno cada día más competitivo para seguir siendo considerados como un aliado de seguridad estratégico que aporta un valor agregado a las operaciones de sus clientes y manteniendo la calidad en la capacitación que ha sido el eje central de su éxito, elevando así la función de la seguridad e influyendo en el éxito organizacional para seguir construyendo una empresa con alto sentido de responsabilidad social y humana.

Y como lo ha expresado en ocasiones anteriores el Licenciado Pedro Sanabria, CPP, Socio Director de Trust Group "No buscamos ser la empresa más grande, sino la mejor, **"Porque en Trust Group no sólo Enseñamos, Demostramos",** y ahora nuestro reto es seguir impactando en las experiencias que ofrecemos a nuestros clientes, quienes nos han brindado su confianza a lo largo de estos años y esperando así alcanzar veinte años más de nuestra pasión por servir a la sociedad a través de la seguridad, pues el camino de la perseverancia, es lo que nos dará la permanencia". ■

Trust Group
En seguridad "Nadie Conoce México como Nosotros".

Fuente: Trust Group
Fotos: Mónica Ramos / SEA

Trust Group cuenta con cerca de mil colaboradores a nivel operativo y administrativo, con lo que garantizan y refuerzan su dominio en temas de seguridad nacional, pública y privada sobresaliendo con éxito en un entorno cada día más competitivo para seguir siendo considerados como un aliado de seguridad estratégico

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

MÉXICO **Hermelindo Rodríguez Sánchez**

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

REVISIÓN DE EFECTOS PERSONALES Y PERTENENCIAS

1) Para el caso del personal que labora en áreas de Producción, Almacén, Distribución, Limpieza y Mantenimiento, y por Política de Seguridad de la Empresa, el guardia de seguridad debe realizar una revisión a las pertenencias del empleado al entrar y salir de las instalaciones. En la revisión de pertenencias se consideran mochilas, bolsos de mano, loncheras y recipientes de alimentos, interior de chamarras y cualquier objeto o ropa utilizado para la guarda de objetos.

2) Al momento de entrar a las instalaciones, se debe llevar a cabo la revisión de pertenencias con la finalidad de detectar cualquier artículo que ponga en riesgo la seguridad de la empresa.

3) Durante la revisión de los bolsos o mochilas, el guardia de seguridad no debe introducir las manos abiertamente. En caso necesario o duda, debe solicitar al empleado que muestre totalmente el contenido, colocando los artículos sobre una mesa de revisión y dentro de una charola de acrílico transparente instalada junto a la caseta de vigilancia.

4) Queda estrictamente prohibido el ingreso de artículos que afecten la seguridad de las personas y de las instalaciones, entre los que se señalan:

- **a)** Prohibida la entrada de armas y objetos punzo cortantes.
- **b)** Prohibido el ingreso con sustancias tóxicas o inflamables.
- **c)** Prohibido el ingreso de drogas en cualquiera de sus modalidades, incluyendo medicamento controlado sin prescripción médica expedita.

5) Prohibido el ingreso a las áreas operacionales con materiales o producto iguales o similares a los que se comercializan en la empresa.

6) Para el desempeño de sus labores el trabajador deberá usar faja, tapones auditivos, lentes, guantes y zapatos de seguridad o zapato cerrado, debiendo reportar al personal que esté laborando y que por comodidad use tenis, huaraches, Walkman, teléfonos celulares o cualquier vestimenta que represente un riesgo al trabajador.

CONTROL DE VISITAS DE DEPENDENCIAS DE GOBIERNO

- Los representantes de cualquier dependencia de gobierno tienen la obligación de cumplir con el reglamento interno de identificación y control de la empresa. Sólo si se autoriza su acceso podrá ingresar, siendo S.A.T. S.T.P.S. M.P. Ejecutores de Juzgados, IMSS, S.S.A., entre otras.

Foto: Freepick

Durante la revisión de los bolsos o mochilas, el guardia de seguridad no debe introducir las manos abiertamente. En caso necesario o duda, debe solicitar al empleado que muestre totalmente el contenido, colocando los artículos sobre una mesa de revisión y dentro de una charola de acrílico transparente

- La persona debe identificarse plenamente, por lo que permanecerá en la recepción hasta ser anunciado o cerciorarse que cuenta con cita previa.
- El guardia de seguridad en turno debe avisar al departamento que corresponda, de acuerdo a las instrucciones que tienen por parte del Departamento Jurídico de la empresa y/o la Gerencia de Recursos Humanos.
- Nombre Completo.
- Dependencia.
- Asunto a tratar.
- Número de acompañantes.
- Si presentó oficio, citatorio o algún otro que lo acredite.

El representante de la empresa, debe autorizar el ingreso a través del filtro y el guardia de seguridad deberá custodiarlo hasta el lugar donde será atendido. Para oficiales de policía, en caso de portar armas, se les solicitará que las dejen a resguardo en la caseta de vigilancia o las dejen en la unidad; en caso de negarse a cumplir con esta medida de seguridad, no se le permitirá el acceso.

La entrada de los representantes de gobierno, de medios de comunicación, agrupaciones o cualquier otro visitante con equipo fotográfico, de grabación o filmación, deberá ser autorizado por la Gerencia correspondiente, preferentemente a través de un memorándum previo y debidamente firmado.

El guardia de seguridad no está autorizado para recibir la documentación especial de los representantes de las dependencias de gobierno, como son citatorios por parte de la autoridad local o federal y menos aún firmar de recibido ningún documento.

Para el caso de facturas, dinero, cheques, tarjetas de crédito, vales de despensa o gasolina debe solicitar indicaciones específicas del área correspondiente; y registrar las incidencias en su bitácora de novedades.

PATIO DE MANIOBRAS

Objetivo: establecer los Procedimientos de Revisión que deben cumplir la empresa transportista y de las condiciones de las unidades de transporte de carga al entrar y salir de las instalaciones.

Alcance: este procedimiento aplica a todas las unidades de carga que entren y salgan con producto de la planta, incluyendo a los vehículos de uso particular y/o de proveedores.

Definiciones:

- **Transporte de carga.** Todo vehículo utilizado para la distribución del producto terminado, particularmente las unidades de reparto de la empresa.
- **Vehículo particular.** Todo automóvil propio o de terceros que ingresen al centro de distribución.
- **Transportista.** Persona que tiene la responsabilidad de la unidad de transporte.
- **Patio de maniobras.** Área interna de la planta para uso de operaciones de carga y descarga.

LINEAMIENTOS

1) Al ingresar al Centro de Distribución o Patio de Maniobras de la empresa, toda línea de transporte de carga debe registrarse en la bitácora de control de entrada y salida de proveedores, en el cual se anota:
   - Fecha.
   - Nombre Completo.
   - Empresa que representa / Línea transportista.
   - Datos de la unidad de transporte / Persona que visita.
   - Motivo de la visita carga / descarga.
   - Hora de entrada.
   - Hora de salida.
   - Cantidad / unidades / tarimas / bultos, etc.
   - Firma / observaciones.

2) El guardia de seguridad del control de accesos debe informar al jefe de Almacén acerca de la llegada del transportista, para que dé su autorización e ingrese a las instalaciones.

3) El operador del transporte de carga podrá ingresar a las instalaciones con un asistente debidamente identificado y registrado, ya sea para ayudar a cargar o descargar la unidad.

4) Una vez autorizada la entrada de la unidad de carga, el guardia de Seguridad debe realizar una observación en el interior de la cabina del conductor, a la caja de carga y a las condiciones generales de la unidad de transporte; a fin de identificar y de prevenir la posible introducción de armas de cualquier tipo, (de fuego y/o punzo cortantes, así como bebidas embriagantes o enervantes) o contrabando. Dicha revisión es de forma aleatoria y se debe llevar a cabo dentro de la planta, a la vista, en el patio de maniobras.

5) A los operadores, transportistas y ayudantes que se detecten en estado de ebriedad o bajo los efectos de algún enervante, incluyendo medicamento sin prescripción médica y/o sustancias toxicas o inflamables, se le negará la autorización para cargar o descargar, procediendo a informar dicha situación al jefe de Almacén, jefe de Distribución y a la Gerencia de Planta, quienes tomarán las medidas correspondientes y determinarán las instrucciones específicas a seguir. Se debe considerar que, si se transporta producto perecedero, no se puede regresar o negar el acceso al transporte de carga.

6) Se debe poner especial atención en detectar la presencia de sustancias tóxicas o inflamables, en caso de detectarse, se negará el acceso a las instalaciones, informando al personal responsable lo acontecido, para que a través de ellos, se reciban indicaciones al respecto.

7) También queda prohibido el ingreso a la planta de las unidades de carga durante la noche, a menos que dicha unidad esté programada para ser recibida o para que salga durante la madrugada.

8) Cuando se detecte alguna anomalía, o bajo sospecha, como resultado de la inspección a la unidad de transporte, antes de permitir la carga o descarga, se debe reportar dicha situación al gerente de Operaciones, a la persona encargada de tráfico y/o a la Gerencia de la Planta, para que determinen las acciones a seguir y se reciban las instrucciones correspondientes.

9) El guardia debe verificar el cumplimiento del uso apropiado del Equipo de Protección Personal (EPP), las restricciones de acceso en áreas de Producción o Almacén y el área destinada para sus operaciones. ■

Foto: Freepick

Una vez autorizada la entrada de la unidad de carga, el guardia de Seguridad debe realizar una observación en el interior de la cabina del conductor, a la caja de carga y a las condiciones generales de la unidad de transporte

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

DECÁLOGO DE ASPECTOS A CONSIDERAR AL MOMENTO DE CONTRATAR UN SERVICIO DE GUARDIAS INTRAMUROS

Revisa estos 10 importantes consejos antes de contratar el servicio

BYTEK SEGURIDAD
La tranquilidad que da una buena seguridad


Foto: Freepick

MÉXICO | **Arturo Carrasco**

1) La personalidad jurídica de la empresa de Seguridad Privada. La ausencia de uno o varios elementos en la materialidad jurídica del prestador de servicios, podría incurrir en multas por arriba de los cinco millones de pesos (284 mil dólares) para el contratante y/o la clausura del establecimiento.

2) Noción del mercado. Derivado del punto anterior, es importante averiguar las prácticas, procesos, precios, referencias comerciales y la oferta en general de los prestadores de servicios legalmente constituidos, para que en este sentido, la decisión no se base solamente en el precio más barato.

3) Elegir una empresa íntegra. Es importante que el proveedor ofrezca un portafolio complementario a los guardias intramuros, tal y como lo es: tecnología, consultoría, rastreo, monitoreo o diversas especializaciones que sirvan como herramienta al servicio que se brinda.

4) Distintivos y diferenciadores del mercado. Las empresas de seguridad privada deben de certificar su experiencia con un CV empresarial donde se condecore su experiencia, a base de certificaciones, distintivos de calidad, formación académica, registros, participación en asociaciones, acreditaciones o diversos títulos que demuestren su construcción a lo largo del tiempo.

5) Ubicar sus instalaciones. Una visita a sus oficinas para conocer un poco de sus procesos es algo que pocos o casi nadie realiza y puede salvarte de contratar problemas o fraudes.

6) Solicitar referencias comerciales o casos de éxito documentados. Es fácil presumir logros que no existieron, pero que mejor cuando son narrados directamente de la clientela vigente del proveedor, para afianzar la confianza de tomar una buena decisión.

7) Solicitar fichas técnicas de personal asignado. Conocer los procesos de selección y contratación del proveedor es elemental para asegurar la tranquilidad e inocuidad del servicio.

8) Auditar al proveedor de servicios de seguridad privada. Tener un proceso de auditoría interna con el proveedor es indispensable para garantizar el cumplimiento posventa del servicio, al solicitarle información calendarizada de sus renovaciones, fianzas, procesos, pagos, recibos de nómina, ICOSE, SISUB, etc.

9) Reunirse mensualmente con el representante de su servicio. No prestar atención o tiempo a este punto es una de las principales causas de fracaso de cualquier prestación de servicio, ya que esto permite identificar y pulir áreas de oportunidad antes de que detonen en errores o situaciones irremediables.

10) Pagar digna y oportunamente. La parte medular de cualquier negocio es salvaguardar una buena salud financiera y mantener al corriente esta parte con tu proveedor le permitirá mantener un porcentaje de rotación bajo, y sus procesos al día para garantizar el cumplimiento de tus necesidades. ■

Arturo Carrasco, CEO de Bytek Seguridad Privada. *Más sobre el autor:*


Foto: Freepick

Asistencia Legal

ALES

Gestoría Jurídica
en materia de
Seguridad Privada

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

Asumimos la responsiva de su empresa en los siguientes rubros:

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

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

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

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

· Juicios de nulidad y amparo administrativo.

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

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

· Elaboración de manuales operativos o de capacitación.

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

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

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

licdantegarciamtz@outlook.com

Whats: 477 828 1291

Columna
EL TIGRE TIENE RAYAS

ballesteros.barrera@hotmail.com

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

Más sobre el autor:

ENTREVISTA CON LA CONFEDERACIÓN DE PROFESIONALES EN COMERCIO EXTERIOR (COPCE)

MÉXICO

¡Saludos, amigos! Ya saben que siempre es un honor dirigirme a ustedes a través de esta columna que es para ustedes: "EL TIGRE TIENE RAYAS". Les mando a todos unos fuertes abrazos.

Les comparto en esta ocasión la entrevista que me hicieron los amigos de la Confederación de Profesionales en Comercio Exterior (COPCE) el 1° de mayo del año en curso, que está dedicada a la cadena de suministro y todo lo relacionado al transporte de productos y aduanas. Esta organización está reconocida en el país como una de las más confiables en su ramo y su director, el Lic. David Rangel, fue reconocido también como una de las 100 personas más influyentes en su ramo.

Tuve el honor de ser tomado en cuenta como especialista en el ramo de la seguridad privada para hablar en esta ocasión de cómo la delincuencia está afectando la cadena de suministros[1], como a continuación se presenta:

David Rangel (DR): ¿Cuál es la percepción de la inseguridad actualmente?

Omar Ballesteros (OB): es de risa, no es creíble, pero salió en un conocido periódico de circulación local que está en siete, pero en octubre de 2021 estaba en 8.1.

DR: ¿Cómo está golpeando el crimen la cadena de suministro?

OB: ¡Muy duro! En una reunión con los amigos de la Cámara de Curtiduría, nos comentaron que, en cifras de la Policía Estatal-Federal, lo primero que se están robando son tráilers de comida, y en segundo lugar, la electrónica.

DR: ¿Sabes algo sobre el índice criminal en la carretera del Bajío – Ciudad de México?

OB: las cifras que aparecen en la página de Segob (Secretaría de Gobernación), están sesgadas, ya que en la revista **Seguridad en América** (**SEA**), donde participo con dos columnas ("El Silencio Habla" y "El Tigre Tiene Rayas"), sale información acerca de que el robo de tráilers está cada vez más alto y las empresas de transporte no ven respuesta de las autoridades. La Canacar (Cámara Nacional del Autotransporte de Carga) habla de eso, mencionando que están sobrepasados[2].


Daniel 35 años de ardua labor

Triunfa la Fiera

vivir

La violencia en Guanajuato ha provocado que la inflación sea la más elevada de la zona de El Bajío

Sube precios inseguridad

Dejan más lesionados accidentes

Todo Sube

ASTERISCOS

***LA BUENA

Las tres ciudades de Guanajuato que mide la Encuesta Nacional de Seguridad Pública Urbana (ENSU) del Inegi de marzo, reportan una mejora en el índice de percepción de la inseguridad respecto a diciembre de 2022. El Gobierno del Estado ya salió a presumir la mejora gracias al trabajo de los tres niveles, dicen.

***LA REGULAR

En León e Irapuato la percepción del 79.5% y 85.3%, respectivamente, los ubica muy por encima del promedio nacional de 90 localidades, que es 62.1%. La ciudad fresera abandonó el tercer peor puesto, pero está en el siete. Nada para celebrar.

***LA MALA

Además, contrario al comunicado de ayer del Estado que insiste en una tendencia a la baja en homicidios dolosos, las cifras oficiales reflejan que el primer trimestre las víctimas suman 810, que es 5.7% más que el mismo periodo del 2022. Atentos.

DR: La cosa no es fácil y, a pesar de que las autoridades hablan de apoyar a las empresas de transporte, la realidad demuestra lo contrario. ¿Qué deben hacer las empresas de transporte para poder atender este mal?

OB: como criminólogo dentro del análisis de riesgos vemos algo llamado "cifra negra", que corresponde a lo no reportado, siendo que por cada delito cometido hay tres que no se reportaron. Eso ya quedo atrás, la delincuencia se volvió exponencial y la cifra negra aumentó a diez o más. Por lo anterior, las empresas de transporte no puede esperanzarse ni confiar que las autoridades van a resolver el problema, ellas tiene que protegerse y crear sus propios sistema de protección.

En 2022 la misma asociación le comentó a la autoridad federal sobre crear un equipo de respuesta para que en caso de robo de un tráiler, salieran agentes especiales de manera inmediata a recuperarlo. Obvia-


A 2 | LEÓN

am.com.mx / Jueves 20 de abril de 2023 / AM Guanajuato

Incrementa percepción de seguridad

» Irapuato mejora siete puntos porcentuales respecto al último trimestre del año anterior; León y Guanajuato también, según la Encuesta de Seguridad Urbana de Inegi

PERCEPCIÓN DE SEGURIDAD

LAS PEORES

Ciudad	Porcentaje
• Fresnillo	90%
• Zacatecas	94.3%
• Nuevo Laredo	88.0%
• Ciudad Obregón	86.4%
• Uruapan	86.2%
• Colima	85.7%
• Irapuato	85.3%

LAS MEJORES

Ciudad	Porcentaje
• San Pedro Garza García	18.3%
• Benito Juárez (CDMX)	n.d.

Fuente: Encuesta de Seguridad Pública Urbana (ENSU) de Inegi

Martha Silva
msilva@am.com.mx

SEGURIDAD

Irapuato tuvo un decremento importante, de siete puntos porcentuales, desde el trimestre anterior cuando fue tercera en percepción de inseguridad en el País.

También en León y en Guanajuato mejoró la percepción, de acuerdo con la más reciente Encuesta de Seguridad Pública Urbana de Inegi publicada ayer.

Ambas ciudades quedaron en la posición 35 y 41 respectivamente entre 90 ciudades y alcaldías.

A nivel nacional, Irapuato fue en el trimestre el séptimo municipio donde la población percibe más inseguridad, con un 85.3 %.

En general a nivel nacional, en el primer trimestre de 2023 bajó ligeramente la percepción de inseguridad en las ciudades, en personas mayores de 18 años.

Pasó del 64.2 al 62.1 %.

No obstante, los municipios que se perciben más inseguros en el País son Fresnillo y Zacatecas capital, en Zacatecas, y Nuevo Laredo, en el Estado de México.

Y respecto a Irapuato, la percepción bajó del 92.6 a 85.3 %, mientras que en León pasó de 82.2 a 79.5 %, casi tres puntos.

La capital del estado fue de 68.2 a 62.6 %, casi seis puntos.

La encuesta se levantó del 27 de febrero al 15 de marzo de 2023 a personas de 18 años o más en 27 mil 210 viviendas distribuidas en todo el territorio nacional.

Respecto a la comparativa anual (marzo 2022–marzo 2023) también muestra decremento el porcentaje de personas que consideraban a la ciudad de Irapuato como insegura: el año pasado era de 87.6% y ahora fue de 85.3 %.

En León, en marzo de 2022 era de 81.3 contra el actual 79.5 %. En Guanajuato pasó del 67.8 al 62.6 %.

Conflictos, expectativas

La encuesta muestra que menos pobladores de León e Irapuato estuvo expuesta a conflictos o enfrentamientos, de manera directa, con familiares, vecinos, compañeros de trabajo o escuela, establecimientos o con autoridades de gobierno respecto al trimestre anterior.

En el caso de Irapuato, pasó de 40.3 a 32.8 % y en León, de 33.0 a 26.9 %.

En el caso de la ciudad de Guanajuato, aumentó. En diciembre pasado se registró un porcentaje de 28.2, contra el 30.3 actual.

Respecto a las expectativas sobre la delincuencia, es decir, el porcentaje de la población que considera que la delincuencia seguirá igual de mal o empeorará en los próximos 12 meses es alta en Irapuato y Guanajuato, con 78.0 y 72.8 % respectivamente.

En León es menor esa percepción, de 67.8 %.

Sobre cambio de hábitos por temor a la delincuencia, como visitar parientes o amigos en el primer trimestre de 2023, Irapuato aparece como uno de los más altos a nivel nacional con 52.9 % de las personas encuestadas, mientras que León tiene 37.0 y Guanajuato registró 34.1.

León fue la cuarta ciudad en México con menor confianza en la Guardia Nacional, con 61.6 %; Irapuato reportó 82.3 y Guanajuato 66.2 %.

Y apenas la mitad de la población encuestada de las tres ciudades identifica que la Policía Preventiva Municipal es una autoridad que le inspira confianza.

En Guanajuato el porcentaje es ligeramente más alto que en Irapuato y León.

Vive Léon el mes más sangriento

Francisco Viéjar

VIOLENCIA

Con 89 homicidios dolosos, León vivió en abril el mes más violento desde que Alejandra Gutiérrez Campos llegó a la Presidencia Municipal.

De acuerdo con los conteos que día a día realizan A M y A l Día, en León se registraron 84 asesinatos en octubre de 2023, cuando Gutiérrez Campos llegó al gobierno.

Pero luego se produjo una tendencia a la baja, aunque irregular, pero en febrero de 2022 se registraron 64 casos, la mitad que hubo este abril.

Sin embargo, la reducción no se mantuvo y en septiembre del año pasado hubo 88 homicidios dolosos, aunque la cifra disminuyó luego a 76 en octubre, 66 en noviembre y 57 en diciembre.

Pero 2023 ha sido malo para los leoneses. En enero los crímenes volvieron a crecer hasta 65, subieron a 68 en febrero, a 82 en marzo y registraron en abril la cifra más alta, con 89.

De acuerdo con nuestro conteo, durante abril hubo en Guanajuato 301 casos de homicidio doloso, con lo cual suman 1 mil 111 los casos en 2023.

La cifra es ya superior a la registrada durante 2022, cuando en los primeros cuatro meses del año se produjeron 993 homicidios dolosos, de acuerdo con el Sistema Nacional de Seguridad Pública.

Durante abril, 10 menores fueron asesinados.

CONCENTRA LA VIOLENCIA

León registró durante abril casi tantos casos de homicidio doloso como los otros cuatro municipios más violentos del estado. El balance de 2023 en los cinco municipios es el siguiente:

Abril		Marzo	
• León	89	• León	82
• Celaya	41	• Celaya	34
• Irapuato	22	• Irapuato	18
• Salvatierra	16	• Salvatierra	13
• Salamanca	14	• Salamanca	25
Febrero		**Enero**	
• León	68	• León	65
• Celaya	35	• Celaya	54
• Irapuato	18	• Irapuato	14
• Salvatierra	10	• Salvatierra	29
• Salamanca	28	• Salamanca	22
Total:			
• León	304	• Salvatierra	67
• Celaya	164	• Salamanca	89
• Irapuato	72		

LOCAL PÁG. 2

GUANAJUATO

Mejora la percepción, aumentan homicidios

Ciudadanos de Irapuato, León y Guanajuato capital afirmaron sentirse más seguros en la encuesta trimestral que realiza el Inegi. En cambio, entre enero y marzo se incrementaron los homicidios dolosos, en comparación con 2022.

LOCAL PÁG. 2

Advierten que la inseguridad se ha generalizado a lo largo de toda la vía

Tocan en Guanajuato tres municipios, en un tramo de 88 kilómetros; en San Luis Potosí señalan una situación fuera de control

Enfrentan riesgos en la carretera 57

Erbaldo Gutiérrez

mente de lo que piensan los empresarios de transporte a lo que cree que la autoridad, hay una diferencia abismal, nada de eso se tomó en cuenta. El problema hoy es mayúsculo.

DR: ¿Cuáles delitos están fuera de control al día de hoy?

OB: la delincuencia jamás ha estado controlada, eso es una falacia. Los delitos que están en el top, conforme a lo que reportan los periódicos y la SEGOB en su página, son: homicidio-asesinato, robo (todas las modalidades) y secuestro-extorsión.

Algo que te puedo comentar en esta entrevista, es que el crimen organizado no sólo tiene el control de más de 300 municipios y casi todos los estados del país, también es infiltrado en las principales empresas del país, filtrando la información para el robo de unidades de la cadena de suministros, así como también en bancos, y nada de lo que haga la autoridad dará resultados, porque no hay voluntad para para este tema.

Un amigo que está en contacto con el sistema de seguridad nacional, me comentó que el principal uso de la tecnología de investigación y espionaje es usada contra los partidos y sus políticos, en eso está metida tanta inversión de tecnología vs. crimen.

DR: Se podría denotar entonces que el crimen tiene un control de las actividades de la policía, lo cual se ve en redes y en los periódicos, es increíble que cada día el tema de la se inseguridad va en aumento en lugar de disminuir, ya que el gobierno presume que hace de todo por atender el tema.

OB: es muy fácil decir que como autoridad estás atendiendo el tema cuando eres juez, jurado y verdugo, y que tus "cifras oficiales" son ley de Dios y pobre de ti que las cuestiones.

Pero la realidad es que el sol no se puede tapar con un dedo, el sistema de seguridad de cualquier nivel de gobierno, lo comparo a lo siguiente: la pelota del tigre. Eso es, que la autoridad se para a las cámaras diciendo que la pelota que tiene en las manos es una pelota contra tigres, y cuando se le cuestiona cómo funciona eso, la autoridad responde: "¿Ves algún tigre en la sala? Obvio que no, entonces la pelota funciona". Así es el sistema de seguridad de los gobiernos de México en cualquier nivel y en cualquier lado.

DR: ¿Qué deben hacer las empresas para evitar la infiltración del crimen organizado?

OB: siempre he recomendado que sus reclutadores y el mismo director de la empresa aprendan de lenguaje corporal – lenguaje no verbal, debido a que los métodos que actualmente utilizan los reclutadores como MMPI, Stanton, Nuevo Stanton, Hombre bajo la lluvia, etc., no son suficientes al momento de estar entrevistando a una persona.

Se debe preguntar de manera directa, pero inesperada, si el candidato está involucrado con el crimen organizado y ver su respuesta inconsciente. Eso nos ha ayudado mucho para reducir la probabilidad de infiltrados delincuentes en nuestras empresas de seguridad privada.

Hoy por hoy el lenguaje corporal, sabiendo interpretarlo, sirve para evitar hacer negocios con inversionistas que no lo son, empleados desleales, operarios que están infiltrando la información, etc.

DR: ¿Cuáles son tus sugerencias a las empresas de transporte para reducir los problemas de robo?

OB: las empresas de seguridad privada somos una excelente opción, conocemos nuestro negocio, no sólo por la experiencia que nos caracteriza, sino porque usamos la ciencia para mejorar en nuestros procesos, a la vez que nos actualizamos en las nuevas modalidad de robo, asistimos a seminarios, cursos y capacitaciones que nos permiten desarrollar un sentido de criterio amplio y enfocado.

Sabemos que todos estamos cuidando los pesos, pero no puedes escatimar en tu imagen, cada robo de tráiler afecta no sólo la imagen de la empresa de transporte, como ineficiente, y deja de manifiesto que la carga del cliente se perderá sin importar que esté asegurada (ninguna aseguradora atiende una reclamación de manera pronta), ya que no llegó a su destino.

Si el transportista prefiere atender su propio sistema de seguridad-protección, tienen que hacerlo con asesoramiento de profesionales como nosotros, pero eso también quieren ahorrarse. Al final por la falta de atención a este tema, las empresas de transporte perderán credibilidad, porque la mercancía de sus clientes no está segura. Recomiendo ampliamente que sus choferes se capaciten en manejo ofensivo-evasivo-defensivo, además de que el carro debe estar blindado y que no vaya solo.

Teniendo esos aspectos desarrollados, la probabilidad de pérdida será mucho menor. Sabemos que hay una crisis de choferes, no hay gente que quiera trabajar de conductores, por lo que el Departamento de Reclutamiento tiene que ofrecer algo más acorde a las generaciones jóvenes del año 2000 para acá, ya que dicha generación lo que busca es estar metida en redes sociales. ■

Referencias:

[1] *Les comparto el link de la entrevista, la cual se encuentra en YouTube: https://www.youtube.com/watch?v=saioY5ypVds*

[2] *https://solcat.com.mx/estamos-rebasados-por-la-delincuencia-canacar-custodia-de-mercancia/*

SEGURIDAD EN OFICINAS *CORPORATIVAS*

Monterrey y Ciudad de México son los mercados más atractivos y predominantes para el sector inmobiliario de oficinas, situación que va al alza, así como los retos de seguridad a los que estos se enfrentan

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

El año 2023 fue el inicio de la reactivación de diferentes industrias después de los estragos vividos por la pandemia de COVID-19, uno de estos sectores económicos fue el segmento inmobiliario de oficinas en México, ya que las empresas aumentaron sus actividades presenciales y regresaron a sus empleados a los corporativos de forma paulatina. "En el país, existen 737 inmuebles corporativos de primera categoría, los cuales reportan un 23% de espacio disponible y ocupan 10.3 millones de metros cuadrados (m^2)"[1], siendo los mercados más grandes de este giro, Monterrey, Guadalajara, Querétaro y Ciudad de México; ésta última concentra el 80% de los espacios corporativos de todo el país.

Otras de las razones, además de la pospandemia, que motivó a las empresas a continuar con sus actividades presenciales en corporativos, fue el nearshoring, estrategia que están utilizando diferentes empresas en todo el mundo, para transferir parte de su producción a terceros, pero que tienen una ubicación geográfica más inmediata y que puede traer beneficios a la empresa.

La Ciudad de México concentra a gran parte de los corporativos en las colonias de Chapultepec, Polanco, Nuevo Polanco, Ampliación Nuevo Polanco, así como Insurgentes, Reforma, Santa Fe, Lomas Altas y Bosque de las Lomas, "ubicándose en ellas las 100 empresas más grandes del país en los sectores financieros, de seguros, automotriz, telecomunicaciones, constructoras, logística y hoteles de gran turismo"[2].

Siendo una ciudad que ha sufrido lamentables pérdidas por los terremotos (1985, 2017), la seguridad desde la construcción de estos edificios hasta el tránsito de personas que tienen a diario, es una prioridad para los responsables del área de Seguridad y Protección Civil. Pero no sólo los riesgos naturales amenazan a los corporativos, es por ello que realizamos una serie de entrevistas con especialistas en el tema para conocer las medidas de seguridad implementadas en estas grandes edificaciones, una vez que las actividades de este sector van al alza.

PRINCIPALES RIESGOS DE SEGURIDAD

Como cada sector, el inmobiliario y específicamente los corporativos, tiene riesgos generales y otros más específicos, dependiendo de la ubicación, giro de la empresa, número de ocupantes, visitantes, etc. De acuerdo con Kael Malo-Juvera, CPP, *Regional Security Manager* en IBM Corporate Security, los riesgos actuales, y generales, a los que se enfrenta este sector son:

"En México, como en otros países, los corporativos deben sensibilizar a sus empleados al riesgo de extorsión para que no caigan", **Marguerite Desmichelle**

- Seguridad Física:
  - Ingresos no autorizados a las instalaciones con el fin de obtener información confidencial o crítica (*tailgaiting*).
  - Intrusión de un empleado-ex empleado con armas para realizar una venganza (*Active Shooter*).
  - Intrusión furtiva para robar equipos.
- Seguridad Cibernética:
  - Robo de información por medios electrónicos.
  - Intrusión a las redes y bases de datos buscando afectar a la empresa.
  - Hackeo de páginas y servidores.
  - Hackeo de cámaras IP, servidores de video y sistemas de control de accesos.
- Seguridad Logística:
  - Robo de mercancía dentro de los centros de distribución.
  - Robo de mercancía en trayecto.
  - Incidentes con importaciones y exportaciones (drogas, armas y dinero sembrado en contenedores).
- Seguridad del Personal:
  - Ingreso de elementos de la delincuencia organizada a la estructura de la empresa.
  - Sabotaje por diferentes razones.
  - Extorsiones, cobro de piso, secuestros.

Estos son desde el análisis general del sector, pero el especialista comentó que las áreas de Seguridad deben tener presente además el tema de Manejo de Crisis Corporativas y el soporte a la corporación en otro tipo de emergencias.

Y un riesgo que hoy en día está muy presente y que no se puede prevenir, es un terremoto. Lo que sí se puede hacer es que en coordinación con Protección Civil se genere una concientización y una capacitación a todo el personal ante emergencias de este tipo. Para ello, Ildefonso Jacinto compartió algunos tips de seguridad en un corporativo al momento de un sismo:

- Si suenan las alarmas, busque la ruta de evacuación llegue al punto de reunión.
- Realizar la evacuación en orden y con responsabilidad.
- Si puede y tiene la orientación mínima, ayude a sus compañeros.
- Al momento de la evacuación, no tome algún liderazgo si no le fue asignado.
- No ponga en riesgo su vida y mucho menos la de sus compañeros.

Referente a la seguridad del personal, y sobre todo si dentro del corporativo se encuentran los altos mandos, se deben implementar otras estrategias más específicas y con inteligencia. Desafortunadamente México vive una situación de inseguridad preocupante, la extorsión y el secuestro son malas prácticas que también vuelven vulnerables a los ocupantes de los corporativos.

"Si tomamos el caso de un corporativo en un país como México, existe el riesgo de extorsión. De hecho, ya es un espacio de trabajo asociado a las funciones de gestión y administración, tal como Finanzas o Recursos Humanos, llama la atención de los delincuentes. Tomando este ejemplo, en México, como en otros países, los corporativos deben sensibilizar a sus empleados al riesgo de extorsión para que no caigan", comentó Marguerite Desmichelle, *Latin America Security Manager* en Alstom, compañía francesa de movilidad y transporte, involucrada en el proyecto del Tren Maya en México.

Marguerite agregó que, para generar estrategias de seguridad efectivas para los empleados en los corporativos, se deben comprender los riesgos a los que están expuestos dependiendo de sus funciones. "Cuando se trata de los empleados, hay que tomar en cuenta el perfil de éste, o sea tanto su estatus en la empresa como su entorno de trabajo. No se implementan las mismas políticas para los directores, los equipos operativos en campo, los expatriados o los visitantes extranjeros. Y hay que considerar también la responsabilidad de la empresa, el llamado Duty of Care, que no aplica de la misma manera para todos los perfiles". Ilustró con el siguiente ejemplo:

"Un empleado en viaje de trabajo en un país distinto a su país de origen (un canadiense en Brasil, por ejemplo), se encuentra bajo la responsabilidad de la empresa 24/7 durante su estadía (business trip). Por lo tanto, se van a implementar medidas adicionales para los viajeros, que para los empleados locales (un procedimiento de *Meet and Greet* con chófer a la llegada en el país, la asesoría de los alojamientos, una inducción de seguridad, etc.).

"Las condiciones psicosociales de los empleados son riesgos que deben ser atendidos para mantener espacios de trabajo seguros y libres de violencia", **Dr. Adalberto Barrales**

"En caso de que una persona no deseada haya accedido a un corporativo, los protocolos de actuación pueden variar según la empresa y la situación específica", ***Iliana Fernández***

Mientras que, para un equipo operando en campo en un lugar remoto con exposición a riesgos externos (asaltos, por ejemplo), la empresa podrá implementar un servicio de traslado de los empleados al campo o un servicio de monitoreo GPS con botón de alerta, entre otros".

Por su parte, el Dr. Adalberto Barrales, *director – Global Security & Asset Protection* (GSAP) para North LATAM (México y Centroamérica) en The Coca-Cola Company, explicó que los riesgos van cambiando, mutando y hasta podría decir que se reinventan; de ahí la importancia de la Gestión de Riesgos para identificarlos, entender el Estado del Arte existente y minimizarlos para evitar que se conviertan en amenazas. En el caso específico de la compañía donde desarrolla sus funciones, la ubicación geográfica de ésta, considera otros riesgos de seguridad.

"El impacto delictivo para los empleados debe ser considerado dentro de los riesgos. En la región estamos siendo vulnerados por la alta violencia en las calles, el incremento de las extorsiones y sus variantes; los problemas de ciberseguridad, así como secuestros, los asaltos y la inseguridad en carreteras. Las condiciones psicosociales de los empleados son riesgos que deben ser atendidos para mantener espacios de trabajo seguros y libres de violencia. Por eso toma una importancia relevante el crear y mantener una cultura de la seguridad (*Security / Safety*) para todos quienes integran una empresa, pues como comunidad es válido mantener acciones de prevención de incidentes y delitos", señaló el especialista.

"En Schneider contamos con un programa anual de capacitación para todo el personal empleado que incluye temas como: concientización en seguridad, seguridad personal, manejo defensivo, seguridad de la información", ***Ildefonso Jacinto***

ESTRATEGIAS DE SEGURIDAD

Cada responsable de Seguridad de los Corporativos, desarrolla estrategias de seguridad basadas en un robusto análisis de riesgos, sin dejar de lado las emergencias. Una estrategia que le ha funcionado, no sólo a este sector, es la implementación de tecnología para el control de accesos e impedir la intrusión de personas no deseadas. Javier Pichardo, CPP, *Head of Security* para Latinoamérica Norte y el Caribe para British American Tobacco, compartió algunas de estas herramientas:

- Torniquetes de cuerpo completo con tecnología de reconocimiento facial.
- Implementación de credenciales electrónicas con segmentación de acceso a zonas críticas.
- Cámaras de CCTV (digitales, reconocimiento facial) en áreas generales y zonas críticas de la instalación- conectado a Central de Monitoreo.
- Presencia de personal de seguridad en lobby de acceso, rondines al interior de las instalación - sistemas de control de rondas.
- Botones de pánico.

