SEGURIDAD EN AMÉRICA

Especiales:

Falsificación de medicamentos

Seguridad en maquiladoras

Reportaje: Seguridad en centros educativos

INTELIGENCIA ARTIFICIAL: EFICIENCIA EN LAS OPERACIONES

M360

Año 25 / No.145
Julio - Agosto

www.seguridadenamerica.com.mx

COBERTURA NACIONAL

A QUIEN VALOR MERECE

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

@MultiprosegOficial @MULTIPROSEGOFICIAL MULTIPROSEG OFICIAL

ALGUNOS DE NUESTROS CLIENTES

AUDI, TELCEL, INNOPHOS, CEMEX, NIKE, CRYOINFRA, LACTALIS, MERCADO LIBRE, GENERAL ELECTRIC

AMESP

CDMX

CNS

ASIS INTERNATIONAL

redconocer

ISO

BAC

ema entidad mexicana de acreditación, a.c.

ANERPV

COPARMEX

REPSE

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

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

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

+ 52 (55) 79599598

INFO@MULTIPROSEG.COM.MX

SEGURIDAD EN AMÉRICA

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

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

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

Coordinación de Diseño
José Arturo Bobadilla Mulia

Administración
Oswaldo Roldán
oroldan@seguridadenamerica.com.mx

Reportera
Mónica Ramos
redaccion1@seguridadenamerica.com.mx

Medios Digitales
Estefania Hernández
mdigital@seguridadenamerica.com.mx

Circulación
Alberto Camacho
acamacho@seguridadenamerica.com.mx

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

María Esther Gálvez Serrato
egalvez@seguridadenamerica.com.mx

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

Año 25 / No. 145 / Julio - Agosto / 2024

Portada:
M360

Síguenos por

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

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. De esta edición fueron impresos 12,000 ejemplares. European Article Number EAN-13: 9771665658004. Hecho en México. Se imprimió en los talleres de Esténtor Impresos, Calle Virgen de Chiquinquira 706, Col. La Virgen, Ixtapaluca, Estado de México, C.P. 56530.

Apoyando a:

ASIS · ALAS Asociación Latinoamericana de Seguridad · AMESP · Circulo Logistic · ANERPV

Protectio

Seguridad Logística

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

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

EMPRESA SOCIALMENTE RESPONSABLE

COPARMEX
CIUDAD DE MEXICO

AMESP

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

EDITORIAL

De acuerdo con el Índice de Paz Global 2024, del Institute for Economics and Peace, revela que en el mundo actualmente hay 56 conflictos en curso, la cifra más alta desde la Segunda Guerra Mundial. Según el informe, América del Norte experimentó el mayor deterioro regional, impulsado por el aumento del crimen violento y el temor a la violencia, además, el riesgo de que hostilidades de baja intensidad estallen en conflictos abiertos también ha crecido.

Sudamérica experimentó la segunda mayor caída en el nivel de paz, con un deterioro promedio del 3.6%. Ahora es la quinta región más pacífica del mundo. A pesar de las denuncias por violaciones de los derechos humanos y tener el mayor índice de encarcelamiento del mundo, el informe destaca que El Salvador mejoró 21 puestos al reducir la tasa de homicidios. Argentina es el único país sudamericano que se encuentra entre los 50 países más pacíficos del mundo.

La paz en México mejoró un 1.4% en 2023. Este fue el cuarto año consecutivo de mejora después de cuatro años consecutivos de deterioro. Sin embargo, empeoraron más estados de los que mejoraron: 15 estados mostraron mejora y 17 deterioro. En 2023, los estados con mayores tasas de homicidios fueron Colima, Morelos, Baja California, Zacatecas y Chihuahua. Colima se ubicó como el estado menos pacífico del país el año pasado, seguido de Baja California, Morelos, Guanajuato y Zacatecas. En contraste, Yucatán volvió a ser el estado más pacífico de México, seguido de Tlaxcala, Chiapas, Durango y Coahuila.

Existe una gran divergencia en la violencia en todo el país: los estados más pacíficos registran una tasa promedio de homicidios de 4.2 muertes por cada 100 mil personas, en comparación con una tasa promedio de 72 en los estados menos pacíficos.

En 2023, las mayores mejoras en materia de paz se produjeron en Zacatecas, Michoacán, Durango, Sonora y Tabasco. En contraste, Morelos, Sinaloa, Quintana Roo, Chihuahua y Nayarit registraron los mayores deterioros.

La violencia contra las fuerzas de seguridad en México ha ido en aumento en los últimos años. Entre 2018 y 2023, más de 2 mil 600 policías han sido asesinados en México; Guanajuato registró la mayor cantidad de agentes asesinados y Zacatecas registró la tasa de homicidios de policías más alta. Durante este tiempo, el país registró una tasa promedio anual de homicidios de policías de 96.8 asesinatos por cada 100 mil agentes, lo que significa que ser policía en México es aproximadamente cuatro veces más peligroso que ser miembro de la población general.

Tan solo combatir los factores que impulsan la violencia no es suficiente para mantener la paz. Mejorar los niveles de paz en México requiere estrategias más amplias que incluyan abordar la corrupción y crear instituciones eficaces en las que la población confíe.

El informe del IPM 2024 proporciona evidencia para que los responsables políticos, los líderes empresariales y las organizaciones de la sociedad civil ayuden a desarrollar nuevas y más amplias soluciones de construcción de paz. ■


La dosis perfecta
de tecnología
www.sissadigital.com
SISSA
DIGITAL
SISSA
DIGITAL

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 Modesto Miguez, consultor en seguridad 4.0, docente y socio de negocios, quien en generosas ocasiones ha presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

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

Si desea conocer más acerca del experto, consulte su currículo:

ENTREVISTA EXPRÉS CON

Adhaf Raúl Hatem López,

director general de MEXSEPRO

¿Considera al Nearshoring como una oportunidad de negocio en seguridad privada?

Sí, la seguridad privada proporciona un entorno seguro y confiable para las empresas extranjeras que deciden establecer operaciones en el país y juega un papel importante y fundamental en el *nearshoring* en México, estas empresas protegerán sus activos, empleados y operaciones y con ello podrán operar de forma eficiente y sin interrupciones, es una necesidad de negocio garantizar todo esto, y para ello es fundamental la seguridad privada. En México el crecimiento debido a las oportunidades de negocio para aquellas empresas dedicadas a la exportación e importación de mercancías es exponencial, dada nuestra ubicación y cercanía con Estados Unidos, México se ha posicionado como su principal socio comercial al alcanzar una cifra récord de exportaciones, definitivamente la seguridad privada entrará en el juego como un aliado primordial y coadyuvará en garantizar la continuidad de negocio, las empresas reguladas podemos brindar la protección necesaria a través de las diferentes modalidades de servicio que existen, desde la seguridad física, seguridad electrónica, el uso de tecnologías, protección, traslado y custodias de mercancías, así como el monitoreo 24/7. ■

Uncover The Unseen™

GARRETT

¡Paragon establece el estándar para el futuro!

Ambiscan

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

ESCANEAR PARA MÁS INFORMACIÓN

MADE IN THE USA

ÍNDICE

Julio - Agosto

La transformación de la seguridad en **Grupo IPS, lleva liderazgo femenino.**

IPS

ESR · Great Place To Work. · CRESE · SUPER EMPRESAS 2024 TOP · COPARMEX Ciudad de México · ASUME · CCE Consejo Coordinador Empresarial

grupoipsmexico.com

SCATI *CLOUD*, LA EVOLUCIÓN DE LA VIDEOVIGILANCIA A LA NUBE

ESPAÑA

Basado en un concepto de suscripción mensual por cámara, SCATI CLOUD permite la centralización y supervisión de las grabaciones en tiempo real desde cualquier lugar mediante navegador web o aplicación para dispositivos móviles iOs y Android

SCATI, fabricante de soluciones inteligentes de seguridad, lanza su solución para la grabación y supervisión en tiempo real de imágenes en la Nube: SCATI CLOUD, un sistema de grabación y gestión de video en la Nube diseñado para transformar la forma en que las empresas protegen sus activos y garantizan la seguridad.

BONDADES

Basado en un concepto de suscripción mensual por cámara, SCATI CLOUD es compatible con los principales fabricantes del mercado (ONVIF) y permite la centralización y supervisión de las grabaciones en tiempo real desde cualquier lugar sin comprometer su seguridad.

De instalación fácil y de forma remota, no requiere configuración de red ni redireccionamiento de puertos, basta con conectarse a la red local.

En caso de interrupción de red, Scati Cloud Bridge es un dispositivo pasarela entre las cámaras y la Nube que almacena localmente las grabaciones y las sube a la Nube cuando se reestablece el servicio.

Con avanzados protocolos de cifrado y almacenamiento seguro en la Nube gracias a la tecnología de Amazon Web Services (AWS), garantiza la integridad de las grabaciones. Gracias a una instalación sencilla y una amplia compatibilidad, ofrece a las empresas una solución fiable, rentable y escalable.

SCATI CLOUD no es simplemente una solución de videovigilancia en la Nube; es una evolución en la forma en que las empresas abordan la seguridad. Desde la centralización eficiente hasta la escalabilidad sin complicaciones y los más altos estándares de ciberseguridad, está diseñado para satisfacer las demandas de las empresas modernas. ■

Fotos: SCATI

SISSA
Monitoring Integral

SEGURIDAD INTELIGENTE PARA MENTES BRILLANTES

EL EFECTO ESCOTOMA, UNA AMENAZA **"INVISIBLE"**

La mente ve lo que puede y quiere ver

Foto: Freepick

MÉXICO **David Chong Chong**

El potencial de efectividad de las acciones humanas para lograr sus objetivos depende del nivel de pertinencia de las decisiones de las que se derivan, lo cual a su vez está determinado, no tanto por la "cantidad" sino de la "calidad" de la información en que se sustentan.

Se puede considerar que el ser humano se desempeña como una "fábrica", la cual se alimenta de información (entendida como datos útiles para decidir acerca de un tema en particular) como "materia prima", que se "transforma" por medio de un "proceso" en que se aplican ciertos "criterios de valoración", el razonamiento, para "producir" las decisiones que determinan las acciones que ha de emprender. Para ello, esta información se conforma a través de otro "proceso", en el que se extraen los "datos útiles" de un acervo de datos adquiridos, aplicando ciertos "criterios de selección", lo que en conjunto se puede considera como un virtual "proceso de datos".

El "funcionamiento" global de este "proceso" se sustenta en el mecanismo DIDA (Detectar, Identificar, Decidir, Actuar), en el cual con la Detección se adquiere el Acervo de Datos, y se realiza a través de los sentidos (Vista, Oído, Olfato, Gusto y Tacto). El problema surge cuando alguno o algunos de los sentidos presenta alguna deficiencia en su funcionamiento, ya sea temporal o permanente, ya que esto podría comprometer la calidad de datos adquiridos, lo cual repercutirá, inevitablemente y por un efecto de encadenamiento, en la calidad de la información, la pertinencia de las decisiones y, por ende, en el potencial de efectividad de las acciones que se emprendan.

¿CÓMO IMPACTA EN LA SEGURIDAD?

En el contexto del ejercicio profesional en el ámbito de la Seguridad, estas posibles deficiencias en el funcionamiento de los sentidos, que inciden en la Detección, pueden repercutir en las cruciales tareas de la Observación, a través de las cuales se puede detectar el surgimiento de riesgos y amenazas. De todos los sentidos, el de mayor impacto es la Vista, ya que el ser humano es una entidad primordialmente visual, de tal suerte que las deficiencias en un sentido "visual" tienen un gran impacto en la actuación del factor humano en estas tareas.

Existe una cierta diversidad de deficiencias en la vista, algunas de las cuales son corregibles por medio de soluciones de prótesis (lentes) como la miopía, la hipermetropía o el astigmatismo, otras que requieren de un tratamiento clínico (cirugía) como las cata-

TIMUR
Latinoamérica

GALEAM

NUESTRO VALOR, SU SEGURIDAD

CONSULTORÍA

GUARDIAS INTRAMUROS

PROTECCIÓN EJECUTIVA

info@galeam.mx
info@timurlatinoamerica.com

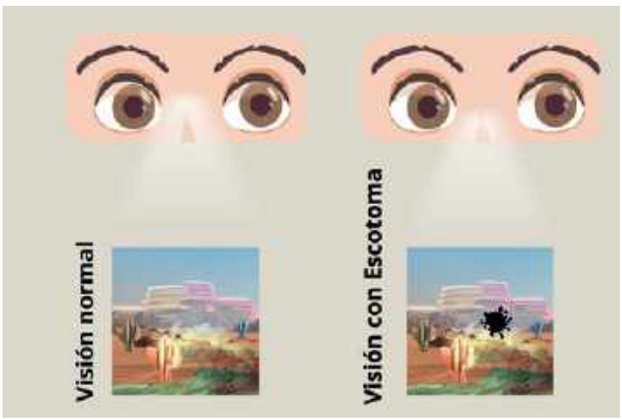
56 3048 9610 / 55 6840 1036

www.galeam.mx
www. timurlatinoamerica.com

ratas, así como algunas que prácticamente son irremediables, como el daltonismo, que incluso pueden ser un impedimento para realizar ciertas labores, como la Videovigilancia. Entre estas deficiencias se tiene el escotoma (del griego *skotos* que significa "obscuridad" o "tinieblas") que se puede proyectar en tres vertientes: física o fisiológica, mental-psicológica y de reciente surgimiento, tecnológica.

Lo que se puede considerar como la vertiente original es el escotoma físico o fisiológico que consiste en una deficiencia en el sentido de la vista, que provoca la presencia de un "punto ciego" en la visión del observador, lo que es una condición "natural" en la visión monocular (cuando sólo se enfoca con un solo ojo), que se "corrige" con la visión estereoscópica "normal" de la vista humana (enfocando con los dos ojos) que permite la percepción tridimensional de profundidad.

Pero que también puede ser provocada como secuela de una lesión en la retina o el nervio óptico, en las áreas visuales del cerebro o por una alteración vascular, por ejemplo, el estrés o los ataques de migraña. Esta deficiencia puede ser de carácter temporal (estrés, alteración en los niveles de glucosa en la sangre o ataques de migraña), parcial o permanente (causas congénitas o patológicas) y presentarse en forma de escotoma positivo (si el observador de percata de la deficiencia) o negativo (si el observador no se percata de la deficiencia). Esta vertiente es superable cuando se presenta de manera temporal o parcial y en forma positiva, mediane una simple maniobra de "barrido" del campo visual, para compensar la ubicación del "punto ciego". El efecto resultante de esta vertiente es que "la mente ve lo que puede ver".



ESCOTOMA MENTAL, TECNOLÓGICO Y FÍSICO

El escotoma mental o psicológico se produce cuando la "imagen" con los datos o información entregada a la mente del observador, se "procesa" aplicando como referentes ciertos patrones prestablecidos, por lo regular en forma de estereotipos o paradigmas, e incluso en situaciones de crisis, por ejemplo en emergencias, por el "síndrome de túnel cognitivo", a consecuencia de las inevitables alteraciones emocionales la aplicación de estos referentes provoca que la atención, y eventual valoración por parte del observador se enfoque en los parámetros de estos paradigmas, y en consecuencia se omita o ignore la presencia de otros componentes en el contenido de la "imagen" que pudieran ser indicativos del surgimiento de fenómenos no previstos, que a su vez podrran entrañar mayor potencial de riesgo o amenaza que los ya conocidos.

Algunas formas de esta vertiente podrían ser las visiones de tipo clasista, racista o incluso sexista, que ignoran o no perciben la presencia de personal de servicio, personas de otra raza o personas de otro género, por lo regular femenino, que pueden ser vectores de alto riesgo, como los guerrilleros urbanos del Vietcong durante la Guerra de Vietnam, los espías afroamericanos infiltrados en el Ejército Confederado en la Guerra Civil, o las mujeres musulmanas en atentados suicidas en los conflictos de Medio Oriente.


Foto: Freepick

Esta vertiente se puede presentar en forma positiva o negativa, si el observador se percata o no de ello, y es superable sólo en su forma positiva y además se tiene una actitud abierta, con disposición para trascender los estereotipos o paradigmas, y considerar otras posibilidades para identificar y aceptar variaciones en lo conocida, así como condiciones y situaciones inéditas (lo que ya ha ocurrido puede volver a ocurrir, pero de diferente manera, y lo que nunca ha ocurrido puede llegar a ocurrir). El efecto resultante de esta vertiente es una especie de virtual "autocensura" en la que "la mente ve lo que quiere ver".

Lo que se puede describir como el escotoma tecnológico es una vertiente que surge a partir del uso cada día más amplio de recursos de tecnología en apoyo a las tareas de observación, y está determinada por las funcionalidades de estos recursos, pero en especial en sus limitaciones. El efecto que se produce con esta vertiente es que el contenido de la "imagen" con los datos o información entregada a la mente del observador no incluye todos los elementos presentes en el lugar y momento en que ocurren los hechos captados, lo que se proyecta como una degradación de su fidelidad, que a su vez podría omitir o "enmascarar" indicadores de condiciones y situaciones con mayor potencial de riesgo. El efecto resultante de esta vertiente es una especie "censura" en la que "la mente sólo ve lo que le permiten ver", con el agravante del desconocimiento e incertidumbre en cuanto a que puede haber algo más que lo mostrado.

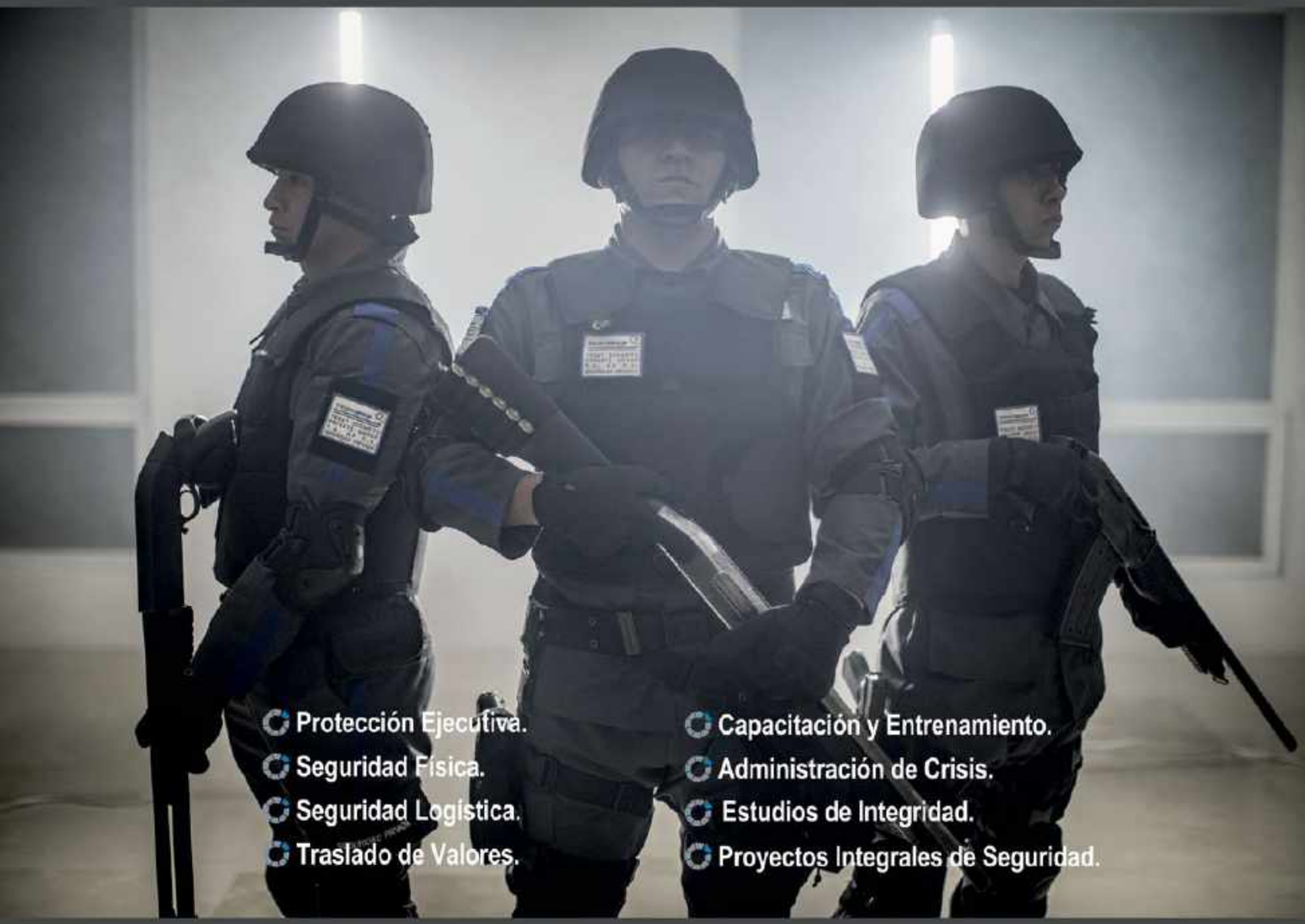
FIDELIDAD DE IMAGEN

El ejemplo más ilustrativo de no sólo de este efecto, sino de la conjunción de los efectos de las tres vertientes, son los sistemas de videovigilancia, con el nivel de degradación de la fidelidad del contenido de la "imagen" con los datos de lo ocurrido respecto a lo entregado está determinado por los siguientes factores:

- Las facilidades de "visualización" en el espacio bajo vigilancia para poder localizar e identificar los componentes de "contenido de imagen" (iluminación, visibilidad y "distinguibilidad").

TRUSTGROUP MR

En Seguridad, "Nadie Conoce México Como Nosotros".



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

www.trustgroup.com.mx

Veinte años brindando servicios profesionales de seguridad

ASIS

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

- El efecto de escotoma tecnológico compuesto por:

a) Las capacidades funcionales de "campo visual" del lente para captar "imágenes" en el espacio bajo vigilancia (alcance y ángulo de apertura).

b) Las capacidades funcionales de la cámara para registrar las "imágenes" del "campo visual" cubierto por el lente (resolución, sensibilidad y *"shooter")*.

c) La capacidad operativa del medo de transmisión para transferir sin distorsiones las "imágenes" (ancho de banda).

d) Los algoritmos de procesamiento de las "imágenes", en especial las funciones de "filtrado" con el uso de herramientas de inteligencia artificial (IA), que configuran un efecto similar al escotoma mental o psicológico, pero sin la capacidad de discernimiento del factor humano para trascender estas limitaciones.

e) Las capacidades funcionales del monitor para proyectar las "imágenes" en forma discernible para el observador (multiplicidad de imágenes y resolución).

- El efecto integral de las diversas deficiencias en el sentido de la vista, ya sea propios (miopía, hipermetropía, astigmatismo, presbicia, cataratas, glaucoma), o asociados a otras condiciones (estrés, ritmos circadianos cuyo efecto se puede reducir con el consumo de melatonina) o padecimientos (migraña, variaciones de le glucosa en la sangre por diabetes), en especial las que provocan el efecto del escotoma físico o fisiológico en la percepción del campo visual del observador.
- El efecto de escotoma mental o psicológico en la mente del observador, que se puede intensificar por algunas circunstancias de índole personal y particular, como el desgaste físico asociado a la dinámica biológica de los ritmos circadianos, los sesgos y matices de percepción inducidas por vivencias y experiencias de alguna forma traumáticas a nivel personal, así como un "exceso de confianza" en los apoyos de las funcionalidades de los recursos de tecnología, por lo que se puede considerar como un "síndrome de espejismo".

Foto: Freepick

Algunas de estas deficiencias pueden ser un impedimento para realizar ciertas tareas, pero otras en el marco de las tareas de Videovigilancia. En la vertiente del escotoma mental, es el caso de las personas con obsesión compulsiva o paranoia, que podrían "sobrerreaccionar" en situaciones de contingencia, pero ser útiles en el análisis forense de las imágenes para percatarse de anomalías precisamente por su obsesión por los detalles, que pasarían desapercibidas para personas "normales".

En la vertiente del escotoma físico, es el caso de los daltónicos, que no serían útiles en la operación por la distorsión cromática, pero sí en el análisis forense precisamente porque podrían percatarse de algunos detalles difíciles de detectar con los perfiles de sensibilidad cromática "normales". Incluso, personas con escotoma monocular (en un solo ojo), sólo verían afectada su capacidad de percepción tridimensional, lo que no es impedimento para la observación de un monitor que proyectan imágenes bidimensionales, en donde la dimensión de "profundidad" se obtiene mediante técnicas de valoración comparativa entre componentes del contenido de las mismas imágenes.

La degradación de la fidelidad que resulta de la conjunción de estos factores produce en efecto integrado en el que "la mente ve lo que le permiten, puede y quiere ver", lo que limita los referentes para el razonamiento de valoración, compromete la pertinencia de las decisiones y por ende el potencial de efectividad en la actuación.