"El uso de la app Life 360, es muy útil, ya que los familiares cercanos pueden ver dónde se encuentran los seres queridos. Nosotros hemos instalado sistemas de geolocalización en vehículos que se trasladan a zonas de mayores riesgos", ***Uwe Fischer***

En dado caso de que, pese a las estrategias de control de accesos implementadas, alguna persona o grupo de personas no deseadas, hayan logrado esquivar esta barrera, Iliana Fernández, *Sr. Regional Security Manager Central* – LATAM en Microsoft, explicó un ejemplo de protocolo de reacción ante este incidente:

"En caso de que una persona no deseada haya accedido a un corporativo, los protocolos de actuación pueden variar según la empresa y la situación específica. Algunas acciones comunes pueden incluir:

- **Colocar un botón de alerta en la recepción:** Con esta acción el centro de monitoreo puede apoyar y tomar acción si fuera necesario.
- **Educar a los empleados para que entiendan la responsabilidad de tener un gafete,** no den paso a personas sin gafete. Es como la llave de tu casa; no se las dé a cualquiera.
- **Evaluar el alcance del incidente:** Es importante evaluar el alcance del incidente para determinar qué información o sistemas se han visto comprometidos y tomar medidas para mitigar cualquier daño adicional.
- **Realizar una investigación interna:** Después del incidente, es importante llevar a cabo una investigación interna para determinar cómo ocurrió el incidente y qué medidas se pueden tomar para prevenir incidentes similares en el futuro.

Estas son sólo algunas de las estrategias y acciones que se pueden tomar para evitar el acceso no deseado en los corporativos y responder a incidentes de seguridad. Es importante tener en cuenta que cada empresa puede tener sus propios protocolos y políticas específicas en función de sus necesidades y requisitos".

Respecto a la cultura de seguridad que debe incentivarse entre los empleados del corporativo, Ildefonso Jacinto, *Site Security Leader* en Schneider Electric, concordó en que es importante capacitar al personal para que pueda reaccionar de la mejor manera ante un incidente de seguridad.

"En Schneider contamos con un programa anual de capacitación para todo el personal empleado que incluye temas como: concientización en seguridad, seguridad personal, manejo defensivo, seguridad de la información, seguridad de la carga, Plan de Continuidad del Negocio, entre otros temas acordes al corporativo".

La implementación de un control de accesos, con base en el análisis de Uwe Fischer, director global de Seguridad para la empresa Draslovka, debe permitir no solamente identificar a las personas en el ingreso o en la salida, se debe buscar la autentificación para evitar, por ejemplo, que tarjetas de acceso sean prestadas a otras personas. El uso de tecnología biométrica de cualquier tipo es útil para lograr esto. Adicionalmente deben considerarse sistemas de videovigilancia, video analíticos, alarmas de intrusión y sistemas de detección y combate de incendios, así como notificación masiva para situaciones de emergencia como incendios o temblores.

"Todos estos sistemas deben estar integrados en una sola plataforma que puede ser un Sistema de Gestión de Edificios (BMS), este tipo de sistemas permiten además de correlacionar eventos detectados por los sistemas de seguridad, otros eventos como un bloqueo de elevadores, altas temperaturas, acumulación de gases en cuartos de baterías, entre otros", explicó.

CIBERATAQUES Y FILTRACIÓN DE INFORMACIÓN

En la actualidad no se puede dejar de lado la importancia de la ciberseguridad en cualquier organización pública y privada, sobre todo cuando existe información sensible y que muchas veces es manipulada por diferentes áreas, por ejemplo, en un corporativo, el problema es que no siempre se cuenta con la suficiente prevención ante un posible hackeo; también está el riesgo de que el propio personal sea quien comparta esta información o intente obtener un beneficio personal de ésta.

"En relación con las medidas que toman para proteger la propiedad intelectual y los activos de una empresa, existen diferentes estrategias y prácticas implementadas. Algunas de estas medidas incluyen: contratos de protección de propiedad intelectual; protección legal, seguridad informática, y muy importante la educación y concienciación de los colaboradores", indicó Iliana Fernández.

*"Para proteger datos sensibles, en British American Tobacco, todos los empleados firman en su contrato un acuerdo en el cual declaran que toda la información que manejen dentro de su relación laboral es propiedad de la empresa", **Javier Pichardo, CPP***

*"En Volvo nos enfocamos en prevenir la divulgación de información propiedad de la compañía no autorizada, mediante: capacitación a los empleados en técnicas de protección de la información, políticas de cambios frecuentes en configuración de contraseñas más complejas, entre otras", **Ángel Alfaro***

Por su parte, Kael Malo-Juvera coincidió en que actualmente existen múltiples acciones, políticas y procedimientos que aseguran a la empresa mantener su información fuera del alcance de la delincuencia, por supuesto todo se maneja con un grado alto de confidencialidad. Aquí se entiende la importancia del compliance para que este tipo de riesgo esté previsto y se atienda conforme a las normas, leyes y buenas prácticas especificadas.

"En British American Tobacco, todos los empleados firman en su contrato un acuerdo en el cual declaran que toda la información que manejen dentro de su relación laboral es propiedad de la empresa. Se cuenta con políticas de seguridad corporativa y procedimientos de seguridad, *compliance*, así como estándares de conducta corporativos. Todos los activos son inventariados por el departamento competente dependiendo de su naturaleza (IDT, *Facilities,* Ingeniería) y los empleados firman acuerdos de uso responsable de los mismos", indicó Javier Pichardo.

Ángel Alfaro, *Safety, Security & Health* en Volvo Group México, compartió algunas medidas de seguridad para la protección de datos implementadas en Volvo. "En la compañía hay distintas políticas y herramientas tecnológicas que permiten controlar el manejo de la información sensible, es decir, nos enfocamos en prevenir la divulgación de información propiedad de la compañía no autorizada, mediante:

- Capacitación a los empleados de técnicas de protección de la información.
- Políticas de cambios frecuentes en configuración de contraseñas más complejas.
- Restricciones de acceso a la información sensible.
- Tecnologías de la información que monitorean y supervisan la seguridad de los servidores".

RIESGOS DE SEGURIDAD EXTERNOS

Como algunos especialistas lo comentaron, no se puede dejar de lado la situación política, social, económica y de inseguridad donde se ubiquen los corporativos; así sean marchas, plantones o lo que actualmente está sucediendo con los enfrentamientos entre cárteles que cierran caminos e impiden el paso de los trabajadores a su destino, estas situaciones pueden afectar el desarrollo de las actividades, su operación y la seguridad del corporativo. Respecto a las medidas de seguridad que los empleados deben considerar en las inmediaciones del corporativo y al trasladarse de su casa a éste, Marguerite Desmichelle compartió lo siguiente:

"La primera recomendación, y eso en cualquier parte del mundo, es mantener un perfil bajo en todo momento. Con ello, me refiero a tratar de no identificarse como empleado de una empresa multinacional fuera de las instalaciones de dicha empresa a menos de que sea necesario. Cuidar de sus pertenencias y de las de la empresa, también es un tema de suma importancia. Hay muchos, por no decir demasiados, incidentes de robo de equipo de cómputo de la empresa dentro de los vehículos personales de los empleados porque fueron dejados sin vigilancia y/o a la vista".

En cuanto al traslado hogar – oficina corporativa, Marguerite explicó que no necesariamente existen medidas de seguridad. Sin embargo, se puede implementar el traslado a ciertos centros de trabajo, en particular de noche. El acceso a un beneficio puntal de taxi al salir de sitio de trabajo es también una opción para mitigar la exposición del personal si las condiciones de seguridad del entorno lo justifican.

Por su parte, el Dr. Adalberto Barrales señaló que ante la situación de inseguridad que enfrentan en las inmediaciones de la compañía, ha sido necesario construir y fortalecer una cultura del autocuidado. "La participación de todos en acciones preventivas es un ejercicio muy valioso; pláticas y cápsulas con información conducente a fortalecer la cooperación en la construcción de la seguridad y la reflexión sobre el rol de todos, es un excelente ejercicio holístico. Así como la conciencia situacional; el tener una comunicación oportuna y completa; evitar rutinas, mantener bajo perfil (permanecer anónimo); el manejo de redes sociales, todas estas son pautas que siempre deben ser consideradas para la seguridad de las personas".

Los especialistas coincidieron en que cuando se trata de personal de alto rango, mantener el perfil bajo es una estrategia básica para la seguridad de éste, así como el cuidar sus traslados, rutas, el vehículo en que se mueve, etc. Todo debe coincidir y estar planeado estratégicamente para evitar el incremento de riesgos hacia su persona.

Uwe Fischer también recomendó para la seguridad del personal el no relacionarse con personas de dudosa reputación, así como no viajar solos en altas horas

*"Entre los riesgos de Seguridad Física de un corporativo están los ingresos no autorizados a las instalaciones con el fin de obtener información confidencial o crítica (tailgaiting), la intrusión de un empleado-exempleado con armas para realizar una venganza (Active Shooter), entre otros", **Kael Malo-Juvera***

de la noche, y evitar zonas de riesgo. "En mi experiencia ha sido muy útil el uso de la *app* Life 360, la cual permite que los familiares cercanos puedan ver dónde se encuentran los seres queridos. Nosotros hemos instalado sistemas de geolocalización en vehículos que se trasladan a zonas de mayores riesgos".

Retomando los riesgos a los que se enfrentan los altos mandos que asisten a los corporativos internos y externos, el secuestro es uno de ellos y hay que estar conscientes de que puede suceder, es por ello que Ángel Alfaro compartió cinco tips para prevenir el secuestro de funcionarios o *CEO's* a las afueras de los corporativos:

1) Incorporar un programa de capacitación a los empleados y ejecutivos, el cual les permita entender el fenómeno del secuestro y sensibilizar sobre el tema.
2) Reducir al nivel de visibilidad de los empleados y ejecutivos, mediante información útil en la vida diaria de cada persona.
3) Incorporar un mayor número de cámaras de seguridad en los accesos y salidas de la compañía, esto genera un efecto disuasorio, además estas deben ser monitoreadas para detectar anomalías y reportar a las autoridades.
4) Variar horarios de salida de los empleados, privilegiando la salida con luz de día, el trabajo remoto puede ser también una alternativa, para evitar rutinas en horarios predecibles.
5) Incorporar servicios de transporte de personal en grupos grandes, con rutas definidas, además del uso de geolocalizadores en cada transporte. ■

Referencias:

1 Escobar, S. (2022). Trabajadores de regreso a la oficina! Edificios corporativos están cada vez menos vacíos. El Economista, Recuperado de: https://www.eleconomista.com.mx/econohabitat /Trabajadores-de-regreso-a-la-oficina-Edificios-corporativos- estan-cada-vez-menos-vacios-20230507-0067.html

2 "La Ciudad de México es la Entidad con más corporativos en el País", Jefatura de Gobierno (CDMX) 06/09/2022 https://www.jefaturadegobierno.cdmx.gob.mx/comunicacion/nota/la-ciudad-de-mexico-es-la-entidad-con-mas-corporativos-en-el-pais

Fotos: Mónica Ramos / SEA

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

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

Cursos de Manejo Evasivo y Defensivo

La capacitación más avanzada del mundo

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

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

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

Programas de Capacitación

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

Contáctanos

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

Email
contacto@as3.mx

Web
as3.mx

Teléfono
+52 1 55 4181 8373

MÉXICO

Antonio Venegas / *Staff* Seguridad en América

Nuevas tendencias en manejo de crisis y continuidad de negocios

Distinguidos miembros de la industria de la seguridad acudieron a la segunda edición de la Cumbre de Seguridad Corporativa, organizada por **Seguridad en América** (**SEA**), teniendo como sede el Centro Citibanamex en la Ciudad de México. Durante dos días (29 y 30 de agosto), los asistentes presenciaron más de 30 conferencias especializadas impartidas por distinguidos expertos representantes del sector enfatizadas en el manejo de crisis y los riesgos corporativos.

CORTE DE LISTÓN

El evento dio inicio en punto de las 08:00 am, con un discurso de bienvenida otorgado por Samuel Ortiz Coleman, director general de SEA, en el que agradeció la presencia de invitados, conferencistas, miembros del gremio, patrocinadores y el *staff* de SEA, ya que, sin ellos, la realización del evento no hubiera sido posible. Posteriormente, el director de esta casa editorial realizó el corte del listón que dio comienzo al magno evento, en compañía de los presidentes de las asociaciones de seguridad más representativas e importantes del país: en reprentación de Brisa Espinosa Ávila, presidente de ASIS Capítulo México; José Luis Alvarado, vicepresidente; en representación de Armando Zúñiga Salinas, presidente de ASUME; Herschel Schultz, director general; Gabriel Bernal Gómez, presidente de AMESP; Ana Guzmán Contreras, presidenta de AMEXSI; David Román Tamez, presidente de ANERPV; Ricardo Bustamante Medina, presidente de AMESIS; Carlos Martínez Sánchez, presidente de ALAS Comité Nacional México; Héctor Robles Conde, presidente de IFPO Capítulo México; Héctor Coronado Navarro, presidente de GEMARC; y Héctor Romero Sánchez, presidente de Círculo Logístico.

ICEBREAKER

Antes de comenzar con las conferencias, Antonio Gaona Rosete, director de Seguridad en Codere México, realizó una actividad denominada *'icebreaker'*, con el objetivo de servir como introducción al evento, enfatizando un poco acerca de los riesgos dentro de la seguridad corporativa y las 4 C's del *crisis management* (cultura, comando, comunicación y control), ofreciendo un mensaje a los asistentes basado en sus conocimientos y experiencia, los cuales también ha compartido en su más reciente libro "Seguridad Corporativa, pieza clave en el ajedrez corporativo". Dentro de la dinámica fomentó la participación y el debate entre los expertos y asistentes, estas participaciones de Antonio Gaona se realizaron al principio y al final de ambos días de la Cumbre.

CONFERENCIAS MAGISTRALES

DÍA 1

La primera conferencia del día 29 de agosto, estuvo a cargo de Salvador Morales, *Senior Director Security and Resiliency* México y Costa Rica de FLEX; y Orlando Poncelis, *Corporate Security Manager*, quienes presentaron la ponencia titulada "Manejo de Crisis en Protección de Productos y Marcas". Dentro de su presentación, Salvador y Orlando compartieron la importancia de mantener reputación y calidad hacia la marca dentro del servicio que se ofrece al mercado. De igual forma, compartieron distintos ejemplos de estas crisis que algunas conocidas marcas han sufrido, este tipo de incidentes que representan una vista negativa dentro de los consumidores. Los expertos compartieron técnicas de manejo ante estas situaciones que pueden ayudar a disminuir el impacto y prevenir el riesgo.

Después fue turno de los conferencistas Gustavo Melo, Corporate Security Manager para Daimler Trucks México; y Arturo Martínez Avalos, director general adjunto para MSPV, con la ponencia titulada "Cómo capitalizar mejores prácticas después de la crisis". En esta presentación destacó la participación de Gustavo, quien compartió su trágica experiencia al sufrir un secuestro. Dentro de su desafortunada experiencia, Gustavo le compartió a Arturo y a la audiencia cómo fueron los procesos que la empresa que lo empleaba al momento del suceso desarrolló para lograr su rescate con éxito, también compartió otros procesos que él mismo implementó dentro de su círculo social, teniendo en cuenta primero la seguridad de su familia. La valentía de Gustavo, así como su resiliencia ante tan traumático hecho fueron aplaudidos por la audiencia, lo que sirvió para ejemplificar con su caso las formas de reaccionar de manera adecuada cuando se presenta una crisis.

Los siguientes conferencistas fueron Dora Elena Cortés, Associate Director of Asset Security & Crisis Management-LATAM para Cargill; y Oscar Arias, LATAM Regional Security Officer para Danone. Su presentación estuvo titulada "Mitos y Realidades del Manejo de Crisis". Dentro de esta conferencia los expertos compartieron una metodología que emplean en el manejo de crisis, que consiste en la predicción, la escalación, la simplicidad, la organización y la preparación.

Ante estos casos, Dora y Oscar coincidieron que es mejor hacer las cosas que obtenerlas perfectas, llamar oportunamente a los expertos hace la diferencia, también que la seguridad corporativa no tiene que estar en todas las batallas durante una crisis, hecho que significa delegar las responsabilidades. Con estas reflexiones terminó su muy completa conferencia, destacando estos principios del manejo de crisis que pueden ser replicados dentro de las organizaciones.

Acto seguido, fue turno de los expertos Jorge Luis Acatitla, director corporativo de Seguridad Integral para Grupo Xcaret; y Erick Mancera, Corporate Director of Security para Karisma Hotels & Resorts, quienes presentaron su ponencia nombrada "Aspectos esenciales en el manejo de crisis en un resort". Como lo indica su nombre, su conferencia estuvo enfocada en el sector turístico, hablando más de su experiencia manejando hoteles y resorts en la zona turística dentro de la Riviera Maya. Jorge y Erick destacaron la importancia de mantener altos estándares de seguridad en este sector, al igual que en otros, por lo que representa el nivel turístico a la economía y el desarrollo del país.

México es uno de los principales destinos turísticos en el mundo, zonas como Cancún, Playa del Carmen, Tulum, etc., representan un gran flujo en la economía, con miles de visitantes nacionales y extranjeros al año, por lo cual la seguridad de estos complejos turísticos es imperativa. Proteger los complejos y a sus visitantes de riesgos como situaciones delictivas, crisis naturales como incendios o huracanes, derivadas por la zona geográfica, y conflictos político-económicos como la problemática en Cancún de los taxistas contra los choferes de plataformas, como Uber y Didi, es lo primordial.

La siguiente conferencia estuvo titulada "Continuidad del negocio en la propiedad de activos fijos", presentada por Paulina Bustos, directora de Seguridad Patrimonial para Clase Azul México; y Mercedes Escudero, presidenta de CPTED México ICA Chapter. Dentro de su conferencia, ambas expertas compartieron un caso de éxito, un proyecto en conjunto con la finalidad de apoyar a comunidades indígenas o en situaciones de falta de desarrollo, como el que ambas desarrollaron en el municipio de Temascalcingo, Estado de México, donde apoyaron a una comunidad mazahua realizando un diagnóstico de las principales necesidades de la comunidad, tanto sociales como de infraestructura.

Posteriormente realizaron el diseño de un plan para abastecer dichas necesidades, mismo que ejecutaron de una manera que al principio fue complicada debido a la naturaleza cerrada de la comunidad, relación que se fue abriendo conforme avanzó el proyecto y que culminó de manera cálida y amistosa. El apoyo a la comunidad en materia de infraestructura como con luz eléctrica, comunicación, pavimentación, etc., así como el refuerzo de actividades sociales y culturales para la integración, trajo consigo una comunidad más sana y prospera, algo que Paulina y Mercedes coincidieron que es una gran retribución junto con la excelente relación con la comunidad. Ambas realizan el proyecto en muchas otras comunidades del país.

La penúltima conferencia del primer día titulada "El rol del director de seguridad ante una crisis corporativa", estuvo a cargo de los expertos Kael Malo-Juvera Castañeda, Regional Security Manager para IBM; y Pedro A. Castolo, Regional Security Director LATAM Regulatory Compliance para Geodis. Ambos expertos reforzaron varios conceptos presentados en anteriores conferencias, aunque también difirieron con algunos, como el hecho de que el director de Seguridad debe estar presente en todos los aspectos de una crisis, declarando que, si bien es bueno delegar responsabilidades, también es importante que el director conozca toda la información y determine cómo y de qué manera actuar ante la crisis, siempre teniendo en cuenta las prioridades. Los conferencistas, como mismos directores de Seguridad, hablaron desde su experiencia en el cargo, conociendo los riesgos, compartiendo técnicas ante el manejo de las situaciones y los procesos que evalúan para las mismas.

La última conferencia del primer día estuvo conformada por un panel con la participación de Gloria Meléndez, directora de Prevención de Pérdidas para Grupo Chedraui; Coral Meza Hidalgo, gerente de Seguridad y Resiliencia LATAM para Levi Strauss & Co.; Jorge Rodríguez, director de Seguridad para Soriana; Iván Gustavo Islas, director de Prevención de Pérdidas para Palacio de Hierro; Juan Ramón Becerra, gerente nacional e Inteligencia y Prevención del Delito para Grupo Coppel; y José Arturo Moreno, gerente de Prevención de Pérdidas para Palacio de Hierro. En el panel, los expertos de las empresas compartieron sus técnicas al enfrentarse a crisis con características en común dada la similitud de sus organizaciones.

DÍA 2

El segundo día de la Cumbre de Seguridad Corporativa comenzó con una conferencia a cargo de Alicia Sorroza, directora de Seguridad Corporativa para DHL Supply Chain. La conferencia llevó por nombre "Seguridad en la cadena de suministro: innovación, estandarización y cultura de Seguridad", en la que compartió conceptos que utiliza en su área como la innovación y la estandarización para mejorar los procesos, reducir errores y tiempos de entrenamiento, aumentar eficiencia, mejora la flexibilidad, creatividad y facilita el cambio.

Hablando de los cambios, Alicia compartió un esquema que representa los tipos de cambio y la curva de la resiliencia ante éste. Comentó que los cambios pueden ser tecnológicos, estructurales, de productos o servicios, culturales o personales. Estos procesos pueden ser útiles en la cultura de la seguridad y los beneficios que trae consigo son vastos.

La segunda conferencia del día estuvo a cargo de dos expertas en la seguridad: Ana Guzmán, directora de Seguridad Corporativa para GICSA; y Midori Llanes, comisaria de ASIS Capítulo México 217. Ambas profesionales compartieron casos de crisis que enfrentaron en sus respectivos sectores. Ana compartió dos casos que sucedieron en los centros comerciales que maneja GICSA, el primero fue una balacera que se presentó en el centro comercial Forum Cuernavaca, el cual no contó con heridos y al parecer fue una falsa alarma.

El segundo hecho fue una mujer que cometió suicidio en la plaza de Forum Buenavista en la Ciudad de México, algo que desafortunadamente se ha vuelto común en este centro comercial, Ana compartió las estrategias implementadas en ambos casos, diferentes por la variedad de los hechos.

Por otro lado, Midori expuso algunos casos de su experiencia en la Dirección de Seguridad en Gas Natural Fenosa, como los destrozos en el pueblo de Juchitán, Oaxaca, generados por el temblor del 19 de septiembre de 2017, y el otro fue la explosión de una casa en San Nicolás de los Garza, Nuevo León, gracias a una fuga de gas. Midori, de igual forma, explicó los procesos que se realizaron en ambos casos. Las expertas coincidieron con varios conceptos mencionados en conferencias anteriores para el manejo de las crisis.

Después continuó la conferencia de Lourdes Morales, líder tribu de Prevención Legal para Walmart; y Gonzalo Alamillo, director de Seguridad Integral para Grupo Alsea, titulada "Descontinuando para continuar y avanzar en los negocios". Ambos expertos en el área de retail, compartieron sus estrategias de manejo para el desarrollo del sector. Gonzalo explicó los procesos que Alsea conlleva en sus múltiples negocios que incluyen marcas grandes como Starbucks, Burger King, Vips, entre muchas otras; mientras que Lourdes compartió el desarrollo que Walmart ejecuta al ser una de las tiendas más grandes y con mayor presencia tan sólo a nivel nacional. El entender el nivel de ambas organizaciones es comprender que la innovación y el constante cambio o adaptación ante el desarrollo del negocio es imperativo.

Los siguientes en presentarse fueron Fabiola Enríquez, gerente general de Prevención para Grupo Presidente; y Rodrigo Funcia, Country Security Manager para Abbie Farmacéuticos. Su conferencia estuvo titulada "Lecciones aprendidas en el manejo de crisis", en la que ambos expertos definieron si las situaciones que se presentan entran como crisis, los procesos que se determinan al reaccionar ante las crisis y la ejecución de planes establecidos para acatar dicha crisis.

De igual forma, compartieron recomendaciones para el manejo como ser positivos, establecer áreas de oportunidad, evitar culpar o responsabilizar a otros de los fracasos, evaluar el comportamiento de los líderes ante las crisis, así como las estrategias que contribuyeron al éxito. La experiencia de ambos conferencistas les permitió compartir sus estrategias en el manejo de crisis.

La siguiente conferencia estuvo titulada "Manejo de crisis y continuidad operativa en instalaciones hospitalarias", impartida por Enrique Higuera, director de Prevención de Riesgos para Médica Sur; y Francisco Javier Villegas, subdirector de Protección Patrimonial para Christus Muguerza. Ambos expertos enfocaron su conferencia al sector hospitalario, detallando cómo han manejado diversas crisis que van desde situaciones de carácter delictivas como grupos armados que entran a las instalaciones a atacar a pacientes específicos, o crisis de nivel mundial como la pandemia por COVID-19, y que, si bien la enfermedad no ha cesado y se sigue tratando, el impacto ya no es tan grave comparado con años previos. La volatilidad de las crisis presentadas en este sector implica distintas estrategias para el manejo y distintos procesos para acatar estas situaciones.

Antes de concluir tocó el turno de Juan Antonio Bernal, director Senior de Seguridad y Gestión de Crisis LATAM para G.E.; y Darío Preza, Brand Protection, Security & Resilience Director, North Region para FLEX, quienes se presentaron con una conferencia titulada "Gestionando la Crisis en entornos hostiles". Dentro de su plática, ambos expertos destacaron la importancia de conocer el umbral de riesgo de la organización, compartiendo estrategias de mitigación ante la gestión de crisis en entornos hostiles con un esquema de probabilidades y significados, y derivado de esto señalar cómo reducir la amenaza, reducir las consecuencias, reducir o eliminar la exposición y transferir riesgos.

La última conferencia del evento llevó por nombre "Centro de Control y Manejo de Emergencias", presentada por Carlos Mera, gerente de Seguridad de Arcos Dorados (McDonald's); y Marco Alejandro Hernández, director de Prevención de Pérdidas y Siniestros para Grupo Salinas. Ambos expertos manejan los procesos de seguridad de dos marcas importantes y posicionadas dentro del país. Carlos compartió los procesos y estrategias que Arcos Dorados (McDonald's) implementan en las miles de sucursales que hay en el país, apoyando a los empleados, en su mayoría jóvenes, estableciendo manuales de prevención y botones de alerta que sirvan ante una crisis, entre otras implementaciones.

Por otro lado, englobando marcas como Elektra, Banco Azteca, Totalplay y TV Azteca, dentro de Grupo Salinas, se entiende que las situaciones de crisis pueden ser de distintas características. Marco compartió casos de crisis generadas dentro de algunos complejos, así como la forma de evaluar la situación y generar un plan de acción, así como analizar las consecuencias para prevenir la reincidencia del suceso.

ENTREGA DE PREMIOS

Después de la participación final de Antonio Gaona, se dio paso a la entrega de premios, entre los que estuvieron sistemas antihackeo para diversos dispositivos, una beca para el EP SUMMIT, y un viaje a Cancún, Quintana Roo, por tres días y dos noches, con todos los gastos pagados. Posterior a la entrega, Samuel Ortiz Coleman otorgó unas palabras de cierre en las que agradeció la asistencia, a los ponentes por sus extraordinarias conferencias, el apoyo de los patrocinadores y el equipo de SEA, y, por último, invitó a los asistentes a concluir con un brindis de honor.

A lo largo de ambos días, distintas empresas enfocadas en el desarrollo de productos y servicios para la seguridad, y que fungieron como patrocinadores del evento, estuvieron presentes e incluso algunas establecieron stands afuera de la sala, entre ellas estuvieron ADISES, Altair Consulting & Training, CIA Kapital, Density, Dilme, Everbridge, Siayek, JVP, M360, Protectio, PSI, SCATI, SISSA, Solcat y Tracking Systems. Los asistentes tuvieron la oportunidad de conocer las empresas, así como su amplia variedad de productos y servicios para el sector.

De esta manera, el evento que tuvo como objetivo ampliar el conocimiento sobre los temas de manejo de crisis, generar networking en los asistentes, y promover el aprendizaje y la actualización en materia de seguridad, concluyó su segunda edición. La III Cumbre de Seguridad Corporativa se llevará a cabo en agosto de 2024, contando con más conferencias, nuevos temas y siempre con el objetivo de promover la cultura de prevención, la innovación, las estrategias, el conocimiento y aprendizaje que trae consigo implementar la seguridad. ■

Fotos: Mónica Ramos y Antonio Venegas / SEA

amesis MR

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

24/365 DÍAS
Atención personalizada de nuestro centro de monitoreo.

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

ACCESO
Total acceso a reportes de estadísticas de robos.

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

NUESTROS SOCIOS

Tracking Systems de México S.A. de C.V. · sintel Seguridad Satelital · Holkan Rastreo Satelital · skyguardian · skymeduza · ADS LOGIC Telematics · SECUREWITNESS · INFO TRAX · TECNO LOGISTIK · RAINDE · SEGURIDAD360.com · ATLANTIDA · GEOTRACKING Rastreo Satelital · Tecno GPS · TTC · DUMAX Smart Tracking · ISIS Seguridad Integral · GEOTRUCKS · GRUPO ALFIL · SEC Soluciones · RCU Sistemas · TSVISION · MAGNI Tracking · GPSMonitor Rastreo Satelital · GPS TRACKER MX Vamos contigo · SATECH · BLNC

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

COMUNÍCATE
55 3334 4707

SAN JUANICO: UNA TRAGEDIA DIFÍCIL DE OLVIDAR

Más de 500 personas perdieron la vida por la falta de prevención en San Juan Ixhuatepec (Edo. Mex.), a 39 años de este suceso, aún hay lecciones por aprender

Foto: Freepick

MÉXICO

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

La madrugada del 19 de noviembre de 1984, las estruendosas explosiones en una de las plantas de almacenamiento y distribución de PEMEX (Petróleos Mexicanos) en San Juan Ixhuatepec, Tlalnepantla, Estado de México, provocadas por la fuga de gas, fueron el comienzo de una de las tragedias más lamentables del país.

"De acuerdo con las crónicas publicadas en Excélsior, se registraron 11 explosiones. En cada una de ellas las llamas se elevaron a cientos de metros. Los registros fotográficos exhiben a gente corriendo desnuda, con quemaduras, cargando niños, huyendo del infierno, mientras los rugidos ensordecedores de las llamas retumbaban por todo el valle de San Juanico"[1].

Las llamas que resultaron a consecuencia de la fuga de gas licuado de petróleo 4\u200b, alcanzaron hasta los 600 metros de altura, provocando la muerte de más de 500 personas (carbonizadas, asfixiadas por el gas propano o a consecuencia de serias quemaduras), y de acuerdo al portal del Gobierno de México, fueron más de siete mil personas las que sufrieron algún tipo de lesión.

Han pasado 39 años de este hecho tan lamentable, considerado "uno de los peores accidentes industriales" registrados, y que ocurrió en un lugar donde no se contaba con un departamento de Protección Civil ni Bomberos, en donde todas las personas se vieron superadas y sin poder reaccionar para salvaguardar su vida y la de sus familias, a todas y cada una de esas personas que presenciaron y perdieron a sus seres queridos, nuestras más sentidas condolencias.

ANTECEDENTES

Fue en la década de los 50 que, como resultado de la urbanización y el crecimiento de los municipios conurbados de la Zona Metropolitana del Valle de México, se fomentó la industrialización en municipios como Ecatepec, Naucalpan y, en este caso, Tlalnepantla de Baz. En 1959, los gobiernos estatales y federales comenzaron una serie de expropiaciones de tierras de ejido para el establecimiento de industrias, y es de esta manera como la empresa de Petróleos Mexicanos establece una planta que procesaría gas licuado de petróleo proveniente de distintas refinerías del país, en el poblado de San Juan Ixhuatepec, popularmente conocido como San Juanico, en la zona oriente de Tlalnepantla.

La infraestructura de las plantas establecidas por PEMEX, mantenía niveles de riesgos de bajos a intermedios, niveles que se consideraban aceptables para las industrias que realizan este tipo de actividades. Sin embargo, reportes indicaban que se contaba con diversas estructuras encargadas de la detección y prevención de cualquier incidente que se presentara.

La madrugada del 19 de noviembre, testigos aseguraron que a las tres de la mañana se percibía un fuerte olor a gas. Reportes posteriores indicaron que trabajadores de la planta realizaron peticiones reiteradas a la empresa por falta de mantenimiento en estructuras y piezas fundamentales como algunas válvulas que se encontraban dañadas. Se reportó que, en ese momento, 55 personas se encontraban laborando en la planta.

CAUSAS Y AFECTACIONES

De acuerdo con el Centro Nacional de Prevención de Desastres (CENAPRED), "la capacidad total de almacenamiento en las instalaciones de PEMEX era de 16 mil metros cúbicos de gas LP, distribui-

Foto: Infobae

"Los desastres ocurren cuando no hay apego a las normas y disposiciones que establecen medidas de prevención en cualquier ámbito"

dos en seis esferas y 48 cilindros de diferentes capacidades, que provenía de las refinerías de Minatitlán, Coatzacoalcos y Azcapotzalco.

El accidente inició debido a la ruptura de una tubería de 20 centímetros de diámetro que transportaba gas LP. Probablemente diez minutos después se originó un incendio, al encontrar el gas una chispa, generándose una serie de explosiones tipo explosión de vapores que se expanden al hervir el líquido (por sus siglas en inglés, BLEVE)"[2].

Las explosiones que duraron hasta el día siguiente (20 de noviembre), además causaron que 60 mil personas fueran evacuadas, y alrededor de 149 viviendas destruidas, sin dejar de lado que la planta de PEMEX quedó totalmente destruida.

"De los estudios realizados a lo largo de los años, se determinó como causas probables: la falta de sistemas de detección de posibles fugas de gas, de mantenimiento a los equipos e instalaciones y la fractura en la tubería que transportaba gas LP a las plantas de almacenamiento que estaban cerca de los parques conformados con tanques compuestos por seis esferas y 48 cilindros de diferentes capacidades, así como la falta de previsión al haber instalado dicho complejo al pie de un asentamiento urbano que carecía de las medidas mínimas de protección", explicó en entrevista Jacqueline Flores Alvarado, especialista en *Safety*.

La especialista comentó que la forma en la que pudo haberse evitado esta desgracia, consiste en establecer medidas preventivas en el manejo de riesgos químicos, apegándose a las normas dictadas para este tipo de riesgos y sobre todo, que se debió haber realizado un análisis de riesgos y un estudio de factibilidad para definir el establecimiento de este complejo en un parque especial para industrias de origen químico, distantes a cualquier mancha urbana.

Sin embargo, las familias que perdieron la vida, vivían en viviendas "precarias" a menos de 150 metros de los tanques de almacenamiento de gas LP. "Los desastres ocurren cuando no hay apego a las normas y disposiciones que establecen medidas de prevención en cualquier ámbito", señaló Jacqueline Flores.

LA NECESARIA PRESENCIA DE PROTECCIÓN CIVIL

Hay quienes todavía hoy en día, no contemplan a la Seguridad como un área prioritaria, no sólo en alguna organización, empresa, institución, sino en la vida cotidiana de cualquier ser humano. En la "Crónica de San Juanico: los hechos, las interpretaciones, las mitologías", de Carlos Monsiváis, el autor describe detalle a detalle el sufrimiento de las víctimas, así como la actuación de las autoridades y el cuerpo de Bomberos, que aunque se vieron superados por la catástrofe y no había elementos locales para auxiliar al momento, hicieron todo lo que pudieron para resolver la situación.

"Desde las siete, el esfuerzo del cuerpo de bomberos se concentra en impedir la explosión de la esfera, que provocaría un desastre aún más drástico. Los bomberos y los socorristas (de la Cruz Roja, la Cruz Verde, etcétera) inician la evacuación de los habitantes de las colonias aledañas a San Juanico. A las 08:10 am, el III Batallón de la Policía Militar acordona la zona, evita el paso a los sitios más riesgosos y dirige la salida de quienes aún se resisten a hacerlo. Los socorristas trasladan heridos, muchos de ellos mutilados y en condiciones muy graves, a distintos hospitales. Se corre sobre cadáveres. En la carretera México-Pachuca el tránsito se congestiona. Los damnificados suplican se les aleje del infierno"[3].

Tanto PEMEX como las autoridades de San Juan Ixhuatepec, carecían de medidas de prevención, planeación, organización, equipamiento y personal calificado. "En cualquier sociedad, las Autoridades juegan un papel preponderante en la gestión de riesgos. Su participación es fundamental en la definición y respuesta ante cualquier emergencia que ponga en riesgo la integridad de las personas", comentó Jacqueline Flores.

LA RESPUESTA DE LAS AUTORIDADES

Distintas fuentes indican que el número de víctimas fue mucho más alto, pero no pudieron ser contabilizadas debido a la magnitud del accidente. En días posteriores comenzaron las actividades de entierros de los fallecidos y sus restos en panteones aledaños a la zona. Muchas de estas personas fueron inhumadas como anónimas, debido a las condiciones de la tragedia, en fosas comunes.

Más de 10 mil personas fueron trasladadas a sitios cercanos que fueron habilitados en función de albergues como la Basílica de Guadalupe y las instalaciones de Zacatenco del Instituto Politécnico Nacional (IPN). El suceso atrajo la atención mediática tanto nacional como internacional.

En materia gubernamental, el lugar fue visitado por Miguel de la Madrid, presidente de la república en ese entonces, y por Alfredo del Mazo González, gobernador del Estado de México, la noche del 20 de noviembre. Como mandato presidencial, se creó la Comisión Intersecretarial de Auxilio a los damnifica-

Foto: Infobae

"San Juanico para todos representó un parteaguas entre una emergencia tradicional y una hecatombe. Hoy día, quienes lo vivimos desde los aparatos de televisión o desde el radio de nuestras casas, podemos reflexionar sobre las diferentes formas de aprender de este triste suceso"

dos de San Juan Ixhuatepec, la cual dispuso de cantidades millonarias tanto para la atención de víctimas, como para la reconstrucción de viviendas y el pago de indemnizaciones.

Por otro lado, Mario Ramón Beteta, director de PEMEX (Petróleos Mexicanos), así como diversos funcionarios del gobierno, trataron de señalar a las gaseras privadas que distribuían gas en torno a la planta, como responsables de la tragedia. No obstante, gracias a la movilización popular y a la presión social y mediática, el 22 de diciembre de 1984, la Procuraduría General de la República (PGR) determinó como responsable de las explosiones a PEMEX, quienes comenzaron con el pago de indemnizaciones en 1985. Dicho proceso se vio afectado con irregularidades y corrupción, según informaron reportes periodísticos.

GESTIÓN DE RIESGOS QUÍMICOS EN MÉXICO

De los errores y las tragedias se aprende, y definitivamente la gestión de riesgos químicos en México ha evolucionado ya que hoy en día existe legislación específica para cada tipo de riesgo, así como la forma de almacenarlos, clasificarlos, transportarlos y en su caso sancionarlos. La especialista enumeró algunas de las medidas preventivas que se implementaron en el país después de lo sucedido en San Juanico:

- Desarrollo de una cultura de la prevención de riesgos.
- Contratación de especialistas certificados en riesgos químicos.
- Desarrollo de Instituciones destinadas a la prevención de riesgos químicos.
- Desarrollo de una cultura de protección Civil.
- Creación de instituciones especializadas en el desarrollo y certificación de profesionales en el manejo de riesgos químicos.
- Desarrollo de leyes y reglamentos por cada tipo de riesgo.
- Aplicación de sanciones por negligencia y/u omisiones a la ley.