Todas las acciones del factor humano pretenden el logro de algún objetivo y son producto de ciertas decisiones, cuyas perspectivas de efectividad, y eventual éxito, están determinadas por la pertinencia de tales decisiones, lo que, a su vez, depende de la medida en que en el "contenido" de la información en que se sustentan se contemplen todos los factores involucrados, en especial los que puedan proyectar repercusiones de riesgo. Para este propósito, la omisión de alguno de estos factores "de riesgo" puede comprometer significativamente la pertinencia de las decisiones, y en consecuencia las perspectivas de efectividad y eventual éxito de dichas acciones.

En este contexto, precisamente por las posibles repercusiones de riesgo que se proyectan, este efecto escotoma se perfila como un vector de amenaza virtualmente "invisible" en dos sentidos: en principio, porque oculta y enmascara la presencia de factores con un posible mayor potencial de riesgo, principalmente por su carácter imprevisible y por ende impredecible; pero también porque su presencia y condición como "problema" en muchas ocasiones no son perceptibles para tener la oportunidad de buscar alguna forma de "solución" para anular o al menos reducir las repercusiones de los posibles riesgos. Y en particular en el ámbito de la Seguridad, dichas repercusiones son de gran impacto, de consecuencias críticas, ya que pueden provocar alguna forma de pérdidas, en especial de vidas humanas.

Este efecto escotoma es un fenómeno que siempre ha existido por las características físicas y mentales propias de la naturaleza humana con repercusiones en todos los ámbitos. Un ejemplo muy ilustrativo de ello se presenta en los altos niveles de mando en las grandes organizaciones (empresariales o políticas), en donde sus líderes dependen de colaboradores para "dosificar" el suministro de información para reducir el problema de saturación, pero se depende del criterio de éstos últimos, de forma similar al escotoma tecnológico, para "filtrar" dicha información, lo que cuestiona el mito de que "el líder máximo (director o presidente) es la persona mejor informada".

En el ámbito particular de la Seguridad, las repercusiones, sobre

EMPRESA DE SEGURIDAD ELECTRÓNICA INTEGRADOR

SYSTEM AI

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

Totalmente conectado a ti

comexa_seguridad comexa ComexaSeguridad

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

Av. Universidad 989 - 402 • Col. Del Valle • Benito Juárez, 03100 • CDMX

55 5685 7830 t 55 5685 7837 • 800 2 COMEXA

En la vertiente del escotoma mental, es el caso de las personas con obsesión compulsiva o paranoia, que podrían "sobrerreaccionar" en situaciones de contingencia, pero ser útiles en el análisis forense de las imágenes para percatarse de anomalías precisamente por su obsesión por los detalles, que pasarían desapercibidas para personas "normales"

Foto: Freepick

En la vertiente del escotoma físico, es el caso de los daltónicos, que no serían útiles en la operación por la distorsión cromática, pero sí en el análisis forense precisamente porque podrían percatarse de algunos detalles difíciles de detectar con los perfiles de sensibilidad cromática "normales"

todo las adversas, inciden primordialmente en los servicios de Seguridad Física, en todas sus modalidades (guardaespaldas, intramuros y custodios), y Monitoreo de Videovigilancia, pero también en los de Monitoreo de Sistemas de Alarmas y de Rastreo Vehicular al menos en las vertientes mental y tecnológica. Por ello, y ante la intensificación de estas repercusiones por las innovaciones funcionales de los avances tecnológicos en procesamiento de datos (en la práctica como alguna forma de "filtrado"), se puede proyectar a este efecto escotoma como un fenómeno en constante evolución, dinámico y heterogéneo, para el que se debe construir alguna forma de respuestas innovadoras para evitar que se puedan convertir en problemas críticos, las cuales muy probablemente requerirá del desarrollo e implementación de esquemas de regulación y organización de la operación, así como modelos de formación (capacitación y adiestramiento) del factor humano acordes a estas nuevas condiciones.

"El que no aplique nuevos remedios debe esperar nuevos males, porque el tiempo es el máximo innovador", Sir Francis Bacon

Con la colaboración del Dr. Arturo Pérez Barragán (Oftalmólogo), Dr. José Gerardo Sierra Díaz (Oftalmólogo), Dra. Nadine Terrein Roccatti (Psicóloga), Mtra. Ileana Marisol Rojas López (Seguridad), Lic. Gabriel Esteban Escobar González (Seguridad), Ing. Heriberto Moncada Medrano (C5, Tamaulipas), Elida Maribel Gallardo Marín (C5, Matamoros, Tamaulipas) y Arturo Toledo Ibarra (C5 Escudo Urbano, Jalisco). ■

Puede consultar una versión ampliada de ese artículo en este enlace: https://www.ceasmexico.org.mx/beta/php/difusion/articulo.php?pid=000246

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

ISIS SEGURIDAD INTEGRAL

Creamos entornos seguros

Servicios:

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

AFAC
AGENCIA FEDERAL DE AVIACIÓN CIVIL

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE

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

ASIS INTERNATIONAL

mesis

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

SUPERVISIÓN DE PROCESOS PRODUCTIVOS EN LA INDUSTRIA FARMACÉUTICA MEDIANTE TECNOLOGÍA

ESPAÑA | **Raquel Elías Gutiérrez**

Este laboratorio farmacéutico es un claro ejemplo de transformación digital que adapta sus procesos y procedimientos a la nueva revolución industrial

RETO

El laboratorio cuenta dos plantas de producción con la última tecnología en España que suman más de 70 mil metros cuadrados, en las que gestionan el proceso de elaboración integral de sus medicamentos con los más altos estándares de calidad.

En sus instalaciones destaca un almacén con una capacidad de más de 20 mil *pallets*, una zona de *picking* donde son capaces de preparar hasta un millón de estuches diarios y una zona donde son envasados hasta 54 mil comprimidos por minuto.

Para garantizar que las referencias de sus medicamente cumplen con los requisitos de seguridad exigidos y la industria controle su legalidad, el laboratorio farmacéutico adecúa su maquinaria y sus instalaciones al Sistema Español de Verificación de medicamentos (SEVeM).

La empresa, que lidera la transformación digital de la industria farmacéutica, instala los sistemas de video de SCATI para el control y supervisión de sus procesos productivos.

SOLUCIÓN SISTEMA DE VIDEOVIGILANCIA

La instalación de los sistemas de video inteligente de SCATI cumple una doble función; por un lado, garantizar la seguridad de sus instalaciones y activos; y por otra, asegurar la trazabilidad de cada medicamento dispensado asociando su información con imágenes de video (a través de SCATI PARCEL).

La instalación de cámaras de videovigilancia la completan un total de 30 cámaras de alta definición que incluyen cámaras *fisheye* 360° bajo una red de comunicaciones TCP/IP independiente a la existente en la planta. La separación de redes actúa como un cortafuego natural en el caso de que hubiese una infección/ataque sobre una de ellas. Por otra parte, el nivel de calidad de servicio también es importante, ya que permiten dimensionar bien las prioridades de ambas redes con mecanismo QoS. Gracias a ello, el laboratorio dispone de una instalación cibersegura.

TRAZABILIDAD DE LA PRODUCCIÓN MEDIANTE VIDEO

Con el objetivo de evitar falsificaciones en los medicamentos y adaptarse a la normativa (SEVeM), se incorpora un doble sistema de seguridad. Cada estuche lleva un código datamatrix que contiene un número de serie único asignado a cada estuche de medicamento y que permitirá verificar su autenticidad, así como su identificación. Por otra parte, cada estuche cuenta con un precinto que asegura que este no haya sido abierto o manipulado.

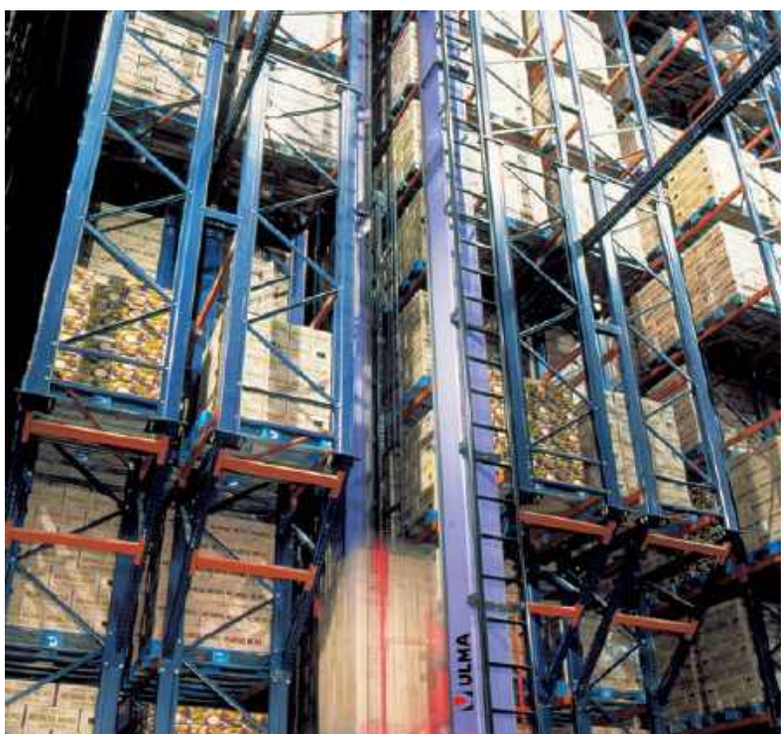
La codificación datamatrix es un código bidimensional situado en la solapa lateral del medicamento, similar a la codificación QR, que permite incluir un gran volumen de información en un formato muy reducido, y que incorpora información básica de lote, caducidad y código EAN, etc., en cada producto.

La supervisión del proceso productivo se realiza a través de cámaras de videovigilancia. Las imágenes que recogen estas cámaras se asocian a cada medicamento gracias a SCATI PARCEL, que integra el Sistema de Gestión de Almacenes (SGA) con el sistema de video. Esta integración permite que el SGA trace la posición de cada *palet* (contenedor) y la indexe con el video facilitando la búsqueda de imágenes asociadas a cada paquete y por cualquier parámetro (código EAN, fecha de caducidad, etc.).

TRANSELEVADORES

Nos encontramos ante un almacén completamente automatizado que cuenta con transelevadores, sistemas de almacenaje automático para cajas o bandejas que integra las estanterías, y que están completamente integrados con el SGA. Este sistema optimiza la capacidad del almacén, los procesos de *picking* y es autodidacta, si registra alta demanda de un producto, lo almacena lo más cercano posible para tenerlo accesible y ahorrar tiempo.

Existe un transelevador por cada uno de los siete pasillos existentes en el almacén. Las cámaras instaladas ofrecen un ángulo de visión de 360° y ofrecen una resolución de hasta seis megapixeles (SEM-3701NR-EO). Para la transmisión del video IP, se opta por una red inalámbrica wifi.



SCATI RECKON

Además de incorporar lo último en tecnología de video para proteger las instalaciones, supervisar los procesos productivos y logísticos y garantizar la trazabilidad de cada mercancía, este laboratorio farmacéutico apuesta por la herramienta de Business Intelligence de SCATI: RECKON, el cual es un *software* que centraliza y gestiona una gran cantidad de datos procedentes de cámaras, grabadores o, incluso de sistemas de terceros.

Transforma los datos en información útil, permite crear gráficas y cuadros de mando integrales de forma simplificada, muestra esa información de forma organizada a las personas que necesiten interpretarla y tomar decisiones a partir de ellas. Es nuestro *software* de BI, que centraliza y gestiona.

BENEFICIOS

La compañía apuesta por la inversión en tecnologías que le permitan adaptarse a la nueva revolución industrial (Industria 4.0). Esta transformación digital implica cambios en los procesos productivos, logísticos, sociolaborales, etc. y para ello no duda en contar con un partner como SCATI con el que afrontar este desafío.

Las nuevas tecnologías asociadas a la Industria 4.0, utilizadas de forma inteligente, ayudan a mejorar la eficiencia operativa de las organizaciones y su rentabilidad. No sólo desde el punto vista de la eficiencia o del ahorro de costos, también desde el punto de vista de diferenciación, posicionamiento en el mercado o innovación y nuevos modelos de negocio.

SCATI ofrece una solución que, basada en video inteligente, le permite disponer de información puntual para una rápida resolución de incidencias generadas en la instalación del cliente. A través de la visualización y monitorización de procesos industriales mediante cámaras inteligentes se identifican fallos en el sistema en tiempo real implementando correcciones de forma inmediata.

Las soluciones de video de SCATI dan un paso más allá e incorporan *Business Intelligence*, que permite la toma de decisiones acertada gracias a la gestión de datos procedentes de las múltiples cámaras instaladas en sus dependencias.

SCATI es más que un fabricante de sistemas seguridad inteligentes. Es un *partner* con el que afrontar los retos de la transformación digital a los que se enfrentan la industria y la logística, a través del diseño y desarrollo de soluciones adaptadas a las particularidades de cada cliente. ■

Fotos: SCATI

Raquel Elías Gutiérrez, *Marketing Manager* de SCATI. *Más sobre la autora:*

ASEGURANDO LA CADENA DE SUMINISTRO: DESAFÍOS Y ESTRATEGIAS

Al abordar las complejidades inherentes y las vulnerabilidades en las redes de cadena de suministro, las organizaciones pueden mejorar su resiliencia a las amenazas cibernéticas y proteger activos críticos

MÉXICO | Gigi Agassini

Foto: Freepick

El reciente aumento en los ataques a la cadena de suministro ha puesto de relieve las vulnerabilidades inherentes en los ecosistemas empresariales interconectados de hoy en día. Las cadenas de suministro son el motor del comercio global; permiten el flujo sin problemas de bienes, servicios e información a través de las fronteras. Sin embargo, esta interconexión también expone a las cadenas de suministro a una creciente gama de amenazas cibernéticas.

Desde SolarWinds hasta Kaseya, las brechas de alto perfil han subrayado la necesidad crítica de medidas robustas de seguridad en la cadena de suministro. Desde actores maliciosos infiltrando redes de proveedores hasta ataques sofisticados a infraestructuras críticas, los riesgos son reales y omnipresentes. Fortalecer la seguridad de la cadena de suministro ha surgido como una preocupación apremiante para las empresas en todo el mundo.

En el mundo hiperconectado de hoy, las medidas de seguridad tradicionales centradas únicamente en proteger a las organizaciones de manera individual, ya no son suficientes. En su lugar, las empresas deben adoptar un enfoque holístico que abarque toda la red de relaciones dentro de las cadenas de suministro modernas. De hecho, la solidez de su seguridad es tan fuerte como el eslabón más débil dentro de su cadena de suministro.

¿Qué impulsa este cambio? Los directores de Cadena de Suministro están respondiendo a las demandas cambiantes de los clientes y las dinámicas del mercado al orquestar cadenas de suministro inteligentes. Estas cadenas de suministro reconfiguradas priorizan la resiliencia, la transparencia y la agilidad, alejándose de los modelos lineales del pasado para abrazar redes interconectadas, lo que sin duda trae otros retos y riesgos.

Consecuentemente, las empresas modernas se encuentran más y más interconectadas con el entorno externo, facilitando el flujo sin problemas de datos y bienes. Si bien esta interconexión mejora la agilidad y la eficiencia empresarial, simultáneamente amplifica el panorama de riesgos. El volumen de datos que atraviesa las cadenas de suministro, junto con la superficie de ataque expandida, subraya la importancia crítica de las medidas de ciberseguridad para proteger los activos organizacionales.

Según el estudio de Prevalent sobre "Gestión de Riesgos de Terceros de 2022", los programas de gestión de riesgos de terceros todavía se centran principalmente en abordar los riesgos enfrentados al trabajar con proveedores de TI (45%). Sin embargo, sorprendentemente, el 40% de los encuestados en 2022 del estudio, están enfocados en gestionar tanto los riesgos de proveedores de TI como los que no son de TI.

El mismo estudio destacó que el 45% de las organizaciones experimentaron un incidente de seguridad de terceros en el último año, pero están utilizando herramientas dispersas que alargan los tiempos de respuesta a incidentes. Algo debe estar mal, debido a que, en el mismo estudio, los encuestados dicen que sus métodos actuales para evaluar a los proveedores no pueden proporcionar informes para demostrar el cumplimiento (57%). Menos de la mitad de las empresas están rastreando riesgos en etapas posteriores del ciclo de vida del proveedor. Consecuentemente es claro que existe una falta de procesos y políticas que nos ayuden a cerrar esta distancia y gestionar de manera eficiente los riesgos que surgen y cambian dinámicamente, entre más nos interconectamos.

Foto: Freepick

DESAFÍOS EN LA SEGURIDAD DE LA CADENA DE SUMINISTRO

Los actores de amenazas cibernéticas están aprovechando las crisis geopolíticas para lanzar señuelos de *phishing*, campañas de *malware* y desinformación. Las redes criminales están creciendo y fortaleciéndose, los grupos de amenazas están encontrando puntos débiles, evadiendo las defensas de red y vendiendo este acceso a otros grupos de amenazas.

A medida que las empresas mejoran su seguridad, los actores maliciosos ahora están dirigiendo su atención a sus proveedores, por lo tanto, integrar inteligencia de amenazas cibernéticas en fusiones y adquisiciones e incorporar pruebas de proveedores y fábricas en sus procesos, es clave.

Además, las empresas deben hacer de la seguridad una parte fundamental de la cadena de suministro inteligente. Las organizaciones necesitan incorporar principios de seguridad en toda la red de la cadena de suministro. Eso incluye hacer de la ciberseguridad una prioridad no sólo dentro de la empresa, sino también con todas las organizaciones asociadas y conectadas.

Los vendedores y proveedores externos a menudo tienen acceso a datos y sistemas sensibles, lo que los convierte en objetivos atractivos para los atacantes. Según el informe "Estado de la Gestión de Riesgos de Terceros de 2021" de Security Scorecard, el 80% de las organizaciones encuestadas experimentaron una violación de datos causada por un proveedor externo.

Las cadenas de suministro modernas son redes intrincadas que involucran a múltiples partes interesadas, cada una con su propio conjunto de protocolos y prácticas de seguridad. La naturaleza interconectada de las cadenas de suministro aumenta la superficie de ataque y amplifica el impacto potencial de las brechas de seguridad.

La limitada visibilidad en toda la cadena de suministro dificulta la capacidad de las organizaciones para detectar y responder a incidentes de seguridad de manera oportuna. Un estudio de Deloitte encontró que solo el 6% de las organizaciones tienen visibilidad completa en sus redes de terceros. Lo que nos demuestra que existe mucho camino por recorrer aún.

ESTRATEGIAS PARA UNA SEGURIDAD EFECTIVA DE LA CADENA DE SUMINISTRO

Uno de los principales desafíos para muchas empresas es la complejidad, multifacética y a menudo fragmentada de la seguridad de la cadena de suministro. Al crear un programa único de coordinación para la seguridad de la cadena de suministro, las organizaciones pueden ayudar a superar estas dificultades. Obtener visibilidad en toda la cadena de suministro, por ejemplo, implementar procesos robustos de gestión de riesgos de proveedores es crucial para evaluar y monitorear los riesgos de seguridad de terceros. Esto implica realizar una diligencia debida exhaustiva sobre los proveedores, evaluar su postura de seguridad y establecer obligaciones contractuales claras. Recursos como el Marco de Ciberseguridad de NIST y la norma ISO 27001 proporcionan pautas para prácticas efectivas de gestión de riesgos de proveedores.

La adopción de soluciones de monitoreo continuo permite a las organizaciones rastrear y analizar la actividad en toda la cadena de suministro en tiempo real. Al aprovechar herramientas como los sistemas de gestión de información y eventos de seguridad (SIEM) y las plataformas de inteligencia de amenazas, las organizaciones pueden identificar y responder proactivamente a posibles amenazas de seguridad.

Fomentar prácticas de desarrollo seguro entre los proveedores ayuda a mitigar el riesgo de introducir vulnerabilidades en productos y servicios. La implementación de estándares de codificación segura, la realización de evaluaciones de seguridad regulares e integrar la seguridad en el ciclo de vida del desarrollo de *software* (SDLC) son pasos esenciales en este sentido.

Desarrollar planes de resiliencia de la cadena de suministro permite a las organizaciones mantener operaciones y mitigar interrupciones en caso de incidentes de seguridad. Esto implica identificar dependencias críticas, establecer medidas de contingencia y realizar ejercicios de mesa periódicos para probar las capacidades de respuesta.

Asegurar la cadena de suministro es un desafío multifacético que requiere colaboración, vigilancia y planificación estratégica. Al abordar las complejidades inherentes y las vulnerabilidades en las redes de cadena de suministro, las organizaciones pueden mejorar su resiliencia a las amenazas cibernéticas y proteger activos críticos. Al implementar las estrategias descritas y más, las empresas pueden fortalecer su postura de seguridad en la cadena de suministro y mitigar los riesgos planteados por el panorama de amenazas en constante evolución de hoy en día.

Si estás implementando un nuevo programa o revisando tu programa de seguridad, no olvides que existen varios estándares globales que podrán apoyarte en este camino, adicional a la constante revisión de tus procesos y procedimientos, es vital. ■

¡Hasta la próxima!


Foto: Freepick

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

INTELIGENCIA ARTIFICIAL:
EFICIENCIA EN LAS OPERACIONES

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Foto: Freepick

La empresa de seguridad electrónica Monitoreo 360 está trabajando en la integración de la IA a sus diferentes soluciones de rastreo y monitoreo

Sin lugar a dudas, la tecnología se ha convertido en la pieza clave del ser humano para mejorar su vida, desarrollarse, y utilizarla de acuerdo a sus necesidades y conveniencia. La seguridad ha ido adaptándose a los avances tecnológicos que han mejorado los procesos de prevención y reacción, una de las grandes aportaciones de la tecnología a este sector ha sido la videovigilancia, que no se ha quedado sólo como un ente que observa y guarda información, sino que ha evolucionado a una herramienta que simplifica, alerta y clasifica todos los datos que va recopilando.

En el caso específico de la seguridad al transporte de carga, tanto las cámaras, los GPS y el monitoreo inteligente, han ayudado a mejorar los procesos de la cadena de suministro, puesto que una pronta alerta puede significar la reducción de pérdidas y, por ende, mejorar la productividad y eficiencia de la empresa.

"A finales del año pasado decidimos cambiar nuestra estructura, cambiar toda nuestra organización para orientar todos los esfuerzos futuros y la innovación futura en el mundo de la inteligencia artificial"


Foto: Freepick

Foto: Freepick

"Nuestros clientes son lo más importante para nosotros, también nos caracterizamos por mantener una disciplina, la constancia de mejorar cada día, y valoramos también el conocimiento"

APLICACIÓN DE LA IA

Una de las compañías especializadas en seguridad electrónica con experiencia en la mejora de procesos a través de la tecnología, es Monitoreo 360, la cual ha sido disruptiva este último medio año y se encuentra en un proceso de transformación, adaptando y estudiando cómo el recurso tecnológico del momento puede alinearse a las necesidades de seguridad de sus clientes, es decir, cómo la Inteligencia Artificial cambiará lo que hasta hoy conocemos en monitoreo y seguridad.

"Recientemente, Monitoreo 360 tuvo un cambio. Durante los últimos siete años hemos estado construyendo una estructura de servicios y soluciones, tanto para cuidar vehículos como para cuidar ubicaciones, que implicó mucho trabajo en diseño, innovación, en procesos, y que nos ha llevado hasta donde estamos; lo que nos tiene muy orgullosos. Hemos logrado obtener las certificaciones de calidad, ISO 9001, la de Seguridad de Información, la 27000, y también tenemos Recuperación de Desastres o Continuidad de Negocios, y Anticorrupción. Pero a finales del año pasado decidimos cambiar nuestra estructura, cambiar toda nuestra organización para orientar todos los esfuerzos futuros y la innovación futura en el mundo de la inteligencia artificial", comentó Roberto Rossello, director general de M360, en compañía de Erick Cuenca y Saturnino Soria, socios consejeros de M360.

El entrevistado también explicó que el mundo de la inteligencia artificial es un mundo muy nuevo y cambiante, así como una palabra muy "sobreutilizada" y bastante incomprendida. "La inteligencia artificial existe hace mucho tiempo, pero hoy por hoy nos solemos referir a la inteligencia artificial como unas redes neuronales muy específicas y muy grandes, con algunos casos de uso bastante específicos. Esos casos de uso, por ejemplo, pueden ser texto, imágenes, videos, y que la computadora puede lograr una especie de comprensión de esa información de entrada y a partir de ella genere una salida. Del texto, una imagen; de la imagen, texto; del video, texto; que pueda clasificar, especificar, lograr algunas actividades que naturalmente se consideraron que sólo hacía el hombre, y que son muy poderosas", indicó.

La más simple de estas actividades, son las de clasificar, obtener datos clave, y luego actividades más complejas como, por ejemplo, traducir o resumir, una nueva capacidad de procesamiento. "Con la videovigilancia, que es un campo enorme, puedo realizar distintas actividades: desde contar personas, identificar a la gente, contar vehículos, revisar si están bien aparcados, dar matrículas, dar carteles; pero con la Inteligencia Artificial no sólo puedo dirigir una búsqueda específica, sino que puedo interpretar lo que en la imagen sucede, clasificarla, transformarla en texto, y resumirla; o bien, un audio".