Ahora bien, en cuanto a las empresas dedicadas al tratamiento de productos químicos o de alto riesgo que comparten, por una u otra razón, territorio con poblados, la especialista nos compartió las siguientes recomendaciones:

- Verificar con las autoridades si su establecimiento en la zona está autorizado, en caso de que sea negativa solicitar la aplicación de la legislación correspondiente.
- En caso de que la respuesta sea afirmativa, solicitar a la autoridad una capacitación por parte de la empresa para conocer el plan de emergencia y qué tipo de riesgo es el que maneja la empresa.
- Solicitar simulacros para la población de acuerdo con el tipo de sustancia química que maneje la empresa.
- Conocer si la empresa cuenta con un hospital y/o seguro para la población en caso de emergencia.

DESAFÍOS PERSISTENTES

Además de lo que ocasionó las explosiones de 1984, las industrias que concentran y manejan productos químicos o de otra índole que resulten peligrosos, deben realizar un análisis de riesgo cuidadoso e irlo actualizando, tanto en el sector público y privado, ya que los desafíos de seguridad están al día.

"Es importante para la prevención de riesgos químicos o de otra índole, realizar inspecciones estrictas y continuas a las plantas, así como regularizar todas las industrias de riesgo de tipo químico, y el traslado de estos productos. De igual manera evitar la instalación de estas industrias en zonas urbanizadas, establecer sanciones más contundentes para evitar la corrupción o el mal manejo de los materiales, y crear campañas de sensibilización y capacitar a las poblaciones donde ya están instaladas dichas empresas", puntualizó Jacqueline Flores.

LECCIONES APRENDIDAS

Todo evento o catástrofe además de dejar una huella de devastación, debe dejar un aprendizaje en la sociedad para no repetir sus errores.

"San Juanico para todos representó un parteaguas entre una emergencia tradicional y una hecatombe. Hoy día, quienes lo vivimos desde los aparatos de televisión o desde el radio de nuestras casas, podemos reflexionar sobre las diferentes formas de aprender de este triste suceso", es por ello que nuestra entrevistada nos compartió algunas de las lecciones aprendidas que, desde sus conocimientos y *expertise*, le dejó esta lamentable tragedia.

1. Respetar las áreas destinadas a la vivienda antes de instalar parques industriales de alto riesgo (apego a la legislación).
2. Realizar una estricta planeación de las emergencias.
3. Certificar al personal destinado a atender emergencias y equiparlo correctamente.

JACQUELINE FLORES ALVARADO, ESPECIALISTA EN *SAFETY*

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

4. Desarrollar centros de entrenamiento y de atención de emergencias.
5. Con base en la experiencia, realizar una detección minuciosa de necesidades para definir el equipamiento acorde al tipo de riesgo.
6. Contar medios eficientes de reporte y respuesta a las emergencias.
7. Definir vías de escape o rutas de evacuación que contribuyan al desalojo inmediato de las zonas urbanas comprometidas en una emergencia mayor o desastre.

SAN JUANICO NO SE OLVIDA

Varios incidentes cercanos a la zona se han registrado en fechas posteriores a la explosión, aunque en menor magnitud. En noviembre de 1990, aconteció una explosión y un incendio en una planta de PEMEX; y en noviembre de 1996, dos depósitos de gasolina regular estallaron en la planta de Satélite Norte, el incendio pudo combatirse hasta la madrugada del día posterior y fuentes oficiales reportaron dos muertos y 12 heridos; en esta ocasión, los mecanismos de alerta y evacuación funcionaron correctamente y se pudo evacuar la zona para minimizar el daño.

Las consecuencias emocionales en la comunidad siguen latentes, a lo largo de estos años se realizan misas y ceremonias en conmemoración de las víctimas de la explosión. El año pasado, Marco Antonio Rodríguez, presidente actual de Tlalnepantla de Baz, llevó a cabo una ceremonia de conmemoración en el Parque Hidalgo, lugar que fue donde se encontraban las esferas que detonaron aquella madrugada, para honrar la memoria de los familiares y vecinos de la localidad, posteriormente se dio un recorrido hacia el panteón municipal de Caracoles, en San Isidro Ixhuatepec, donde se develó una placa conmemorativa al aniversario luctuoso.

Se espera que las mismas actividades sean realizadas en noviembre de este año, cumpliéndose 39 años de esta tragedia. Los habitantes de la zona siguen intranquilos, ya que, incluso después de tantos años, las personas indican reportes de olor a gas. Asimismo, se siguen presentando sucesos como incendios de empresas, o fugas de sustancias tóxicas; ante esto, los habitantes de San Juanico han optado por resolver estas situaciones por cuenta propia, ante la falta de respuesta y atención de las autoridades.

Testimonios recalcan las afectaciones que las zonas industriales representan para las personas, ya que, si bien son una fuente de empleo para las comunidades, su presencia y establecimiento tan cercana a zonas urbanas donde las familias viven, representa un peligro y un riesgo latente. Aun así, decenas de gaseras siguen operando en la zona y realizando transporte de cientos de cilindros de gas licuado de petróleo hacia la Zona Metropolitana del Valle de México. ■

Referencias:

[1] *"Así fue la explosión de San Juanico", Excélsior. Arturo Páramo y Agencias, 19/11/2019 https://www.excelsior.com.mx/comunidad/asi-fue-la-explosion-de-san-juanico/1348517*

[2] *"A 35 años del 19 de noviembre de 1984", Centro Nacional de Prevención de Desastres | 19 de noviembre de 2019. https://www.gob.mx/cenapred/articulos/a-35-anos-del-19-de-noviembre-de-1984*

[3] *"Crónica de San Juanico: los hechos, las interpretaciones, las mitologías", Carlos Monsiváis. Cuadernos Políticos, número 42, México D.F., ed. Era, enero-marzo,*

Foto: Infobae

EN MEMORIA DE
FERNANDO POLANCO SÁNCHEZ

MÉXICO

Antonio Venegas / *Staff* Seguridad en América

Un gran amigo, profesional de la seguridad y excelente ser humano que deja un legado lleno de experiencias, aprendizajes y abrazos apachurrados

El gremio de la seguridad privada sufrió una gran pérdida recientemente, alguien a quien muchos consideraron amigo, hermano, colega, compañero, padre, ser querido, ha trascendido. Fernando Polanco Sánchez es sinónimo de alegría, disciplina, esfuerzo, innovación, y muchos otros adjetivos, pero más allá de eso, los recuerdos, las experiencias y los aprendizajes que deja es lo que hacen que su figura permanezca grabada en las vidas de aquellos con quienes coincidió. Hablar de alguien tan emblemático no es sencillo, por lo cual, para honrarlo, personas queridas y cercanas a él compartieron un poco de lo mucho que significó y lo que deja Fernando en sus vidas.

SEMBLANZA

Fernando Polanco Sánchez contó con una amplia experiencia que lo hizo convertirse en un personaje importante al momento de hablar de la seguridad privada. Académicamente, se graduó como Licenciado en Psicología, con estudios en Ingeniería Industrial, con un posgrado en Dirección de Seguridad en Empresas en la Universidad Pontificia Comillas de Madrid, y múltiples diplomados en Habilidades para el Directivo de la Seguridad Integral y en Dirección de Programas de Protección Civil, por mencionar algunos; contó con distintas certificaciones como en Ciberterrorismo por el Instituto Superior de Seguridad Israelí, su certificación en Crisis Management por ASIS International y uno como consultor y capacitador por la STPS, Protección Civil y Entidades Federativas. Además, fungió como docente de varios diplomados especializados en distintas áreas como Liderazgo y Gerencia Integral en Seguridad, la Industria de la Música y Espectáculo, Habilidades para el Directivo de Seguridad Integral y en Protección Civil y Prevención de Desastres, impartidos en distintas instituciones de renombre como la Universidad Panamericana, la Universidad Anáhuac México Norte, entre otras.

DENTRO DE LA COMUNIDAD DE LA SEGURIDAD

Profesionalmente, su experiencia fue vasta, pero sin duda, destaca su labor como director de Seguridad Integral en Corporación Interamericana de Entretenimiento (Grupo CIE), donde desde el año 2000, desempeñó los esfuerzos que caracterizaron a los espectáculos de entretenimiento más importantes de México. Su presencia dentro de las asociaciones de seguridad también fue muy activa, Fernando fue miembro de ASUME (Agrupación de Asociaciones Unidas por México), presidente de la Asociación Mexicana de Especialistas en Seguridad Integral (AMEXSI) en el periodo de 2015 a 2016, y por supuesto, fungió como presidente de ASIS International Capítulo México en el año 2020, donde también ocupó otros cargos dentro de la mesa directiva como vicepresidente de Enlace, coordinador de Comités y vicepresidente ejecutivo.

UN GRAN AMIGO, PADRE, PAREJA, SER HUMANO

Para conocer un poco más sobre la persona que fue y que seguirá siendo Fernando, platicamos con Emilia Vidal, "Mili", directora general en Lafayette México, presidenta del Consejo Nacional de Mujeres Empresarias y pareja sentimental de Fernando desde hace dos años, quien externó unas palabras para recordarlo de la mejor manera: "Fernando siempre fue un hombre muy generoso, era muy buen amigo, muy buen hermano, muy buena pareja y muy buen padre. Adoraba a sus hijos: Sofía y Max, la luz de sus ojos, y su hija mayor, Minerva. Un hombre que nunca dejaba solo a nadie cuando le pedían ayuda. Él tenía más hermanos por decisión de vida que de sangre, y a ellos los consideraba, los veía y los procuraba".

"Siempre fue un hombre que se preocupaba por los demás, no por lo que representaban, sino por los seres humanos realmente, disponía de su tiempo para poder estar ahí, escuchando. Un hombre siempre alegre, que nunca se quejaba de nada, así estuviera enfermo, siempre buscaba cómo salir adelante de cualquier situación, es algo que admiraba de él, siempre estaba dispuesto ante lo que la vida le quisiera mostrar, un hombre que vivió a su manera, la cual también recuerda una de sus canciones favoritas", expresó Emilia.

Emilia describió a Fernando como una persona que optaba por el contacto humano en lugar de usar aparatos tecnológicos, señalando la importancia que le daba a la comunicación humana en su vida: "Siempre fue un hombre muy detallista, en cumpleaños, o si sabía que alguien estaba pasando por un momento difícil, él procuraba estar ahí, sabía que la presencia física, el escuchar, el ver, el sentir era importante para cualquier ser humano y eso es algo que promulgaba con todas las personas a su alrededor. En la pandemia, él salvo vidas, estaba a cargo del Hospital Citibanamex, procurando a las personas que sabía que estaban enfermas, siempre estuvo arriesgando su propia vida para poder salvar la vida de otros", comentó.

INNOVANDO Y PREVINIENDO SIEMPRE

En el ámbito profesional, Emilia pudo externarnos un poco sobre su excelente desempeño y trayectoria, describiéndolo como alguien disciplinado enfocado en su trabajo y que generaba un impacto: "Fue siempre un hombre que impactó con ideas, siempre impactó con su propio sello como ser humano. En ASIS firmaba de verde, porque era su color favorito. Como colaborador, era un hombre muy brillante, siempre preocupado por la Protección Civil, por el cuidado, por la prevención, por cosas que tal vez mucha gente le pareciera normal pero era para una cuestión de prevención. Siempre quiso innovar, siempre estuvo presente en lo que se dedicaba que era el entretenimiento, algo en lo que, cuando le preguntaban a qué se dedicaba, él respondía 'a cortar boletos', además destacaba la importancia de estar en el filtro de prevención, para poder detectar situaciones que pudieran ser problemáticas en algún evento. Siempre estaba a la vanguardia, siempre le gustaba aprender y aprendía de los desastres de los demás".

"ÉL PROCURABA ESTAR AHÍ, SABÍA QUE LA PRESENCIA FÍSICA, EL ESCUCHAR, EL VER, EL SENTIR ERA IMPORTANTE PARA CUALQUIER SER HUMANO Y ESO ES ALGO QUE PROMULGABA CON TODAS LAS PERSONAS A SU ALREDEDOR"

"Él fue innovador implementando protocolos para los eventos tan grandes que manejaba como la Fórmula 1, ésta no se hacía en un día, yo pude constatarlo que se empezaba a desarrollar desde el primer día posterior al final de la Fórmula 1 anterior. No era algo simple, Fernando coordinaba todo, tenía una mente tan grande que todo era como un reloj. No era lo mismo desarrollar este evento en países como Estados Unidos u otras naciones donde finalmente la seguridad no era tan complicada porque él tenía que lidiar con muchas cosas, no sólo la gente, sino con lo que se podía suscitar, con la prevención, con la seguridad, y supervisaba personalmente que todo estuviera en orden, un proceso que conllevaba esfuerzos todo el año. En este tipo de eventos masivos, él siempre estuvo al pendiente, cuidando que no sucediera absolutamente nada, porque sabía que cualquier situación podía afectar a lo que él más amaba que era a su país", agregó.

AMOR POR MÉXICO

Fernando era una persona que se caracterizaba por su amor a la nación, el servirla y mejorarla era algo que disfrutaba, y dejando de lado los partidos políticos, trataba con respeto y dedicación los símbolos nacionales, tal como detalló Emilia: "El servicio al país, a la investidura presidencial, a los mexicanos era parte de su mandamiento, él amaba al lábaro patrio, nunca perdía la oportunidad de tomarse una foto cuando lo veía, era algo que disfrutaba. No conozco ser humano que pudiera disfrutar tanto estar sirviendo al país. Además, quería que las nuevas generaciones pudieran llegar a apasionarse por el servicio a la patria. Siempre respetaba la investidura presidencial, porque como mexicano cuidaba la investidura sabiendo que cuidaba nuestro país. Una de sus cosas favoritas era ver como hondeaba la bandera de Campo Marte sentado en el pasto. Volar era una de sus grandes pasiones en conjunto con las motocicletas. La parte institucional también es algo que para él fue muy importante, algo tan sencillo como un corte de cabello, perfectamente alineado, siempre pulcro con su ropa, era un hombre de disciplina y costumbres".

ABRAZO APACHURRADO

Su personalidad efusiva y carismática eran rasgos característicos de Fernando, quien no dudaba en demostrar su afecto en maneras emblemáticas para sus conocidos y sus seres queridos. "Algo que lo caracterizaba era el lema "Que la fuerza te acompañe", al ser fanático de Star Wars, o su particular "abrazo apachurrado", que consistía en abrazar y cargar a las personas de tal manera que te dejara sin aire, ya lo conocían, a donde fuéramos, ya sea en la calle, en un restaurante, etc., él iba y les daba un abrazo apachurrado a quien se dejara".

LEGADO

Al cuestionarle qué es lo que le deja el haber compartido su vida con Fernando, Emilia reflexionó: "Su legado es estar haciendo siempre lo mismo para que no te pase nada que sea diferente, habrá cuestiones externas que pueden llegar a surgir, pero justo ese blindaje, no descuidar absolutamente nada, porque en el momento en el que bajas la guardia es cuando se puede dar el suceso, eso lo hacía en su vida diaria, su seguridad dependía precisamente de él, de todos sus protocolos que él mismo instituía".

"Su legado es el servicio a la patria, fue un hombre que hizo cosas extraordinarias, desde luchar con un cocodrilo que andaba por ahí en una situación de inundaciones en Tabasco, hasta resguardar los Hospitales de Citibanamex y estar al pendiente que no ocurriera ningún desastre. Su película favorita era Top Gun, además de "A mi manera", "La incondicional" era de sus canciones preferidas, le encantaba por los aviones y lo que mostraba. Esa es una forma de recordarlo. Un hombre muy comprometido, alguien que sabía que el deber estaba antes que cualquier cosa, y a pesar de que le dolía al dejar a sus hijos, para él el deber era importante. Eso era lo que Fernando Polanco siempre intentó compartirle a todos".

El pasado 18 de septiembre, se le organizó una misa para conmemorar su partida en la Iglesia Club de Golf en Tlalpan en la Ciudad de México, Emilia detalló que en la ceremonia estuvieron presentes sus hijos en compañía de su madre, amigos, familia, vecinos, gente cercana a la pareja, miembros de asociaciones como AMESP y AMEXSI, gente de instituciones como la Marina, y sobre todo quienes estuvieron en su vida a nivel personal.

"Un hombre muy comprometido, alguien que sabía que el deber estaba antes que cualquier cosa, y a pesar de que le dolía al dejar a sus hijos, para él el deber era importante. Eso era lo que Fernando Polanco siempre intentó compartirle a todos"

EN HONOR A NUESTRO QUERIDO FERNANDO

La tarde del 28 de septiembre, amigos cercanos de Fernando pertenecientes al gremio se reunieron en el restaurante Torre de Castilla en la Ciudad de México, para disfrutar una comida en honor de quien fuera su colega y hermano. Algunos de ellos lo recordaron y expresaron unas palabras hacia él:

"Un gran amigo, alguien con quien siempre que necesité de algo lo tuve junto a mí, muy joven, muy inquieto y pues lo que nos deja a nosotros es esta reunión donde nos convoca a 30 amigos que lo queremos de corazón", comentó Arturo Ávila, presidente de Share y Asociados.

"Considero que el hacer esta comida en su honor refleja el cariño, la amistad, el profesionalismo y todo aquello que él promulgaba con su famoso abrazo apachurrado, el cual nos hacía sentir siempre aceptados y dispuesto siempre a ayudarnos a resolver cualquier tipo de situación. Mucho gusto poder estar comentando esto y, simplemente, que descanse en paz", compartió Thomas Gottlieb, CEO de Vongosslar Consulting Group.

"Estamos reunidos el día de hoy recordando al buen amigo Fernando Polanco y sus abrazos apachurrados, gran personaje de la seguridad con una personalidad única que lo hacía inconfundible, pero sobre todo un gran amigo, gran profesional, conocedor de su negocio, de los mejores en cuestión de la seguridad de eventos masivos y Protección Civil. A mí no me resta más que comentar que estoy aquí con mucho gusto en su memoria, y donde quiera que esté, le mando un abrazo apachurrado. Fer, que Dios te bendiga y cuídanos a los que nos quedamos por acá", expresó José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México.

"Para mí, Fer fue un gran amigo, un buen compañero, siempre ayudando a todos en la hermandad y obviamente siempre deseándonos a todos abrazos apachurrados, igualmente yo creo que ahorita nos está aventando sus apapachos a todos. Le deseo a su familia que tengan una pronta resignación", compartió Zeferino Guzmán, asesor externo de seguridad.

"Admiré mucho a Fernando porque, además de que era un estupendo ser humano y tuvimos una amistad muy profunda, la posición que tenía de seguridad dentro de CIE era estratégica, el manejar el nivel de los espectáculos que él hacía me parece que es la persona que manejó los espectáculos más importantes de este país, y su dedicación, su entrega y profesionalismo hicieron de él ese gran hombre profesional además de ser buen catedrático en diversos diplomados. Le guardo un gran aprecio", comentó Enrique Tapia, socio director de Altair, Security Consulting & Training. ■

Agradecimientos a Emilia Vidal, Arturo Ávila, Thomas Gottlieb, José Luis Alvarado, Zeferino Guzmán y Enrique Tapia por sus aportaciones a este homenaje.

Fotos: Cortesía Emilia Vidal

ISIS SEGURIDAD INTEGRAL | Creamos entornos seguros

Servicios:

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

AFAC AGENCIA FEDERAL DE AVIACIÓN CIVIL

BASC Business Alliance for Secure Commerce Certification /Certificacion Nº MEXGDL00175-1

Consejo Nacional CNSP Seguridad Privada A.C. Empresas de Calidad MR

ASIS INTERNATIONAL

mesis MR

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

SEGURIDAD EN LA INDUSTRIA MANUFACTURERA

La industria manufacturera en México emplea a más de nueve millones de personas, y representa el 18% del PIB, por lo que asegurar su funcionamiento en cada proceso, es fundamental para continuar con su crecimiento

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La industria manufacturera en México sigue siendo un gran sostén para la economía del país, tan sólo en el primer trimestre de este año (2023), se registró un Producto Interno Bruto (PIB) de 5.48, con un incremento del 0.93% respecto al trimestre anterior (octubre, noviembre y diciembre 2022)[1]. Este año, tanto el Estado de México como Jalisco y Guanajuato concentraron la mayor población ocupada en esa industria, estados que desafortunadamente las autoridades han informado que pertenecen a los más peligrosos del país, es por ello que realizamos una serie de entrevistas para conocer cómo enfrenta la industria manufacturera los actuales riesgos de seguridad en donde se desarrolla dicha actividad.

RIESGOS DE SEGURIDAD

De acuerdo con la Cámara Nacional del Autotransporte de Carga (CANACAR), los estados de México, Puebla, Guanajuato, Jalisco, San Luis Potosí, Michoacán, Querétaro, Hidalgo, Veracruz y Tlaxcala son las entidades con mayor incidencia delictiva, y desde el primer bimestre del año, hubo un incremento del 10.8% en el robo al transporte de carga[2].

Por su parte, la Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV), reportó que, hasta el mes de agosto, el Estado de México había acumulado 287 vehículos pesados robados, mientras que Guanajuato, 87, y Jalisco 85; estas cifras del robo al transporte de carga impactan en las otras industrias que están relacionadas a dicha actividad, en este caso, también afectan a la industria manufacturera y es uno de los riesgos que los especialistas en seguridad deben tener en cuenta.

"En la actualidad, uno de los riesgos constantes a los que se enfrenta la industria manufacturera es la disrupción de la cadena de suministro, ya que puede afectar no sólo la entrega de productos, sino también la credibilidad de la marca y por consecuencia la continuidad del negocio perjudicando también a las personas. Como premisa de seguridad siempre tomamos como base los 3 P's: Personas, Propiedad y Producto, y ya hace algún tiempo, se adiciona la Información como uno de los principales puntos de protección que Seguridad en conjunto con el equipo de *Cyber Security* trabaja para siempre estar actualizados y mantener la protección de los 3 P's. No obstante, considero que la disrupción de la cadena de suministro, es el principal riesgo que debemos atender en esta industria", explicó Ronaldo J. Maiante, *GIS Security & Hospitality Director* LATAM en Cummins.

Otro de los problemas de seguridad a los que se enfrenta no sólo esta industria, sino todo el país, es el aumento del crimen organizado, que geográficamente está afectando más a ciertos estados y su paso por ellos, así como a las industrias que están instaladas en sus localidades. El trasladar a los empleados a sus puestos de trabajo y los productos a su siguiente destino, se han vuelto un reto para el área de Seguridad de las empresas maquiladoras.

"La diversidad de los escenarios para la logística de los productos y la movilidad de los empleados representan un desafío para los esquemas de seguridad, la capacidad de estar receptivos y la anticipación son elementos esenciales para mantener la estrategia de seguridad corporativa lo más efectiva posible", externó Julio Porras, *Security Mexico* en Grupo Daltile (conformado por las marcas: Big Green Egg, Vitromex y Daltile).

En el primer trimestre de este año (2023), se registró un Producto Interno Bruto (PIB) de 5.48, con un incremento del 0.93% respecto al trimestre anterior. Este año, tanto el Estado de México como Jalisco y Guanajuato concentraron la mayor población ocupada en la industria manufacturera

Respecto a la seguridad en el traslado de los productos, Ronaldo Maiante comentó que Cummins cuenta con la certificación de C-TPAT (Asociación de Aduanas y Comercio contra el Terrorismo) y OEA (Operador Económico Autorizado) que son excelentes estándares de protección. "Con el correcto mantenimiento de las certificaciones y comprometimiento de todos los involucrados, como cadena logística y liderazgo, generamos una protección que nos garantiza, hasta ahora, un proceso logístico seguro y confiable manteniendo la credibilidad ante las autoridades. Es cierto que tener procesos claros y constantes auditorías en parceros comerciales ayuda a garantizar el comprometimiento de todos con el objetivo final que es hacer el producto salir de planta y llegar a su destino lo más rápido e intocable posible".

En Daltile, comentó Julio Porras, lo que les ayuda a mantener sus productos seguros en la transportación, son los esquemas de seguridad móvil, planteados desde una base evolutiva y receptiva a los cambios del entorno y necesidad del negocio que hacen que su logística sea efectiva, además de la elaboración de una adecuada gestión de riesgo al negocio.

ESTRATEGIAS DE SEGURIDAD EFECTIVAS

Otros factores que la industria de la manufactura debe considerar dentro de los procesos de seguridad, son las inmediaciones de las fábricas, el robo interno y de propiedad, así como la seguridad de los empleados. En Daltile, desarrollan una estrategia en capas que permite actualizar conforme a cada interés-producto-escenario del negocio, un esquema continuo de gestión del riesgo, y esto les ha funcionado no sólo en México, sino en otros países. Esta empresa de manufactura es líder en la fabricación y distribución de pisos, muros, porcelánicos, cerámicos y de piedra natural.

Mientras que Cummins se especializa en motores y generadores diésel y de combustible alternativo, teniendo riesgos de seguridad generales y específicos de acuerdo con su rubro. "Hay varios riesgos importantes que necesitamos tener en cuenta, internamente pensando en el negocio, tenemos el riesgo de pérdidas de piezas, los componentes de motores son de diversos tamaños y precios, el mercado negro acepta este tipo de ventas y así siempre hay un riesgo. Además de esto, la contaminación de mercancías por drogas es algo que siempre estamos trabajando para evitar ya que como empresa confiable tenemos garantías de exportación más rápidos. Los riesgos externos son muchos, uno de los que más tenemos en enfoque son con la seguridad de las personas cuando están viajando, sea por carretera o en avión en áreas de mayores riesgos", señaló Ronaldo Maiante.

"La diversidad de los escenarios para la logística de los productos y la movilidad de los empleados representan un desafío para los esquemas de seguridad", Julio Porras

JULIO PORRAS, *SECURITY MEXICO* EN GRUPO DALTILE

Egresado de la Universidad Autónoma de Nuevo León (UANL), Licenciado en Criminología con diplomados en EGADE ITESM en Business Management, Project Management y Gestión - Manejo de Conflictos. Cuenta con más de 15 años de experiencia como responsable de las áreas de Seguridad Corporativa de empresas manufactureras del sector automotriz (japonesa y alemana) y actualmente en el sector cerámico como *Security Mexico* en Grupo Daltile (marcas Big Green Egg, Vitromex y Daltile).

Una de las estrategias que le han funcionado a Cummins en cuanto a la seguridad de los empleados, es el uso de anillos de defensa, iniciando por monitoreo de escenarios externos, utilización de tecnologías de intrusión, cámaras y control de acceso. "Se requiere constante entrenamiento a las personas para que tengamos un cambio de comportamiento de seguridad, comprendemos que ésta es responsabilidad del equipo que allí está para proteger a las personas, pero todos los que son parte del grupo Cummins, tienen su corresponsabilidad en 'parar, apuntar y reportar', esto hace que los trabajos del equipo sean más rápidos y las respuestas de protección las más adecuadas. Y por supuesto, tener un equipo de seguridad bien entrenado y un grupo de liderazgo comprometido, ayuda a mantener los procesos siempre en evolución", resaltó el especialista.

Para la seguridad en las inmediaciones de la fábrica o bien en áreas de gran extensión, Julio Porras compartió que como Seguridad Corporativa es importante estar alineados a la estrategia del negocio. "Esa es la clave para que desde la plantación de los *sites* o unidades de negocio de gran extensión, estemos involucrados en su construcción y desarrollo; así como tener proveedores sólidos en la parte de seguridad física, ya que ese es el complemento necesario para el diseño adecuado a cada condición de lo *sites*".

La industria manufacturera en México, emplea a más de nueve millones de personas y representa el 18% del PIB, de ahí la importancia de que cada proceso de esta industria se lleve a cabo con altos estándares de seguridad, estrategias efectivas y tecnología que ayude a cumplir con los objetivos de seguridad. ■

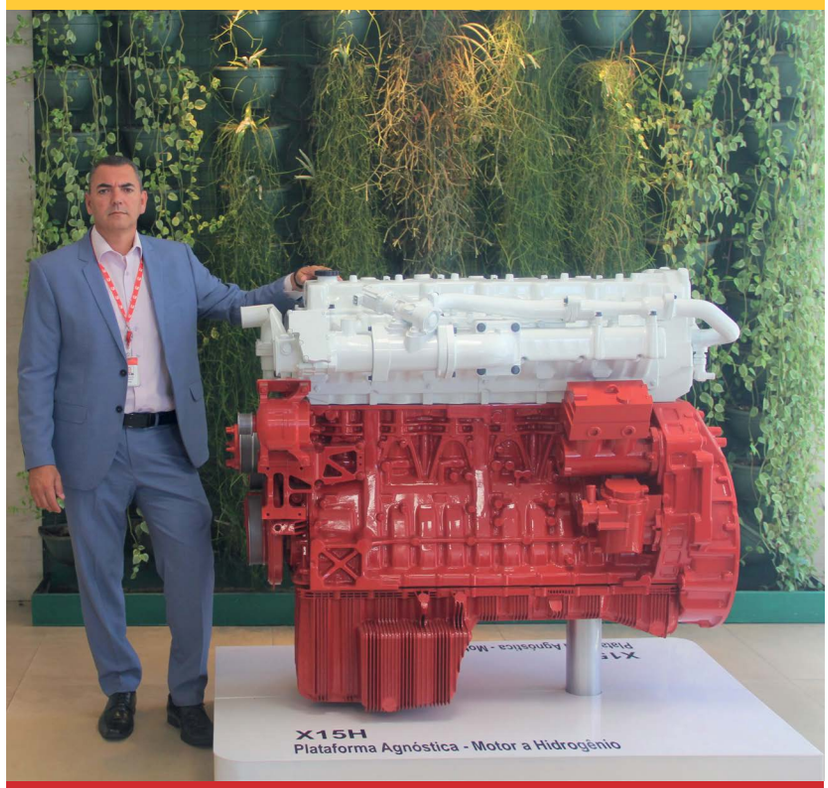
Referencias:

1 *"Industrias Manufactureras SECTOR (31-33)", DATA México, Gobierno de México https://www.economia.gob.mx/datamexico/es/profile/industry/manufacturing#:~:text=En%20el%20primer%20trimestre%20de%202023%2C%20Industrias%20Manufactureras%20registr%C3%B3%20un,mismo%20periodo%20del%20a%C3%B1o%20anterior*

2 *"Robos a transportistas en México: ¿Cuáles son las entidades más afectadas?", El Economista, Lilia González. 06/04/2023, https://www.eleconomista.com.mx/empresas/Robos-a-transportistas-en-Mexico-Cuales-son-las-entidades-mas-afectadas-20230406-0007.html*

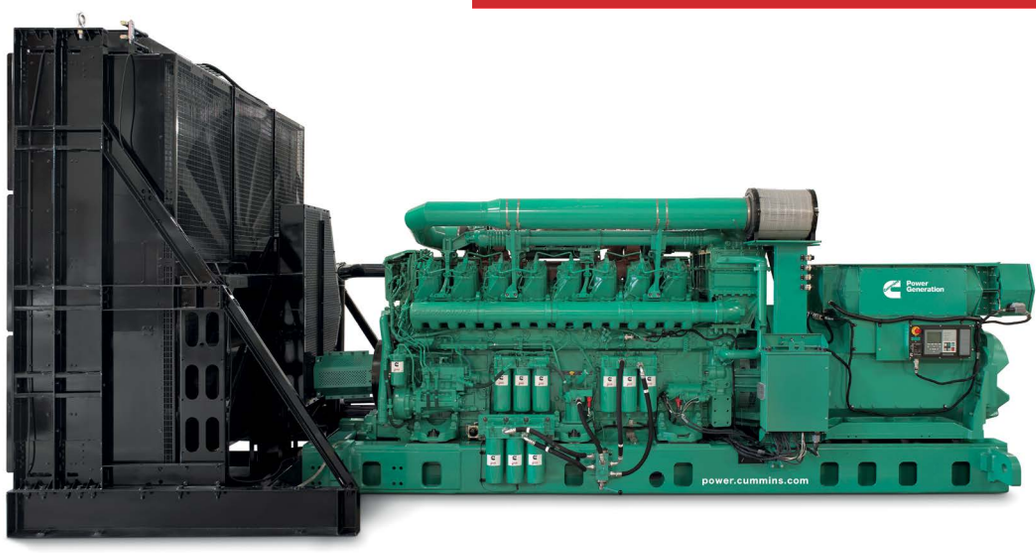
Fotos: Cummins; Daltile

"La disrupción de la cadena de suministro, es el principal riesgo que debemos atender en esta industria", Ronaldo J. Maiante



RONALDO J. MAIANTE, *GIS SECURITY & HOSPITALITY DIRECTOR* LATAM EN CUMMINS

Cuenta con 26 años de experiencia en Seguridad Corporativa en empresas globales, con vivencia en países como México, Argentina y Brasil, una buena experiencia en grandes eventos, como organización de protección para los juegos Olímpicos de Brasil. Su formación es en gestión de Seguridad Privada, con MBA en gestión de Personas y MBA en Gestión Estratégica de Negocio. Además, cuenta con otros entrenamientos y cursos específicos de seguridad. Pero la mejor formación que él considera en su carrera, es la red de contactos, la cual genera grandes oportunidades para compartir experiencias e *insights* para la mejora continua de los estándares de seguridad.



GRUPO LK

"Protegemos tu patrimonio con profesionalismo y pasión"

Oficiales de Seguridad

Monitoreo y Rastreo

Custodias de Transporte

Estudios de Vulnerabilidad

Lago Tana No. 77-B, Col. Torre Blanca, Miguel Hidalgo, 11280, CDMX.

grupolkseguridadprivada.com

55-8848-8264

SEGURIDAD EN LA INDUSTRIA ENERGÉTICA

Entendiendo los retos de seguridad que existen en un sector imponente que opera a niveles exponenciales

Foto: - Freepik

MÉXICO

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

Uno de los sectores con una de las infraestructuras más complejas en su ramo es, sin duda, el que abarca la industria energética; debido a la dificultad de sus procesos, este sector representa un gran reto para la seguridad de sus operaciones, ya que procura salvaguardar la integridad de activos que igualan grandes inversiones económicas y productos que se comercializan incluso de manera internacional, esto sin dejar de lado el factor humano, ya que emplear en este sector es una labor de alto riesgo. Para entender un poco más el tema, dos expertos comparten sus conocimientos para explicar los procesos que se emplean y las estrategias que se implementan a fin de entender mejor los riesgos existentes de la industria, generando así medidas óptimas para el sector.

PRINCIPALES RETOS DE SEGURIDAD

Cada industria tiene sus propios retos generales y particulares, de acuerdo con José Echeverría, responsable de Seguridad y Transportes de Andes Petroleum Ecuador Ltd., estos también varían de acuerdo a la zona o territorio donde se desarrolla cada industria, en el caso del sector petrolero, el especialista hizo una comparación entre los años 2022 y 2023 a nivel mundial, en la que explicó que tanto la productividad y costos han subido, y que cada vez es más difícil llegar a los yacimientos donde están los hidrocarburos, ya que hay muchos factores que hacen que los costos respecto a la producción se eleven, por ejemplo, la guerra entre Ucrania y Rusia que encareció varios productos.

"Otros conflictos económicos que existen, por ejemplo, en China como en Occidente han hecho que incrementen los riesgos. Pero el reto principal de esta industria es el tema ambiental y social, algo que afecta directamente la imagen de las empresas hidrocarbureras. Hoy en día hay mucha tendencia hacia las energías renovables y ecológicas, lo que hace que exista un señalamiento a la industria como responsables del calentamiento global", señaló el especialista.

Por su parte, Uwe Fischer, director global de Seguridad en Draslovka, nos platicó sobre los principales riesgos que enfrenta la industria energética en general hoy en día. "Considero que en primer lugar están los ataques cibernéticos. Las redes de distribución de energía fueron instaladas ya hace muchos años. Aún y cuando los sistemas computarizados que soportan las operaciones han mejorado con el tiempo, las amenazas cibernéticas son ya demasiado sofisticadas. Los Ciberdelincuentes pueden ir relativamente fácil a la 'Dark Web' y conseguir todo tipo de herramientas para atacar a cualquier red virtual en el mundo. Tan sólo la CFE en México, sufrió entre los años 2016 y 2021, 368 mil 883 ciberataques de los cuales, 64 mil 738 estuvieron relacionados con *ransomware*".

De acuerdo con el especialista, además de la amenaza cibernética, la industria energética de cualquier país se tiene que enfrentar cada día más a los desastres naturales que pueden destrozar la infraestructura, a posibles sabotajes relacionados con guerras como

Foto: - Freepik

"El reto principal de esta industria es el tema ambiental y social, algo que afecta directamente la imagen de las empresas hidrocarbureras", José Echeverría

en el caso de Rusia y Ucrania, y no menos preocupante, a la falta de mantenimiento en sus redes de transmisión que puede afectar gravemente a un país, como es el caso de Sudáfrica donde el principal productor de energía, ESKOM, no ha sido capaz de modernizar de forma suficiente la infraestructura, causando largos episodios de falta de energía en el país.

Mientras que José Echeverría ejemplificó de la siguiente manera la operación petrolera y sus macroprocesos para entender los riesgos a los que se enfrenta:

- **La exploración sísmica:** trazar una cuadrícula virtual en un mapa, se moviliza gente a diferentes sitios para que hagan excavaciones dentro de la tierra y se obtenga la información. Hay dos activos importantes, que es la gente que desarrolla la actividad y los dispositivos explosivos.
- **Perforación:** posterior a la exploración, se determina cuáles son las zonas que se pueden taladrar a la capa deseada, lo cual conlleva una operación enorme.
- **Producción:** se coloca una bomba en la zona perforada que extrae el crudo a la superficie para su separación. Se debe tener seguridad perimetral para la custodia de los activos.
- **Transporte:** se traslada el crudo a otro sitio, puede ser de dos formas, las cuales son por transporte o por tubería, que dependen del impacto ambiental que genere. Su custodia es delicada.
- **Refinación:** una infraestructura de alto riesgo y mucha seguridad, se obtiene el producto final como la gasolina, vuelve a ser transportado a la última fase.
- **Comercialización:** llegada del producto al usuario final como a las gasolineras.

José Echeverría destacó un tema especial, en la mayoría de los países en Sudamérica no se toma en cuenta que ésta es una infraestructura crítica, en Ecuador se le considera como un sector estratégico, pero de acuerdo con él, entendiéndolo de esta manera, se puede aprovechar el concepto para mejorar las facilidades. En su opinión, el Estado debería ser quien impulse con leyes y reglamentos cómo debería ser protegida la infraestructura.