Roberto Rossello considera que quien no integre la IA a su compañía, a la seguridad, no podrá competir en el mercado. "El que no lo integre la Inteligencia Artificial antes del 2030, se arrepentirá de no haberlo hecho, porque si mi competencia puede hacer lo mismo que hago yo, con un mejor precio, con una mayor calidad, por ende, con una mayor productividad, evidentemente, yo me quedo sobre el terreno marcado. Por otro lado, el mundo de la seguridad es un mundo que tiene algunas particularidades, así como la geografía, lo que pasa en el norte no es lo mismo que pasa en el sur, en el este o en el oeste. También es un mundo muy visual, entonces, el hecho de que podamos automatizar la información visual, nos genera una cantidad de posibilidades".

Monitoreo 360 continúa innovando en el sector de la seguridad siempre pensando en las necesidades de sus clientes y en la mejora de los procesos que ayuden a prevenir y reaccionar, a proteger y mejorar la seguridad. "Nuestros clientes son lo más importante para nosotros, también nos caracterizamos por mantener una disciplina, la constancia de mejorar cada día, y valoramos también el conocimiento, que nuestro recurso humano, operativo y administrativo, tengan ese interés por aprender más", concluyó Roberto Rossello. ■

Columna de
Jaime A. Moncada
jam@ifsc.us

ES DIRECTOR DE INTERNATIONAL FIRE SAFETY CONSULTING (IFSC), UNA FIRMA CONSULTORA EN INGENIERÍA DE PROTECCIÓN CONTRA INCENDIOS CON SEDE EN WASHINGTON, DC. Y CON OFICINAS EN LATINOAMÉRICA.

Más sobre el autor:

SEGURIDAD CONTRA INCENDIOS EN EDIFICIOS DE OFICINAS

Foto: Freepick

EUA

Un tipo de edificio muy común en nuestras ciudades son los edificios de oficinas, clasificados como ocupaciones de negocios en los códigos de construcción. Las ocupaciones de negocios han cambiado considerablemente desde el año 2000. Las oficinas de cubículos que eran comunes hace un par de décadas han sido reemplazadas por las estaciones de trabajo abiertas, entremezcladas con áreas de reunión y trabajo en grupo.

Aunque la pandemia del 2020 desencadenó un aumento dramático en el trabajo remoto y puso presión en la viabilidad económica de los edificios de oficinas, a medida que las economías han retornado a un nuevo "normal", la necesidad de espacios de oficinas está otra vez en aumento. Por ejemplo, el sector de los "servicios" en nuestras economías modernas, ha continuado creciendo, representando dos tercios del PIB de la región y proporcionando más de la mitad de los empleos[1]. Este es el principal sector que está requiriendo los mayores espacios para llevar adelante sus funciones productivas.

Los ocupantes de los edificios de oficinas generalmente se caracterizan por estar despiertos, alertas y familiarizados con su entorno. Es decir, su riesgo en un incendio no es alto y se puede manejar razonablemente. Sin embargo, su movilidad puede ser un tema de cuidado para los que diseñan y analizan este tipo de ocupaciones, pues es cada vez más común encontrar personas con discapacidades laborando en oficinas.

No todas estas ocupaciones son grandes edificios pues debemos reconocer que en Latinoamérica la mayoría de los negocios son empresas pequeñas y medianas (llamados pymes). De acuerdo con la Organización para la Cooperación y el Desarrollo Económico (OCDE), el 60% del empleo productivo formal en Latinoamérica está en las pymes. Es decir, muchas de estas empresas se alojan en edificios de uno o pocos pisos, en lugar de la típica torre de oficinas de gran altura.

TENDENCIAS ESTADÍSTICAS DE LOS INCENDIOS:

Como he venido comentando en esta revista, en un país como los Estados Unidos, donde la mayoría de las ocupaciones han sido diseñadas y mantenidas durante décadas bajo un código de construcción moderno y efectivo, no debería ser una sorpresa que haya habido una reducción significativa en el número de incendios y en el número de muertos por los incendios, como se muestra en la figura 1. Esta tendencia no puede ser atribuida a sólo una causa, sino a la protección de más y más edificaciones con rociadores automáticos, al aumento de los esfuerzos en la prevención de incendios y la educación pública, y otros esfuerzos más, los cuales todos en conjunto han jugado un papel fundamental en esta reducción.

Figura 1

Por ejemplo, el número de incendios ocurridos entre 1980 y el 2022 se han reducido a una tercera parte, si eliminamos de esta estadística los incendios residenciales. Debemos recordar que entre el 70% al 80% de los muertos por incendios ocurren en las ocupaciones residenciales[2]. Las causas principales de los incendios en oficinas son la preparación de alimentos (31% de los casos), los equipos de iluminación y distribución eléctrica (17%), y los incendios premeditados (10%). El área de origen más común es la cocina (19% de los casos), seguida de las áreas dentro de los despachos (11%)[3].

CRITERIOS DE PROTECCIÓN

Como he escrito en el pasado, los requerimientos de seguridad humana y protección contra incendios están definidos por el uso o la ocupación del edificio. A continuación, resumo los sistemas de seguridad contra incendios más importantes para la protección de un edificio nuevo de oficinas. Para edificios existentes se debería consultar el *International Building Code* (IBC) y la NFPA 1, Código de Prevención de Incendios:

Sistemas de Supresión de Incendios: todos los edificios nuevos de tres o más pisos de altura sobre el nivel del suelo y los sótanos que excedan los 232 m^2 deben estar protegidos en todo momento por un sistema de rociadores automáticos aprobado de acuerdo con NFPA 13.

Como he también mencionado en esta columna, ya no se utilizan gabinetes de mangueras (o bocas de incendios equipadas). En su lugar, se requiere la instalación de una o varias "conexiones" para mangueras, la cual es llamada Columna de Agua Clase I, en lugar de estos gabine-

tes equipados con mangueras (conocidos como Clase II). El Sistema Clase I provee una columna o montante, 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), como se muestra en la figura 2.

***Figura 2** - Montante de agua con conexión Clase I y conexión al sistema de rociadores automáticos*

Estas conexiones Clase I, diseñadas e instaladas de acuerdo con NFPA 14, se requieren en edificios nuevos cuando exista alguna de las siguientes condiciones:

- Cuatro o más pisos de altura sobre el plano de rasante cuando el edificio está protegido por un sistema de rociadores automáticos.
- Tres o más pisos de altura sobre el nivel del suelo cuando el edificio no está protegido por un sistema de rociadores automáticos.
- Más de 50 pies (15 m) sobre el plano de rasante y que contenga pisos intermedios o balcones.
- Más de un piso por debajo del plano de rasante o más de 20 pies (6.1 m) por debajo del plano de rasante.

La efectividad de los extintores manuales en incendios incipientes está más que documentada, y estos son de uso requerido en todas las ocupaciones que ocupan edificios de oficina. La selección o distribución de los extintores debe seguir la norma NFPA 10. Los empleados designados deben ser capacitados periódicamente para conocer la ubicación y el uso adecuado de los extintores de incendios portátiles.

Sistemas de Detección y Alarma: se debe diseñar, instalar y mantener un sistema de alarma contra incendios de acuerdo con NFPA 72 en todas las nuevas ocupaciones de negocios donde exista cualquiera de las siguientes condiciones:

- El edificio tiene tres o más pisos de altura.
- El edificio está ocupado por 50 o más ocupantes por encima o por debajo del nivel de descarga de salida.
- El edificio está ocupado por un total de 300 ocupantes o más.

Esto implica la instalación de pulsadores manuales y bocinas de alarma a través del edificio, pero no se requiere específicamente la instalación de detectores de humo. La normativa de la NFPA sólo está requiriendo detección de humo en áreas donde alguien pueda dormir (hoteles, dormitorios, hospitales, residencias, etc.), en el *lobby* de los elevadores, o en ocupaciones muy delicadas (como un cuarto de cómputos o de telecomunicaciones). Dependiendo del diseño del sistema de aire acondicionado, es muy probable que se requieran detectores de humo en los conductos de aire (para prevenir que el sistema de aire acondicionado distribuya el humo a través del edificio).

Construcción Resistente al Fuego: un área incipiente en seguridad contra incendios, en nuestra región, es la definición del tipo de construcción que debe tener un edificio, desde el punto de vista de resistencia al fuego. Esto está definido en el *International Building Code* (IBC), donde se limita el área por piso y el número de pisos que puede tener un edificio dependiendo de su tipo de construcción. Además, estas limitaciones se eliminan o incrementan cuando el edificio es protegido con rociadores automáticos.

Similarmente, se deben evaluar los terminados o revestimientos interiores (definidos a través de ensayos que miden su índice de propagación de la llama y cantidad de humo desarrollado), lo cual también es muy difícil de obtener por la falta de información existente sobre los terminados interiores que utilizamos en nuestra región (tapetes, papeles de colgadura, techos suspendidos o elementos decorativos plásticos).

Evacuación: es un tema que requiere un estudio específico del edificio a través de la norma NFPA 101, Código de Seguridad Humana, donde se establecen los criterios específicos para el diseño de las vías de evacuación (localización, cantidad, ancho, distancia). En todos los edificios de oficinas ocupados por más de 500 personas, o por más de 100 personas por encima o por debajo del nivel de la calle, los empleados y el personal de supervisión deben recibir instrucciones periódicas sobre el proceso de evacuación durante un incendio y deben realizar simulacros periódicamente cuando sea posible. Típicamente, estos simulacros se efectúan de manera anual.

Elevadores: los elevadores en un edificio deben cumplir con ASME A.17.1, Código de Seguridad en Elevadores y Escaleras Mecánicas. Debido a que un elevador pudiera parar en el piso del incendio o que los productos de combustión entren en el hueco de los elevadores, es importante que se inicie un re-llamado luego de la operación de detectores de humo en sus vestíbulos o en su cuarto de máquinas, para que queden fuera de servicio y sean operados solo por los bomberos.

Edificios de gran altura: en esta revista he escrito anteriormente sobre edificios de gran altura (*high-rise buildings*)[4], los cuales están definidos como aquellos que tienen áreas ocupadas de más de 23 m (75 pies) de altura sobre el nivel de rasante, o aproximadamente siete pisos. Esta altura se ha asociado con la altura máxima que un cuerpo de bomberos puede evacuar a los ocupantes a través de sus fachadas. Este tipo de edificaciones además de requerir rociadores automáticos, requieren sistemas de alarma de notificación por voz, presurización en las escaleras de evacuación e iluminación de emergencia, entre otros. ■

Referencias:

[1] *Innovation and Internationalization of Latin American Services, CEPAL, 2016.*

[2] *La Seguridad Contra Incendios en Rascacielos, por Jaime A Moncada, Seguridad en América, Año 19, No. 149, Julio-Agosto 2018.*

[3] *Fire Loss in the United States During 2022 by Shelby Hall, NFPA, November 2023.*

[4] *Fire Protection Handbook, 21st Edition, NFPA, pg. 20-127.*

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

SOCIO DIRECTOR, ALTAIR, SECURITY CONSULTING & TRAINING.

Más sobre el autor:

LA SEGURIDAD EN ENTORNOS DIGITALES Y SU COMPLEJIDAD

LATINOAMÉRICA

No deja de impresionar el incremento brutal año con año de tres dígitos porcentuales del delito de ciberataques en sus diferentes modalidades, no sólo en Latinoamérica sino a nivel mundial.

Hoy más que nunca recibo *spam* en mi *e-mail*, SMS's pidiendo información o mencionando que un paquete no ha sido entregado y que requieren mayor información, contactado por mensajería instantánea por números desconocidos ofreciendo trabajos, haciéndose pasar por terceros, instituciones o personas, llamadas de teléfonos reportados por el delito de fraude que ya no contesto. La lista podría seguir sin parar.

ALGUNOS NÚMEROS Y SU COMPLEJIDAD

En la región de América Latina y el Caribe, se registraron en total más de doscientos mil millones de intentos de ciberataques el año pasado (en números es 200,000,000,000), lo que representa un 14.5% del total global de ciberataques reportados. México registró un total de noventa y cuatro mil millones (94,000,000,000) de ciberataques en 2023, de acuerdo con el laboratorio de análisis e inteligencia de amenazas de Fortinet.