Existen varios factores que José determina como "generadores de amenazas" para el sector de la seguridad petrolera; debido al tipo de procedimientos que se realizan y lo que implica, así como a las zonas geográficas o demográficas, no es raro que se presenten estos sucesos que dificulten la operación. Dentro de ellos se encuentran los grupos radicales, grupos armados ilegales, la delincuencia organizada y la delincuencia común. La presencia de estos factores genera distintos conflictos sociales como agresiones al personal, retenciones ilegales, sabotaje a los procesos, daños a la propiedad, toma de instalaciones o bloqueo de vías. También presentan consecuencias severas como asalto y robo de combustible, extorsión, secuestro, asalto en vías, robo a locaciones, entre otros conflictos más grandes.

Enfocándose en los retos de la operación petrolera, José habla acerca de la gran cantidad de personas y cargas críticas en desplazamiento, las extensiones para supervisar o inspeccionar, asedio a la imagen de las operadoras en la industria y el estrés psicosocial en los colaboradores de la empresa; ante esto, él presenta como opciones de soluciones el uso de la tecnología y protocolos actualizados, la protección de activos utilizando elementos tecnológicos como cámaras equipadas con inteligencia artificial detrás de la analítica de estos dispositivos, los cuales considera que poseen mucha ventaja que pueden generar un proyecto de implementación con otras áreas que traerá consigo un beneficio a la empresa general; también menciona recursos costo-eficientes, trabajo integral y comunicación, y más importante, la conciencia, capacitación y confianza.

Foto: - Freepik

"Considero que el riesgo principal de la industria energética son los ataques cibernéticos. Los ciberdelincuentes pueden ir relativamente fácil a la 'Dark Web' y conseguir todo tipo de herramientas para atacar a cualquier red virtual en el mundo", Uwe Fischer

UN POCO SOBRE ANDES PETROLEUM ECUADOR LTD.

La industria energética es parte de la infraestructura crítica de cualquier país; es fundamental para el funcionamiento de la sociedad y de la economía local y global, cualquier afectación tiene impactos severos para cualquier sector de la población. Imaginemos que un hospital se quede sin energía por una semana o más, los daños serían irreparables. Esta industria a la vez es la base de operación de las demás, pues sin energía, la movilidad, operación, producción, etc., se vuelven incapaces de realizar todos sus procesos de manera efectiva.

Andes Petroleum Ecuador Ltd. "es un consorcio de exploración y producción de petróleo creado por las empresas estatales chinas: China National Petroleum Corp. (CNPC, 55%) y China Petrochemical Corp. (Sinopec, 45%) en 2006"[1]. La sede de la empresa se ubica en Quito y opera el bloque Tarapoa y la estación de transferencia y almacenamiento Lago Agrio, ambos ubicados en la provincia de Sucumbíos.

UN POCO SOBRE DRASLOVKA

Uwe Fischer compartió un poco sobre otra industria que es necesaria para el desarrollo de los procesos de las demás, así como la energética.

"Draslovka es una compañía familiar con un enfoque global, con base en República Checa y presencia en más de 80 países. Es líder global en la producción de cianuro de sodio y químicos especializados basados en tecnología del cianuro, con más de 100 años experiencia en el mercado. Cuenta con tres divisiones de negocio: Soluciones Agrícolas, Soluciones Mineras y Especialidades Químicas. Siendo la minería el negocio más importante actualmente, con la red de distribución más grande de América".

En la actualidad, Draslovka es reconocida como líder mundial en investigación y desarrollo de productos químicos basados en CN. Otros productos químicos son utilizados en la agricultura en forma de fertilizantes y pesticidas y en el sector automotriz, específicamente como componente para la producción de llantas.

"Reconociendo estas necesidades esenciales de la industria minera, Draslovka ha desarrollado la Tecnología de Lixiviación de Glicina (GLT) para proporcionar un medio más sostenible de extraer metales esenciales, incluyendo depósitos previamente no viables. GLT es totalmente reciclable, no tóxico y reduce considerablemente la necesidad de cianuro de sodio como parte del proceso de lixiviación, eliminando los requisitos de desintoxicación y fundición del proceso. Otras innovaciones involucran inteligencia artificial para la mejora del proceso de recuperación". ■

Referencias:

1 bnamericas https://www.bnamericas.com/es/perfil-empresa/andes-petroleum-ecuador-ltd-andes-petroleum#:~:text=Descripci%C3%B3n%3A-, Andes%20 Petroleum%20Ecuador%20Ltd.,Sinopec%2C%2045%25)%20en%202006

- Otras fuentes consultadas: https://www.reporteindigo.com/reporte/datos-de-la-cfe-bajo-ciberataques-ransomware/

Foto: - Freepik

SOMOS PROFESIONALISMO
COMPROMISO
LEALTAD

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

Servicios:

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

SÍGUENOS EN REDES SOCIALES

@grupocorporativodeprevencion

CONTACTO

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

Contamos con las Afiliaciones y Certificaciones:

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

Javier Fernandez Soto: AFILADOR, PARAGÜERO Y ESPECIALISTA EN SEGURIDAD ELECTRÓNICA

Hijo de españoles, con gran pasión por la restauración de antigüedades, siempre consciente de la necesidad de una cultura de la seguridad, de la lealtad, honradez y confianza

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Para llegar a ser esa persona que nos propusimos en la vida, es importante recordar nuestros orígenes, para así preservar todos esos aprendizajes del pasado, hayan sido buenos o un poco complicados. En el año 1964 nació en el extinto Distrito Federal (ahora Ciudad de México), Javier Fernández Soto, hijo de padres españoles quienes se dedicaban al comercio en este país y de quienes aún conserva dos oficios poco convencionales, pero parte de la historia.

"Mi familia estaba dedicada al comercio, y dado que mis padres se divorciaron cuando yo era muy pequeño, la situación económica fue algo apretada en mi niñez. A partir de los 13 años empecé a apoyar en el negocio familiar, en el que, por las tardes (después de la escuela) y los sábados, me encargaba de dirigir. De ahí conservo dos oficios familiares que vienen desde mi abuelo: afilador (afilar cualquier instrumento que se utilice para cortar), y paragüero (venta, reparación y restauración de paraguas)".

Javier Fernández es el director de Occidente en Mak Extinguisher, una de las empresas familiares más reconocidas en el sector de la seguridad privada, y en la que ahora Javier comparte su experiencia de más de 35 años en el sector, principalmente enfocada en seguridad tecnológica.

Estudió Ingeniería Electrónica en la Universidad La Salle, cuenta con el Diplomado en Calidad Total, impartido por el Tecnológico de Monterrey; es egresado del Programa de Dirección de Seguridad en Empresas (DSE), de la Universidad de Comillas de Madrid; así como del Diplomado en Liderazgo y Gerencia Integral en Seguridad en UDLAP, y del Diplomado en Desarrollo de Empresas de Seguridad Exitosas y Sustentables en la Universidad Panamericana.

Desde 1997 está, de acuerdo a sus palabras y sonrisa, felizmente casado con Susana Osorio, con quien tiene dos hijos: Rodrigo y Sofia, el motor de su vida.

ORÍGENES EN LA SEGURIDAD

Treinta y cinco años es toda una vida dedicada a la seguridad, una gran trayectoria con muchos aprendizajes. Javier Fernández Soto inició en temas de tecnología en seguridad en 1988, con la venta e instalación de alarmas ultrasónicas para automóviles.

Entre 1988 y 1996 trabajó en el ramo de las instalaciones eléctricas, comunicaciones, fabricación de cinescopios para televisión, bancos y regresó al tema de la tecnología y seguridad, porque Johnson Controls (JCI) lo buscó para el tema de edificios inteligentes, donde la seguridad en estos edificios representaba un 70% de la facturación: detección de humos e incendios, control de accesos y, en aquel momento, CCTV (Circuito Cerrado de Televisión), lo que hoy en día evolucionó a videovigilancia.

En 2002 entró como director comercial a Telefónica Ingeniería de Seguridad (TIS), donde su enfoque de trabajo fue 100% a soluciones de seguridad tecnológica, y justo en esas fechas fue cuando se involucró con ASIS Internacional, aprendiendo sobre gestión de riesgos y todo lo que conlleva con seguridad desde el punto de vista de administración de éstos.

"En 2006 ingreso a Código Empresarial (Human Factor) en la Dirección General, empresa que me abrió la perspectiva hacia el desarrollo de *software*, gestión del personal y la productividad. Y logramos obtener integraciones interesantes en universidades y en el sector penitenciario. En 2008 me invitan a Schneider Electric (PELCO y Andover) como director de Desarrollo de Negocios de Soluciones de Edificios; en esta etapa fui vicepresidente de AMERIC (Instalaciones Especiales). Para 2011, inicié mi aventura como empre-

sario con la firma Nuevas Tecnologías en Información e Identificación (NTI&I) y en paralelo inició el proceso de resurgimiento de Seccomm, la cual dirijo desde 2013 hasta la fecha", nos compartió el entrevistado.

Y como todo profesional de la Seguridad, Javier Fernández tuvo la oportunidad de contribuir con el sector como presidente de la Asociación Latinoamericana de Seguridad (ALAS) Capítulo México, en el periodo 2011-2014, dejando todo un legado de paneles y conferencias de otros especialistas en seguridad electrónica, en mayo de 2022, se integró a las filas de Mak Extinguisher como director de Occidente, con el objetivo de establecer oficinas en esa región y promover productos y servicios que aportan en esa área del país.

"Mak representa la oportunidad de especializarme en temas que siempre me han parecido importantes y en los que sólo me había involucrado, pero no especializado, como son la detección de humos y la extinción de incendios. Esta oportunidad abre la perspectiva de no sólo ver a la seguridad como prevención, protección y reacción de bienes y activos, sino esta especialidad está totalmente dirigida a prevenir y salvar vidas humanas como primordial y luego los bienes y reputación", comentó.

Desde sus inicios, Mak Extinguisher se especializó en extintores, sistemas de detección y supresión de incendios, sin embargo, en su evolución como empresa y en el mercado, ha venido integrando otras alternativas en sistemas y soluciones de seguridad, la mayoría de ellos tecnológicos, sumando experiencia de ambas partes, aportando valor, el cual se tiene que ver en el corto y mediano plazo reflejado hacia los clientes finales. El abrir nuevas oficinas para toda una región, es un gran reto, mismo que el entrevistado ha enfrentado y ha logrado obtener posicionamiento en tan poco tiempo.

"En este año y medio de trabajos en la zona, nos hemos podido posicionar con empresas de todo tipo con nuestras soluciones vanguardistas y consultoría. Ya conseguimos el registro como proveedores del estado de Jalisco y los municipios más importantes de la zona metropolitana de Guadalajara, así como la participación en varias asociaciones y cámaras locales", explicó.

EJEMPLOS DE VIDA EN LA SEGURIDAD

A lo largo de nuestra vida, vamos conociendo diferentes personas y personajes, algunos de ellos muy significativos y de los cuales tomamos esas enseñanzas que nos sirven para ser mejores personas y/o profesionistas. Javier Fernández Soto admira a uno de los emblemas de la Seguridad Privada de México, conocido por su dedicación, su empeño y trabajo colaborativo en el sector, siempre en busca de mejores oportunidades.

"En mi vida he conocido a muchos líderes y personajes muy interesantes, pero si tengo que mencionar a alguien, pongo en la mesa al Capitán Salvador López, él es un ejemplo de superación personal, de lealtad como empresario (socio) y como amigo; filántropo, creyente de que la unión hace la fuerza, un leal colaborador, promotor, fundador y representante de asociaciones civiles, dando el ejemplo de que hablando se entiende la gente y que todo tiene solución menos la muerte", compartió.

El Capitán Salvador López Contreras es el director general de CIA Kapital, así como de Grupo Consultores Seguridad Privada Integral, y tiene una larga trayectoria en la seguridad, involucrando a la seguridad privada y a la pública en beneficio del país, es entendible por qué es una de las figuras que nuestro entrevistado admira.

Más allá de la seguridad	
Grupo de música o cantante favorito:	Miguel Bosé.
Programa o serie de TV favorito:	The Black List.
Película favorita:	Robin Hood, de Walt Disney.
Libro favorito:	*"Eutanasia para vivir".*
Destino favorito de vacaciones:	España.
Bebida favorita:	Licor de café.
Comida favorita:	Española.
Actor favorito:	Anthony Hopkins.
Personaje favorito:	El Demonio de Tasmania.

"Tengo planeado seguir contribuyendo a una sociedad civil que tanto me ha dado, impulsando la profesionalización y concientización en temas de cultura de prevención"

Asociación de palabras	
México:	A ojo de buen cubero.
Seguridad:	Es mejor prevenir que lamentar.
Presidente:	Autoridad y liderazgo.
Gobierno:	Representación del poder político.
Policía:	Orden y respeto.
Familia:	Lo más importante.
Amigos:	Familia extendida.
Mak Extinguisher:	Perseverancia y constancia.

La seguridad privada en México es muy importante, porque apoya a la seguridad pública y a los empresarios con factores diversos, como la actividad delictiva y los riesgos asociados a ciertas economías, esto al reducir la vulnerabilidad y aumentar la confianza en la protección de personas y bienes.

"La seguridad privada es un sistema integrado por personas, elementos técnicos y administrativos con el objetivo de eliminar, reducir, controlar los riesgos y las amenazas que pueden causar a las personas, a un establecimiento, algún objeto o entidad. Hay muchos ramos en la seguridad privada, pero en el que considero que contribuyo de manera importante es en el tema tecnológico, aportando mi experiencia para buscar soluciones que en conjunto con los análisis de riesgos e implementación de procedimientos y normas adecuadas para cada una de estas, no sólo cumplan con el objetivo de proteger a personas y activos, sino que apoyen a una mejor productividad operativa y puedan garantizar a los usuarios finales la continuidad de sus operaciones o negocios", explicó.

Una de las filosofías de Mak Extinguisher, es valorar a su personal y crear un equipo de trabajo apasionado y comprometido, características que también comparte Javier Fernández, y quien nos explicó cómo incentiva a los colaboradores de su dirección.

"Me gusta incentivar al personal que trabaja para mí, con respeto y dándole su lugar como persona y como profesional. Considerándolos en las decisiones que haya que tomar para conseguir la mejora continua en el trabajo y enseñándoles parte de lo que yo he aprendido a través de los años relacionado a la experiencia en proyecto, como en lo aprendido en diferentes cursos y diplomados que quizá ellos aún no tienen la oportunidad para tomar".

AMOR POR LO CLÁSICO

Aunque todas las personas que pertenecen al sector de la seguridad, son apasionados por esta industria y llevan cada proceso, estrategia, práctica y conocimiento tanto en su vida profesional como personal, porque la seguridad es una necesidad, hay actividades en donde no sólo se habla de este tema.

Uno de los gustos de nuestro entrevistado, son las antigüedades (cosas viejas) y una actividad que disfruta en sus tiempos libres, es el reparar y restaurar cosas, en específico automóviles antiguos, tanto que posee un Vocho verde antiguo (Volkswagen) al cual lo ha ido restaurando y conservado a lo largo de 33 años.

"Además de mi Vochito, me gusta socializar, asistir a reuniones de asociaciones o clubes con el objetivo de conocer gente y aprender de lo que toda esa gente hace o le gusta hacer. También aprecio mucho estar con mi familia y apoyar lo más que se pueda para promover los valores de honestidad, orden, compromiso con la sociedad y lo más importante la felicidad".

Además de compartirnos un poco de su historia, de su presente, Javier Fernández nos platicó acerca de sus planes a mediano plazo, siempre teniendo presente que tanto el pasado y lo que está construyendo día a día, será lo que en un futuro le rinda todavía más satisfacciones.

"Tengo planeado seguir contribuyendo a una sociedad civil que tanto me ha dado, impulsando la profesionalización y concientización en temas de cultura de prevención. Esto desde el ámbito personal y profesional, ya que uno va de la mano con el otro. Pienso que, si dedico tiempo a asociaciones e instituciones con la promoción de la cultura de la prevención, la parte profesional se va enriqueciendo, porque para poder impartir conocimiento, hay que estudiar y aprender todos los días. Con todo lo comentado devuelvo de alguna manera a la sociedad parte de lo que me ha dado a través de los años", finalizó. ■

Fotos: Cortesía Javier Fernández Soto

LA TECNOLOGÍA Y EL SOPORTE TÉCNICO

APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA

38 ANIVERSARIO

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

REGISTRO FEDERAL DGSP/303-16/3302 PERMISO SSP PUEBLA
SSP/SUBCOP/DGSP/506-23/460
REPSE AR10508/2021

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

LAS 5 FASES DE LA SEGURIDAD EN OFICINAS CORPORATIVAS

La seguridad en las oficinas corporativas debe ser considerada como una inversión estratégica para el éxito a largo plazo de cualquier empresa

MÉXICO **José Luis Sánchez Gutiérrez**

Estimados lectores, hablemos de la seguridad en las oficinas corporativas, que como sabemos es una preocupación primordial para las empresas en el mundo actual. La protección de los empleados, los activos y la información confidencial es esencial para mantener la continuidad de los negocios y la reputación de la organización. En este artículo, exploraremos los pros y contras de la seguridad en las oficinas corporativas, destacando la importancia de un enfoque integral para abordar los desafíos de seguridad en el entorno empresarial.

Les presento un enfoque integral en cinco fases para la Seguridad de Oficinas Corporativas.

Recordemos algo muy importante: la seguridad es un proceso en constante evolución. Las amenazas y los riesgos cambian con el tiempo, por lo que todas las empresas deben estar preparadas para adaptarse y mejorar continuamente sus medidas de seguridad. Esto implica realizar evaluaciones periódicas, mantenerse actualizado con las últimas tecnologías y prácticas de seguridad, y estar dispuestos a realizar ajustes cuando sea necesario.

- **Fase 1: Introducción y contexto de la seguridad en las oficinas corporativas.** En esta fase, se establecerá el contexto y la importancia de la seguridad en las oficinas corporativas. Se discutirán los riesgos y amenazas comunes que enfrentan estas instalaciones, como robos, intrusiones, sabotajes y violaciones de la privacidad. Además, se destacará la importancia de implementar medidas de seguridad efectivas para proteger a los empleados, los activos de la empresa y la información confidencial.

LAS AMENAZAS Y LOS RIESGOS CAMBIAN CON EL TIEMPO, POR LO QUE TODAS LAS EMPRESAS DEBEN ESTAR PREPARADAS PARA ADAPTARSE Y MEJORAR CONTINUAMENTE SUS MEDIDAS DE SEGURIDAD. ESTO IMPLICA REALIZAR EVALUACIONES PERIÓDICAS Y MANTENERSE ACTUALIZADO CON LAS ÚLTIMAS TECNOLOGÍAS Y PRÁCTICAS DE SEGURIDAD

Foto: - Freepik

- **Fase 2: Evaluación de riesgos y análisis de vulnerabilidades.** En esta fase, se realizará una evaluación completa de los riesgos y se llevará a cabo un análisis de vulnerabilidades en las oficinas corporativas. Se identificarán las posibles debilidades en la seguridad física, como sistemas de acceso inadecuados, cámaras de vigilancia insuficientes u obsoletas, falta de controles de ingreso y salidas, entre otros. También se examinarán los aspectos relacionados con la seguridad cibernética, como la protección de redes, sistemas de seguridad informática y políticas de acceso a la información.
- **Fase 3: Diseño e implementación de medidas de seguridad.** En esta fase, se desarrollarán planes y estrategias para mejorar la seguridad en las oficinas corporativas. Esto incluirá el diseño e implementación de medidas de seguridad física, como sistemas de vigilancia avanzados, sistemas de control de acceso, barreras físicas, alarmas y sistemas de detección de intrusos. Asimismo, se abordarán aspectos de seguridad cibernética, como firewalls, encriptación de datos, autenticación de usuarios y políticas de seguridad informática.
- **Fase 4: Capacitación y concienciación de los empleados.** La seguridad no sólo depende de las medidas técnicas implementadas, sino también de la capacitación y concienciación de los empleados. En esta fase, se desarrollarán programas de capacitación en seguridad para educar a los empleados sobre los riesgos y las mejores prácticas de seguridad. Esto incluirá la enseñanza de procedimientos de seguridad, políticas de acceso, manejo de información confidencial y conciencia sobre posibles amenazas. Se promoverá una cultura de seguridad en la que los empleados sean proactivos y estén comprometidos con la protección de la empresa y sus activos.
- **Fase 5: Monitoreo y mejora continua.** La seguridad en las oficinas corporativas debe ser un proceso continuo y en constante evolución. En esta fase, se establecerán programas de monitoreo y evaluación para asegurar que las medidas de seguridad implementadas sean efectivas y estén en línea con las necesidades cambiantes de la empresa. Se realizarán evaluaciones periódicas de seguridad, se revisarán las políticas y se implementarán mejoras según sea necesario. Además, se fomentará la retroalimentación de los empleados y se establecerán canales de comunicación para reportar incidentes de seguridad o sugerir mejoras.

BENEFICIOS DE LOS SISTEMAS DE SEGURIDAD FÍSICA

Nunca hay que olvidar que, al proteger las oficinas corporativas con sistemas de seguridad física y tecnológica, se obtienen varios beneficios y ventajas significativas, así como un valor agregado para la empresa. Estos incluyen:

a) **Protección de activos y recursos:** Los sistemas de seguridad física, como sistemas de vigilancia, sistemas de control de acceso y barreras físicas, ayudan a prevenir robos, intrusiones y daños a los activos de la empresa, como equipos, tecnología, documentos y materiales valiosos. Del mismo modo, los sistemas de seguridad tecnológica, como firewalls, encriptación de datos y sistemas de detección de intrusos, protegen los recursos digitales y la información confidencial de la empresa contra amenazas cibernéticas.

b) **Salvaguardia de la integridad y confidencialidad de la información:** Las oficinas corporativas suelen manejar información sensible y confidencial, como datos de clientes, estrategias comerciales, secretos industriales y datos financieros. Los sistemas de seguridad tecnológica, como el mo-

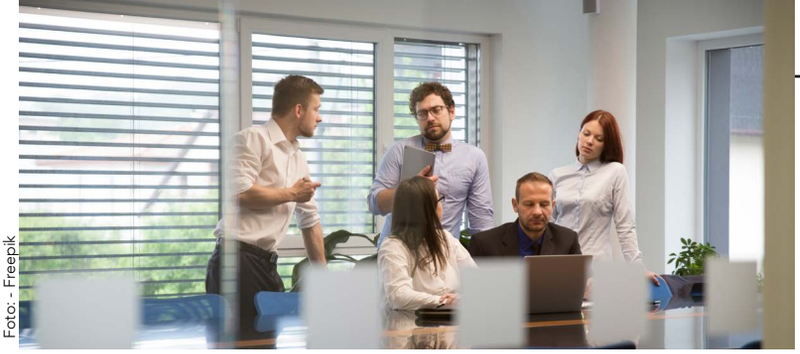


Foto: - Freepik

nitoreo de redes, la autenticación de usuarios y las políticas de acceso restringido, protegen la integridad y la confidencialidad de esta información, evitando fugas o accesos no autorizados.

c) **Mejora de la productividad y el bienestar de los empleados:** Al contar con sistemas de seguridad física, como cámaras de vigilancia y sistemas de control de acceso, se crea un entorno laboral seguro y se fomenta la confianza y el bienestar de los empleados. Además, los sistemas de seguridad tecnológica, como protección contra malware y filtrado de contenido, ayudan a evitar interrupciones en el trabajo causadas por ataques cibernéticos, lo que resulta en una mayor productividad.

d) **Cumplimiento normativo y legal:** Muchas empresas están sujetas a regulaciones y requisitos legales en cuanto a la protección de la información y la seguridad en general. Al implementar sistemas de seguridad física y tecnológica adecuados, las empresas pueden asegurarse de cumplir con estas regulaciones y evitar sanciones legales.

e) **Mejora de la imagen y reputación de la empresa:** La seguridad es un factor importante para clientes, socios comerciales y empleados potenciales al evaluar la confiabilidad y profesionalidad de una empresa. Al demostrar un compromiso sólido con la seguridad y protección de sus oficinas corporativas, una empresa mejora su imagen y reputación en el mercado.

No olvidemos que en todo análisis siempre encontramos pros y contras, y en lo que se refiere a la Seguridad en Oficinas Corporativas identifico los siguientes:

PROS DE LA SEGURIDAD EN OFICINAS CORPORATIVAS

- **Protección del personal y los activos:** La seguridad en las oficinas corporativas garantiza la integridad física y emocional de los empleados, lo que fomenta un entorno laboral seguro y productivo. Con la implementación de medidas de seguridad adecuadas, como sistemas de acceso controlado y vigilancia, se reduce el riesgo de robo, intrusiones y daños a la propiedad corporativa.
- **Prevención de riesgos y amenazas:** Las estrategias de seguridad en oficinas corporativas permiten identificar y mitigar riesgos potenciales, como incendios, fugas de información confidencial o intrusiones cibernéticas. La adopción de políticas y procedimientos de seguridad efectivos promueve la conciencia y el cumplimiento de los protocolos de seguridad entre los empleados.
- **Cumplimiento normativo y legal:** La seguridad en las oficinas corporativas ayuda a garantizar que la organización cumpla con las regulaciones y normativas pertinentes en materia de seguridad laboral, privacidad de datos y protección contra incendios, entre otras. Cumplir con los estándares legales y normativos no sólo evita sanciones legales, sino que también fortalece la reputación y la confianza en la empresa.
- **Fortalecimiento de la imagen corporativa:** Una sólida infraestructura de seguridad en las oficinas corporativas puede transmitir una imagen de confianza y profesionalismo tanto a los empleados como a los clientes. La percepción de que la empresa se preocupa por la seguridad de sus empleados y la protección de sus activos puede generar lealtad y satisfacción entre los stakeholders

Las estrategias de seguridad en oficinas corporativas permiten identificar y mitigar riesgos potenciales, como incendios, fugas de información confidencial o intrusiones cibernéticas

CONTRAS DE LA SEGURIDAD EN OFICINAS CORPORATIVAS

- **Costos asociados:** Implementar medidas de seguridad efectivas puede ser costoso, especialmente si se requiere tecnología avanzada, personal especializado y sistemas de vigilancia sofisticados. Los gastos continuos para mantener y actualizar los sistemas de seguridad pueden representar una carga financiera para las empresas, especialmente para las pequeñas y medianas empresas con recursos limitados.
- **Posible disrupción de la productividad:** Algunas medidas de seguridad, como controles de acceso rigurosos o procedimientos de identificación adicionales, pueden ralentizar el flujo de personas y tener un impacto en la eficiencia y la productividad de los empleados. Es importante encontrar un equilibrio entre la seguridad y la facilidad de movimiento dentro de las instalaciones para minimizar la interrupción en las operaciones diarias.
- **Percepción negativa entre los empleados:** En algunos casos, los empleados pueden sentir que las medidas de seguridad son invasivas o que violan su privacidad personal. La falta de comunicación efectiva sobre las políticas y prácticas de seguridad puede generar descontento y desconfianza entre los empleados, lo que puede afectar negativamente el ambiente laboral.
- **Posibilidad de falsa sensación de seguridad:** A pesar de la implementación de medidas de seguridad, siempre existe un riesgo residual de amenazas y vulnerabilidades que podrían no ser completamente eliminadas. Si los empleados confían demasiado en las medidas de seguridad y descuidan su propia vigilancia y sentido de responsabilidad, la eficacia de las medidas puede verse comprometida.

Aunque siempre encontramos diferentes desafíos, los beneficios superan con creces los inconvenientes potenciales. Al adoptar un enfoque integral, equilibrando la seguridad con la productividad y la confianza de los empleados, las organizaciones pueden garantizar un entorno de trabajo seguro y fortalecer su posición en el mercado. La seguridad en las oficinas corporativas debe ser considerada como una inversión estratégica para el éxito a largo plazo de cualquier empresa.

Esperando sea de utilidad la información de este artículo y poder contar con su acostumbrado apoyo de lectura, me permitiré seguir compartiendo material que les genere un real valor agregado como lectores. ■

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

LA CULTURA ÉTICA EMPRESARIAL COMO MODELO DE PREVENCIÓN DEL FRAUDE OCUPACIONAL: UN ENFOQUE CRIMINOLÓGICO

Es indispensable incluir en las políticas de prevención del fraude ocupacional controles y estrategias que integren el estudio del comportamiento humano, aunado a los factores criminógenos de riesgos asociados a la conciencia moral, ya que las conductas que nos ocupa detectar y contener son realizadas por personas que forman parte de la organización

Foto: Freepick

NICARAGUA MÉXICO **Jessica Alexandra Flores Páiz**

El presente artículo se encamina a analizar desde la Criminología la importancia de establecer un modelo de prevención del fraude ocupacional en las empresas, sustentado en la influencia de la cultura ética vista como medida de control social informal aplicada en las organizaciones, por tanto, siendo la ciencia criminológica la encargada de estudiar el fenómeno criminal, así como sus formas de controlarlo y prevenirlo, se requiere atribuir a los criminólogos el análisis de los factores criminógenos de riesgos de fraudes en el ámbito empresarial, la administración de los mismos, y el diseño de programas de seguridad o políticas preventivas que incluya, entre otras, estrategias orientadas a la ética como uno de los valores principales de la cultura empresarial.

ASPECTOS RELEVANTES DEL FRAUDE OCUPACIONAL

El fraude es uno de los grandes riesgos que interesa prevenir a la alta gerencia de las empresas debido al impacto negativo que implicaría su comisión en los activos de la organización, que podrían generarle consecuencias que van desde pérdidas económicas, reputacionales, como jurídicas, estas últimas debido a las obligaciones impuestas por ley a las personas jurídicas de poseer los controles adecuados para evitar los delitos que pudieran ser cometidos en su nombre, por su cuenta, en su beneficio o a través de los medios que ellas proporcionen, o de lo contrario serán penalmente responsables, lo cual podría afectar los intereses y continuidad de las operaciones del negocio.

Para entender el fraude ocupacional y sus modalidades, es necesario conocer su definición genérica, en este sentido, para el Instituto de Auditores Internos (IIA) se define como todo acto ilegal caracterizado por engaño, ocultación o abuso de confianza, los cuales son cometidos por personas y organizaciones para obtener dinero, bienes o servicios, para evitar el pago o la pérdida de servicios, o para obtener una ventaja personal o comercial.

Cuando hablamos de fraudes nos estamos refiriendo a un delito de engaño, sin embargo, desde una perspectiva genérica, éste agrupa diversas conductas o delitos que le son equiparables, entre ellos bajo la de denominación jurídico penal hurto, robo, abuso de confianza, administración fraudulenta, falsificación documental, o defraudación tributaria, etcétera (Errol, 2009).

Atendiendo lo antes referido, en el contexto empresarial, existen diversas tipologías de fraudes tanto internas como externas, en las que la Entidad puede ser el victimario en perjuicio de terceros conocido en la doctrina como delitos de cuello blanco, o bien puede ser víctima por parte de sujetos externos no vinculados a la organización o por parte de sus colaboradores internos. En este último aspecto, es que se configura el fraude interno u ocupacional, mediante la comisión de diversas conductas delictivas, haciendo uso del oficio y funciones dentro de la organización, con el objetivo de obtener un provecho ilícito de la empresa.

Acerca del empleado como victimario el ACFE (2016) define el fraude ocupacional como "el uso deliberado de la ocupación para el enriquecimiento personal, mediante el mal uso o desvío de los recursos o activos de la organización contratante (p. 6).

PANORAMA ACTUAL DEL FRAUDE OCUPACIONAL

México tiene la mayor incidencia de fraude ocupacional en la región, seguido de Brasil y Colombia, según el Informe a las Naciones, Estudio Mundial sobre Fraude y Abuso Ocupacional de 2016, realizado por el ACFE. Continuando con su estudio, en 2018 detalló que entre los diversos tipos de fraude que las organizaciones podrían enfrentar, el fraude ocupacional es la amenaza más grande y frecuente, por su parte, en el informe de 2020, como se citó en (Torre y Quiroz, 2020) se provee un análisis de 2 mil 504 casos de fraude ocupacional que ocurrieron en 125 países alrededor del mundo. Estos casos fueron investigados entre enero de 2018 y septiembre de 2019, revelando que se generó una pérdida total de más de 3 mil 600 millones de dólares.

EL ROL DE LA CRIMINOLOGÍA EN LA PREVENCIÓN DEL FRAUDE OCUPACIONAL APLICANDO LA TEORÍA DEL CONTROL SOCIAL INFORMAL

A como lo ha referido García Pablos de Molina, a la criminología le preocupa no sólo el delincuente, el delito y la víctima, sino también el control

social del comportamiento desviado, esto es según Wolff y Kaiser (como se citó en García-Pablos 2003) "el estudio de los mecanismos a través de los cuales la sociedad despliega su supremacía sobre los individuos que la componen, consiguiendo que estos acaten sus normas" (p. 82).

Por su parte acerca del control social Cohen (1988) afirma: "es el conjunto de formas organizadas en que la sociedad responde a comportamientos y personas que contempla como desviados, problemáticos, preocupantes, amenazantes, molestos o indeseables de una u otra manera (…) Esta respuesta aparece de diversas formas: castigo, disuasión, tratamiento, prevención, segregación, justicia, resocialización, reforma o defensa social" (p. 81).

Las teorías de control, propiamente dichas tienen su origen a finales de los años sesenta en los Estados Unidos gracias a los trabajos de Travis Hirschi, y para el análisis y desarrollo del concepto de control social se requiere dividirlo en dos clases de agentes de control a saber: las instancias formales e informales, las primeras son ejercidas por el Estado, constituidas por las entidades públicas creadas para definir, individualizar, detectar, manejar o suprimir las conductas prohibidas, son la policía, sistema de justicia y la administración penitenciaria, y las segundas, que son objeto de este estudio, son principalmente la familia, la escuela, el trabajo y los medios de comunicación de masas, las cuales tienen la misión de condicionar a cada miembro del grupo desde su infancia, a las normas sociales.

Atendiendo a lo anterior, se puede resumir que la teoría del control social es aplicable al ámbito empresarial en cuanto la empresa como espacio laboral es un agente de control que influye en el comportamiento de sus trabajadores, y por ende, tiene la responsabilidad social de contribuir en la prevención y control de las conductas antisociales o declitivas que ocurran desde el seno de la organización.

EL CONTROL SOCIAL INFORMAL QUE OPERA A TRAVÉS DE AGENTES SECUNDARIOS: EL ÁMBITO LABORAL

Cabe destacar lo señalado por Vega (2017) respecto a la influencia del entorno laboral en el comportamiento del individuo y la modulación de su conducta, refiere que "es en el ámbito laboral donde el sujeto va a seguir recibiendo influencia en sus principios, valores y actitudes. Las influencias que recibe el individuo en el trabajo son altamente aceptadas y determinantes, según García-Pablos (1999), que rigen el destino del trabajador: permanencia en su empleo, ascensos, salarios, etc." (p. 175).

Esto nos indica que al ser este entorno, donde el sujeto pasa mayor parte de su tiempo, los representantes de la entidad tienen la responsabilidad social de atender el factor humano como primer eslabón de control para prevenir conductas antiéticas como los fraudes.

Es importante que los directivos de la empresa reconozcan de qué manera la conciencia moral de los trabajadores puede deteriorarse y descender a la práctica fraudulenta. Para ello juega un papel fundamental en el deterioro de la conciencia moral la convergencia de tres fuerzas motivacionales en el interior del individuo: las presiones, las oportunidades y las justificaciones morales. Por tanto, cualquier ingeniería ética anti fraude debe detectarlas y controlarlas debidamente (Franca, 2016).

FOMENTO DE LA CULTURA ÉTICA EMPRESARIAL COMO MEDIDA DE CONTROL SOCIAL INFORMAL PARA LA PREVENCIÓN DEL FRAUDE OCUPACIONAL

Es imprescindible comprender que la cultura empresarial trata de los valores de una entidad, por tanto, la ética es uno de esos valores que constituyen la cultura de la organización y que debe ser trasmitida a todos los empleados marcando mediante reglas informales el comportamiento de estos; y es, a su vez, este comportamiento el que establece los límites de la legalidad en los actos de un individuo. En otras palabras, si el fraude supone un engaño fruto de una mala conducta por parte del empleado, existe la posibilidad de que ésta haya sido influenciada por una cultura. Algunas de las herramientas que se pueden aplicar para la transmisión de la cultura empresarial son los códigos de ética y conductas (Minguez, 2019).

Entendido lo antes expuesto, podemos encontrar la relación o influencia de la cultura empresarial con la prevención del fraude ocupacional. En este sentido, algunos autores sugieren establecer y aplicar diversas estrategias focalizadas en la mejora de la práctica ética de la empresa tomando principalmente en consideración los aspectos morales y los factores que pueden llegar a degradarlos hasta caer en conductas anti éticas o delictivas. Son algunas líneas de recomendaciones a considerar en los planes de prevención las siguientes aseveraciones:

Establecer la ética como uno de los valores principales de la cultura empresarial (Minguez, 2019); practicar en forma efectiva el *tone at the top* o comportamiento ético al más alto nivel directivo y gerencial, contar con una fuerte cultura ética corporativa, asimismo, entrenamiento al personal sobre programas antifraude (Maiola, 2014); fomentar una cultura ética empresarial que disminuya las racionalizaciones, justificación de la conducta anti ética o antisocial, contrarias a las calificaciones decididas a nivel institucional sobre lo que es considerado conducta prohibida (Tarragó, 2016); y, afianzar el compromiso que deben asumir las organizaciones de procurar una cultura de prevención como de disuasión y erradicación del fraude desde el seno del gobierno corporativo, una de sus tareas fundamentales es la comunicación e información relevante como una tónica de cultura cotidiana en la empresa o entidad de gobierno, así como establecer y comunicar los valores de la organización (Bautista, 2019).

A modo de conclusión, es indispensable incluir en las políticas de prevención del fraude ocupacional controles y estrategias que integren el estudio del comportamiento humano, aunado a los factores criminógenos de riesgos asociados a la conciencia moral, ya que las conductas que nos ocupa detectar y contener son realizadas por personas que forman parte de la organización, y cuyo actuar dependerá en gran medida de la influencia de la cultura o valores percibidos en la empresa, siendo ésta, un agente de control social informal de las conductas antisociales y delictivas. Finalmente, la alta dirección de la empresa deberá comprender la responsabilidad social y jurídica que tiene la Entidad de adquirir el compromiso de control a través del fomento de la cultura ética empresarial partiendo de su buen gobierno corporativo. ■

Jessica Alexandra Flores Páiz, investigadora y estudiante de Doctorado en Criminología de la Universidad Autónoma de Nuevo León. *Más sobre la autora:*

ANÁLISIS FRACTAL Y GESTIÓN DE RIESGOS

El análisis de fractales es una herramienta valiosa para la gestión de riesgos, ya que permite analizar y modelar fenómenos complejos e irregulares que pueden tener consecuencias negativas o positivas para una organización o un proyecto

Foto: Freepick

VENEZUELA | **Alfredo Yuncoza**

El análisis de fractales es una herramienta matemática que permite estudiar la estructura y el comportamiento de fenómenos complejos e irregulares, como los sistemas financieros, los mercados bursátiles, los ataques terroristas o los desastres naturales. Esta técnica se basa en la idea de que muchos de estos fenómenos presentan una propiedad llamada autosimilaridad, que consiste en que sus partes se parecen al todo en diferentes escalas. Así, por ejemplo, un copo de nieve, una costa o un árbol son objetos fractales, ya que se pueden dividir en fragmentos más pequeños que conservan la forma del original.

OBJETIVO

La aplicación del análisis de fractales en la gestión de riesgos tiene como objetivo identificar y cuantificar los patrones y las tendencias que subyacen a los eventos aleatorios e impredecibles que pueden afectar a la seguridad, la rentabilidad o la sostenibilidad de una organización o un proyecto. Al utilizar esta herramienta, se puede obtener una mejor comprensión de la dinámica y la evolución de los riesgos, así como diseñar estrategias más eficaces y adaptativas para prevenirlos, mitigarlos o aprovecharlos.

Un ejemplo de la utilidad del análisis de fractales en la gestión de riesgos es el estudio de las fluctuaciones del precio de las acciones, que pueden tener un impacto significativo en el valor de una empresa o una inversión. Al aplicar esta técnica, se puede detectar la existencia de ciclos, tendencias y anomalías en el comportamiento del mercado, así como estimar la probabilidad y la magnitud de los cambios bruscos o las crisis financieras. De esta manera, se puede optimizar la toma de decisiones y el diseño de portafolios, reduciendo el riesgo y aumentando el rendimiento.

Otro ejemplo es el análisis de los fenómenos naturales que pueden provocar daños materiales o humanos, como los terremotos, los huracanes o las inundaciones. Al utilizar el análisis de fractales, se puede evaluar la frecuencia y la intensidad de estos eventos, así como su distribución espacial y temporal. Así, se puede mejorar la planificación y la gestión de los recursos, las infraestructuras y las medidas de protección civil, minimizando el impacto y las pérdidas derivadas de estos desastres.

Además de estas aplicaciones en el campo de la gestión de riesgos, el análisis de fractales también se utiliza en otros campos científicos y tecnológicos. Por ejemplo:

- En medicina, se usa la dimensión fractal para diagnosticar ciertas enfermedades de los huesos o para analizar la morfología y las propiedades de las células cancerígenas.

Foto: Freepick

La aplicación del análisis de fractales en la gestión de riesgos tiene como objetivo identificar y cuantificar los patrones y las tendencias que subyacen a los eventos aleatorios e impredecibles que pueden afectar a la seguridad, la rentabilidad o la sostenibilidad de una organización o un proyecto

El análisis fractal debe integrarse con otras disciplinas y fuentes de información, como la estadística, la economía, la sociología, la psicología o la historia, para obtener una visión más completa y realista de los fenómenos complejos y sus implicaciones

Foto: Freepick

- En geología, se usa para estudiar la sismicidad y la geometría de las fallas tectónicas o para caracterizar la porosidad y la permeabilidad de las rocas.
- En química, se usa para modelar el crecimiento y la estructura de los cristales o para medir la reactividad y la difusión de los elementos.
- En computación, se usa para comprimir imágenes o para generar gráficos realistas.

LIMITACIONES

Una de las limitaciones del análisis fractal es que no siempre es fácil identificar la dimensión fractal de un fenómeno, es decir, el número que mide su grado de complejidad o irregularidad. Existen diferentes métodos para estimar la dimensión fractal, pero no todos son aplicables a cualquier tipo de datos o situaciones. Además, la dimensión fractal puede variar según el nivel de detalle o la escala de observación que se utilice.

Otra limitación del análisis fractal es que no tiene en cuenta las causas o los mecanismos que generan los fenómenos complejos. El análisis fractal se centra en describir la forma o la estructura de los datos, pero no explica por qué se producen o cómo se pueden prevenir o mitigar los riesgos asociados. Por ejemplo, el análisis fractal puede mostrar que las crisis financieras tienen una periodicidad o una frecuencia determinada, pero no puede explicar qué factores económicos, políticos o sociales las provocan o cómo se pueden evitar.

Finalmente, una limitación del análisis fractal es que no es suficiente por sí solo para gestionar los riesgos complejos. El análisis fractal puede ser una herramienta útil para complementar otros métodos o enfoques, pero no puede sustituirlos ni ignorarlos. El análisis fractal debe integrarse con otras disciplinas y fuentes de información, como la estadística, la economía, la sociología, la psicología o la historia, para obtener una visión más completa y realista de los fenómenos complejos y sus implicaciones.

En conclusión, el análisis de fractales es una herramienta valiosa para la gestión de riesgos, ya que permite analizar y modelar fenómenos complejos e irregulares que pueden tener consecuencias negativas o positivas para una organización o un proyecto. Al utilizar esta técnica, se puede obtener una visión más profunda y precisa de la realidad, así como anticiparse y adaptarse a los cambios y las oportunidades que surgen en un entorno incierto y dinámico.

Asimismo, el análisis de fractales tiene múltiples aplicaciones en otros campos del conocimiento, donde se pueden aprovechar sus ventajas para resolver problemas o generar innovaciones. Sin embargo, también tiene sus limitaciones, que deben ser reconocidas y tenidas en cuenta a la hora de aplicarlo en la gestión de riesgos. El análisis fractal no puede resolver todos los problemas ni responder a todas las preguntas, pero puede ayudar a entender mejor la realidad y a tomar decisiones más informadas y racionales. ■

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

EL MOMENTO QUE LO DIFERENCIA TODO

Foto: Freepick

ARGENTINA

Modesto Miguez

El mundo cambia constantemente y hay nuevas amenazas que se deben considerar para evitar futuras pérdidas

DESARROLLO

Inspirado en el artículo escrito anteriormente llamado "Seguridad Bilateral" en la edición 119 de la revista **Seguridad en América**. Tengo una tendencia a hacer resúmenes binarios, los que clasifican en blanco o negro, claro u oscuro, bueno o malo, antes o después.

En este sentido, esta nota tiene que ver con el momento justo que separa "el antes del después". Este momento es de la pérdida, el momento exacto en donde el daño se produce. Ese momento, cuando el hecho no deseado ocurre. Sabemos que cada hecho tiene una probabilidad de ocurrencia llamada riesgo. Esos son los eventos que cuando se concretan producen pérdidas y daños.

Regresando al análisis binario, la función de la seguridad es vista desde dos aspectos, uno desde el antes y otro desde el después.

ANTES

En mi opinión, la verdadera seguridad consiste en lo que se hace desde el antes, desde el lado de la prevención, o sea, ver antes de que el hecho ocurra para hacer verdadera reducción del riesgo. Esto se logra con un análisis de seguridad, de riesgos, las métricas y las entrevistas, considerando el contexto del momento futuro en el que se estudia la probabilidad de ocurrencia de determinado evento. Lo anterior implica un análisis de amenazas.

Imaginar todas esas amenazas que se pueden producir, no es fácil. En caso de que se produjeran, ¿cuáles son nuestras vulnerabilidades? ¿Para defendernos de qué, estamos preparados? ¿Qué es lo que no tenemos planificado para reducir la pérdida? ¿Cómo restablecemos el daño y la pérdida?

Preguntas que deberíamos respondernos para calcular cuánto invertir en enfrentar amenazas reduciendo vulnerabilidades:

- ¿Qué es lo que deberíamos hacer?
- ¿Cuál es el costo-beneficio de hacerlas para bajar la probabilidad de ocurrencia y en qué intensidad?
- ¿Sabemos medir para cuantificar las consecuencias positivas y negativas del daño?
- ¿Analizamos y medimos el nivel de impacto o de criticidad de esa pérdida?

La verdadera seguridad consiste en la prevención y la reducción de pérdidas antes de que ocurran

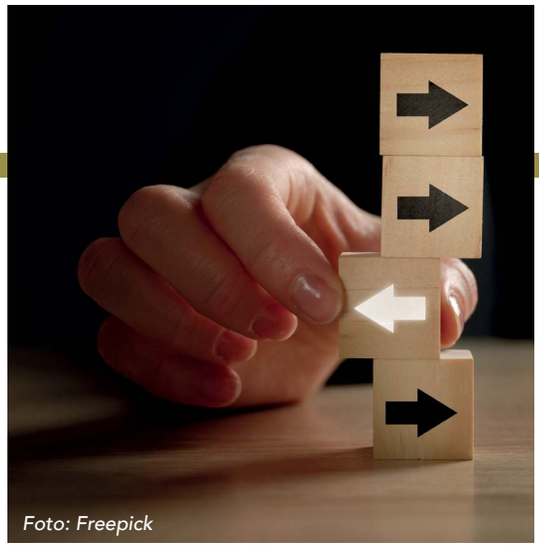


Foto: Freepick

Mucha gente se concentra en proveer soluciones después del daño, pero se debe actuar antes

Insisto, para mí la verdadera seguridad consiste en la previsión, la planificación, en la reducción de las pérdidas desde el antes, desde las medidas que se toman antes de que el hecho se produzca.

Esto es lo que va a generar ese retorno de inversión para la ayuda a la construcción de la seguridad y en obtener el menor costo total de protección.

Prestando además especial atención a las pérdidas irreparables como son: la muerte humana, una discapacidad permanente, el cierre del negocio o algún tipo de daño ambiental.

DESPUÉS

La otra forma de verlo -la antigua y habitual- es el después. Consiste en instalar el sistema de alarma de robo después que se produce el robo, el sistema de incendio después que se produce el incendio, proveer los guardias luego del conflicto, siempre luego de que se produce el daño, luego de que se vive la mala experiencia de haber sufrido la pérdida. Pérdida "impensada" porque no se incluyó en el análisis de riesgos, o se descartó por considerarla poco probable o no se midió lo suficiente.

Observo que mucha gente se dedica a esto, se dedican a actuar para "el después", se dedican a proveer sistemas, guardias, armas, servicio penitenciario, policía, reclaman leyes, regulaciones, etc., todas aplican en el después. Pero muy poco se hace para el antes.

Observo en las empresas e instituciones que no cuentan con asesores de seguridad, que no consideran las normas técnicas que ayudan a realizar y mantener planes de seguridad, que hagan análisis de amenazas, que hagan el análisis costo-beneficio de mejorar sus vulnerabilidades ante esas amenazas y determinan los beneficios de tomar esas acciones previas para minimizar esas pérdidas.

También observo que en este mundo tan vertiginoso en cuanto a cambios, los profesionales no están concientizados en cuanto a las nuevas amenazas que ya se están produciendo. Aquí hay una excelente oportunidad para un desarrollo comercial, profesional y exitoso, en cuanto a la prevención de esas futuras pérdidas que más tarde o más temprano se producirán.

Con los cambios que estamos viviendo como consecuencia de la llegada de Internet en el año 2000, de la pandemia en el 2020 y lo que lo aceleró todo con el teletrabajo, el aumento del riesgo de acceso a la información por las personas indebidas, el fraude y la mayor posibilidad de tener al "enemigo en casa".

Esa forma de hacer Seguridad 3.0, sólo basada en experiencia empírica de los siglos XIX y XX tratando de resolver problemas del siglo XXI no funciona.

Estas empresas y organizaciones que continúan con la cultura de la seguridad del siglo XX, son las principales víctimas de lo que se está observando con algo que recién comienza. Organizaciones que creen que con más personas y más monitores venderán más seguridad y es al revés, se cavan su propia fosa.

En la Seguridad 4.0, la inteligencia artificial reemplaza toda actividad humana rutinaria, las PC's no se necesitarán más, en el futuro cercano no existirán humanos mirando imágenes *'online'* ni tampoco pantallas o monitores colgando de las paredes, obviamente tampoco las centrales de monitoreo o los centros de control.

No es el futuro, es el presente, de un proceso inevitable que podemos prever "antes" para disfrutar como oportunidad o resistirnos y "después" sufrir. Cada cual decide, esperar a "ver qué pasa" también es una decisión.

Muchas gracias. ■

Modesto Miguez, CPP, asesor permanente en 300 empresas de monitoreo y seguridad en toda Latinoamérica y España. *Más sobre el autor:*

CANALES ÉTICOS DE DENUNCIA

Un canal de denuncia efectivo puede ayudar a prevenir problemas antes de que se conviertan en una amenaza costosa para la empresa. Por ejemplo, si se detecta temprano, un fraude o uso indebido de activos, se pueden tomar medidas para prevenir la pérdida de ingresos, inclusive es posible evitar sanciones o multas

MÉXICO

Jaime Gómez

¿QUÉ SON LOS CANALES DE DENUNCIAS?

Son mecanismos que las organizaciones establecen con la finalidad de permitir al personal denunciar o reportar internamente sobre situaciones que transgreden los derechos de los individuos o bien que violan lo establecido por los códigos de ética o de disciplina.

Han tomado mayor relevancia para las organizaciones toda vez que la conciencia y los esfuerzos por establecer ambientes de colaboración, de respeto, honestidad y transparencia se van procurando con mucho mayor empeño a raíz de la evolución del buen gobierno corporativo.

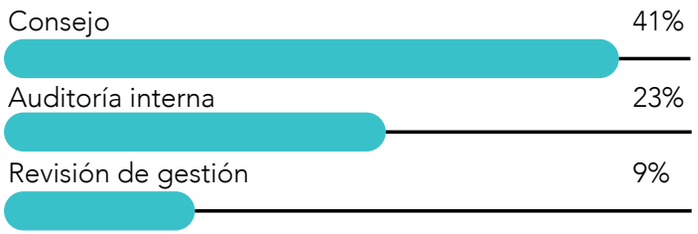
¿QUÉ VALOR APORTAN A LAS ORGANIZACIONES?

Las organizaciones comúnmente establecen "líneas de defensa" para vigilar y controlar que las actividades del día a día se lleven bajo las reglas del juego establecidas. Estas líneas de defensa típicamente son las áreas de riesgos, control interno, auditoría, calidad, prevención de perdidas, recursos humanos, legal, etc. Estas áreas establecen programas de revisión y vigilancia para asegurar que la operación se mantiene alineada a las expectativas de desempeño y rentabilidad que la Dirección General, Comité Directivo o los dueños del negocio se fijan.

Estudios que año con año realizan la Asociación de Examinadores de Fraude (ACFE) y el Instituto de Auditores Internos (IIA), entre otros, siguen comprobando que la fuente más común a través de la cual las empresas se enteran de situaciones irregulares son justamente denuncias que los colaboradores colocan en los canales de denuncia.

Un contundente 41% de las ocasiones en que las empresas detectan alguna conducta irregular proviene de algún empleado que levantó la mano o hizo valer su voz a través de un canal de denuncia. En segundo lugar en nivel de importancia se encuentran los hallazgos de revisiones realizadas por el área de Auditoría Interna.

¿Cómo se detecta inicialmente el fraude ocupacional en América Latina y el Caribe?



Otro de los primordiales objetivos que debe procurar la implementación de un canal de denuncia es la detección temprana. Las organizaciones que cuentan con estos mecanismos logran saber de alguna problemática con mayor anticipación que aquellas quienes no han dado el paso en este sentido. Por consecuencia, los impactos patrimoniales y reputacionales que resultan de las irregularidades identificadas han resultado de menor efecto.

ANONIMATO Y CONFIDENCIALIDAD

Se debe tener presente el estrés psicológico por el que pasa un denunciante para hacerse del valor requerido al levantar la voz. Especialistas han confirmado que la principal razón por la cual las personas que son víctimas o testigos de algo que debe ser denunciado no lo hacen, es por el temor que les ocasiona una potencial represalia.

Lo anterior respalda la relevancia que requiere darse al manejo de estos canales poniendo como principal fundamento de su operación el manejo de los reportes, asegurando a los denunciantes que su identidad y la integridad de su denuncia serán atendidos e investigados bajo la más estricta política de confidencialidad y privilegiando su anonimato.

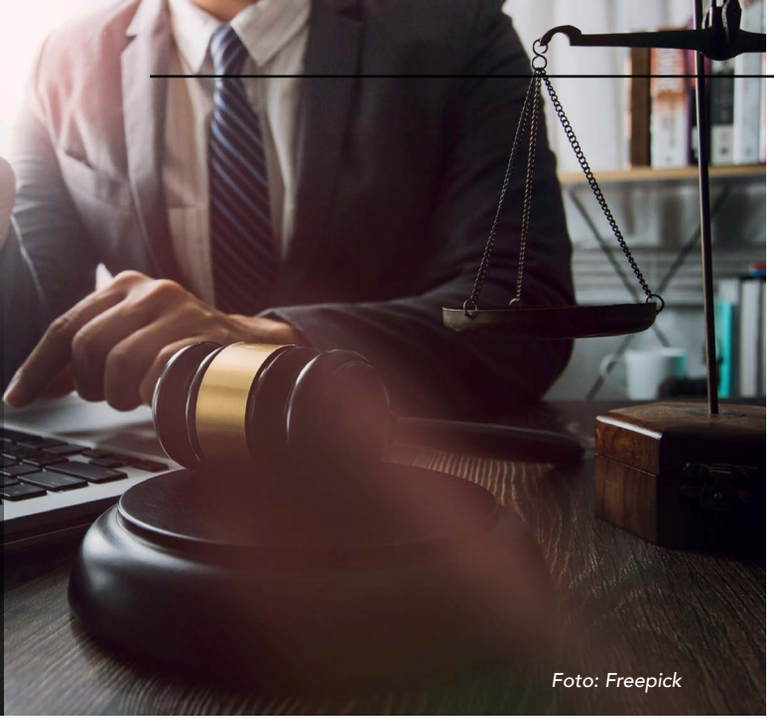


Foto: Freepick

La organización debe cerciorarse de establecer los procesos necesarios para centrarse en el "qué sucedió" de las denuncias y no en el "quién denunció". Al fomentar una cultura de apertura y transparencia protegiendo el anonimato, la empresa mejorará la confianza y el compromiso de los empleados con los valores de la organización.

¿QUÉ RETOS DEBE SOBREPONER UNA EMPRESA PARA IMPLEMENTARLO?

Algunos de los más comunes desafíos que se enfrentan incluyen:

- **Crear e instituir una cultura de confianza:** Para que los colaboradores se sientan cómodos denunciando anomalías, es importante crear una cultura de confianza y transparencia en la organización.
- **Asegurar la privacidad y confidencialidad:** Es fundamental asegurar la privacidad y confidencialidad de los denunciantes para protegerlos de posibles represalias y evitar la divulgación no autorizada de la información confidencial.
- **Garantizar la eficacia del canal de denuncia:** La empresa debe cerciorarse de que sea fácil de usar y accesible para todos los colaboradores. Así mismo, el establecer procesos claros para la atención, investigación y resolución de informes recibidos.
- **Evitar informes falsos o maliciosos:** La empresa debe establecer políticas y procedimientos para prevenir, detectar y de ser necesario sancionar informes que puedan perjudicar a alguna persona inocente o dañar la reputación de la empresa.
- **Capacitar al personal:** Deben ejecutarse los suficientes esfuerzos para dotar al personal de la información respecto al uso apropiado y los beneficios del canal de denuncia.

En resumen, la efectiva implementación de un canal de denuncia puede ser un desafío, pero el abordarlo de una manera adecuada, ayudará a la empresa a detectar y resolver problemas internos y con esto mejorar la cultura de ética y cumplimiento.

¿CUÁLES SON LOS PRINCIPALES FACTORES DE RETORNO DE INVERSIÓN QUE APORTAN ESTOS CANALES?

Los principales factores de retorno de inversión (ROI) que aportan a las empresas, incluyen:

- **Reducción de costos:** Un canal de denuncia efectivo puede ayudar a prevenir problemas antes de que se conviertan en una amenaza costosa para la empresa. Por ejemplo, si se detecta un fraude o uso indebido de activos temprano, se pueden tomar medidas para prevenir la pérdida de ingresos, inclusive es posible evitar sanciones o multas.
- **Protección de la reputación:** Estos canales pueden ayudar a prevenir deterioro de la reputación de la empresa al permitir que los problemas se aborden internamente antes de que se hagan públicos. Si los problemas se manejan de manera pertinente, la empresa puede mejorar su reputación y la confianza de los empleados, los clientes y otras partes interesadas.
- **Prevención de pérdidas económicas:** La línea anónima también puede ayudar a prevenir pérdidas económicas. Por ejemplo, si un empleado está robando o realizando actividades fraudulentas, la línea de denuncia puede ayudar a detectar estos problemas y evitar mayores pérdidas.
- **Mejora de la cultura de ética y cumplimiento:** Ayuda a fomentar una cultura de ética y cumplimiento en la empresa, lo que ayuda a mejorar la moral y la motivación de los empleados, contribuye reducir el riesgo de problemas internos.
- **Aumento de la productividad:** Al prevenir problemas y mejorar la cultura de la empresa, los canales de denuncia pueden ayudar a aumentar la productividad y la eficiencia de la empresa.
- **Cumplimiento normativo:** La implementación de un canal de denuncia efectivo puede ayudar a la empresa a cumplir con las leyes y regulaciones relacionadas con la privacidad y la protección de datos personales.

¿QUÉ NORMAS O LEYES EXIGEN A UNA ORGANIZACIÓN A CONTAR CON UNA LÍNEA DE DENUNCIA ANÓNIMA?

Dependiendo del país en el que se encuentre la empresa. Algunas de las leyes y normas más relevantes son:

- **Norma Oficial Mexicana NOM-035-STPS-2018:** establece las medidas para identificar, prevenir y controlar los factores de riesgo psicosocial en el trabajo, requiere a las empresas contar con mecanismos seguros y confidenciales para que los trabajadores puedan presentar quejas y denuncias sobre posibles violaciones a la norma. Esta norma es exigible bajo vigilancia de la Ley Federal del Trabajo.
- **Ley de Protección de Datos Personales:** En algunos países, como México, existe una ley de protección de datos personales que requiere que las empresas establezcan medidas de seguridad para proteger la información personal, incluyendo la implementación de canales de denuncia anónimos para reportar violaciones de seguridad o privacidad.
- **Código Nacional de Procedimientos Penales:** En México, este código establece que toda persona tiene la obligación de denunciar la perpetración de cualquier delito público que presencia pudiendo ser sancionado con multa por falta de colaboración con la Administración de Justicia en caso de no hacerlo. En otras palabras, toda persona a quien le conste que se ha cometido un hecho probablemente constitutivo de un delito está obligada a denunciarlo.


Foto: Freepick

- **ISO 37002:** es una sólida guía para la implementación de un sistema o canal de denuncias.
- **Ley Sarbanes-Oxley:** Esta ley estadounidense obliga a las empresas a implementar canales de denuncia anónimos para reportar actividades ilegales o no éticas. Si haces negocios con empresas norteamericanas es muy probable que te cuestionen si tus empleados pueden remitir denuncias anónimas y te exijan conocer cómo se atienden.
- **Reglamento General de Protección de Datos (GDPR):** Esta norma europea de protección de datos personales establece la obligación de las empresas de proteger la privacidad y los datos personales de sus empleados y clientes, y puede requerir la implementación de canales de denuncia anónimos para cumplir con estas obligaciones.

En general, las leyes y normas relacionadas con la ética empresarial, la privacidad y la protección de datos personales suelen requerir que las empresas implementen canales de denuncia anónimos para permitir a los empleados y otras partes interesadas reportar irregularidades de manera confidencial. Sin embargo, es importante verificar las leyes y regulaciones específicas de cada país en el que opera la empresa para garantizar el cumplimiento adecuado.

¿QUÉ RIESGOS ENFRENTA UNA EMPRESA QUE NO CUENTA CON UN CANAL DE DENUNCIA ANÓNIMA?

Una empresa que no cuenta con un canal de denuncia anónima podría enfrentar varios riesgos, entre ellos:

- **Incumplimiento de la ley:** En México, existe la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Esta establece que las empresas deben contar con medidas de seguridad adecuadas para proteger los datos personales que manejan, incluyendo la implementación de canales de denuncia anónima. Si una empresa no cuenta con este mecanismo, podría enfrentar sanciones económicas y legales. Respecto al incumplimiento concerniente al canal de denuncia al que refiere la NOM035, las sanciones económicas ascienden hasta 600 mil pesos (33 mil 151 dólares).
- **Conductas inapropiadas del personal:** Las empresas pueden enfrentar conductas inapropiadas por parte de sus empleados, como robos, actos de corrupción, acoso laboral o sexual, o incumplimiento de los protocolos de seguridad, abuso de autoridad, intimidación, etc. Estas conductas pueden afectar negativamente el desempeño del personal y la confianza de los clientes.
- **Reputación:** La falta de un canal de denuncia anónima podría afectar negativamente la reputación de la empresa, ya que podría percibirse que no se toman en serio las denuncias de los empleados y que no se está comprometido con la ética empresarial y el cumplimiento de la ley.
- **Pérdida de confianza de los clientes:** La falta de los mecanismos en cuestión también podría generar desconfianza entre los clientes de la empresa, quienes podrían preferir contratar servicios de una empresa que cuente con medidas de transparencia y denuncia efectivas.
- **Pérdida de talento:** Estudios confirman que los colaboradores suelen sentirse desmotivados y desalentados si perciben que no existen las condiciones para informar sobre posibles violaciones a la ley o a la normativa interna de la empresa, lo que podría llevar a una pérdida de talento y dificultades para retener al personal clave.

En resumen, una línea de denuncia anónima es un componente estratégico en las organizaciones que complementa a las líneas de defensa a prevenir y abordar problemas de conductas inapropiadas, mejorar la calidad del servicio y cumplir con las regulaciones aplicables.

CONCLUSIÓN

Más allá de las exigencias regulatorias o normativas, que por supuesto hay que atender, existen diversos estudios y análisis de expertos que demuestran reiteradamente la efectividad de estos mecanismos. Organizaciones tan serias como la Asociación de Examinadores de Fraude (ACFE, por sus siglas en inglés), el Instituto de Auditores Internos (IIA, por sus siglas en inglés), Harvard Law School, el Consejo Nacional de Seguridad Privada, la Policía Cibernética y otras han estudiado y analizado el contexto general de las conductas irregulares en las organizaciones.
Las prácticas líderes a nivel mundial indican que una solución debe:

- Privilegiar el anonimato.
- Poner disponibles diversos canales o medios para remitir las denuncias.
- Ser operada por un tercero especializado.
- Permitir al denunciante dar seguimiento a su denuncia manteniendo el anonimato.
- Concentrar toda la información en un repositorio único y seguro donde gestionar los casos.

En general, contar con un canal de denuncia anónima efectivo es beneficioso para toda organización, ya que refuerza la cultura de ética y cumplimiento, fortalece la reputación y la confianza de los clientes y el personal, y prevenir posibles incumplimientos legales. ■

Jaime Gómez, socio director en Ética Integral. *Más sobre el autor*

Socio Amesis amesis.org.mx · AMESP · ANTP · ASIS INTERNATIONAL CAPÍTULO MÉXICO 217 · CANACAR Cámara Nacional del Autotransporte de Carga · CNSP Consejo Nacional de Seguridad Privada A.C. Empresas de Calidad · COPARMEX · ConaLog Consejo Nacional de Ejecutivos en Logística y Cadena de Suministro, A.C.

Contáctanos
55·5374·9320

Foto: - Freepik

CÁRCELES EN LATINOAMÉRICA (PARTE II)

Nuevas cárceles. Emprendimiento público-privada

ESPAÑA | **Manuel Sánchez Gómez-Merelo**

Los centros penitenciarios o dependencias carcelarias son también espacios complejos con base en su tamaño y arquitectura y, a medida que se incrementa la población de reclusos, se hace más importante contar con sistemas y tecnologías para la gestión y resolución de los desafíos que se presentan, a fin de garantizar la seguridad de su funcionamiento.

Las múltiples deficiencias evidenciadas en los sistemas penitenciarios de la región, hacen urgente el desarrollo de una amplia reforma penitenciaria que abarque distintos ámbitos.

Son imprescindibles y urgentes las reformas de los sistemas penitenciarios, destinando los recursos necesarios para acometer, adecuar y/o construir nuevas cárceles. Este es el verdadero desafío regional: abordar definitivamente la insuficiencia de infraestructuras, la escasez del presupuesto destinado a resolver o al menos paliar ese abandono, los déficits crónicos en la administración y gestión penitenciaria, la deficiente calidad de los servicios y tratamientos, así como las carencias en los programas para la resocialización y reinserción de los penados.

En este sentido, la Corte Interamericana de Derechos Humanos (CIDH) expresa que: "los Estados no pueden alegar dificultades económicas para justificar condiciones poco dignas de las personas privadas de la libertad en establecimientos penitenciarios…". "El Estado tiene el deber de adoptar las medidas necesarias para proteger la integridad personal de los privados de libertad y abstenerse, bajo cualquier circunstancia, de actuar de manera tal que se vulnere la vida y la integridad de estas".

Las carencias y situaciones actuales son las principales causas que generan el aumento cada vez mayor de la conflictividad y el hacinamiento en la población carcelaria. Sin embargo, hay quienes consideran que el hacinamiento no es una causa, sino más bien una consecuencia de la ineficiente intervención estatal, dado que, en la mayoría de los países de la región, se ha preferido usar medios coercitivos o represivos en vez de educativos.

SON IMPRESCINDIBLES Y URGENTES LAS REFORMAS DE LOS SISTEMAS PENITENCIARIOS, DESTINANDO LOS RECURSOS NECESARIOS PARA ACOMETER, ADECUAR Y/O CONSTRUIR NUEVAS CÁRCELES

No obstante, si bien las medidas de aseguramiento y tratamiento pueden tomarse como un medio para lograr la resocialización y reinserción social, lo cierto es que hay que dotar de nuevos recursos al Sistema Penitenciario y establecer mecanismos donde prevalezca la garantía de los derechos humanos.

Así, el nuevo planteamiento de las Alianzas Público-Privadas (APPs) puede ser el medio idóneo para que el Estado, en colaboración armónica con entidades privadas, desarrolle y organice un nuevo diseño, financiación, gestión y reestructuración del Sistema Penitenciario en los distintos países, con miras a que la población reclusa goce de los derechos constitucionales y, sobre todo, se garantice su seguridad y tratamiento para la reinserción social.

En este sentido, tenemos interesantes experiencias internacionales en la implementación de las asociaciones público- privadas en el sector penitenciario para la creación de nuevas cárceles o modernización de las existentes, medida adoptada en varios países para hacer frente a la crisis carcelaria.

La incorporación de capital privado y/o gestión colegiada en los nuevos establecimientos penitenciarios puede ayudar a la disminución de la carga Estatal, paliando sus carencias y contribuyendo a una mayor eficacia y eficiencia en la resolución de este grave conflicto.

Como demuestra la experiencia de otros países, mejorando el sistema judicial y facilitando unas infraestructuras dignas y suficientes, así como la tecnología de control imprescindible, es posible la creación de un sistema penitenciario que propicie la instauración de un código de conducta correcto, tanto en los funcionarios como en los reclusos (que responderán como personas siempre que sean tratados como tales), permitiendo con ello el cumplimiento del fin último de resocializar y reinsertar al mayor número de reclusos posible, mediante la eliminación de las demoras judiciales, el hacinamiento, la sobrepoblación carcelaria y los nichos internos de delincuencia.

Para ello, la construcción de nuevos centros penitenciarios es prioritaria y, como mínimo y mientras tanto, sería imprescindible actualizar las infraestructuras y seguridad de los actuales, mejorando con carácter de urgencia las condiciones laborales del personal y planificando el trabajo con las demás Instituciones implicadas, así como con las instancias judiciales.

Todo ello, teniendo en cuenta que no se debe delegar funciones que son intransferibles e inherentemente del Estado.

SEGURIDAD PENITENCIARIA

En la actualidad, son muchas las amenazas que atentan contra la seguridad del sistema penitenciario y carcelario. Entre ellas, la falta de personal y su adecuada capacitación, que es una de las mayores deficiencias que ponen en peligro y vulneran la propia seguridad, tanto del personal, como de los internos y de las instalaciones.

El tema de la seguridad penaliza al sistema, los Gobiernos sólo favorecen medidas represivas porque, es tan negativa la visión sobre quien comete delitos, que nunca se ha tenido una política adecuada de prevención e integración social del penado y sólo entra en programa la represión, cuando una inversión adecuada y a tiempo en la clasificación y tratamiento podría ahorrar muchas vidas e incluso abaratar costes de reinserción.

Los objetivos principales de la seguridad en los centros penitenciarios son: impedir que se produzcan fugas de presos o altercados y motines; garantizar la seguridad de los internos e instalaciones; favorecer el objetivo de reinserción social. Se contempla en dos conceptos generales clave: la protección externa, para evitar fugas y agresiones, y el control y la vigilancia interna, para evitar incidentes.

El planteamiento del sistema de seguridad se ha de hacer de forma integral y debe ser objeto del proyecto la implementación de una plataforma de gestión integral. Esta plataforma permitirá integrar todos los sistemas de control y seguridad tanto del interior (módulos y patios) como del exterior (perímetro y accesos), así como todas las lecturas del sistema de control de accesos (personas y vehículos) y todos metadatos de las cámaras y servidores de inteligencia artificial más avanzados.

CONCLUSIONES

A modo de resumen, puede afirmarse que la política pública penitenciaria en Latinoamérica ha fracasado, dado que no ha podido afrontar con éxito el crecimiento significativo de la población penitenciaria, el modelo actual no ha sido capaz de generar los resultados en recuperación, rehabilitación y resocialización de las personas privadas de la libertad, lo que está directamente relacionado con una inadecuada gestión de seguridad, tratamiento y salud penitenciaria.

Prácticamente la totalidad de los establecimientos penitenciarios está en malas condiciones o con infraestructuras obsoletas, situación que ha llevado a la imposibilidad de la ejecución y el desarrollo de los "planes" y "programas" de seguridad en el tratamiento penitenciario.

En la práctica, como lo demuestra la información empírica, no se está cumpliendo con la gestión de seguridad, tratamiento y salud penitenciaria, a pesar de la obligación legal, y lo estipulado en los manuales operativos. La gestión de las autoridades de los establecimientos penitenciarios se ha centrado principalmente en la custodia y represión de las personas privadas de la libertad.

En general, la percepción de los funcionarios sobre el modelo del sistema penitenciario vigente ha fracasado, al no centrar su gestión en la seguridad y tratamiento para la reinserción, así como carecer de los recursos presupuestarios que permitan el seguimiento de los resultados.


Foto: - Freepik

Los objetivos principales de la seguridad en los centros penitenciarios son: impedir que se produzcan fugas de presos o altercados y motines; garantizar la seguridad de los internos e instalaciones; favorecer el objetivo de reinserción social

Además de construir más recintos carcelarios, urge reestructurar el régimen penitenciario y establecer políticas de tolerancia cero, para avanzar con una verdadera política de Estado que se haga cargo de la situación de los penados de cara a su reinserción y resocialización, tanto dentro, como cuando dejan los recintos penitenciarios.

El nuevo modelo de gestión penitenciaria debe contemplar y enfocar su gestión en la seguridad, el tratamiento y la salud de la población penitenciaria, centrándose en:

- Reformar la inoperativa política judicial imperante, con un menor uso de la prisión preventiva.
- Atender a la formación integral y especializada del personal penitenciario.
- Establecer una política penitenciaria que se enmarque dentro de una Estrategia de Reinserción Social.
- Considerar las alianzas público-privadas que pueden ser el medio idóneo para que el Estado ejecute sus planes de desarrollo, facilitando la administración, el financiamiento, la gestión y la reestructuración de un Sistema Nacional Penitenciario verdaderamente eficiente.

La creación de nuevas cárceles o modernización de las existentes es sólo parte de las medidas que deben adoptarse en los distintos países de la región para hacer frente a la larga crisis penitenciaria. ■

Manuel Sánchez Gómez-Merelo,
consultor internacional de Seguridad y ex-coordinador de Seguridad en Instituciones Penitenciarias. *Más sobre el autor:*


Foto: - Freepik

LA MEDIACIÓN DE CONFLICTOS
COMO ÁREA DE OPORTUNIDAD LABORAL
PARA EL CRIMINÓLOGO

La Criminología de la Consejería Social es el estudio de los problemas que se dan en el desarrollo de las relaciones sociales, así como problemas de adaptación

MÉXICO **Wael Sarwat Hikal Carreón**

INTRODUCCIÓN

La criminología en su labor preventiva tiene como función el emplear los medios y técnicas necesarias para evitar que los conflictos concluyan en un proceso penal y penitenciario. La Criminología de la Consejería Social busca solucionar las problemáticas enseñando a los ciudadanos a identificar, entender y solucionar sus conflictos, lo que será clave para una prevención del delito.

La solución tradicional de los conflictos en materia penal, civil u otras afines, ha causado un aumento en las consecuencias negativas que mejora, derivado en parte por las contiendas que se generan entre los involucrados y la falta de flexibilidad de estos para ceder a la finalización del problema. Por ello, se originan los mecanismos alternativos de solución de controversias como una herramienta que atenúe el impacto de las problemáticas.

Los especialistas que facilitan los procesos alternos pueden ser públicos o privados, ya sea que se desempeñen en el ámbito gubernamental o comercial. Los medios alternos de solución de conflictos en materia son mecanismos llevados a cabo por las partes, donde se promueve la concientización del problema en el que se está involucrado, determinar su grado de responsabilidad, fomentar la solución entre los intervinientes para el mantenimiento de la paz en sociedad. El criminólogo al provenir de las áreas de ciencias sociales, legales y humanidades está facultado para ejercer como especialista o facilitador.

La metodología empleada es de análisis documental (Peña Vera y Pirela Morillo, 2007) para extraer conceptos torales de Criminología general, Criminología de la Consejería Social, criminólogo como profesional, criminólogo en su formación universitaria, así como conceptos de mediación. Finalmente, derivado de la revisión de las 32 leyes de cada entidad federativa en México (Cámara de Diputados, 2021), se resume en tablas la entidad, el marco legal y los artículos que describen los perfiles profesionales para ocuparse como facilitador-mediador. El objetivo último del presente artículo es ser una propuesta laboral para los egresados de Criminología en México.