Foto: Freepick

Foto: Freepick

En la región de América Latina y el Caribe, se registraron en total más de doscientos mil millones de intentos de ciberataques el año pasado, lo que representa un 14.5% del total global de ciberataques reportados

Hay una creciente sofisticación y agresividad en las formar de contactar a las posibles víctimas, intentando subir el porcentaje de bateo, ser más eficientes y lograr que más víctimas caigan, con más y mejores impactos

Foto: Freepick

Todas las estadísticas globales desafortunadamente no mencionan una mejoría en la seguridad en entornos digitales; por el contrario, todas enfatizan un nivel ascendente. Hay una creciente sofisticación y agresividad en las formar de contactar a las posibles víctimas, intentando subir el porcentaje de bateo, ser más eficientes y lograr que más víctimas caigan, con más y mejores impactos.

Las estimaciones son que seguirán incrementándose en ese mismo ritmo, más ahora con el apoyo y auge de la Inteligencia Artificial y por lo cual debemos estar atentos, con una conciencia situacional, en un mundo más disperso con gente totalmente distraída y ausente en los diferentes medios electrónicos y el *multitasking*.

BUSCANDO SOLUCIONES

Es claro que las autoridades, locales, regionales e internacionales están totalmente rebasadas ante esta medusa y sus constantes mutaciones, por lo que no podemos sentarnos cruzados de brazos y esperar soluciones en el corto plazo por parte de los gobiernos. Por ello es que acudo, convencido, de nueva cuenta a la cultura de la seguridad, a hacernos corresponsables y responsables de nuestra propia seguridad y aportando dentro de las organizaciones. De lograr una conciencia en seguridad colectiva y alentando a la mejora continua.

Una de las recomendaciones más importantes que puedo compartir es que la gente, la sociedad, aprenda a autoprotegerse. Mientras se implementan en las organizaciones por parte de los expertos en IT toda clase de *firewalls* y otras barreras, además de controles para intentar que los impactos no penetren en las membranas digitales de las organizaciones, el eslabón más débil siguen y seguirán siendo las personas. Si alguien da clic en un enlace incorrecto, si alguien proporciona información privilegiada por los diferentes medios a desconocidos o a conocidos con intenciones no éticas, se abrirán las puertas a los delitos.

Por ello es la importancia de los programas integrales, por un lado sensibilizar continuamente a las personas de los riesgos potenciales y posteriormente otorgarles recomendaciones a través de los diferentes canales, no sólo para su conocimiento sino para influir, motivar, a que las personas lo adopten en sus vidas cotidianas. Que estén convencidos que son parte fundamental de la cadena de seguridad y que su actuar es imperativo para mantener entornos de manor seguridad y tranquilidad. El compromiso por parte de ellos resulta esencial en el logro de los objetivos de seguridad.

No invierto espacio en este artículo proporcionando las decenas de decálogos existentes para evitar que los delitos sucedan y que, en caso de suceden poder reaccionar con calidad, lo que sí quiero enfatizar es la importancia que toda esta cadena conlleva, la importancia de una conciencia situacional y de implementar una cultura de seguridad al interior de las organizaciones.

En los números previos de **SEA**, podrán revisar todas las recomendaciones que hago, de ir de la A a la Z y tener entornos (en este caso digitales) más seguros.

El reto será nuestra capacidad permanente de adaptación a los entornos tan cambiantes de la actualidad. Insistir y nunca desistir. ■

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

PREVENCIÓN Y PROTECCIÓN EN EL *RETAIL*: APLICACIÓN PRÁCTICA DE GEOINT Y TÉCNICAS ANALÍTICAS

Al integrar el GEOINT y el IMINT, no sólo fortalecemos nuestra capacidad de seguridad y vigilancia, sino que también ganamos insights valiosos para la toma de decisiones estratégicas, desde la expansión del negocio hasta la gestión de crisis

Foto: Freepick

MÉXICO ESPAÑA **Germán Sánchez Beltrán**

INTRODUCCIÓN

Los negocios dedicados al *retail* enfrentan nuevos desafíos hoy en día. Ya no sólo es el robo o el fraude. Ahora también hay ataques cibernéticos y cadenas de suministro complejas. En este ambiente que cambia rápido, el análisis de inteligencia es fundamental.

Este artículo explora cómo el análisis estratégico de inteligencia puede redefinir la seguridad en el sector *retail*. Al recolectar información, podemos generar conocimiento específico que nos permite tomar decisiones con menos incertidumbre, lo que se traduce en una menor probabilidad de riesgos en el negocio.

LA IMPORTANCIA DEL ANÁLISIS DE INTELIGENCIA EN EL *RETAIL*: ENFOQUE EN GEOINT Y IMINT

El análisis de inteligencia en el sector del *retail* es una pieza clave en seguridad del negocio y sirve para adaptarse y responder con anticipación a la complejidad de las amenazas. Sin embargo, antes de realizar un análisis sistémico debemos esforzarnos por recolectar información relevante y pertinente.

Existen numerosas formas de recolectar información, pero para el sector del *retail* propondremos el GEOINT y el IMINT como aquellas esenciales en la recolección de esa información pertinente y relevante.

GEOINT: MAPEANDO EL PANORAMA DEL *RETAIL*

La Inteligencia Geoespacial (GEOINT) implica el uso y análisis de datos geográficos para comprender mejor y visualizar físicamente los espacios relacionados con nuestro sector del *retail*.

A través de SIG (Sistemas de Información Geográfica[1]) podemos determinar la ubicación de tiendas, la distribución geográfica de los clientes, patrones de tráfico y accesos, así como la proximidad a posibles amenazas como zonas de alta criminalidad o competidores.

Al emplear el GEOINT, las empresas de *retail*, pueden optimizar la ubicación de las tiendas, planificar de manera eficiente y eficaz las estrategias de seguridad en la distribución, y entender mejor el entorno en el que se opera evitando los Hot Spots[2] que pueden condicionar la operación. Además, el GEOINT permite una planificación más eficiente en casos de emergencia, como desastres naturales o crisis urbanas, asegurando una respuesta rápida y efectiva para proteger tanto a nuestros clientes como a nuestros empleados y activos.


Foto: Freepick

MINT: LA VISIÓN REVELADORA DE LA SEGURIDAD

Por otro lado con la Inteligencia de Imágenes (IMINT) se puede utilizar para monitorear eficazmente las actividades que ocurren dentro y alrededor de las tiendas. Esto no sólo incluye la prevención del hurto o el seguimiento de los movimientos de los clientes, sino también la identificación de patrones sospechosos o anómalos que podrían indicar una amenaza emergente, como la concentración inusual de personas o vehículos.

Además, el IMINT puede ser valioso en la estrategia de navegación de cliente por las tiendas, distribuyendo los *Hot products*[3] en lugares estratégicos sin afectar la experiencia del cliente.

Al integrar el GEOINT y el IMINT, no sólo fortalecemos nuestra capacidad de seguridad y vigilancia, sino que también ganamos *insights* valiosos para la toma de decisiones estratégicas, desde la expansión del negocio hasta la gestión de crisis.

INTEGRANDO GEOINT, IMINT Y TÉCNICAS ANALÍTICAS ESTRUCTURADAS PARA POTENCIAR LA SEGURIDAD EN EL *RETAIL*

Heuer y Pherson proponen ocho bloques de técnicas analíticas estructuradas. Para la particularidad del análisis de Inteligencia en el sector del *retail* nos enfocaremos en el bloque "Evaluación de causa y efecto" y usaremos dos técnicas bien definidas, los juegos de roles y el análisis de sombrero rojo, que conducen a una comprensión más profunda y a la anticipación eficaz de posibles amenazas de este sector productivo.

JUEGOS DE ROLES EN EL CONTEXTO DEL *RETAIL*

Mediante la adopción de juegos de roles, los profesionales de seguridad en el *retail* pueden situarse en la posición de varios actores, como potenciales delincuentes, competidores o incluso clientes. Esta perspectiva les permite anticipar una gama más amplia de amenazas y vulnerabilidades que podrían ser pasadas por alto desde una perspectiva más tradicional. Por ejemplo, al asumir el rol de un delincuente, según los patrones analizados desde el "Dónde opera" (GEOINT) y "Cómo opera" (IMINT) podemos identificar nuestros puntos débiles en materia de seguridad tanto en las tiendas como en los procesos de logística.

ANÁLISIS DE SOMBRERO ROJO PARA LA INTUICIÓN EN SEGURIDAD

En el ámbito del comercio minorista, afirma Hayes (2007), la efectividad de las estrategias de seguridad reside en la capacidad de anticiparse a las acciones del adversario, analizando los antecedentes de pérdida y los programas de protección en vigor, al igual que examinar detalladamente los incidentes de pérdida anteriores.

El Análisis de Sombrero Rojo se enfoca en adoptar la perspectiva del adversario, analizando variables como la ubicación geográfica de incidentes previos y el análisis detallado de imágenes de vigilancia. El objetivo es identificar patrones que el adversario podría explotar, como rutas de suministro predecibles o la presencia de productos de alto valor en áreas con insuficientes medidas de seguridad. De esta manera, en lugar de preguntarse "¿Qué haría yo en su lugar?", el profesional de seguridad se cuestiona estratégicamente "¿Cómo actuaría mi adversario?", lo que permite una asignación de prioridades más efectiva en la gestión de riesgos y el diseño de un sistema de seguridad más sólido e infranqueable.

CONCLUSIÓN

En resumen, la integración del GEOINT y el IMINT con técnicas como los juegos de roles y el análisis de sombrero rojo proporciona al sector del *retail* herramientas avanzadas para una seguridad más efectiva. Esta sinergia no sólo mejora la recolección y análisis de información relevante, sino que también fortalece la capacidad de anticiparse y responder proactivamente a las amenazas, asegurando una operación segura y resiliente en el dinámico entorno del *retail*.

Referencias:

1 Software para reunir, gestionar y analizar datos geográficos.

2 Los puntos calientes, un concepto geográfico, se refiere a lugares (o direcciones) que tienen una alta tasa de delitos denunciados o llamadas de asistencia policial.

3 Artículos de consumo que resultan más atractivos para el delincuente.

- Hayes, R. (2007). Retail Security and Loss Prevention. Palgrave Macmillan.

- Heuer, R. J., & Pherson, R. H. (2015). Técnicas analíticas estructuradas para el análisis de inteligencia. Plaza y Valdés.

Germán Sánchez Beltrán, CEO de KRIMIVA. *Más sobre el autor:*

NUEVO PARADIGMA DE SEGURIDAD: NUEVAS TECNOLOGÍAS Y APLICACIONES

Estamos metidos de lleno dentro de un nuevo paradigma de seguridad, nuevos sistemas de investigación, prevención, protección y respuesta inteligente a los nuevos riesgos y amenazas a enfrentar

Foto: Freepick

ESPAÑA **Manuel Sánchez Gómez-Merelo**

Se hace evidente que vivimos en una sociedad donde el espacio a cubrir es cada vez más grande y el tiempo exigido para las respuestas resulta cada vez más corto, por lo que, los mejores resultados en seguridad que podemos ofrecer radican en nuestra capacidad de adaptación a la globalización y los cambios ante los nuevos retos y exigencias. Los avances tecnológicos y su constante evolución nos dan la oportunidad de desarrollar nuevos métodos, herramientas y habilidades para mantenernos seguros.

La seguridad ya no se encuentra en la estabilidad, sino en nuestra capacidad de adaptación al cambio de los tiempos y a las particulares exigencias de cada caso y momento.

NUEVOS RETOS Y EXIGENCIAS DE SEGURIDAD

Es necesario recordar que estamos ante nuevos retos y exigencias que han aparecido en el escenario generado por la pandemia y por el nuevo orden mundial que ha registrado un incremento sin precedentes de la superficie de exposición, principalmente, por nuevos riesgos y amenazas derivadas del incremento del teletrabajo, el uso de dispositivos no corporativos, la migración al *Cloud*, la globalización de los servicios, la eclosión de Internet de las cosas (IoT), los nuevos conflictos, etcétera.

Un contexto de inseguridad global, donde conceptos como el ciberterrorismo o cibercrimen se encuentran cada vez más presentes en nuestras actividades, lo que exige nuevos desarrollos de mecanismos de ciberseguridad.

Un nuevo campo de batalla digital, el ciberespacio, donde las ciberamenazas, riesgos y vulnerabilidades aumentan, con una creciente actividad, tanto por parte de los Estados (en plena expansión de sus intereses geopolíticos a través de acciones cibernéticas de carácter exploratorio u ofensivo), como de organizaciones terroristas, grupos de crimen organizado y otros actores individuales.

Así, dentro del ámbito de la Unión Europea, el ciberespacio se define, como "el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo". Para esta organización supranacional a la que pertenecemos: "Mantener un ciberespacio abierto, libre y seguro es un reto mundial al que la UE ha de hacer frente junto con los socios y organizaciones internacionales pertinentes, el sector privado y la sociedad civil" (Consejo de la Unión Europea 2013 (12.02) (OR. en) 6225/13).

Frente a nuevos retos y exigencias, en lo referente a los riesgos y amenazas, se debe avanzar en un concepto de seguridad global y conceptual, que, a diferencia de épocas precedentes, se renueva de manera constante, y dentro de un espacio definido por cuatro referentes: circulación, complejidad, contingencia y resiliencia.

En este renovado contexto de las seguridades, es necesario prestar especial atención a los problemas que presentan las interdependencias de seguridad interior y seguridad exterior, procurando esa mayor dedicación de recursos al tratamiento global de los riesgos y amenazas.

NUEVO PARADIGMA DE SEGURIDAD

Estamos ante el planteamiento de un nuevo paradigma afectado por un conjunto de conceptos, tecnologías, métodos y planes con visión y aplicación global ante los nuevos retos y exigencias de seguridad.

Hay que hacer frente a las ciberamenazas a nivel global pues en el actual ambiente internacional, caracterizado por tensiones de baja intensidad, con zonas limitadas de conflictos violentos, la "circulación global" provoca una amplia gama de problemas, entre ellos la seguridad de la información y las comunicaciones, y se debe hacer frente a las ciberamenazas, prevenirlas, analizarlas y combatirlas aportando soluciones y respuestas rápidas para eliminarlas.

NUEVOS SISTEMAS Y TECNOLOGÍAS

En la actualidad, estamos asistiendo a una progresiva convergencia de los sistemas de tecnología de la información (IT) con sistemas de tecnología operacional (OT) y la gestión de la seguridad, utilizados para el control y seguimiento de eventos, procesos, dispositivos e incidencias, realizando ajustes en las operaciones empresariales e industriales, lo que indica que la innovación tecnológica será decisiva en su transformación.

Así, se acelera la convergencia de las prestaciones en la nube, impulsando la aparición de servicios más rápidos y eficientes. Esto está dando lugar a soluciones inteligentes en tiempo real, como un control y una gestión más eficiente de los sistemas de seguridad basados

en la Nube, lo que nos permite disponer de análisis inmediatos y tomar mejores decisiones en la gestión de los sistemas en tiempo real.

Igualmente, en la realización del Sicur 2024 (Salón Internacional de la Seguridad), la innovación y el desarrollo tecnológico han sido los grandes protagonistas de este encuentro profesional donde se abordó la seguridad integral desde cinco grandes áreas (*security*, ciberseguridad, seguridad contra incendios y emergencias, seguridad laboral). Allí han destacado las soluciones de seguridad más innovadoras del mercado, fruto de los últimos avances en investigación, desarrollo e innovación llevados a cabo por las empresas del sector.

En este sentido, cabe destacar la presentación de las tecnologías de Procesamiento de Señales de Imagen con Inteligencia Artificial (AI-ISP), que vienen a revolucionar las imágenes de video y proporcionan visuales de alta calidad gracias a la reducción inteligente del ruido, con imágenes más claras y nítidas en entornos con poca luz, dando lugar a respuestas más orientadas y eficientes. Las nuevas soluciones de seguridad para la autenticación de la identidad digital, la salvaguardia en materia de ciberseguridad y la verificación y autorización de las identidades, constituyen avances fundamentales.

Así mismo la IA está acelerando la transformación del sector de la seguridad al aumentar las capacidades perceptivas de los sistemas. Esto es posible gracias a la integración con tecnologías de luz visible, audio, rayos X, luz infrarroja, radar y otras tecnologías.

Hay que tener en cuenta que las aplicaciones basadas en IA están llamadas a revolucionar diversos sectores, y una preparación que aporte el conocimiento básico suficiente en estas nuevas tecnologías ayudará a reforzar el buen uso y a acelerar las aplicaciones en el ámbito de las seguridades.

No obstante, hay que tener en cuenta que la IA aporta indudables ventajas en la recopilación de información, su tratamiento, la toma de decisiones y la autonomía de sistemas, pero supone grandes desafíos éticos, legales y estratégicos.

La IA ha experimentado avances significativos en las últimas décadas, y su aplicación en el ámbito de la seguridad y defensa ha revolucionado la forma en que los gobiernos y las fuerzas armadas abordan los desafíos contemporáneos. Desde la recopilación de información hasta la toma de decisiones estratégicas, la IA ha demostrado su valía en diversas áreas cruciales para la seguridad nacional.

CULTURA DE SEGURIDAD Y FORMACIÓN

Los profesionales de la nueva seguridad no nacen, se hacen. Así, las habilidades y los conocimientos necesarios para poder utilizar las nuevas tecnologías dentro de este nuevo paradigma de seguridad van a verse reflejadas en la resolución de problemas, la capacidad de adoptar rápidas soluciones o de crear servicios nuevos, eficientes y eficaces, planteados bajo el concepto de una seguridad global, integral e integrada.

Para ello, es fundamental renovarse, salir de nuestra zona de confort e invertir en cultura de seguridad y la consiguiente formación continua especializada, desarrollando capacidades de futuro y cultivando la mentalidad de crecimiento y adaptación a los nuevos retos y exigencias que el importante área de la seguridad requiere.

No tengamos miedo al cambio, pues solo a través de la aceptación y la búsqueda activa de nuevas competencias y soluciones podremos garantizar nuestra seguridad (prevención + protección) en una sociedad en constante transformación. El cambio ya no es una amenaza, sino una oportunidad para crecer y alcanzar nuestro máximo potencial de seguridad. Las nuevas necesidades y los nuevos planteamientos de transformación digital y digitalización, traen nuevas herramientas de gestión operativa en Seguridad Pública y Seguridad Privada y nos desafían a enfrentarnos, con preparación y entusiasmo, a la implantación de nuevas soluciones en sistemas y servicios integrados.

Además, este enfoque de seguridad global aporta una visión más completa a la hora de minimizar las obligaciones inherentes a cumplimientos normativos en España, como es el caso de la Ley de Seguridad Privada (Ministerio del Interior, 2014), la Ley Orgánica de Protección de Datos Personales de Carácter Personal (Ministerio de Justicia, 1999) o la Ley para la Protección de las Infraestructuras Críticas (Ministerio del Interior, 2011).

Sin embargo, hay que tener presente que ninguno de los nuevos planteamientos y soluciones para todos estos nuevos retos y exigencias en materia de seguridad serán posibles sin la revisión, adecuación y adaptación al cambio de la propia reglamentación, que está necesitando adaptarse y cubrir exigencias como: la homologación de tipos de contratistas, certificaciones de sistemas de seguridad, certificaciones en el ámbito de seguridad de la información ante las nuevas amenazas (como el ciberataque o el cibercrimen), nuevas medidas de seguridad y ciberseguridad que debieran normativizarse, así como la adecuación y regulación de la capacitación y formación especializada.

A MODO DE RESUMEN

Estamos metidos de lleno dentro de un nuevo paradigma de seguridad, nuevos sistemas de investigación, prevención, protección y respuesta inteligente a los nuevos riesgos y amenazas a enfrentar.

La complejidad derivada de la globalización y la elevada interconexión (de las seguridades y de las inseguridades) se debe adecuar y contrastar con la situación básica de la seguridad que enfrentan en general las infraestructuras estratégicas y críticas, con incidencia especial en algunos países.

En materia de seguridad, es importante no olvidar y asumir permanentemente la realidad de que no tenemos ni podemos tener todo bajo control. La seguridad total no existe. Por tanto, en lugar de limitarnos a resolver las consecuencias de nuestras vulnerabilidades, promovamos la fortaleza que la inteligencia y la coordinación de los medios y medidas de seguridad pueden proporcionarnos. ■

Manuel Sánchez Gómez-Merelo, consultor internacional de Seguridad y ex-coordinador de Seguridad en Instituciones Penitenciarias. *Más sobre el autor:*

Foto: Freepick

LAS AMENAZAS AMBIGUAS ENELCONTEXTO DIGITAL

Un reto emergente para la gestión del riesgo cibernético

Foto: Freepick

COLOMBIA

Jeimy Cano

El aumento de la densidad digital en el desarrollo de la sociedad actual nos advierte del aumento o propensión a los fallos complejos (Edmondson, 2023). Esto es, una mayor interacción y acoplamiento entre diferentes componentes, puede generar nuevas vulnerabilidades o hacer evolucionar otras conocidas en contextos desconocidos con resultados inciertos, cuya materialización puede generar efectos de contagio basado en pequeñas fallas.

Entender que el riesgo cibernético es sistémico (relacional e interconectado), emergente (surge de las relaciones entre sus componentes) y disruptivo (crea condiciones que lleva a que un proceso o sistema no funcione de la forma esperada), es hacer evidente que nos vamos a enfrentar frecuentemente con amenazas ambiguas, esas asociadas con un riesgo potencial que no está muy claro, y que posiblemente por no tener evidencia suficiente, exista una tendencia natural a restarles importancia (Edmondson, 2023, p.152-153).

Siguiendo las reflexiones de Perrow (1984), a medida que se diseñen sistemas digitales más interconectados y más acoplados, habrá una tendencia a esperar lo que el investigador denomina "accidentes normales", esto es, que algunos sistemas funcionen como "accidentes a punto de ocurrir".

Una interacción de múltiples partes con efectos difíciles de pronosticar y acoplamiento donde uno de los componentes lleva inexorablemente a la reacción de otro, lo que genera un espacio de inciertos e inestabilidades que son parte del diseño de la iniciativa digital y muchas veces inadvertidos durante su puesta en operación, lo que lleva a sorpresas indeseables, muchas de ellas aprovechadas por los adversarios.

En este escenario de alta complejidad (lo que significa que no tenemos la capacidad de indicar y distinguir todas las condiciones del sistemas que modelamos) (Espejo & Reyes, 2016) habrá que motivar múltiples situaciones que pongan a prueba el sistema o iniciativa que se diseña con ocasión de observar su comportamiento y los efectos de borde que se pueden ocasionar por interacciones conocidas y otras por descubrir. En este sentido, las pruebas de mal uso (desde la persona), las pruebas de estrés (frente a la infraestructura), el análisis y validación de vulnerabilidades conocidas (en las aplicaciones), así como las condiciones adversas en la ejecución de los servicios propios de las aplicaciones, serán elementos básicos para hacer más resistente el producto tecnológico que se desarrolla.

Las amenazas ambiguas se revelan y surgen de formas inesperadas por las interacciones entre el almacenamiento, procesamiento, uso y generación de los datos, por lo tanto reconocerlas implica hacerse preguntas incómodas y proponer retos novedosos para desafiar el saber previo que tenemos y crear las condiciones inesperadas que nos permitan capturar datos que si bien pueden confirmar nuestras sospechas, igualmente las pueden desestimar. Lo anterior implica habilitar una ventana de oportunidad o de aprendizaje en la cual la recuperación es factible antes que una falla compleja ocurra (Edmondson, 2023).

Abrir una ventana de oportunidad o de aprendizaje es escuchar a todos los involucrados en la iniciativa con el fin de identificar señales débiles que sugieran que la falla puede ocurrir con el fin de evaluar y responder, claro están entendiendo previamente acerca de lo que puede ocurrir y luego tomar las acciones correctivas que haya lugar. Esto implica, habilitar la posibilidad de aprender rápidamente para descubrir diferentes puntos ciegos (Charan, 2015) que pueda tener la aplicación y desde allí establecer las condiciones de una ejecución (interacción y acoplamiento) más confiable, o menos insegura.

PRÁCTICAS CLAVES

Es importante indicar que las amenazas ambiguas pueden generar igualmente señales falsas o alarmas inexistentes, las cuales pueden generar confusión y demora en los análisis cuando se consideran y no generan valor para la iniciativa (Edmondson, 2023). Es una condición natural de un proceso con alta complejidad, y por lo tanto, habrá que diseñar mecanismos de validación y contrastación que permitan afinar el ejercicio de revisión y evaluación de la mejor forma. Esto es, detectando ágilmente los falsos positivos y falsos negativos, que pueden crear más distracción que foco en un proceso de aseguramiento de una iniciativa digital.

Por tanto, se hace necesario mantener una postura vigilante frente a los inevitables fallos complejos con el fin de avanzar su comprensión y abordaje con el fin de anticipar la mayor cantidad de posibles fallas que se puedan concretar con la iniciativa. En esta línea, Edmondson (2023, p.162) sugiere algunas prácticas claves que aumenten la consciencia situacional de los análisis con el fin de establecer una postura proactiva frente a la complejidad propia de las iniciativas. Dichas prácticas se concretan en tres momentos: enmarcar, amplificar y practicar.