DISCUSIÓN

La criminología como la conocemos actualmente emerge primariamente de la antropología, se suman al tiempo la sociología y psicología, a lo que posteriormente se le agregaron otras ciencias y teorías desde la Política, Economía, Demografía, Biología, Derecho entre otras, resultando un abanico de explicaciones desde diferentes visiones permitiendo una explicación holística (Hikal Carreón, 2021).

García-Pablos De Molina define: "Esta estudia el crimen, la personalidad del antisocial y el control social para evitar esta conducta; además, trata de suministrar información científica, contrastada sobre la génesis, dinámica y variables del crimen desde lo individual hasta lo social, así como los programas de prevención y tratamiento del ser antisocial" (1996, p. 19).

Los criminólogos se encuentran ante un panorama de graves problemas que ocurren en la sociedad, por lo que deben estar ampliamente preparados en valores, ética, respeto, empatía, compromiso. Y guardan una estrecha comunión con la responsabilidad social para la atención de los problemas para los cuales ha sido formado universitariamente. "El diseño curricular criminológico, debe buscar formar profesionales para explicar el fenómeno delictivo, desde la integridad de la persona como un sistema biopsicosocial, generando resultados y nuevas propuestas de abordaje, que tengan como meta final tributar a la calidad de vida del ciudadano" (Rodríguez Estrada, 2020, p. 359).

Ríos Patio apunta un concepto de "criminólogo": el criminólogo es un profesional que estudia las causas, factores, condiciones y motivos que generan criminalidad. Su labor es de suyo trascendental porque la cuestión criminal confronta el nivel de seguridad integral del Estado, el cual está íntimamente vinculado al bienestar general, ya que son conceptos interdependientes y complementarios, que apuntan a la aspiración de la organización social toda hacia el bien común (2017, p. 16).

Pasando al tema de la resolución clásica de conflictos civiles y penales, según Pérez Tolentino (2012), ha causado un aumento en las consecuencias negativas que mejora, derivado en parte por las disputas que se generan entre los implicados y la falta de blandura de éstos para ceder a la terminación del problema. Por ello, se originan los mecanismos alternativos de solución de controversias como una herramienta que atenúe el impacto de las problemáticas, buscando que no haya ganadores ni perdedores sino personas que se responsabilicen de sus acciones, sin salir del sistema social.

Criminología de Consejería Social: frecuentemente se presentan situaciones en las que ciertos individuos son problemáticos, no propiamente con delitos legalmente establecidos en las legislaciones, pero sí conductas graves que afectan a sí mismos, familiares o vecinos. Estas acciones tildan en las conductas antisociales con miras a convertirse en delictivas. Esto también incluye a los menores de edad cuyos actos pueden ser destructivos. De tal forma la Criminología en su labor preventiva debe actuar para evitar que dichas conductas continúen y se agraven (Hikal, 2019, p. 140).

Los facilitadores de la mediación que promueven los medios alternos pueden ser públicos o privados, según el ámbito en el que se desempeñen. Cabe plantear las siguientes cuestiones: ¿Qué profesión es la apropiada para ser mediador? ¿Está legalmente habilitado el criminólogo para ejercer profesionalmente como mediador? ¿Es una salida laboral para el criminólogo? (Pérez Tolentino, 2012).

> La criminología como la conocemos actualmente emerge primariamente de la antropología, se suman al tiempo la sociología y psicología, a lo que posteriormente se le agregaron otras ciencias y teorías desde la Política, Economía, Demografía, Biología, Derecho, entre otras

RESULTADOS

En las próximas tablas se presentan los perfiles profesionales requeridos en las 32 entidades federativas de las que se componen los Estados Unidos Mexicanos. Para ello, se realiza la siguiente clasificación: 1. entidades federativas que marcan particularmente la licenciatura solicitada (una), 2. Entidades que implantan de modo enunciativo las licenciaturas requeridas (varias). 3. Entidades federativas que requieren que el especialista, facilitador o mediador cuente con alguna profesión (variedad profesional). 4. Entidades federativas que establecen como requisito que el especialista, facilitador o mediador esté capacitado (curso).

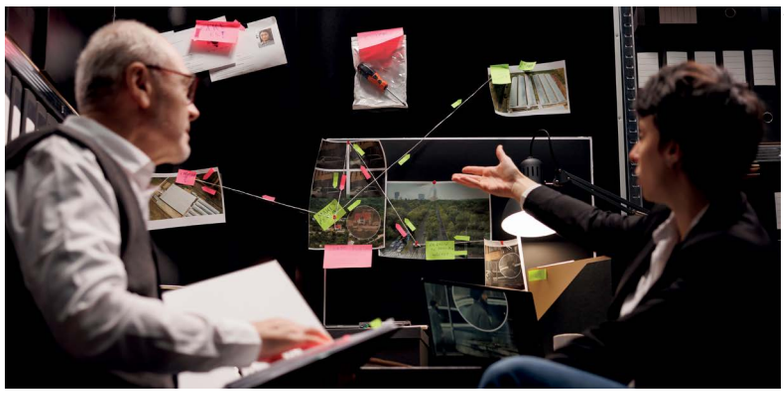


Foto: - Freepik

Tabla 1. Entidades federativas que señalan específicamente la licenciatura requerida.

Entidad	Marco legal	Norma
Ciudad de México	Ley de Justicia Alternativa del Tribunal Superior de Justicia.	Artículo 18, fracción II. Deben contar con título y cédula de la licenciatura en derecho; además, se requieren tres años de experiencia (...).
Tlaxcala	Ley que Regula el Sistema de Mediación y Conciliación.	Artículo 29, fracción II. Ser licenciado en derecho con título y cédula profesional, legalmente expedidos y tener como mínimo tres años en el ejercicio profesional.
Veracruz	Ley de Medios Alternativos para la Solución de Conflictos.	Artículo 10, fracción III. Poseer título de Licenciado en Derecho.
Baja California Sur	Ley de Mecanismos Alternativos de Solución de Controversias del Estado de Baja California Sur.	Artículo 17, fracción III. Tener Cédula y Título de Licenciado en Derecho, debidamente expedidos y registrados conforme la Ley.
Guerrero	Ley que Regula el Sistema de Mediación y Conciliación.	Artículo 91, fracción II. Contar con título profesional de licenciado en derecho.

Nota: Elaboración propia.

Tabla 2. Entidades federativas que mencionan de manera enunciativa las licenciaturas que debe tener el especialista, facilitador o mediador.

Entidad	Marco legal	Norma
Aguascalientes	Ley de Mediación y Conciliación.	Artículo 9, fracción II. Ser licenciado en derecho, trabajo social, psicología, sociología, asesoría psicopedagógica, educación, maestro normalista o afines.
Campeche	Ley de Mediación y Conciliación.	Artículo 31, fracción II. Contar con título y cédula profesional de licenciado en derecho, psicología, sociología, trabajo social u otras licenciaturas en el área de las ciencias sociales y humanidades (…).
Zacatecas	Ley de Justicia Alternativa.	Artículo 33, fracción III. Tener título y cédula de profesional en derecho o en ramas de humanidades, con antigüedad mínima de tres años.
Michoacán	Ley de Justicia Alternativa y Restaurativa para el Estado de	Artículo 16, fracción II. Tener cédula profesional, preferentemente de licenciado en derecho.

Nota: Elaboración propia.

El diseño curricular criminológico debe buscar formar profesionales para explicar el fenómeno delictivo, desde la integridad de la persona como un sistema biopsicosocial, generando resultados y nuevas propuestas de abordaje, que tengan como meta final tributar a la calidad de vida del ciudadano

Tabla 3. Entidades federativas que requieren que el especialista, facilitador o mediador cuenta con alguna profesión.

Entidad	Marco legal	Norma
Baja California	Ley de Justicia Alternativa para el Estado de Baja California.	Artículo 12, fracción III. Tener título profesional, debidamente registrado en el Departamento de Profesiones del Estado.
Chiapas	Ley de Justicia Alternativa del Estado de Chiapas.	Artículo 39, fracción III. Tener título profesional legalmente expedido en alguna rama de las ciencias sociales y, en su caso, de la salud.
Colima	Ley de Justicia Alternativa del Estado de Colima.	Artículo 34, fracción III. Tener título profesional legalmente expedido en alguna rama de las ciencias sociales y, en su caso, de la salud.
Estado de México	Ley de Mediación, Conciliación y Promoción de la Paz Social para el Estado de México.	Artículo 13, fracción II, inciso a. Contar con título profesional.
Jalisco	Ley de Justicia Alternativa del Estado de Jalisco.	Artículo 16, fracción VI. Contar con título profesional, cuando el prestador no sea profesional del Derecho deberá asesorarse de un abogado en la implementación de los convenios que deban suscribirse.
Morelos	Ley de Justicia Alternativa en Materia Penal para el Estado de Morelos.	Artículo 17, fracción VI. *Idem.*
Oaxaca	Ley de Mediación para el Estado de Oaxaca.	Artículo 12, fracción II. Contar con título profesional debidamente expedido en los términos de la legislación estatal de la materia, se exceptúa de esta obligación a las personas que justifiquen haber dado servicio en su comunidad por tres años en cuestiones de resolución de conflictos.
Yucatán	Ley de Mecanismos Alternativos de Solución de Controversias en el Estado de Yucatán.	Artículo 24, fracción VII. Contar con título profesional.
Chihuahua	Ley de Justicia Alternativa del Estado de Chihuahua.	Artículo 25, fracción III. Contar con título y cédula de alguna profesión afín a la prestación del servicio de mecanismos alternativos.

Nota: Elaboración propia.

Foto: - Freepik

Tabla 4. Entidades federativas que establecen como requisito que el especialista, facilitador o mediador esté capacitado.

Entidad	Marco legal	Norma
Nuevo León	Ley de Mecanismos Alternativos para la Solución de Controversias para el Estado de Nuevo León.	Artículo 35. Los facilitadores deberán certificarse ante el Instituto, obligándose a cumplir para ello con los criterios de formación y capacitación en mecanismos alternativos establecidos.
Tamaulipas	Ley de Mediación para el Estado de Tamaulipas.	Artículo 31, inciso c) Acreditar, mediante documento idóneo expedido por institución autorizada, que está capacitado en las técnicas de la mediación con mínimo de ciento veinte horas de carácter teórico y práctico.
Nayarit	Ley de Justicia Alternativa para el Estado de Nayarit.	Artículo 19. Para ser especialista se requiere acreditar los requisitos establecidos en el reglamento de esta ley y obtener del Centro Estatal la certificación y el registro que lo acredite como especialista en medios alternativos de solución de controversias.
Coahuila	Ley de Medios Alternos de Solución de Controversias para el Estado de Coahuila de Zaragoza.	Artículo 12, fracción III. Contar con capacitación en Métodos Alternos de Solución de Controversias.
Guanajuato	Ley de Justicia Alternativa del Estado de Guanajuato.	Artículo 18, fracción II. Ser profesionista, preferentemente Licenciado en Derecho. Fracción IV. Acreditar haber recibido la capacitación especializada en mediación y conciliación.
Hidalgo	Ley de Justicia Alternativa para el Estado de Hidalgo.	Artículo 8, fracción IX. Contar con título profesional legalmente expedido. Fracción XI. Haber obtenido con anterioridad a la certificación y registro como Mediador-Conciliador ante el Consejo en los términos del Reglamento respectivo.
Durango	Ley de Justicia Alternativa del Estado de Durango.	Artículo 40. Sólo podrán desempeñarse como especialistas en el Centro Estatal y en los Centros Distritales, las personas que hayan sido capacitadas o certificadas por éste, inscritas en el registro correspondiente y seleccionadas mediante el examen de oposición que esta Ley establece.
Querétaro	Reglamento del Centro de Mediación del Poder Judicial del Estado de Querétaro Arteaga.	Debe estar capacitado.
Quintana Roo	Ley de Justicia Alternativa para el Estado de Quintana Roo.	Artículo 14. Personal especializado en el manejo de los métodos alternativos de solución de conflictos.
San Luis Potosí	Ley de Mediación y Conciliación para el Estado de San Luis Potosí.	Artículo 3, fracción V. Certificación.
Sinaloa	Ley de Mecanismos Alternativos para la Solución de Controversias del Estado de Sinaloa.	Artículo 64. Los Centros contarán con una planta de facilitadores certificados, capacitados y formados en la conducción de los mecanismos alternativos de solución de controversias.
Sonora	Ley de Mecanismos Alternativos de Solución de Controversias para el Estado de Sonora.	Artículo 27, fracción II. Contar con los conocimientos, aptitudes y habilidades suficientes para desempeñar el cargo de manera eficiente.
Tabasco	Ley de Acceso a la Justicia Alternativa para el Estado de Tabasco.	Artículo 25, fracción VIII. Especialista. Persona capacitada que funge como facilitador de la comunicación entre las partes en los mecanismos alternativos de solución de controversias.

Nota: Elaboración propia. ■

Foto: - Freepik

Referencias:

- *Cámara de Diputados (2021) Leyes de los estados. https://www.diputados.gob.mx/LeyesBiblio/gobiernos.htm*
- *García-Pablos de Molina, A. (1996). Criminología. Una Introducción a sus Fundamentos Teóricos para Juristas. Tirant lo Blanch.*
- *Hikal Carreón, W.S, (2021). De raíces antropológicas: Bastimento epistemológico de la criminología. Anales de Antropología, 55(1), 173-178. http://dx.doi.org/10.22201/iia.24486221e.2021.1.75963*
- *Hikal, W. (2019). Introducción a la Criminología Moderna y Especializada. Porrúa.*
- *Peña Vera, T. y Pirela Morillo, J. (2007). La complejidad del análisis documental. Información, Cultura y Sociedad, (16), 55-82. http://www.scielo.org.ar/pdf/ics/n16/n16a04.pdf*
- *Pérez Tolentino, J.A. (2012). Criminología y medios alternos de solución de conflictos. Archivos de Criminología, Criminalística y Seguridad Privada, 5(9). 37-47. https://drive.google.com/file/d/1QQZHRtFXPoBRBqKrScSDcDjRloBQRjEy/view*
- *Ríos Patio, G. (2017). "El criminólogo en la empresa". A propósito del nuevo modelo de prevención criminal introducido por la Ley N° 30424 modificada por el Decreto Legislativo N° 1352. Instituto de Investigación Jurídica. 1-21. http://www.repositorioacademico.usmp.edu.pe/bitstream/handle/usmp/2675/rios_pg16;jsessionid=4FF0D8F0923D203A05420BCD5D88B620?sequence=1*
- *Rodríguez Estrada, L.E. (2020). Configuración de una Criminología especializada: Importancia de un diseño curricular flexible y moderno. Revista Remembranza, 3(1), 1-10. http://revistas.unellez.edu.ve/index.php/rremembranza/article/view/1142/1029*

Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León, México. *Más sobre el autor:*

Columna de
GEMARC

hcoronanav15@yahoo.com.mx

Cinzia Luna, líder del Comité de Inteligencia en Grupo de Ejecutivos en Manejo de Riesgos Corporativos, A.C. (GEMARC) para el periodo 2023-2025 y *Country Security Manager* de ENGIE.

Más sobre la autora:

CRISIS DE INSEGURIDAD EN CHIAPAS

foto: freepik

La dinámica de la región sureste se ha alterado como resultado de las grandes obras de infraestructura como el Tren Maya y el corredor Transístmico. Esto a su vez se ha traducido en un cambio en su dinámica delictiva, fenómeno más notorio en el Estado de Chiapas.

Si bien, en Chiapas la disputa entre cárteles comenzó en 2021, acciones ocurridas desde marzo de 2023 a la fecha advierten una agudización en la disputa entre grupos delictivos por el control del territorio ocasionando un acelerado deterioro de la seguridad pública, cuya tendencia podría mantenerse en el mediano plazo, ello debido a que en el estado convergen y se ha intensificado la operación de grupos del narcotráfico, guerrillas y pandillas juveniles, muchas de ellas originarias de Centroamérica.

Chiapas se ha convertido en uno de los principales focos de violencia del sur del país y se advierte que en el último año se ha incrementado la presencia del crimen organizado, no sólo de grandes cárteles como el de Sinaloa (CDS) y Jalisco Nueva Generación (CJNG), sino de locales como el de San Juan Chamula (CSJC), el cual es la primera organización indígena de la delincuencia organizada en el país con tácticas similares a las usadas por maras salvadoreñas, así como grupos paramilitares tales como la Organización Regional de Cafeticultores de Ocosingo (Orcao) y elementos de la extinta Brigada de Fuerzas Especiales Kaibil, dedicadas al tráfico de armas y adiestramiento de cárteles mexicanos.

DELINCUENCIA AL ALZA

Lo anterior ha incidido en un deterioro de la seguridad pública, aumentando delitos de alto impacto como son: retenes falsos, secuestros, el reclutamiento forzado, desaparición de personas, extorsiones, asesinatos, robos con violencia; así como decomisos de armamento de grueso calibre, droga de todo tipo y diversas detenciones de extranjeros, principalmente sudamericanos, que ingresan cocaína al territorio.

De concretarse un mayor control territorial de los grupos delictivos se prevé un aumento en los riesgos hacia los activos de las empresas, tanto físicos como humanos, y suponen complicaciones en el desarrollo de los negocios, por lo que se deberá mantener atención ante un escalamiento de dichas acciones.

La zona de mayor alerta es al sur del estado, en los municipios colindantes con Guatemala, donde se ha agudizado la disputa entre el CDS y el CJNG, este último de reciente incursión al estado, presuntamente con el apoyo de exkaibiles y del cártel guatemalteco Los Huistas, quienes antes eran aliados del CDS, por las rutas del tráfico de droga y otros ilícitos.

Destaca Frontera Comalapa, municipio estratégico para el tráfico de cocaína, donde se diversifican los métodos de transporte para las actividades ilegales y alberga pistas clandestinas, hasta el momento, controlados por el CDS. Así como Suchiate, cuya importancia estratégica se debe a que es el punto de entrada al país, en él confluyen intereses políticos y económicos de nivel internacional, lo que ha favorecido una rápida expansión de grupos criminales, incluso de bandas procedentes de otros países, y con ello la proliferación de delitos.

En municipios del noroeste del estado, limítrofe con Tabasco, se encienden las alertas ante decomisos de armamento y droga, así como ataques a instalaciones policiales. Destaca el ataque armado (01 de agosto de 2023) a las instalaciones de la Policía Estatal en el municipio de Reforma con saldo de una persona muerta; los atacantes portaban insignias del Grupo Delta, vinculado al CJNG. Posteriormente, en represalia por la detención de delincuentes, en Huimanguillo y Cárdenas, Tabasco, se reportó el incendio de vehículos, bloqueos carreteros, enfrentamientos y la aparición de narcomantas. En la zona trasciende la operación de células criminales, entre ellas La Barredora, dedicadas primordialmente al robo de carros y asaltos violentos, y a quienes busca combatir el CJNG.

La tensión en la región podría escalar ante los recientes pronunciamientos del Ejército Zapatista de Liberación Nacional (EZLN) en los que denuncia la complicidad activa o pasiva de los tres niveles de gobierno. De continuar la situación, no se descarta el impulso de acciones de resistencia civil, abonando a la conflictividad que se vive en la zona y que podría alcanzar impacto internacional. ■

Protegemos lo **que más valoras.**

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

#EmpresaSegura

Seguridad inquebrantable

Tu confianza está respaldada por nuestra experiencia.

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

www.**remi**.mx

Informes al teléfono:
55 72 58 92 26

SEGURIDAD ENERGÉTICA (PARTE I)

La seguridad energética es un asunto cuya vital importancia lo convierte en uno de los principales asuntos de Estado

Foto: Freepick

ESPAÑA

Jesús De Miguel Sebastián

RESUMEN EJECUTIVO

El presente artículo es una contribución al tema propuesto por la revista **Seguridad en América** sobre su especial dedicado a la seguridad en la industria energética.

En él, se aborda, desde una perspectiva académica el propio concepto de la "Seguridad Energética", el cual está siendo incorporado a las agendas de seguridad de la mayoría de los Estados, formando parte de un modelo más amplio y profundo de entender la seguridad.

Como quiera que los aspectos relacionados con la seguridad energética se encuentran íntimamente relacionados con el país a considerar, entendiendo, por una parte, las diferentes visiones de los países productores frente a losconsumidores, pero también, y no menos importante, su nivel de desarrollo, el cual está asociado a un mayor consumo. Todo ello ha llevado al autor a centrar el contenido del presente artículo al caso de España, país con gran dependencia de los recursos energéticos, pero con un aceptablemente elevado nivel tecnológico y comercial para la obtención, transporte, generación y distribución de energía.

INTRODUCCIÓN

Ya desde la gran crisis energética de los años 70's del pasado siglo se puso de manifiesto la vulnerabilidad que tenían la mayoría de los Estados ante los vaivenes del mercado, claramente dominado por los países productores del Golfo Pérsico. A partir de ese momento se constató que la energía se había convertido en una prioridad para la Seguridad Nacional, tanto para los países productores como para los consumidores. Así, desde el inicio de este siglo, la seguridad energética se ha ido convirtiendo en una prioridad no sólo para las grandes potencias, como China o Estados Unidos, sino para los principales países industrializados como Alemania, Brasil, España, Francia o México, por citar solamente algunos ejemplos.

Se podría decir que la seguridad energética mantiene una relación transversal no solamente con la seguridad del Estado, sino del concepto más amplio de la seguridad económica, en la medida que la energía es un factor determinante en el desarrollo de las diferentes naciones, las cuales precisan de diferentes recursos energéticos que den sustento a las economías de mercado. También se puede vincular a la seguridad humana en la medida que contribuyen, directa e indirectamente, al acceso de las personas a los recursos básicos.

Si ya la seguridad energética se encontraba en entredicho, la guerra en Ucrania, tras la invasión rusa, ha puesto esta cuestión en el primer plano de la agenda internacional. Esta crisis ha puesto de manifiesto, si nos referimos a Europa, una de las grandes debilidades de la UE como es el no contar con una política energética común y su dependencia de regímenes como el de Putin en Rusia.

ENTENDIENDO LA SEGURIDAD ENERGÉTICA

La energía es esencial para toda actividad humana, la alimentación, la obtención de recursos, la construcción, el transporte, etc., necesitan energía. Cuanto más desarrollada, compleja y productiva es una sociedad, mayores son sus necesidades energéticas. Aunque la energía es indispensable en las sociedades modernas, ésta no es inagotable (al menos en lo que se refiere a las actuales fuentes), ni tampoco está siempre disponible cuando se necesita. Es precisamente de la combinación de estos dos factores donde surge el concepto de seguridad energética.

No existe una definición estándar y global de la seguridad energética. La mayoría de los analistas la describen como la garantía de un suministro adecuado de energía asequible para satisfacer las necesidades vitales de un Estado, incluso en tiempos de crisis o conflictos internacionales. En la práctica, como afirma Michael T. Klare[1], abarcar la doble función de asegurar la obtención de suministros suficientes de energía para satisfacer las necesidades fundamentales de una sociedad, así como garantizar su entrega sin obstáculos desde el punto de producción hasta el consumidor final.

Este concepto ha sido ampliamente asumido por los países mayores consumidores tradicionales, como Francia, Alemania, Estados Unidos, el Reino Unido y Japón, los cuales no disponían de los suficientes recursos energéticos propios para satisfacer sus necesidades, siendo dependiente de suministradores de países situados en las zonas de gran inestabilidad y conflictividad. A la ya de por sí tradicional inseguridad energética, en particular si nos referimos a Europa,

hay que añadir las consideraciones derivadas del cambio climático que ha llevado a no pocos países a ir abandonando las energías procedentes de recursos fósiles y de la nuclear para impulsar las renovables, con un innegable déficit en lo que a su rendimiento y almacenamiento se refiere.

La seguridad energética es un asunto cuya vital importancia lo convierte en uno de los principales asuntos de Estado. A diferencia de países con menor nivel de desarrollo o sistemas políticos alejados de las democracias occidentales en los que el Estado retiene el control de la explotación de sus recursos energéticos, como es el caso de Venezuela, México o Brasil, por citar algunos ejemplos, en la mayoría de las democracias liberales la producción, el transporte y la distribución de la energía son realizados por compañías privadas.

Sea como fuere, en la mayoría de los casos la energía está fuertemente regulada por los propios Estados, incluso muchos de ellos han incorporado este asunto en sus Estrategias de Seguridad Nacional.

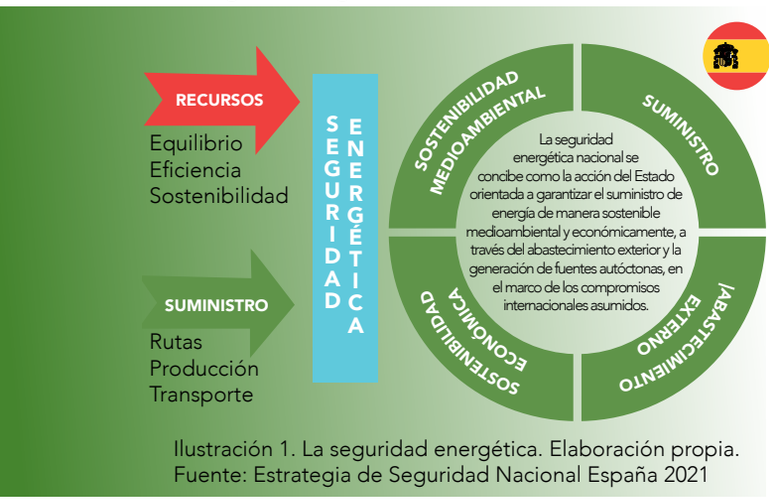


Ilustración 1. La seguridad energética. Elaboración propia. Fuente: Estrategia de Seguridad Nacional España 2021

España no es ajeno a ello, y en el tercer capítulo de la ESN-2021 cita la vulnerabilidad energética como una de las amenazas a las que se enfrenta España, si bien es cierto que lo hace desde una perspectiva preocupante anclada en la política partidista del actual gobierno que, sin ánimo de crítica, no afronta el problema en toda su profundidad, poniendo el énfasis en un cambio de modelo hacia el uso exclusivo de las renovables, algo que rompe un principio estratégico de diversificar las fuentes de obtención.

Como ejemplo de lo anterior se muestra la definición que aporta el Departamento de Seguridad Nacional: "La seguridad energética nacional se concibe como la acción del Estado orientada a garantizar el suministro de energía de manera sostenible medioambiental y económicamente, a través del abastecimiento exterior y la generación de fuentes autóctonas, en el marco de los compromisos internacionales".

De acuerdo con Van de Graaf[2], la intervención de las autoridades estatales en la gestión de la adquisición y distribución de energía suele justificarse en términos de seguridad energética, es decir, para garantizar la existencia de incentivos e instrumentos políticos apropiados para impulsar a las empresas privadas a dar los pasos necesarios para producir y suministrar la energía adecuada para satisfacer las necesidades de la nación; cuando el sector privado se muestra incapaz de llevar a cabo esta tarea crucial, el Estado debe estar preparado para intervenir.

La llegada de China, con su exponencial desarrollo económico, a este club de grandes consumidores le ha obligado a asegurarse el acceso a los recursos (lugares de producción), así como a proteger sus rutas de transporte, lo que explica sus políticas de inversión en los países productores, acceso a los recursos, y su transporte (ductos), por otra parte, el desarrollo de unas más que considerables capacidades navales que aseguren el tránsito de su flota mercante para el transporte de los recursos energéticos. Otro nuevo gigante está siguiendo pasos similares a este país asiático, es el caso de India, potencia económica emergente con escasos recursos energéticos y cada vez más dependiente de ellos.

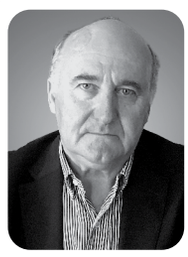
Si hay algo en lo que coinciden los responsables políticos mundiales a la hora de abordar el problema de la seguridad energética, es que más opciones son mejores que menos. En términos de asegurar las fuentes de petróleo en el extranjero, las políticas energéticas nacionales de España deben favorecer la maximización del número de proveedores de los que se deriva el suministro de petróleo o el gas.

No atender estos enfoques sobre seguridad energética, una de las principales consecuencias, si no la principal, que está viviendo la UE a raíz de la crisis con Rusia. Del mismo modo, las políticas nacionales en materia energética deberían favorecer la diversificación de los tipos de combustible que conforman el sistema energético, evitando así una dependencia excesiva de un solo tipo, que pudiera generar una crisis profunda ante su escasez. Otro factor a considerar viene del hecho de reconocer que la creciente preocupación pública por el calentamiento global probablemente conduzca a frenar el uso de combustibles fósiles, los responsables políticos de muchos países están favoreciendo una mayor inversión en alternativas energéticas, como la energía eólica y los biocombustibles. Sin embargo, además de estas generalizaciones, existe un considerable debate sobre aspectos concretos de la seguridad energética y sobre el grado de importancia que debe darse a determinados tipos de combustible y alternativas energéticas.

A modo de conclusión, la seguridad energética debe de ser garantizada en su origen, siendo necesario para ello, alcanzar un adecuado equilibrio entre las energías procedentes de varias fuentes, impulsar la generación eléctrica adaptada a las posibilidades productivas de cada nación, lo que supone no dejar de lado fuentes como la nuclear que además de su seguridad y capacidad de producción, tiene una baja huella medioambiental. Diversificar los proveedores, los cuales, por cierto, se frecuente situarlos en las regiones más inestables del mundo, evitando la dependencia exclusiva de uno de ellos. Uno de los grandes problemas de la UE ha sido y sigue siendo no contar con una política energética común, situación agravada con la actual crisis con Rusia, como consecuencia de la invasión de Ucrania. Por último, la necesidad para asegurar las rutas, recurriendo para ello al empleo de las fuerzas armadas. ■

Referencias:

[1] *Security Studies, 2018, Paul Williams & Matt McDonald, Routledge (pp. 498-500).*
[2] *Citado por Klare en Willians 2018 (p.500).*



Jesús de Miguel Sebastián, Coronel del Ejército de Tierra de España en Retiro y Socio Fundador Two Worlds Collaborative Intelligence. *Más sobre el autor:*

SEGURIDAD PERSONAL EN ÁREAS DE ALTO RIESGO (PARTE III)

Consejos para no ser víctimas de la violencia urbana

Foto: Freepick

GUATEMALA

Enrique Jiménez Soza

Nada está garantizado en un 100% cuando se trata de seguridad: 90% prevención, 5% reacción y 5% suerte. La prevención representa un 90% en seguridad, por eso las acciones se deben concentrar en esta etapa.

PARADO EN EL SEMÁFORO

Cuando el semáforo está en rojo, trate de mantener su auto a la derecha de la calle, esto porque generalmente los ladrones atacan por el lado izquierdo, que es el del conductor. Si es posible póngase en el carril central, evitando tanto el cantero central como la vereda.

Vaya reduciendo la velocidad, tratando de llegar al cruce cuando el semáforo se haya puesto en verde.

Evite las compras en los semáforos, ya que aunque el vendedor no sea un ladrón; usted se distrae, abre el vidrio y se expone.

Los ladrones usan jóvenes para preparar el asalto y encontrar objetivos; el *modus operandi* consta de que el joven se acerca para pedir dinero o vender algo, y observa el interior del vehículo buscando portafolios, computadoras, carteras, celulares u otros objetos de valor. Si el auto es interesante, el joven pega un chicle en el lateral o en el paragolpes trasero, en el siguiente semáforo el delincuente observa los autos marcados y sabe que allí hay una oportunidad de robo.

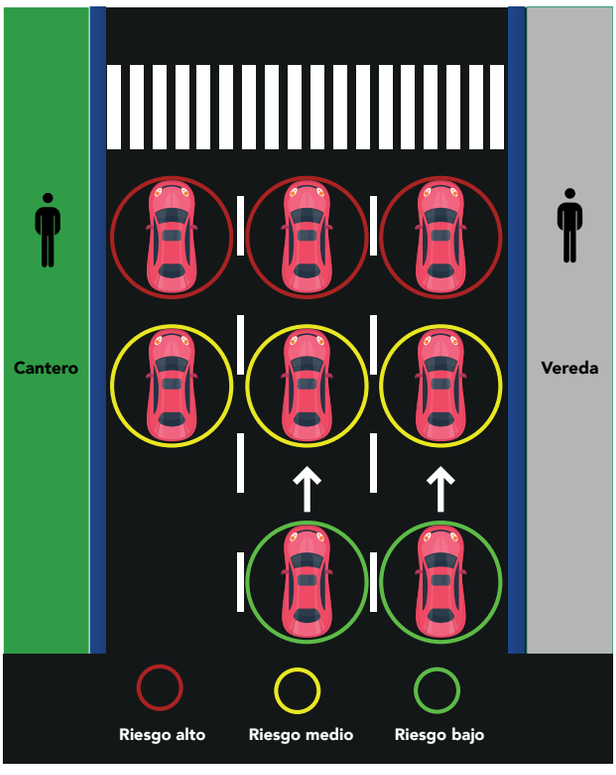
Coloque portafolios y computadoras en el baúl, cartera y celular en la guantera. Si debe detenerse, mantenga siempre la primera marcha puesta.

Si sospecha de algo, procure quedar pegado al lado del auto a su izquierda, con lo que no deja espacio para el abordaje.

Esté atento a todo lo que ocurre a su alrededor y no se distraiga, la sorpresa es la principal arma del delincuente.

ÁREAS DE RIESGO EN EL SEMÁFORO

En general el carril central es el más seguro, esto porque el delincuente actúa en la vereda o en el cantero central.



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

Empresa Socialmente Responsable

redconocer de prestadores de servicios Centro de Evaluación

Certificación del Sistema de Calidad DNV ISO 9001

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

Empresas de GSI Grupo Seguridad Integral

BASC

Procure mantener distancia con el vehículo que lo precede, la suficiente como para ver las ruedas traseras del auto. De esta forma usted puede salir rápidamente del lugar sin hacer maniobras riesgosas.

Si la intención es robar un vehículo, las primeras posiciones son las más peligrosas, porque el delincuente tiene espacio libre por delante para dejar el lugar rápidamente; si la intención es robar objetos, las últimas posiciones son peligrosas, porque el ladrón puede huir por detrás del vehículo sin transitar entre autos detenidos.

EN EL ASCENSOR

El ascensor es un lugar aislado y sin alternativas de fuga. Por eso:

- Si el ascensor llega a su piso vacío, no lo tome.
- Si el ascensor llega a su piso con alguien sospechoso, diga que está esperando a otra persona para subir o bajar juntos y cierre el ascensor.
- Resuelva las dudas siempre a su favor. Si sospecha que es un delincuente, entonces considérelo un delincuente.
- Desconfíe de los motociclistas que están en el ascensor con el casco en la cabeza, ya que esto no es común, y puede tener la intención de ocultar su rostro.

EN EL CAJERO AUTOMÁTICO

Regla N.° 1: nunca utilice cajeros automáticos de noche. Todos los que entran a un cajero automático durante la noche salen con dinero. Nadie va a pagar las cuentas un sábado en la noche.

Utilice sólo cajeros automáticos en supermercados, *shoppings* u otros lugares donde hay personal de seguridad y gran cantidad de personas.

Conviene evitar el uso de cajeros automáticos. Trate de planificar sus necesidades de dinero por anticipado y sacar dinero en lugares seguros.

No confíe en las cámaras de seguridad, ya que no pueden impedir que alguien lo asalte.

Nunca acepte ayuda estando en un cajero automático.

DURANTE LAS COMPRAS

Observe si hay personas con las que se encuentre más de una vez en los corredores o en los negocios. En un *shopping* o un centro comercial hay mucha gente, por lo que no es común encontrarse con la misma persona más de una vez. Puede ser que lo esté observando.

Si nota algo extraño, entre en un negocio poco común (por ejemplo, hombres en negocios de lencería, mujeres en negocios de artículos de pesca). Si la persona entra o se queda afuera observando, es muy probable que usted esté en el proceso de selección de víctimas.

Si ocurre esto busque personal de seguridad del *shopping*, y explique la situación. Cuando se vaya, pida que alguien de seguridad lo acompañe hasta el auto.

El delincuente se va a dar cuenta de que usted no es un blanco fácil y va a desistir de atacar.

No lleve muchas tarjetas, de crédito ni débito, tampoco mucho dinero o chequeras. Programe sus compras, decida cómo va a pagar y salga de su casa solamente con lo necesario.

No abra la cartera frente al cajero, dejando ver sus tarjetas de crédito o cuánto dinero tiene. Se sabe que hay cajeros que forman parte de bandas delictivas, y la técnica consta de que el cajero señala a las mejores víctimas a otros delincuentes, que abordan a la persona en el estacionamiento o fuera del *shopping*.

Los ladrones usan jóvenes para preparar el asalto y encontrar objetivos; el modus operandi consta de que el joven se acerca para pedir dinero o vender algo, y observa el interior del vehículo buscando portafolios, computadoras, carteras, celulares u otros objetos de valor

Los *shoppings* son lugares ideales para que los delincuentes elijan a sus víctimas. Observan durante las compras, lo siguen hasta el estacionamiento, identifican el auto y esperan la mejor oportunidad para atacar.

DURANTE UN ASALTO

Permanezca en calma.

Pida calma al delincuente.

Hágale sentir que él controla la situación.

Nunca se resista, entregue los objetos que le pida. Evite llevar grandes valores, documentos importantes u objetos que usted estima mucho, para no caer en la tendencia psicológica de resistirse al asalto.

No transmita rabia o sentimientos de venganza.

Contra un arma de fuego no existe fuerza física suficiente.

Un ladrón drogado o borracho tiene los reflejos alterados. Por eso haga todo con mucha calma y con movimientos suaves.

Nunca provoque situaciones que hagan sentir al delincuente que está perdiendo el control de la situación.

Nunca reaccione ante agresiones físicas contra usted o contra sus acompañantes.

Recuerde: el objetivo principal es sobrevivir al asalto. Las personas asaltadas que salen vivas ven el día siguiente; las personas muertas, no.

VALORICE LA VIDA

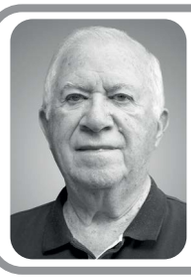
Preocúpese siempre por evitar los asaltos: tome precauciones, adquiera una postura segura.

Ignore las provocaciones en el tránsito, en los bares y en locales de baile. Esto es signo de inteligencia y no de cobardía.

Durante un asalto entregue objetos de valor. No hay nada más valioso que la vida.

Evite toda situación que pueda exponerlo a riesgos.

Estas informaciones son útiles y pueden salvar su vida. No las guarde sólo para usted. ¡Divúlguelas! ■



Enrique Jiménez Soza, asesor profesional de seguridad. *Más sobre el autor:*

VERGARA & ASOCIADOS
BUFETE

Somos expertos en establecer las estrategias más idóneas en Prevención de Delitos; **limitando los posibles daños** que atenten contra su Integridad y su Patrimonio.

Somos una firma especializada en:

- **Prevención del Delito.**
- **Litigio Penal.**
- **Seguridad Corporativa.**

Nuestra Firma le brinda tranquilidad, ya que contamos con amplia experiencia por más de veinte años en todo el territorio nacional así como en el extranjero.

Insurgentes Sur 730. Piso 2,
Col. del Valle. CP 03100. CDMX.

contacto@vergarayasociados.com.mx

55 7698 6817

/VergaraBufete /bufetevergarayasociados /bufetevergarayasociados company/bufete-vergara-y-asociados

DESARROLLO POLICIAL PRESENTA INEFICIENCIA EN MÚLTIPLES ESTADOS

Foto: Freepick

Muchas de estas instituciones no cumplen con los estándares mínimos de calidad y eficiencia exigidos por la ley, lo que pone en riesgo la confianza de la población en las corporaciones de policía

MÉXICO

Antonio Venegas / *Staff* Seguridad en América

Según reportes recientes, los estándares establecidos en la Ley General del Sistema Nacional de Seguridad (LGSNSP) no se cumplen en ninguna de las corporaciones policiacas estatales del país. La organización dio a conocer mediante el Índice de Transparencia Policial (Intrapol), en el cual un puntaje de cero significa el cumplimiento de los parámetros legales y un puntaje de -100 significa incumplimiento de esos estándares, que las policías estatales obtuvieron en promedio un puntaje de -43. El hecho de que ningún estado cumpla con los estándares mínimos establecidos por la LGSNSP pone en evidencia las deficiencias en materia de desarrollo policial y la necesidad de que existan nuevas implementaciones que mejoren esta situación.

EVALUACIÓN

Así fueron calificadas las Policías Estatales en México, según su organización, desarrollo, control y seguridad social:
0 = cumplimiento total
-100 = incumplimiento total
-43 promedio nacional

PEORES	
Yucatán	*-69*
Chihuahua	*-58*
Sinaloa	*-57*
Nuevo León	*-52*
Zacatecas	*-52*
Durango	*-52*

MEJORES	
Querétaro	*-18*
Veracruz	*-25*
Morelos	*-29*
Quintana Roo	*-31*
Baja California	*-33*
Durango	*-52*

Fuente: Índice de Transparencia Policial (Intrapol)

RESULTADOS

Según los datos, los estados con peores resultados fueron Yucatán con -69, Chihuahua con -58, Sinaloa con -57, Nuevo León, Zacatecas y Durango con -52. Por otro lado, los estados con resultados favorables fueron Querétaro con -18, Veracruz con -25, Morelos con -29, Quintana Roo con -31 y Baja California con -33.

Los cuatro ejes de evaluación establecidos por la LGSNSP son: carrera policial, profesionalización, régimen disciplinario y certificación. La organización Causa en Común evaluó el cumplimiento de cada uno de esos parámetros y, además, agregó un estándar adicional: el otorgamiento de seguridad social a los policías. Los datos resultan en que el promedio nacional para cada eje es: carrera policial -38, régimen disciplinario -37, seguridad social -52 y certificación -55.

Analizando estos resultados concluyeron en que el hecho de que las corporaciones de policía hayan obtenido la peor evaluación en certificación trae consigo graves implicaciones para la seguridad ciudadana, denotando que la mayoría de estas instituciones no cumplen con los estándares mínimos de calidad y eficiencia establecidos por la ley, lo que genera que la confianza de la población en la policía se ponga en riesgo.

La organización ciudadana determinó que el desarrollo policial adecuado es fundamental para garantizar la seguridad y protección de los ciudadanos, y de igual forma, fortalecer el Estado de derecho en México. Es imperativo que las autoridades federales, estatales y municipales logren ese trabajo en conjunto para poder abordar estas deficiencias y mejorar la situación en todos los estados. Algo que puede ser útil es la implementación de políticas y estrategias efectivas, la asignación adecuada de recursos y capacitación son aspectos claves para lograr avances significativos en el desarrollo policial. ■

CRNOVA SECURITY

Custodia de Mercancía

Guardia Intramuros

Monitoreo y Rastreo

ISO 9001

ISO 28000

BASC

ISO 18788

ISO 37001

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

ESR

UN GLOBAL COMPACT

ASIS INTERNATIONAL

crnovaoficial

crnovasecurity

www.crnova.com.mx

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

SUSTRACCIÓN PARENTAL, GRAN PARTE DE AUSENCIAS DE MENORES

La abducción parental viola los derechos fundamentales del niño, privándole del contacto con el otro progenitor y con sus familias, así como de la guarda y custodia a la que tiene derecho

Foto: Freepick

MÉXICO

Ricardo Nava Rueda

Dentro del tema de búsqueda de personas desaparecidas, son menores de edad, llamado Sustracción Parental, es decir, por el padre o la madre de los hijos, en algunos casos también participan los abuelos tíos o parejas de quienes los cometen.

El problema es más grande de lo que se pueda pensar, ya que a lo largo de mi experiencia de 33 años en la búsqueda de personas desaparecidas puedo compartir que los daños son: Alineación Parental, por decirlo de una manera simple cuando a los hijos se les habla mal de mamá o papá, de quienes se les separa, palabras como: "tu mamá ya no te quiere", "tu papá nos dejó porque se fue con otra mujer", "tu mamá destruyó tus juguetes y ya no te ama", "tu mamá ya anda con otra persona y te quiere hacer daño y también a mí", etcétera.

También vienen los daños físicos, haciendo una reflexión o análisis del sustractor y a la que su familia le apoya en este delito, considero que no hay bases morales en la misma, ya que una familia con valores no lo permitiría, que es lo que puede suceder, cuando sustraen al hijo o hijos, literalmente no les importa y literalmente "los botan" con familiares como abuelos, tíos, parejas actuales y no hay supervision del desarrollo y vigilancia de quienes "los cuidan", se entiende que pueden ser golpeados por las personas con quienes se les deja, también puede haber otro tipo de abusos sobre los menores y vulnerados todos sus derechos.

Hay que entender que no es un robo o secuestro del padre o la madre, no es robo porque no son un objeto o secuestro porque no se pide un rescate. No hay delito mientras la madre o el padre no tengan la guarda o custodia otorgada por un juez de lo familiar. Sí hay delito cuando la madre o el padre tiene la guarda y custodia, pero también es de conocimiento público que los menores han sido sustraídos durante una visita, con violencia en la calle, hasta allanando los domicilios o escuelas.

LAS VERDADERAS VÍCTIMAS

Es un tema bastante doloroso, pues en algunas de las veces o casi siempre, lo que menos importa son los hijos, es dañar a la ex pareja a través de los mismos, naturalmente que sí logran el objetivo de dañar pero de forma colateral.

Un proyecto o iniciativa de ley que propongo es "quien se lleve al menor o menores del lugar donde vivan, hasta que el juez determine la guarda y custodia, se le castigará con…", en el entendido de multa o cárcel, en el entendido de lo que anteriormente describo, los daños que se ocacionan, independiente de los daños económicos, gastos de búsqueda y otros, hace tiempo me decía una amiga y madre afectada: "Ricardo, llevo más de 200 mil pesos gastados en abogados y otros".

Hay que recordar que como padres somos los garantes del presente y futuro de nuestros hijos, que sólo están de paso en nuestra vida y tenemos que ver por ellos.

El tema de Sustracción Parental no pertenece a una sola clase social o estrato, es de dominio público, puede que suceda en todos.

¿Quién pierde o quién gana? Pierde la mamá o el padre a quien le fue arrebatado el hijo, pierden los niños por todos los daños y los únicos que van a ganar son los abogados de ambas partes. ■

"Los niños no son el futuro del mundo, son el presente", Lost Boy

Ricardo Nava Rueda, *"Lost Boy"*, director de Difusión y Relaciones Públicas de la Asociación Mexicana de Niños Robados y Desaparecidos, A.C. y líder del proyecto Encuéntrame *de* Seguridad por México (Iniciativa Chapultepec, A.C.). *Más* sobre *el* autor:

FACEit

PLATAFORMA TECNOLÓGICA EN LA NUBE
PARA COMPAÑÍAS DE SEGURIDAD

GRUPO SALUS
SEGURIDAD Y BIENESTAR

SOLUCIONES SIMPLES A PROBLEMAS COMPLEJOS

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

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

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

Tel. +52 55 2560 7642

WWW

WWW.GRUPOSALUS.COM.MX/FACEIT

CONTÁCTANOS
Y SOLICITA TU DEMO

Foto: Canva

INTELIGENCIA EMOCIONAL:
HECHOS Y MITOS

En esta ocasión, nuestra colaboradora invitada aclara los mitos que giran en torno al concepto de "inteligencia emocional"

MÉXICO & AUSTRIA | **Marcella Tapia**

"Cuando trates con personas, recuerda que no estás tratando con criaturas de la lógica, sino con criaturas de la emoción", dijo Dale Carnegie. Este consejo se aplica sin duda tanto a nuestro equipo de trabajo como a nuestras familias y amigos, por lo que la inteligencia emocional es una habilidad importante que debemos desarrollar y entrenar. Sin embargo, el término "inteligencia emocional" se presta a interpretaciones y conceptos erróneos, por lo cual existen varios mitos. Empecemos a aclararlos.

MITO: LAS EMOCIONES NO TIENEN LUGAR EN LAS EMPRESAS Y EN LA SEGURIDAD

Muchos de nosotros seguramente hemos escuchado algo parecido a "el negocio no es un lugar para emociones". Pero es un hecho de que las emociones no se quedan en casa porque nos vayamos a trabajar. Nuestras emociones son una gran parte —quizá la mayor parte— de lo que nos hace humanos y no hay ningún botón para apagarlas, están presentes en cada conversación que mantenemos, en cada llamada telefónica que hacemos y en cada decisión que tomamos.

Las emociones tienen efectos significativos en el rendimiento laboral y la interacción con los demás. Ser consciente del papel de las emociones en el trabajo puede servirnos para gestionarnos a nosotros mismos y a los demás de forma mucho más eficaz. Esto puede contribuir a mejorar las decisiones, la productividad y el trabajo en equipo.

SER CONSCIENTE DEL PAPEL DE LAS EMOCIONES EN EL TRABAJO PUEDE SERVIRNOS PARA GESTIONARNOS A NOSOTROS MISMOS Y A LOS DEMÁS DE FORMA MUCHO MÁS EFICAZ

MITO: LA INTELIGENCIA EMOCIONAL NOS HACE VER DÉBILES O VULNERABLES

Es importante aclarar que tener inteligencia emocional no significa reprimir las emociones, pero tampoco es mostrarse vulnerable. Significa estar en contacto con las propias emociones, comprenderlas y utilizarlas eficazmente. Además, permite a las personas responder a las situaciones con equilibrio emocional y madurez.

La inteligencia emocional se considera un activo valioso y un signo de fortaleza emocional. Así que, en lugar de hacer que alguien parezca más débil, generalmente nos capacita para afrontar los retos de la vida con mayor confianza y resiliencia.

MITO: EN EL RAMO DE LA SEGURIDAD LA FUERZA FÍSICA Y LA VALENTÍA ES MAS IMPORTANTE QUE LA INTELIGENCIA EMOCIONAL

Todavía existe el pensamiento de que la valentía y la fuerza física son las cualidades más importantes para muchos puestos operativos en la seguridad. Aunque no se discuta de ninguna forma la importancia de ello en ciertos contextos, la inteligencia emocional también es esencial. Si no hemos desarrollado el poder mental de centrar nuestra atención en situaciones de estrés, entonces no podremos aplicar nuestro poder físico.

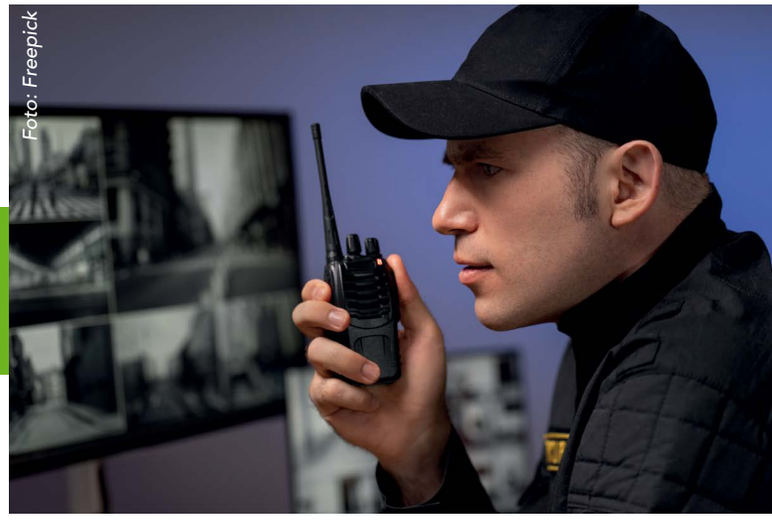


Foto: Freepick

Foto: Freepick

Las interacciones con personas difíciles y las situaciones de gran carga emocional son omnipresentes en muchos puestos de seguridad. La gestión de emociones como la ira o el miedo son relevantes, ya que el comportamiento debe estar siempre orientado a evitar o mitigar los conflictos.

Las emociones influyen poderosamente al pensamiento. Si tenemos a una persona con mucha fuerza física y también un arma, sólo podemos esperar que su inteligencia emocional sea suficientemente desarrollada para gestionar sus emociones de frustración, rabia y miedo.

MITO: TENER INTELIGENCIA EMOCIONAL SIGNIFICA SIEMPRE SER AMABLE Y EVITAR CONFRONTACIONES

Es una idea errónea que desafortunadamente muchos tienen sobre el concepto de la inteligencia emocional, pero está lejos de la realidad y creer esa idea podría hasta causar daño. Muchas veces en un contexto empresarial, la amabilidad también suele interpretarse como un comportamiento que busca evitar la confrontación y es fácil de manipular. ¿Entonces para qué quería uno trabajar en su inteligencia emocional si eso significa que nos van a pisotear?

El autocontrol no consiste en intentar reprimir las emociones y sonreír a todo. Eso incluso puede ser contraproducente, porque nuestros verdaderos sentimientos podrían eventualmente explotar de una manera inapropiada.

Ser amable con el fin de evitar confrontaciones no es una medida que sirva para resolver el problema a largo plazo, sino en muchos casos lo agudiza. Un ejemplo es lo siguiente: un guardia de seguridad se siente continuamente frustrado por cómo lo tratan sus compañeros y supervisores. En lugar de abordar la situación, sigue con su trabajo, obligándose a contener sus sentimientos y poner una cara amable. Al final, todo queda reprimido y un día, cuando su frustración es demasiado grande, golpea al supervisor de forma irracional. Esta explosión le cuesta el puesto de trabajo y perjudica gravemente sus perspectivas laborales.

El autocontrol no consiste en intentar reprimir las emociones y sonreír a todo. Eso incluso puede ser contraproducente, porque nuestros verdaderos sentimientos podrían eventualmente explotar de una manera inapropiada

MITO: PERSONAS CON UN ALTO GRADO DE INTELIGENCIA EMOCIONAL SON PERSONAS MUY EMOCIONALES

Uno de los mayores malentendidos es que las personas emocionalmente inteligentes son demasiado emocionales o sensibles. Es bastante común que se confunda la inteligencia emocional con "ser emocional", pero definitivamente no es lo mismo. Una persona emocionalmente inteligente es capaz de manejar las altas y bajas que conllevan emociones positivas o negativas.

MITO: LA INTELIGENCIA EMOCIONAL ES INNATA

Mientras en el pasado se pensó que después de cierto desarrollo de nuestro cerebro éste ya no cambia, ahora hay estudios que muestran lo contrario. Nuestros cerebros tienen una característica muy especial que se llama neuroplasticidad. Se refiere a la capacidad del cerebro para cambiar y adaptarse en respuesta a nuestras experiencias y aprendizajes. Eso significa que todos podemos desarrollar las habilidades que componen la inteligencia emocional. Sin embargo, es importante recordar que hay una diferencia entre simplemente aprender sobre inteligencia emocional y aplicar ese conocimiento a nuestras vidas.

Después de haber aclarado algunos de los mitos, espero que haya ayudado a ver el verdadero valor de la inteligencia emocional. Es vital para el éxito tanto en la vida privada como en la pública. Pero es un hecho de que la mayoría de nosotros nunca aprendimos a ser conscientes de nuestras emociones, a hablar de ellas o a gestionarlas.

Sin duda, desarrollar la inteligencia emocional no es un proceso rápido, más bien es un proceso constante. Requiere una honestidad brutal con nosotros mismos para admitir nuestros puntos débiles. Pero vale mucho la pena embarcarse en este proceso con valentía y compromiso. Para empezar, les dejo unas preguntas sobre las cuales reflexionar: ¿Cuándo fue la última vez que observaste realmente tus emociones? ¿También te diste cuenta cómo influyen en tu comportamiento? ■

Marcella Tapia, M.A. *Coach y* entrenadora internacional *de* desarrollo personal *y* liderazgo. *Más sobre la autora:*

HAY QUE INVERTIR EN SEGURIDAD

La importancia de crear conciencia acerca de la prevención

Foto: Freepick

ECUADOR

Esteban J. Acosta

Y no nos referimos precisamente al desembolso financiero, a destinar recursos económicos. Invertir en Seguridad también es dedicar uno de los recursos más valiosos que existen, el tiempo, que adecuadamente gestionado nos genera importantes beneficios. La prevención es esencial en Seguridad, planificarla y ejecutarla acertadamente permitirá proteger la integridad de las personas y sus bienes. Inicialmente se debería identificar vulnerabilidades, riesgos y amenazas, presentes y posibles, su probabilidad de concretarse. Establecer medidas para precautelar la vida, activos y patrimonio.

Impartir información sobre Seguridad, concienciar y proporcionar normas, pasos y procedimientos concretos en su aplicación. Iniciar analizando a través de la observación, la Seguridad en nuestros domicilios, en la calle (traslados) y lugares de destino, como trabajo, estudios, deporte, sociales, entre otros, considerar perímetros y accesos y el entorno inmediato de cada uno.

Condiciones de iluminación, disponibilidad de barreras físicas como cerramientos, puertas, ventanas, etc., sus características principales y mecanismos para que estén aseguradas, sistemas y equipos de seguridad electrónica, ubicación, cobertura, finalidad y estado de funcionamiento.

NORMAS DE SEGURIDAD

La mayoría de normas de Seguridad son aplicables para todos los sitios y circunstancias, también existirán particularidades. Determinar horarios de salida, llegada, permanencia dentro y fuera de cada lugar, rutas desde y hacia, comportamientos y actuaciones como estar atentos, mantener un perfil bajo (limitar o disminuir el uso de artículos que llamen la atención), percatarse de quiénes nos rodean, mantener cerradas puertas y ventanas y una vez que se use las mismas, verificar que vuelvan al estado anterior, al conducir y llegar a un sitio con acceso, ingresar y esperar se cierre antes de avanzar.

A nivel de comunidad y laboralmente, conocer y estar bien comunicados con nuestros vecinos y compañeros es básico, aplicar las actividades descritas en normas y protocolos, generar hábitos, reflejar los mismos, derivará en acciones comunes positivas que a su vez tendrán mayores posibilidades de ser replicadas.

En definitiva, una buena parte de la Seguridad es posible realizar sin que esto implique egresos monetarios, sino que más bien capacidades, cualidades, aptitudes y actitudes como el compromiso, perseverancia, liderazgo, el interés por el bien común y otras, serán fundamentales para contar con espacios de convivencia y desarrollo normal de las actividades cotidianas, con mayor tranquilidad. ■

Esteban J. Acosta, gerente general en Grupo Fractal. *Más sobre el autor:*

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

Blindaje Arquitéctonico

JOYERÍAS

PANIC ROOMS

PUERTAS BLINDADAS

EMBAJADAS

Ventas de materiales

Balísticos Certificados

(55) 5216-0050

www.blindaje007.com

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

NO OLVIDES PREDICAR CON EL EJEMPLO Y, MÁS AÚN, SIEMPRE PROBAR EL SISTEMA

Predicar con el ejemplo es la mejor manera para lograr comunicarse e interactuar eficazmente con sus empleados

PERÚ | **Herbert Calderón**

Muy convenientemente hablamos en nuestras profesiones y en las relaciones laborales y hasta familiares, en que siempre se debe predicar con el ejemplo, ¿pero qué significa esto?

El ejemplo puede ser, a todas luces, el mejor método de enseñanza. Pero ejercerlo con honestidad y decisión, de la forma más correcta o idónea, resulta algo muy difícil de lograr. No obstante, también es algo que vale la pena y que puede darle sustancia a más de una vida, incluida la tuya. Predicar con el ejemplo es lo más sabio que puedes transmitir.

Como lo dijo Stephen Covey: "Tus actos siempre hablan más alto y claro que tus palabras". Porque los hechos son la forma de concretar lo que se dice y por qué decir una cosa y luego hacer otra es autodescalificarte. Si no interiorizas verdaderamente lo que expresas, jamás será una realidad.

Definitivamente aplicado en el hogar, la familia, el trabajo, es un método de enseñanza de los más silenciosos y efectivo, sobre todo y las mejores enseñanzas se darán en momentos críticos y como nos comportamos frente a ello.

APLICADO A LA PROTECCIÓN PATRIMONIAL

En casa, nuestros hijos; en el trabajo, nuestros colaboradores, sobre todo en nuestro rubro que es la protección patrimonial. Y porque en nuestro rubro es más complicado el tema, simplemente, porque el profesional de protección patrimonial está en el centro de la gestión de continuidad del negocio y protección, dado que el patrimonio está en cada uno de los procesos, y también en el proceso de continuidad o supervivencia del negocio.

Por lo tanto, nuestro comportamiento y ejemplo no sólo abarca a nuestros colaboradores, sino a toda la organización completamente, ni siquiera linealmente, sino trasversalmente a todas las áreas.

Pienso también, sin lugar a equivocarme, que cuando pensamos con toda justificación que ya cumplimos en formar a nuestra gente, entramos en un periodo de pseudo confianza y que todo anda en automático, motivo por el cual caemos en un desgaste, y el sistema decae en su eficiencia, tristemente nos sorprendemos luego con pérdidas en general.

Foto: - Freepik

Utilizar una buena práctica, que es el probar el sistema permanentemente. El cual consiste en sembrar fallas al sistema, como también esperar o medir la reacción del equipo como, por ejemplo:

- Reacción ante una llamada de alerta.
- Esperar que te comuniquen algo que tú ya lo sabes.
- Medir las acciones que toman el equipo.
- Observar a los potenciales líderes del equipo sin que uno lo asuma.
- Evaluar las soluciones que el equipo da ante contingencias.
- No participar en las decisiones del equipo.
- Escuchar las recomendaciones atentamente en las críticas post eventos.

Por lo tanto, es una buena práctica profesar con el ejemplo, pero más aún es hacer seguimiento a lo enseñado y en general al sistema de respuesta, midiéndolo periódicamente, eliminando la pseudo confianza que se genera cuando se asume en el tiempo que todo anda bien. ■

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

Protectio
Seguridad Logística

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

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

ESR EMPRESA SOCIALMENTE RESPONSABLE

COPARMEX® CIUDAD DE MÉXICO

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

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

PROPUESTA PARA UN TRABAJO EFICIENTE *EN LA RECUPERACIÓN DE VARONES VIOLENTOS*


foto: freepik

ARGENTINA **Juan Manuel Iglesias**

Es importante identificar en qué momento está cada uno para requerirle al haciente cambios o reconocimientos para los cuales todavía no está preparado

Uno de los objetivos que debería contemplar la seguridad es la prevención y el tratamiento de la violencia familiar. Existen dispositivos que se encargan del tratamiento de varones que están atravesados por el campo de la violencia, llamados "hacientes"[1] y que trabajan desde lo individual y lo grupal, siendo este último el logra resultados a mas corto plazo. Para este artículo me basaré en un trabajo de la Licenciada Cecilia Martín.

Para que este proceso sea eficaz, se deberán tener en cuenta la evaluación y seguimiento de los dispositivos a través de la observación de:

1. LOS CUATRO FACTORES QUE CONFIGURAN EL CAMPO DE LA VIOLENCIA:

a. **Cognitivo:** Abarcan elementos culturales tales como valores de masculinidad, creencias sobre los roles del varón y la mujer. Expectativas sobre las relaciones, fantasías sobre qué es ser varón, padre, novio, esposo, etc. Estas últimas suelen ejercer presión y configurar la función personalidad que impacta en la identidad del haciente.

b. **Psicodinámico:** Tiene que ver con los aspectos emocionales y el coeficiente de inteligencia emocional, es decir la capacidad de autorregulación del miedo, el enojo, la frustración, los celos, etc. También los patrones de la experiencia, muchas veces traumática y la historia: estilos de apego (generalmente inseguros y desapegados).

c. **Conductual:** Tipos de comportamientos violentos principalmente hacia la mujer, las formas en que intenta manipular o controlar al entorno. También los cambios conductuales y destrezas que permitan la construcción de una masculinidad no patriarcal.

d. **Interaccional:** ¿Cómo se comunica? Muchas veces aparecen formas de comunicación paradójica (doble vínculo) como estrategia para el "lavado de cerebro" de la víctima. En esta área se trabaja con modelos comunicacionales como la Comunicación no violenta de Marshall Rosenberg, modelos de asertividad para deconstruir modos de interacción controladores y manipuladores.

2. LA EVALUACIÓN DE LOS DIFERENTES ESTADOS DE MOTIVACIÓN DEL HACIENTE:

Siguiendo el Modelo Transteórico de Cambio (MTC), de Prochaska y DiClemente, podemos observar que los hacientes atraviesan durante el tratamiento distintos momentos con características diferentes. Es importante identificar en qué momento está cada uno para requerirle al haciente cambios o reconocimientos para los cuales todavía no está preparado. Cada momento tiene una motivación y necesidad específica.

Cada etapa tiene una estrategia específica que hay que respetar para que el tratamiento sea eficiente.

- **Etapa Precontemplativa:** Aquí aparece una alta resistencia al cambio, ya que por lo general el haciente no reconoce su violencia ni los efectos negativos de su conducta. Lo que buscaremos obtener es que se den cuenta y tomen conciencia de que sus problemas son consecuencia de su conducta y se responsabilicen. Esto implicará un trabajo para desarrollar la empatía (neuronas espejo) que muchas veces se encuentra adormecida por la alexitimia fruto del maltrato. Para ello es importante la escucha empática, procurar que hable de él mismo, abordar las relaciones de pareja previa y sobre todo no juzgar.
- **Etapa Contemplativa:** Comienza a reconocer su responsabilidad y aparece el interés por cambiar, pero todavía no está preparado para la acción. El coordinador deberá ser paciente, ya que es una etapa de mucha ambivalencia "quiere cambiar pero todavía no acciona". En esta etapa el coordinador trabajará para reforzar la responsabilidad, marcar la discrepancia entre conducta abusiva (factor conductual) y justificación (cognitivo) desarrollando herramientas para el cese de la violencia y lograr una experiencia de apego seguro con el grupo.
- **Etapa de Acción:** Se centra en la modificación de la conducta violenta. Para ello debemos contar con una alta predisposición al cambio por el haciente: Para ello se abordarán factores y creencias (cognitivo) que sostienen la violencia, las desigualdades de poder para construir nuevas habilidades que modifiquen esas creencias. Por ejemplo a través de talleres de autoestima, de estereotipos de género, revisión histórica de las relaciones, etc.
- **Etapa de Mantenimiento:** Como los procesos de recuperación no son lineales, es necesario evaluar los niveles de riesgo y prevenir las recaídas para consolidar los resultados de la fase anterior.

Es importante observar cómo aparecen los cuatro factores en las cuatro etapas de motivación teniendo en cuenta que las etapas son dinámicas. Puede haber grados de intensidad en cada una. ■

Referencias:

1 Desde una mirada humanista, los llamamos hacientes, "el/la que hace". Los integrantes de los grupos son actores activos protagonistas del cambio y no meros "pacientes". La recuperación depende del trabajo y la participación activa ellos.

Juan Manuel Iglesias, magíster en Criminología, Victimología y Feminicidio, y coordinador para Grupo de Hombres en Recuperación. *Más sobre el autor:*

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

Conoce y disfruta nuestros BENEFICIOS

REUNIONES MENSUALES SIN COSTO
PROFESIONALIZACIÓN + NETWORKING
Presenciales, Conferencias y sedes de 1er nivel

OFERTA ACADÉMICA ESPECIALIZADA
Webinars sin costo, cursos especializados, masterclasses, y programas de preparación para certificarte (CPP, PSP, PCI Y APP)

+ DE 10 COMUNIDADES ESPECIALIZADAS
Interactúa con tus colegas, intercambia conocimientos y mantente informado.

ACCESO GRATUITO
En cursos, certificaciones, bibliografía y eventos internacionales

COSTO PREFERENCIAL
En cursos, certificaciones, bibliografía y eventos internacionales

ASIS EN LOS MEJORES EVENTOS GLOBALES DE SEGURIDAD
Precios exclusivos, workshops, eventos de networking y más.

BOLSA DE TRABAJO
Especializada y exclusiva para soci@s

NEWSLETTER SEMANAL PADLET DE NOTICIAS

COMUNICACIÓN GLOBAL
De más de 34 mil colegas a través de intercambio de información, mejores prácticas, dudad, recomendación y más.

AFILIACIÓN

ASIS
MÉXICO 217
$5,650 MX

ASIS
INTERNACIONAL
$120 UDS

¡ÚNETE AHORA!
PROMOCIÓN
15 X 12

#JuntosXASIS
#PosibilidadesInfinitas

MAYOR INFORMACIÓN
(55 1321 1289
socios@asis.org.mx

Manuel Zamudio Vázquez,

vicepresidente regional de ASIS Capítulo México (217)

1. ¿Cuál es la importancia a nivel nacional de pertenecer a ASIS Internacional?

Ser miembro de ASIS Internacional en México proporciona un prestigio distintivo al profesional de seguridad, ofreciendo acceso a las mejores prácticas y estándares internacionales, además de la conexión con una red global de especialistas. Asimismo, impulsa la profesionalización y desarrollo sostenido de la seguridad en el país.

2. ¿Cómo contribuye ASIS Internacional con la seguridad privada en México?

ASIS Internacional fortalece la seguridad privada en México a través de capacitaciones continuas, certificaciones de renombre mundial y eventos que facilitan el intercambio de conocimiento. Además, colaboramos activamente con entidades gubernamentales y privadas para robustecer el entorno regulatorio y operacional de la seguridad privada en el país.

3. ¿Cuáles son las funciones del vicepresidente regional de ASIS México?

En mi rol de vicepresidente regional de ASIS Capítulo México, estoy encargado de supervisar las operaciones de los capítulos nacionales, promover la sinergia entre los miembros, representar a ASIS en distintos foros y colaborar con el equipo global para garantizar la pertinencia y valor de nuestras iniciativas para los socios mexicanos.

4. ¿Cuáles son los objetivos hacia la seguridad privada en México desde su cargo en ASIS?

Desde mi posición, y con el respaldo del equipo de vicepresidentes adjuntos, nuestra misión es acercar a los socios mexicanos a los estándares globales y mejores prácticas en seguridad privada. Internacionalmente, aspiramos a resaltar nuestros logros, fortalecer la colaboración entre profesionales y proporcionar a nuestros miembros las herramientas y recursos que ASIS ofrece.

5. ¿Por qué decidió formar parte de ASIS y aceptar el cargo?

Elegí unirme a ASIS al reconocer la importancia de estar en una organización global que apoya el crecimiento profesional en seguridad. Esta membresía me ha brindado una comprensión más profunda del sector, me ha conectado con colegas valiosos y presentado desafíos enriquecedores. Aceptar el cargo significó comprometerme a servir a la comunidad de seguridad en México y América Latina, con el objetivo de impulsar su progreso y consolidar nuestra presencia tanto a nivel local como internacional. Y precisamente fue Samuel Ortiz Coleman, director general de esta revista, quien me invitó por primera vez a formar parte de ASIS Internacional.

Fotos: Cortesía ASIS Capítulo México (217)

TRASECO

Training Security Company

PERSONAL OPERATIVO CUALIFICADO

(Valores, Capacitación y Adiestramiento)

Guardias intramuros

Custodia y vigilancia

Tu tranquilidad nuestra pasión

Seguridad TRASECO Privada

Protección ejecutiva

Consultoría y capacitación

SOMOS UNA NUEVA OPCIÓN EN PROTECCIÓN

Equipo Directivo con 30 años de experiencia en el ramo

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

5524493906

5618829950

CONTRATACIONES:
ventas@traseco.com

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

AMEXSI

MARIO VERGARA ALVA,

Socio Director de Bufete Vergara y Asociados

Cortesía Mario Vergara Alva

- **¿Considera que la comisión de un delito se puede prevenir? Sí, no ¿por qué?**

Hay delitos que se pueden prevenir, sin embargo, hay otros que por sus características resulta casi imposible. Los que en su mayoría se pueden prevenir, son los que están relacionados con temas patrimoniales, de control, y los enfocados a los procedimientos y protocolos, ya sea dentro de una empresa de cualquier giro o un corporativo; de ello depende la formalidad y los procedimientos que tengan para los diferentes escenarios a los que se puede prestar o facilitar la operación de la empresa o corporativo para la comisión de distintas actividades ilícitas; sin dejar de tener presente que la mayoría de los delitos patrimoniales se relacionan con la falta de cumplimiento de dichos protocolos tanto del área de Seguridad como Legal.

- **¿Qué estrategias considera necesarias para la prevención de un delito en una oficina corporativa?**

La mejor estrategia que he visto desde mi experiencia profesional, para la prevención de un delito en un corporativo es integrar un Comité en el que participen y se reúnan al menos una vez al mes, los responsables del área de Finanzas, Jurídica, Seguridad, y *Compliance*; porque con este Comité se analizan los posibles riesgos del Corporativo de cada área en general, y es muy importante que en este análisis todas las áreas puedan emitir su opinión y a partir de ahí se pueda establecer un protocolo de análisis de cada riesgo.

- **¿Qué estrategias de seguridad recomienda para la prevención del robo hormiga en una empresa de *retail*?**

En mi experiencia profesional, lo que nos ha tocado abordar son eventos en los que regularmente, y me atrevería a decir que el 70% de las ocasiones que hemos intervenido en un asunto de estos en una empresa de *retail*, es porque algunos de los controles establecidos no fue cumplido o fue violado, no fue supervisado y por ende algunas personas que laboran dentro de la empresa, sobre todo en el área de Operaciones, vieron las vulnerabilidades que permitieron la comisión de un ilícito, motivo por el cual, mi mejor recomendación para una empresa de estas características es: trabajar duramente con el control tanto del área de Operaciones, que es la principal pauta para el desarrollo de todos los posibles controles.

- **¿Qué tecnología recomienda para la prevención del delito?**

Actualmente hay matrices europeas y más enfocadas al *Compliance* penal, que son básicamente para estructurar procedimientos y protocolos para cada una de las áreas, los posibles riesgos que hay para la comisión de un ilícito, y establecerlos como un programa de Prevención o *Compliance*. Y lo que sigue siendo muy útil y conocido por todos en seguridad, es el uso de tecnología de geolocalización en el transporte, videovigilancia en los almacenes, Circuito Cerrado de Televisión, alarmas antirrobo, sistemas biométricos, control de accesos, entre otros.

- **¿Cómo llegó, desde su profesión, al sector de la Seguridad?**

Hace más de 20 años, yo era el responsable del área Jurídica en materia penal de una empresa que tenía como objetivo el repartir alimentos de distintas marcas a nivel nacional, motivo por el cual al analizar cuáles estaban siendo nuestras afectaciones patrimoniales y cuáles eran los motivos, hice un análisis con un consultor en seguridad de origen extranjero, y fue prácticamente por necesidad que entré a esta área.

El asesor tenía que salir de México y debía haber un responsable de Seguridad aquí; entonces los dueños, que eran mis jefes directos, vieron en mí el perfil por el trabajo que estaba desarrollando en la materia judicial y penal dentro de la empresa y con las relaciones que teníamos en aquella época con las procuradurías del estado, porque la operación era en toda la república, tomaron la decisión de apoyarme, de capacitarme en materia de seguridad con diplomados, cursos, certificaciones y demás, y fue así como llegué al área de Seguridad. ■

Foto: Cortesía Mario Vergara Alva

Oficiales de Seguridad

MEXSEPRO
SEGURIDAD Y PROTECCIÓN DE MÉXICO

LÍNEAS DE SERVICIOS

- Oficiales de Seguridad Privada.
- Sistemas en Seguridad Electrónica.
- Vigilancia y Patrullaje para Comercios e Industrias.
- Alarmas y Monitoreo de CCTV.
- Consultoría en Seguridad.

ISO 9001:2015

COPARMEX CIUDAD DE MÉXICO

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

ASIS INTERNATIONAL CAPÍTULO MÉXICO 217

CÁMARA DE COMERCIO SERVICIOS Y TURISMO CIUDAD DE MÉXICO

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD
SOCIO ALAS

CONSEJO NACIONAL CNSP SEGURIDAD PRIVADA A.C.
EMPRESA DE CALIDAD DESDE 1996

asem Emprendedores de México

redconocer de prestadores de servicios
Centro de Evaluación

mexsepro.com
(55) 6585 4448
(55) 4141 8573
facebook.com/MEXSEPRO
instagram.com/mexsepro

ACONTECIMIENTOS DE LA INDUSTRIA

Fecha: 01 de agosto de 2023.

Lugar: Bárbaro Club House del Hipódromo de las Américas (CDMX).

Asistentes: más de 60 invitados.

ASIS Capítulo México lleva a cabo otra edición del "*Relax Meet & Learn*"

Miembros de ASIS Capítulo México se reunieron para llevar a cabo la reunión mensual de agosto, en donde Brisa Espinosa, presidenta ejecutiva del Capítulo, les dio la bienvenida a los asistentes en esta nueva versión de las reuniones: "*Relax Meet & Learn*", que consiste en charlas más amenas de los expertos en seguridad invitados, así como de los socios quienes responden preguntas al azar sobre su experiencia en ASIS y el sector.

En esta ocasión, le tocó el turno a Héctor Robles Conde, *President Latam / VP Global Operations* en FirstCall CSS; Coral Meza, gerente Seguridad y Resiliencia LATAM en Levi Strauss & CO; y Uwe Fisher, director de Seguridad en Draslovka, los cuales respondieron preguntas como: ¿Por qué te hiciste socio o socia de ASIS? ¿A cuántos nuevos socios ASIS has conocido en los últimos dos meses? ¿Cuál es el beneficio que ofrece la asociación que más has aprovechado, y qué impacto han tenido en tu carrera profesional?, entre otras. La dinámica estuvo moderada por Jorge Uribe, coordinador de la Comunidad Servicios de Seguridad de ASIS Capítulo México. ■

Jorge Uribe, coordinador de la Comunidad Servicios de Seguridad de ASIS Capítulo México; Héctor Robles Conde, President Latam / VP Global Operations en FirstCall; Coral Meza, gerente Seguridad y Resiliencia LATAM en Levi Strauss & CO; y Uwe Fisher, director de Seguridad en Draslovka

Fecha: 03 de agosto de 2023.

Lugar: Hacienda de Los Morales, Ciudad de México.

Asistentes: más de 100 asociados.

AMESP realiza Reunión Mensual con conferencia sobre la IA y el Metaverso

Mtro. Ignacio Hernández Orduña

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) llevó a cabo su reunión del mes de agosto con socios e invitados especiales, entre ellos al Mtro. Ignacio Hernández Orduña, quien estuvo al frente de la Dirección General de Seguridad Privada, de la Secretaría de Seguridad y Protección Ciudadana, y de la Unidad de Política Policial, Penitenciaria y Seguridad Privada, y quien apoyó al sector durante su gestión, e impulsó las buenas prácticas en la seguridad privada.

Durante la reunión, el presidente de la AMESP, Lic. Gabriel Bernal Gómez, además de felicitar y agradecer el trabajo realizado por el Mtro. Hernández Orduña, presentó las actividades en las que ha participado la AMESP tanto en el país, como en el extranjero. Además, se contó con la participación del tecnólogo Carlos Mats, fundador, CEO y diseñador de IKA Platform, empresa dedicada a la inteligencia artificial y quien habló sobre la IA y sus beneficios. ■

Fecha: 09 de agosto de 2023.

Lugar: Ciudad de México.

Asistentes: más de 200 participantes.

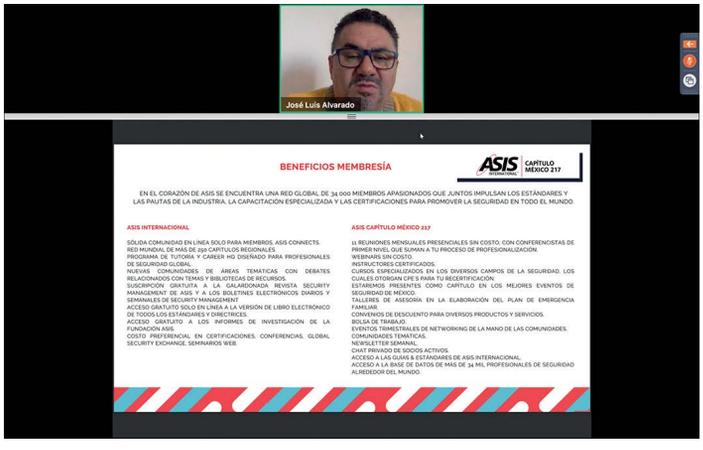
Seguridad en América presenta el ***Roadshow*** "Seguridad en plantas automotrices"

Se llevó a cabo el *roadshow online* organizado por **Seguridad en América** (**SEA**), con la bienvenida por parte de Samuel Ortiz, director general de **SEA** quien, junto con Alex Parker, *Sales Manager* de la misma casa editorial, saludaron a los asistentes. Posteriormente tomó la palabra José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México 217, para hablar acerca de qué es ASIS y los beneficios de pertenecer a ella. Dentro de estos están las reuniones mensuales, cursos especializados, talleres, asesorías, capacitaciones, chat privado con socios activos, certificaciones, entre muchos otros.

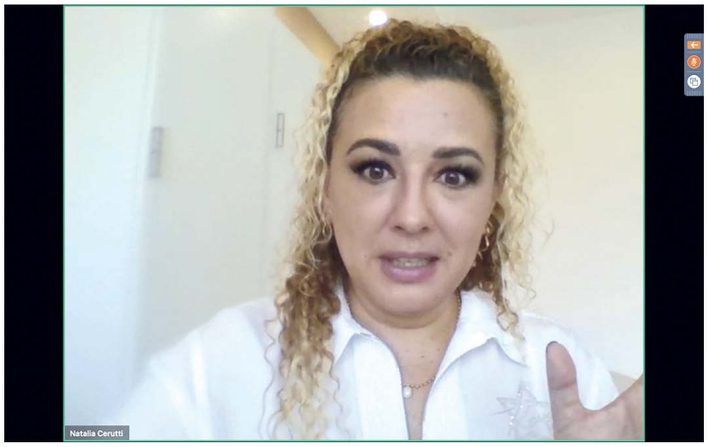
CHARLA MAGISTRAL

Después comenzó la conferencia magistral titulada "Seguridad de Viajeros y Expatriados en México", impartida por Natalia Cerutti, quien es gerente de Seguridad para Mercedes-Benz México International. Natalia comenzó su presentación ofreciendo algunos datos que indican que, en el mes de mayo de 2023, de los casi 6 millones de visitantes en México, 3 millones 626 mil 288 fueron turistas internacionales. Según sus datos, México crecerá más del 3% al cierre de 2023 gracias al impulso del *nearshoring* y el impacto que comienza a percibirse principalmente en el norte del país y el Bajío por la relocalización de empresas. También compartió que, en el primer trimestre de este año, la inversión extranjera directa resultó superior a los 18 mil millones de dólares.

Entrando en materia, Natalia compartió un mapa de la república que indica las plantas de ensamble de vehículos ligeros y motores que se localizan en los diferentes estados del país, arrojando el resultado de que los estados de Guanajuato y Aguascalientes son los que cuentan con un mayor



José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México



Natalia Cerutti, gerente de Seguridad de Mercedes-Benz México International

número de plantas, siendo seis y cuatro respectivamente; otros estados que destacan son Nuevo León, Estado de México, Puebla, Coahuila, San Luis Potosí, con dos o tres plantas, y también Jalisco, Sonora, Chihuahua, Baja California, Morelos y Veracruz con una planta.

La especialista estableció como foco principal de la presentación a las personas que componen la organización y los mecanismos para reducir los diversos riesgos a los que se exponen al viajar en México. Ella divide los tipos de viajeros en tres: mexicanos, empleados locales que pueden estar más familiarizados con el contexto de inseguridad; extranjeros, en compañías multinacionales, viajando del extranjero a México en estancias cortas; y expatriados, empleados extranjeros viviendo en México por motivos laborales. Ante esto, muchas de las soluciones que Natalia comparte incluyen la implementación de habilidades emocionales que fomenten la cultura de la seguridad y las herramientas de apoyo.

Después de finalizar su conferencia y de la sesión de preguntas y respuestas, se le otorgó un reconocimiento a Natalia por su participación en el *roadshow*. ■

Fecha: 14 de agosto de 2023.

Lugar: Ciudad de México.

Asistentes: más de 100 invitados.

Grupo PAPRISA presenta nueva edición de "*Security Monday Night*" con Sergio Aguayo

Grupo PAPRISA realizó otra edición del programa "*Security Monday Night*", presentado por Gabriel Bernal Gómez, presidente de Grupo PAPRISA. En esta ocasión, contando nuevamente con la participación del Mtro. Sergio Aguayo, se presentó la conferencia titulada "Las Corcholatas y Xóchilt Gálvez frente a la inseguridad".

El especialista comenzó comparando las encuestas que posicionan a los diferentes aspirantes a la candidatura presidencial; en el análisis del especialista, las dos candidatas a la presidencia electas serán Claudia Sheinbaum por MORENA y Xóchitl Gálvez por el Frente Amplio (que fue acertado semanas después), dejando pendiente al candidato que proponga Movimiento Ciudadano. En este tema destacó la carrera política de ambas aspirantes, así como también destacó la importancia de que ambas mujeres establezcan una estrategia contra la inseguridad en el país, el cual es visto como el principal problema que afecta a la población. Gabriel Bernal otorgó su reconocimiento (digital) al maestro Aguayo por su ponencia, y expresó su interés de discutir a los candidatos elegidos con el maestro en la próxima sesión. ■

Fecha: 15 de agosto de 2023.

Lugar: Cámara de Diputados, Ciudad de México.

Asistentes: más de 50 invitados.

ASUME y la Universidad Panamericana entregan diplomas a los graduados en "Desarrollo de Empresas de Seguridad Exitosas y Sostenibles"

Agrupaciones de Seguridad Unidas por México (ASUME), en conjunto con la Universidad Panamericana, otorgaron los diplomas a los graduados de la quinta generación del diplomado "Desarrollo de Empresas de Seguridad Exitosas y Sostenibles". Los miembros del presídium estuvieron conformados por la diputada Juanita Guerra, presidenta de la Comisión de Seguridad Ciudadana de la Cámara de Diputados; Armando Zúñiga, presidente de ASUME; la diputada Guadalupe Román Ávila; el diputado Carlos Iriarte; la diputada Susana Cano; la Mtra. Almudena Vaca, directora de Estrategia, Desarrollo y Calidad de Posgrados de la Universidad Panamericana; el Dr. Jorge Peñuñuri, presidente de la Comisión Nacional de Seguridad y Justicia de COPARMEX Nacional; Héctor Coronado, presidente de GEMARC; y Daniel Espinosa, vicepresidente de la AMESP.

Por su parte, Armando Zúñiga resaltó la importancia del escenario para reconocer a los graduados, así como el crecimiento y posicionamiento del sector dentro del desarrollo del país; y Peñuñuri aprovechó para reafirmar la importancia del reconocimiento del sector de la seguridad privada, así como de la continua preparación, capacitación y desarrollo de los miembros que desempeñan sus labores en esta área. ■

Fecha: 17 de agosto de 2023.

Lugar: Hacienda de Los Morales, Ciudad de México.

Asistentes: más de 70 asociados.

La ANERPV realiza su Asamblea General de Asociados y firma convenio con OCRA

La Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV) llevó a cabo su Asamblea General de Asociados con la finalidad de repasar las actividades destacadas, conocer nuevas herramientas tecnológicas para el sector y para una nueva firma de convenio de colaboración. Norma Carrillo, directora de la ANERPV, dio la bienvenida a los asociados, patrocinadores e invitados especiales y comenzó con las minutas del día. Por su parte, David Román Tamez, presidente de la ANERPV, ofreció unas palabras de bienvenida, y comenzó su participación anunciando un par de cambios en el consejo directivo de la asociación, con el nombramiento del nuevo vicepresidente, el cual está pendiente a la aprobación de los asociados.

Se dio la bienvenida a tres nuevos socios: GSI, B-Locator y GeoTab, y se llevó a cabo la firma del convenio de Coordinación Conjunta para la recuperación de vehículos de carga y particulares entre la Oficina Coordinadora de Riesgos Asegurados (OCRA) y la ANERPV, para formar un frente común y compartir estadísticas e inteligencia entre ambas organizaciones y crear así mejores prácticas para la seguridad del país. ■

Patricia Bugarín Gutiérrez, directora general de OCRA; y David Román Tamez, presidente de la ANERPV

Fecha: 23 de agosto de 2023.

Lugar: Ciudad de México.

Asistentes: más de 150 participantes.

Seguridad en América presenta el *Roadshow* "Seguridad en Maquiladoras"

Marco Antonio Sánchez Talavera, gerente de Seguridad de la empresa BRP

Seguridad en América llevó a cabo el *Roadshow* enfocado en Seguridad en Maquiladoras, con la participación de tres especialistas en el tema, iniciando con la bienvenida por parte de Samuel Ortiz Coleman, director general de **SEA**; y Alex Parker, *Sales Manager* de la misma casa editorial. Antes de pasar a las conferencias magistrales, Alberto Friedmann, vicepresidente de Enlace de ASIS Capítulo México, compartió un poco acerca de ASIS y sus beneficios.

CONFERENCIAS MAGISTRALES

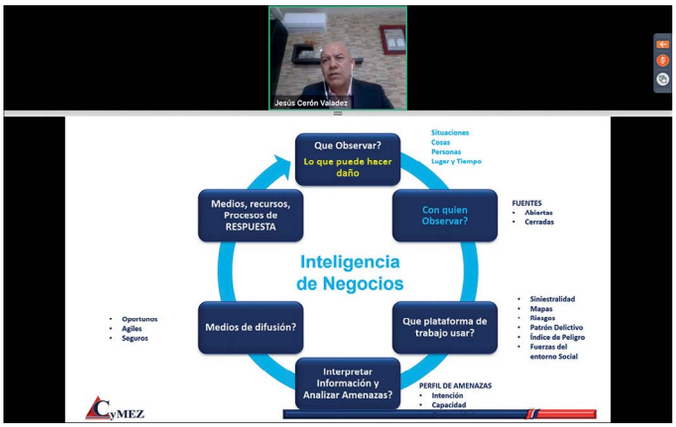
El primero en presentar su ponencia fue Marco Antonio Sánchez Talavera, gerente de Seguridad de la empresa BRP, su presentación estuvo titulada "Criminología corporativa aplicada en la industria maquiladora". Marco comenzó con una breve introducción acerca de la industria maquiladora para quienes desconocieran acerca del sector, definiéndola como un sistema de producción en el cual las empresas importan materiales y componentes a un país para ensamblar o manufacturar productos que luego son exportados. Esta industria es común en países en desarrollo y permite a las empresas aprovechar ventajas competitivas para la fabricación eficiente y la exportación de productos acabados.

Más tarde fue turno de Hans-Dieter Mokross, director de Seguridad Corporativa de la empresa GILDAN, quien expuso su ponencia titulada "Retos de Seguridad Corporativa en un entorno desafiante". Hans comenzó su presentación explicando la naturaleza de la maquila y sus riesgos asociados, señalando las operaciones en un entorno urbano poco controlado explicando los riesgos presentes como altos niveles delictivos, desastres naturales, infraestructura insuficiente, delincuencia común u organizada, clima político, etc. Dicho esto, Hans compartió los componentes positivos de un entorno urbano como son la convivencia participativa con las comunidades, la responsabilidad ambiental, las relaciones sociales, planes de emergencia, entre otros.

PATROCINADORES

La charla del patrocinador en esta ocasión estuvo presentada por Jesús Cerón Valadez, director general de la empresa CYMEZ, quien expuso su ponencia titulada "Gestión de Riesgos en rutas de transporte de personal en zonas hostiles". Entendiendo los riesgos que presentan los sectores que hacen uso de rutas de transporte, como la industria maquiladora, así como la secuencia económica y la protección del negocio ante la perspectiva criminal, Jesús comparte la nueva aplicación que CYMEZ desarrolla.

Bajo la leyenda "tu seguridad primero", la aplicación de CYMEZ es completamente funcional, posee accesos como una contraseña adicional de ingreso y alerta al centro de servicio cuando la contraseña está equivocada. La aplicación también garantiza características como la evaluación del propio nivel de riesgo, provee sugerencias para la seguridad y muestra rutas alternas en cuanto a transporte; además de mostrar información relevante y valiosa como el panorama actual de la zona y los detalles de lo que está pasando. ■



Jesús Cerón Valadez, director general de la empresa CYMEZ

Fecha: 31 de agosto de 2023.

Lugar: Ciudad de México.

Asistentes: más de 70 asociados.

Seguridad en América presenta *webinar* sobre *Nearshoring*

Seguridad en América realizó un *webinar* con el objetivo de instruir en las nuevas soluciones para el comercio y la seguridad en las cadenas de suministro, fue así como Alex Parker, *Sales Manager* de **SEA**, presentó a los asistentes la conferencia titulada "¿Están listas nuestras empresas de seguridad para el *Nearshoring*?", contando con participaciones de José Guillermo Suárez, México & LATAM *Sales Manager* de la empresa TIVE; Roberto Vázquez, CEO de CURV Logistics Group; y una charla especial de Héctor Romero, presidente del Círculo Logístico.

CONFERENCIAS

Héctor Romero tomó la palabra con la conferencia "*Nearshoring*: Una reconfiguración de las cadenas de suministro globales", y comenzó definiendo el termino "*nearshoring*", como la práctica de transferir una operación comercial a un país cercano, ésta surge como respuesta al *offshoring*, con el objetivo de reducir costos, buscar proveedores en otros destinos mucho más lejanos. De acuerdo con Héctor, el objetivo es acercar los centros de producción tercerizada y solucionar los inconvenientes de las largas distancias y la diferencia de horarios entre los continentes.

Posteriormente ofreció un trasfondo histórico del *nearshoring* en México y a nivel mundial, así como su impacto en la industria en niveles económicos. Hablando del tema, Héctor se enfocó en la producción automotriz en México, detallando el crecimiento en los sectores del norte, centro y bajío del país, específicamente en estados como Nuevo León, Chihuahua, Baja California y Tamaulipas. En palabras del especialista, los escenarios en materia de seguridad y geoestrategia obligan a cambiar y a ser más eficientes en respuesta a uno de los principales fenómenos como resultado de los escenarios internacionales.

Más tarde se unieron a la presentación José Guillermo Suárez, México & LATAM *Sales Manager* de la empresa TIVE; y Roberto Vázquez, CEO de CURV Logistics Group, formando un panel de expertos. José Guillermo expuso una presentación de la empresa TIVE, titulada "¿Sus operaciones de carga están listas para el *boom* de relocalización de operaciones en México y LATAM?", con el objetivo de mejorar la seguridad y evitar la pérdida de carga con visibilidad de envío en tiempo real.

Los expertos complementaron la presentación con comentarios respecto al tema. En esta parte de la sesión se abordó el *nearshoring* como la tendencia latinoamericana que redefine el comercio global, de igual forma, José Guillermo compartió las soluciones que ofrece para prevenir daños que se presenten en el comercio, con sus *trackers* que capturan y transmiten datos del envío en tiempo real, la aplicación que gestiona la información y envía notificaciones en tiempo real, y el equipo que supervisa los datos y trabaja con los transportistas para evitar daños.

El panel desarrolló un debate entre los expertos en el que se discutieron las ventajas y desventajas del *nearshoring*, concluyendo que los sectores deben de ser capaces de adaptarse a las nuevas tendencias que se presenten. Alex agradeció a los ponentes por sus participaciones, así como la presencia de los asistentes, y de esta manera concluyó el *webinar*. ■

Fecha: 04 de septiembre de 2023.

Lugar: Club de Golf, Ciudad de México.

Asistentes: más de 100 participantes.

Realizan el primer "Torneo de Golf de la **Seguridad Privada Asociada**"

Se llevó a cabo el primer "Torneo de Golf de la Seguridad Privada Asociada", donde varios miembros del gremio se reunieron para disfrutar de una jornada de golf representando al sector y las asociaciones de ALAS y AMESP, formando alrededor de 40 equipos. Los premios a los ganadores fueron brindados por las empresas JVP, DILME y CIA KAPITAL.

Los tres primeros lugares del torneo fueron reconocidos con trofeos (ya que ninguno logró el objetivo para los premios grandes), el tercer lugar lo obtuvo el equipo establecido por Hermann Seidel, Gerardo Meraz y Enrique Shibayama; el segundo lugar fue para el equipo conformado por Samuel Ortiz, Ricardo Bustamante y Marcos Solórzano; y el primer lugar lo logró el equipo de Gunter Carranza, Víctor Robles y Juan Manuel Valladares. Los organizadores anunciaron la realización del segundo "Torneo de Golf de la Seguridad Privada Asociada" en el mes de septiembre de 2024, mismo que llevará por nombre "Torneo Thomas Gottlieb", como una forma de honrar y celebrar a quien ha sido una figura representativa, un estandarte dentro del sector de la seguridad privada y uno de los organizadores del torneo. ■

Fecha: 05 de septiembre de 2023.

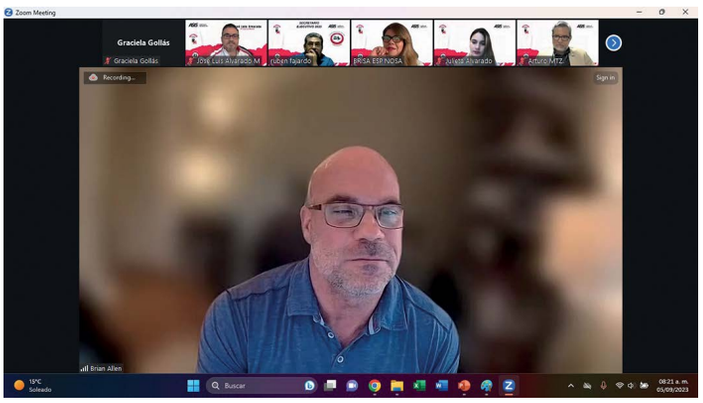
Lugar: Ciudad de México.

Asistentes: más de 100 participantes.

ASIS Capítulo México realiza su Reunión Mensual de septiembre de manera virtual

ASIS Capítulo México llevó a cabo su Reunión Mensual correspondiente al mes de septiembre de manera virtual para revisar los pormenores del mes y escuchar una plática titulada *'Unlocking Opportunities: ESRM and your Career'* ("Desbloqueando Oportunidades: ESRM y tu carrera"), presentada por Brian Allen, *Executive Advisor on* ESRM. Brisa Espinosa, presidenta del Capítulo, comenzó su informe en el que presentó el reporte de actividades de la asociación, destacando los 393 socios activos, un crecimiento notable; así como el desarrollo de las comunidades con más de 64 actividades programadas, entre *webinars*, sesiones y visitas, la colaboración de ASIS con otras asociaciones, entre otras.

El objetivo principal de la reunión fue presentar la conferencia magistral, organizada por la Comunidad de NEXTGEN Young Professionals. De esta manera, tomó la palabra Julieta Alvarado, coordinadora de dicha Comunidad, para presentar a Brian Allen, quien compartió distintos conceptos y técnicas a los asociados presentes para ampliar su conocimiento sobre el tema. ■



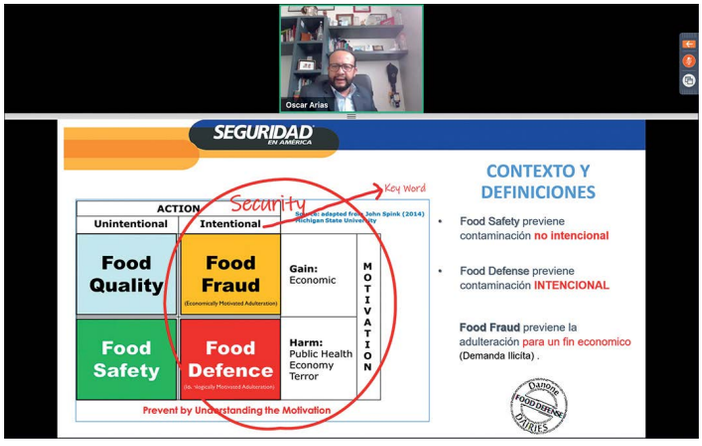
Brian Allen, Executive Advisor on ESRM

Fecha: 06 de septiembre de 2023.

Lugar: Ciudad de México.

Asistentes: más de 200 participantes.

Seguridad en América lleva a cabo *Roadshow* "Seguridad en la industria alimentaria"



Oscar Arias, LATAM Security Officer de DANONE

Seguridad en América realizó una edición más de los *roadshow* enfocándose en esta ocasión en la seguridad de la industria alimentaria. Samuel Ortiz Coleman, director general de **SEA**; Alex Parker, *Sales Manager*; y Katya Rauda, asistente de Dirección, fueron los encargados de coordinar el evento *online*.

CHARLA MAGISTRAL

La charla magistral fue impartida por Oscar Arias, *LATAM Security Officer* de la empresa DANONE, la cual llevó por nombre "Plan de defensa de los alimentos (Food Defense)". Oscar comenzó su participación contextualizando el tema con una breve introducción. De acuerdo con su presentación, el mundo cambió en general posterior a los acontecimientos del 11 de septiembre de 2001 en Estados Unidos, un año después a esto se consolidó la Ley contra el Bioterrorismo, tiempo después, en 2011, la Ley de Modernización para la Inocuidad de los Alimentos (FSMA), y por último, en 2016, se creó la Ley final para la Adulteración Intencional; todas estas leyes son importantes para la regulación y protección de los alimentos en contra de riesgos como la adulteración intencional.

Ante esto, Oscar definió tres conceptos: *Food Safety,* utilizado para prevenir la contaminación no intencional; *Food Defense,* el cual previene la contaminación intencional; y *Food Fraud*, el cual previene la adulteración de los alimentos para un fin económico. Estos riesgos clave para la seguridad son divididos en intencionales y no intencionales, cuya motivación y ganancia es el aspecto económico, pero el daño se refleja en la economía, el terror y el impacto a la salud pública.

De acuerdo con el especialista, dichas acciones se pueden prevenir por medio del entendimiento de la motivación. Continuando con la presentación, Oscar manifestó las razones para contar con un plan de defensa de alimentos, que pueden ser ya sea para proteger los productos y los activos en contra de actos maliciosos y, por ende, la salud de los consumidores, así como también para controlar y minimizar la probabilidad de una contaminación intencional, y por último, para dar confiabilidad y credibilidad a los clientes y a los consumidores de que la empresa cuenta con las medidas adecuadas para proteger los alimentos.

En conclusión, Oscar brindó múltiples consejos para este manejo, como lo son evaluar constantemente el sitio y conocerlo bien, involucrar las áreas relacionadas con la seguridad alimentaria a fin de prevenir una crisis; asegurar los planes de acción en cada auditoría o recorrido, planificar bien las prioridades para capitalizar los proyectos de mejora o inversión, y finalmente, actualizarse ante los sistemas de Gestión de Seguridad Alimentaria. ■

Oscar Arias, LATAM Security Officer de DANONE; Alex Parker, Sales Manager de SEA; y Samuel Ortiz Coleman, director general de SEA

Fecha: 08 de septiembre de 2023.

Lugar: Hacienda de Los Morales, Ciudad de México.

Asistentes: más de 70 participantes.

AMESP realiza su reunión mensual con conferencia de Juan Francisco Torres Landa

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) llevó a cabo su reunión del mes de septiembre con un desayuno y una conferencia especial otorgada por el Mtro. Juan Francisco Torres Landa, socio Mercantil y Financiero de Hogan Lovells, la cual llevó por nombre "En camino al 2 de junio de 2024".

Por su parte Gabriel Bernal Gómez, presidente de la AMESP, presentó su reporte de actividades, habló sobre la Asamblea General de la AMESP realizada en Tijuana, Baja California, en el mes de agosto, dentro de la Primera Asamblea Nacional "Hablemos bien de la Seguridad", y aprovechó para agradecer la presencia y el apoyo de Octavio Vizcaíno, presidente de la Comisión de Relaciones Institucionales y Enlace Gubernamental de la AMESP, así como de Francisco Nieves, director de AMESP región noroeste, por toda la labor realizada en este Congreso. ■

Francisco Nieves, director general de Centurion Seguridad Privada; Gabriel Bernal, presidente de AMESP; y Octavio Vizcaíno, director general de Grupo ODE

Fecha: 20 de septiembre de 2023.

Lugar: Hotel SAFI Valle en San Pedro Garza García, Nuevo León.

SIL Consultores realiza curso "Operación Efectiva del Nuevo Programa de Seguridad OEA"

El Curso "Operación Efectiva del Nuevo Programa de Seguridad OEA", por parte de SIL Consultores, fue un rotundo éxito. Expertos y profesionales se unieron para explorar las claves del Nuevo Perfil de Seguridad OEA y compartir estrategias de cumplimiento del programa. Un día de aprendizaje colaborativo en un entorno inspirador.

El evento no sólo proporcionó información vital, sino que también fomentó un espacio de colaboración, donde se compartieron experiencias desde diferentes puntos de vista de seguridad patrimonial.

La impartición del curso estuvo a cargo del Ing. Edgar Moreno, director de SIL Consultores, repasando todos los estándares del programa de seguridad OEA junto con las modificaciones hechas por la SAT a partir de junio de 2023, manteniendo un enfoque principal en la operación efectiva e implementación de los requerimientos para la certificación. ■

Fecha: 20 de septiembre de 2023.

Lugar: Hotel Courtyard Marriot Revolución de la Ciudad de México.

ASUME convoca conferencia de prensa con expertos de la industria de la Seguridad Privada

Héctor Coronado, presidente de GEMARC; Daniel Espinosa, vicepresidente de AMESP; Armando Zúñiga, presidente de ASUME; y Víctor Presichi, consejero y ex presidente de ANERPV

Agrupaciones de Seguridad Unidas por México (ASUME) realizó una conferencia de prensa con el objetivo de presentar información relevante sobre el estado de la industria de la seguridad privada. El panel principal estuvo conformado por Armando Zúñiga, presidente de ASUME; Héctor Coronado, presidente de GEMARC; Víctor Presichi, consejero y ex presidente de ANERPV; y Daniel Espinosa, vicepresidente de AMESP.

Armando Zúñiga agradeció a las empresas y sus representantes y directores que patrocinaron dicho evento, como Héctor Villareal de COMEXA; Marcos Solórzano de SOLCAT; Grupo IPS; Samuel Cacho de Grupo Alfil; Mario Espinosa y Daniel Espinosa de SERVISEG+; Víctor Aguirre de VIP Protection; Jorge Septién de MSPV; David Vázquez de VPR; CAPESSA; y el Cap. Salvador López de Grupo Consultores. ■

Fecha: 20 de septiembre de 2023.

Lugar: Ciudad de México.

Asistentes: más de 100 participantes.

Seguridad en América presenta el *roadshow* de Seguridad en Petróleo y Energía

Samuel Ortiz Coleman, director general de **Seguridad en América** (**SEA**); y Alex Parker, *Sales Manager* de la misma casa editorial, presentaron el *Roadshow online* titulado "Seguridad en petróleo y energía", el cual contó con la participación de José Echeverría, CPP, responsable de Seguridad y Transportes de Andes Petroleum Ecuador Ltd., con la charla magistral; así como José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México, quien habló de los beneficios de afiliarse a ASIS International.

CHARLA MAGISTRAL

José Echeverría tomó la palabra para comenzar con su charla titulada "La protección de activos en la Industria del Petróleo". El especialista empezó con un recuento general de la operación petrolera, así como sus características y necesidades de protección, analizar buenas prácticas en cuanto al manejo e implementación de los recursos de seguridad y analizar las actividades de seguridad habituales en la operación petrolera y su importancia.

También habló sobre los retos en el sector, para posteriormente comentar los macroprocesos de la operación petrolera, un ciclo de la seguridad que incluye la exploración/sísmica, perforación, producción, transporte, refinación y comercialización. Después explicó los generadores de amenazas en Seguridad Petrolera, que incluyen a los grupos radicales, grupos armados ilegales, la delincuencia organizada y la delincuencia común, ante esto la desinformación influye bastante.

Para concluir, José compartió otros aspectos en la protección de la industria del petróleo basándose en el proceso de ESRM que establece ASIS International, aconsejando a los asistentes el uso del *networking* aprendiendo de seguridad, aplicando lo aprendido, compartiendo lo que practica, manteniéndose informado y siendo solidarios apoyando la colaboración. José finalizó compartiendo con los asistentes la frase "la seguridad no es una tarea, es una actitud".

PATROCINADORES

Después fue el turno de Alejandro Rodríguez, consultor en Sistemas de Video Seguridad para Infraestructuras Críticas; y Alejandro Santos de la empresa PELCO, la cual pertenece a la empresa MOTOROLA, quien se presentó con la conferencia titulada "Seguridad Inteligente para Ambientes Externos". Alejandro Rodríguez presentó los diferentes requerimientos que se emplean en el sector, como las plataformas, plantas industriales, embarcaciones, perforación y ductos.

Ante esto, PELCO presentó una mejor tecnología para detectar, comunicar y responder oportunamente; uno de estos proyectos es la plataforma PELCO Smart Analytics Powered by Motorola Solutions, implementada con tecnología de último nivel, presentando portafolio de productos sumamente completo para poder dar vigilancia en cualquier instalación requerida, como un catálogo de cámaras diseñadas para la protección contra los riesgos existentes en el sector que se desempeñe.

Alejandro Santos habló sobre temas de radiocomunicación que presenta Motorola Solutions, introduciendo el *Safety Reimagined*, un sistema de ecosistema de comunicación de tecnología integral que unifica voz, video, datos y análisis en dicha plataforma. Esto permite crear las bases de seguridad operativa que la empresa necesite para que el personal se mantenga enfocado y seguro. ■

José Echeverría, CPP, responsable de Seguridad y Transportes de Andes Petroleum Ecuador Ltd.

Alejandro Rodríguez, consultor en Sistemas de Video Seguridad para Infraestructuras Críticas

Consejos de seguridad para prevenir el robo de motocicletas

Las motocicletas se han convertido en un vehículo práctico para ciudades que padecen de exceso de tránsito, como lo es la Ciudad de México, también para recorrer distancias cortas, para los comercios, el *e-commerce* y hasta para trasladar a toda una familia en estas (aunque ya se modificó el Reglamento de Tránsito en la CDMX para la prevención de accidentes por este tipo de malas prácticas). Uno de los problemas, además de la lluvia, a la que se enfrentan los motociclistas, es el robo andando o estacionado, de su vehículo, es por ello que extrajimos del Blog de David Lee *"Manual de Seguridad"*, estos consejos para evitar el robo de motocicletas.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Equipamiento.** Adquiera y utilice candados, inmovilizadores profesionales de colores llamativos o equipos antirrobo, que van sujetos a los discos de los frenos, a la cadena o que le permitan anclar o sujetar la motocicleta a otra o a un elemento fijo. También es recomendable contar con equipo de alarma sonora que se active cuando alguien intente mover la motocicleta y te alerta a tu teléfono inteligente, y puede agregar un GPS.
2) **Identificación.** Mantenga una copia de la factura original en un lugar seguro, así como las placas, registro de la moto, y la licencia, de tal manera que puedan ser enviados por correo electrónico en caso de emergencia.
3) **Póliza de seguro.** Adquiera un seguro para su motocicleta que incluya cobertura por robo, daños a terceros, gastos médicos para el conductor y sus acompañantes, así como cobertura de lesiones por asalto o intento del mismo, pérdida total del casco y vestimenta por accidente, reposición o reparación por robo o descompostura o rotura de llave y asistencia en el camino.
4) **Al estacionarte.** Estacione su motocicleta en un lugar iluminado, transitado y donde esté dentro de la visión de cámaras de seguridad instaladas en algún poste, edificio o comercio. Bloqueé la dirección antes de sacar la llave de encendido, así evitará que se lleven empujando a la moto.
5) **En traslados.** Evite tomar atajos por sitios desconocidos. Manténgase alerta al detenerse en semáforos y cruceros. Desconfíe de motociclistas que en pareja o grupo se acerquen a usted e intenten entablar conversación o le indiquen que su moto tiene alguna falla: acelere o cambie de ruta y acuda a un lugar seguro para verificar.
6) **No permanezca detenido a bordo de la motocicleta**, recuerde que la víctima perfecta en la calle es una persona en un vehículo estacionado.
7) **Compra-venta.** Al comprar una motocicleta, hágalo preferentemente en una agencia o sitio especializado, para evitar fraudes y contar con la garantía adecuada. Si vende su moto, considere hacerlo con un amigo o bien a través de una agencia mediante consignación, para reducir el riesgo de que sea visitado por delincuentes quienes, con engaños o con violencia, lo pueden despojar de su vehículo y documentos.

FOMENTE LA CULTURA DE LA SEGURIDAD

SEGURIDAD EN AMÉRICA

Consulte la revista digital en
www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

ÍNDICE DE ANUNCIANTES

ALLIED UNIVERSAL®
SECURITY SERVICES

There for you.

COMPROMETIDOS CON LA SEGURIDAD DE NUESTROS CLIENTES Y LA CALIDAD EN EL SERVICIO

Allied Universal® es la empresa líder global en servicios de seguridad e instalaciones. Ofrecemos servicios de seguridad proactivos, tecnología de vanguardia y soluciones a medida para permitir a los clientes centrarse en su negocio principal.

Nuestros servicios:

- **Profesionales de Seguridad altamente capacitados y experimentados**
  - Investigaciones Corporativas
  - Respuesta a Emergencias
  - Protección Ejecutiva y Servicios de Inteligencia
  - Monitoreo
- **Servicios de Tecnología**
  - Videovigilancia
  - Controles de acceso
  - Diseño, Ingeniería e implementación de Servicios
- **Asesoría y consultoría de Riesgos**
  - Investigaciones e Inteligencia
  - Respuesta a Emergencias
  - Monitoreo y Centro de control

Contáctanos **www.ausecurity.mx/esp** **(+52) 55 5337 0444**

Allied Universal® ha encargado y publicado el primer **Informe Mundial sobre Seguridad.** Esta investigación innovadora documenta las opiniones y preocupaciones de 1,775 jefes de seguridad de 30 países. El informe completo, las principales conclusiones, las opiniones de los expertos en seguridad y los videos están disponibles en **https://www.worldsecurityreport.com/**

incluye gastos de envío

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. **(Marque así X)**

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA 2023	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en banco HSBC a nombre de Editorial Seguridad en América, S.A. de C.V. Cuenta 04016012049

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe 021180040160120491

_____
Firma

DATOS DEL CLIENTE (para el envío de la revista):

Nombre: _____

Compañía: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envío de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato vía: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2023

ANERPV
Asociación Nacional de Empresas de Rastreo y Protección Vehicular

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

ASIS INTERNATIONAL
CAPÍTULO MÉXICO 217

SEGURIDAD - PROTECCIÓN
CONFIANZA

ALARSEGM · B&A · UNIFORMAL · asfáleia · OEMPSA · Jivabe · INSTITUTO GAUDÍ

PAPRISA

asfáleia

En Seguridad, el poder de la tecnología.

CREANDO IDEAS INNOVADORAS

MONITOREO DE FLOTAS - CONTROL DE ACCESOS - MONITOREO SATELITAL - GPS - CCTV

55 8438 2340 · GRUPOPAPRISA.COM · REDES SOCIALES

JUAN RACINE 112-PISO 3, POLANCO, POLANCO I SECC, MIGUEL HIDALGO, 11510 CIUDAD DE MÉXICO, CDMX

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.®

¡Forjando campeones!

Guardias, guardias armados, custodias, custodias blindadas y custodias armadas.

Cobertura a nivel nacional.

www.sepsisa.com.mx comercial@sepsisa.com.mx 55 5351 0402