1) **Enmarcar** implica enfatizar en la complejidad de la iniciativa digital o su novedad que le permite explorar y estar atento a las diferentes

condiciones no estándar que se pueden presentar en el momento de su diseño y puesta en operación. Cada elemento interno del diseño combinado con las interacciones externas propias de la implementación generan escenarios distintos de análisis que deben ser analizados y revisados para encontrar patrones o eventos que puedan afectar directamente su ejecución. El marco general de pruebas no debe destinarse a probar lo que se espera haga la aplicación, sino a generar comportamientos inesperados por interacciones imprevistas.

2) **Amplificar** es identificar y darle visibilidad a las señales débiles reveladas por los participantes de la iniciativa. Esto no significa exagerar o demorar el proyecto de manera indefinida, sino asegurarse que la advertencia o indicación que se hace sea escuchada, es decir, se considere como una forma en la cual se puede concretar un fallo complejo. En la medida que se amplifiquen estas voces habrá mayor cantidad de elementos para analizar que en últimas beneficiará la implementación, disminuyendo la condición de "accidente normal" o condición de falla esperada que se cuenta en sistema de interacción y acoplamiento de plataformas digitales con múltiples actores y múltiples conexiones.
3) **Practicar** implica identificar y afinar constantemente las buenas prácticas de desarrollo y aseguramiento de aplicaciones. Lo anterior no implica que no se pasen errores, sino que se afina el olfato para la cacería de los mismos con el fin de refinar el producto final haciéndolo más resistente a los fallos y sobremanera, mejor preparado para cuando se ejecute en una condición inesperada.

En este ejercicio, la postura de falla segura adquiere un valor fundamental comoquiera que la aplicación se prepara para detener la ejecución y ubicarse en una condición controlada, donde queda aislada y desligada de los permisos de acceso y con una operación limitada donde el adversario no tiene opciones de escalar o avanzar en la infraestructura donde ésta opera.

VALORAR LAS FALLAS

Enfrentar las amenazas ambiguas en el contexto del riesgo cibernético implica reconocer igualmente que se pueden alinear las diferentes fallas complejas en momentos específicos, lo que sugiere indefectiblemente la materialización de un evento desafortunado. Por tanto, se hace necesario todo el tiempo establecer y valorar las condiciones latentes de falla (Reason, 1997), que se materializan cuando se efectúan ajustes o cambios en las aplicaciones o en las arquitecturas donde éstas funcionan, lo que necesariamente obliga a revisar nuevamente el escenario de ejecución dado que las condiciones han cambiado.

Subestimar un cambio, o ignorar una señal débil puede marcar el inicio de un desastre al final, pues la evolución de la falla compleja tanto en la interacción como en el acoplamiento de la iniciativa digital, puede derivar en efectos que no se pueden anticipar dado el recorrido asimétrico de interacciones y condiciones inéditas que se van a materializar (Zukis *et al*., 2022) En consecuencia, por más que queramos identificar y controlar la evolución de la condición adversa, ella ganará más espacio entre aquellas conexiones ignoradas en su diseño e implementación, generando más desconcierto y confusión en todos aquellos que han hecho parte incluso de su diseño.

Afirma la profesora Edmondson (2023, p.122), "errar es de humanos, prevenir las fallas básicas, es divino", lo que implica que las iniciativas digitales deben responder y asegurar las vulnerabilidades básicas, esas que han sido reconocidas y son propias de los errores técnicos tradicionales, para que al interactuar con otros componentes, sean otras la condiciones a evaluar en su nueva relación, y no recabar en condiciones iniciales básicas que deben estar atendidas desde el inicio. Hacer las implementaciones y pruebas fundamentales desde el inicio para reducir el factor de riesgo conocido en las aplicaciones e infraestructura.

Lo anterior se traduce en hacer menos atractiva la organización y sus iniciativas a los adversarios. En la medida que los agresores encuentren que aquello fundamental en la seguridad/ciberseguridad de los diferentes elementos de la iniciativa digital están asegurados: infraestructura, aplicaciones, servicios y comportamientos, podrán generar un efecto disuasivo que redunde en la pérdida del interés de los adversarios en sus desarrollos, pero no un cambio en sus intenciones de generar inestabilidad, incierto y caos, la cuales posiblemente se trasladarán a otro objetivo (Zeijlemaker, 2022).

Las amenazas ambiguas no aparecen en reportes consolidados de tendencias o documentos de industria, son específicas y propias de cada implementación, pues responden a los efectos sistémicos inherentes del riesgo cibernético que se esconde en cada una de las interacciones y acoplamientos dispuesto en las iniciativas digitales diseñadas y puestas en producción.

Así las cosas, cada organización deberá mantener un mapa del territorio digital que tiene en su ecosistema tecnológico con el fin de evaluar de forma permanente sus amenazas ambiguas, las cuales todo el tiempo van a interrogar los resultados de sus análisis de riesgos y por tanto, levantar alertas tempranas que lleven bien, a tomar acciones preventivas o anticipativas que eviten la materialización de dicha amenaza, o a incorporar capacidades resilientes que permitan mitigar los daños, amortiguar los efectos adversos y hacer más flexible la operación. ■

Referencias:

- *Charan, D. (2015). The attacker's advantage. Turning uncertainty into breakthrough opportunities. New York, USA: PublicAffairs.*
- *Edmondson, A. (2023). Right kind fo wrong. The science of failing well. New York, USA: Atria Books.*
- *Espejo, R. & Reyes, A. (2016). Sistemas organizacionales. El manejo de la complejidad con modelo del Sistema viable. Bogotá, Colombia: Ediciones Uniandes–Universidad de Ibagué.*
- *Perrow, C. (1984). Normal accidents. Living with high risk technologies. USA: BasicBooks.*
- *Reason, J. (1997). Managing the Risks of Organizational Accidents. Abigdon, Oxon. England: Routledge.*
- *Zeijlemaker, S. (2022). Managing the dynamic nature of cyber security. A future-proof strategy, this is how it works. Netherlands. Disem Institute.*
- *Zukis, B., Ferrillo, P. & Veltos, C. (2022). The great reboot. Succeeding in a complex digital Word under attack from systemic risk. Second edition. USA: DDN Press.*

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:*

DECÁLOGO DE ASPECTOS LEGALES QUE RESPALDAN AL PERSONAL OPERATIVO DE SEGURIDAD PRIVADA

Conozca los requisitos legales y normativas que debe cumplir

Foto: Freepick

MÉXICO

Dante García Martínez

El conocimiento de la legalidad desde la constitución de una empresa de seguridad privada es fundamental para salvaguardar la integridad de ésta y la operatividad, así como hacer de conocimiento a todo el personal operativo sobre quiénes son aquellas instituciones o entidades que los respaldan en su actuar y como empresa de seguridad privada.

1. **La Constitución Política de los Estados Unidos Mexicanos:** garantiza la legal existencia de la actividad "Seguridad Privada".
2. **La Ley Federal del Trabajo:** da certeza a tu relación laboral.
3. **El Reglamento Interior de Trabajo:** fortalece tu relación hacia el interior de tu empresa.
4. **La Ley Federal de Seguridad Privada:** establece las condiciones y requisitos que debes cumplir, para laborar en la Industria de la Seguridad Privada.
5. **La Secretaría del Trabajo y Previsión Social:** constata la capacitación y profesionalización de la materia.
6. **El Código Penal Federal y sus correlativos:** tipifican y sancionan los delitos cometidos por intención u omisión, en mi actividad.
7. **La Comisión Nacional de Derechos Humanos:** es el árbitro autónomo, ante la violación de Derechos Humanos, que hayan cometido los representantes de las autoridades a nivel federal.
8. **El sector salud:** brinda ayuda en materia de salud, en todo momento a la población, independientemente de la afiliación o como derechohabiente; lo que permite y obliga a acudir a estos en caso de necesidad, propia o de terceros.
9. **Los tribunales de justicia:** dirimen las controversias, juzgan y sancionan, acorde a su materia en atención a los derechos reclamados.
10. **La conciliación y la heterocomposición:** son siempre las mejores opciones como soluciones alternas a los conflictos entre partes. ■

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

GSI
SEGURIDAD PRIVADA

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

Profesionales en Seguridad Privada

Oficiales de Seguridad

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

SOMOS GRUPO GSI,
Orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx

atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

ESR Empresa Socialmente Responsable

redconocer

DNV

AMESP

EMPRESAS DE GSI GRUPO SEGURIDAD INTEGRAL

BASC

EL DESARROLLO DE UNA ESTRATEGIA DE NEGOCIO… ¿Y LOS RIESGOS?

Grupo DILME amplía su portafolio de servicios con la apertura de una nueva dirección

Foto: Freepick

MÉXICO

Con gran responsabilidad una estrategia de negocio se genera en el ámbito de la gestión y planificación en prácticamente cualquier empresa, ya sea en proyectos, expansión o en la evaluación de políticas públicas. Su importancia radica en la capacidad de identificar, evaluar y priorizar riesgos potenciales antes de que estos se materialicen, permitiendo a los responsables tomar decisiones informadas para mitigar o eliminar los impactos negativos en los objetivos planteados.

Este proceso implica no sólo la identificación de los riesgos inherentes a una actividad o proyecto, sino también la evaluación de la probabilidad de que ocurran y el impacto que tendrían en caso de materializarse. De esta manera, se pueden desarrollar estrategias de prevención y respuesta más efectivas, optimizando recursos y reduciendo la incertidumbre. Es un enfoque proactivo que tiene un especial enfoque en asegurar la continuidad y el éxito en la ejecución de proyectos o en el desarrollo de políticas y estrategias organizacionales.

Además, un análisis de riesgo adecuado contribuye a la creación de un entorno de trabajo más seguro, mejora la confianza de los *stakeholders* y puede ser un requisito para el cumplimiento de ciertas normativas y estándares de calidad. En un mundo cada vez más complejo y cambiante, esta herramienta se convierte en un componente crítico para la toma de decisiones estratégicas, ayudando a navegar por el panorama de incertidumbres con mayor seguridad y eficacia.

Adrián G. Charansonnet, colaborador del área Análisis de Riesgo

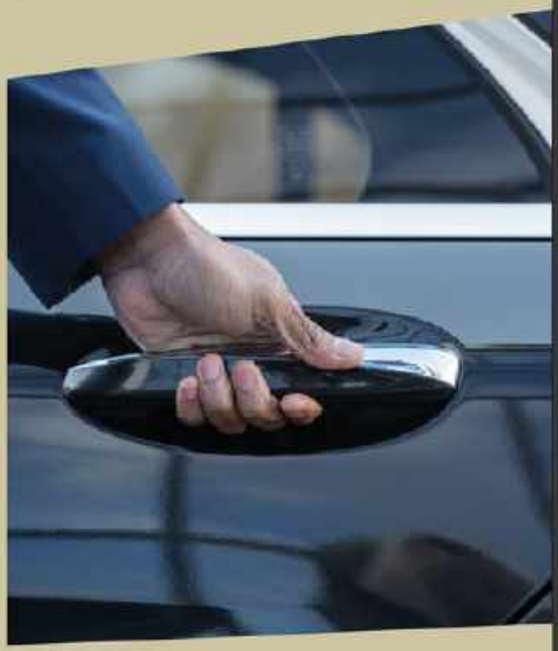
Sergio E. Loyola, director de Análisis de Riesgo

DIRECCIÓN DE ANÁLISIS DE RIESGO

Por ello y en adhesión al portafolio de servicios de Grupo DILME, se ha desarrollado en beneficio del entorno de la seguridad privada en México y Latinoamérica una estructura que permite dar inicio a las operaciones de la Dirección de Análisis de Riesgo. Con ello, Grupo DILME fortalece sus capacidades y pone a disposición de sus clientes actuales y futuros procesos de análisis, identificación y diagnóstico de riesgos como base para planes de mejora en prácticas preventivas.

Bajo la dirección del comandante Hugo Alcántara, en la Dirección de Análisis de Riesgos, colaboran Adrián G. Charansonnet y Sergio E. Loyola con los protocolos de análisis de riesgos, mejores prácticas preventivas, seguridad financiera y continuidad de negocios. ■

Fuente: DILME



SEGURIDAD ESPECIALIZADA

En la vanguardia de la seguridad empresarial, nos comprometemos con la excelencia en cada paso. Nuestra misión es superar las expectativas de nuestros clientes, elevando continuamente nuestros estándares de seguridad y calidad, adaptándonos con precisión a sus necesidades.

Estos son nuestros servicios de seguridad especializada :

- Protección ejecutiva.
- Servicio en más de 100 ciudades en el mundo.
- Integramos servicios de PE terrestres y aéreos en un solo lugar.
- Seguridad de integridad física y personal.
- Pase diplomático en aeropuertos de México.
- Vehículos Blindados.
- Análisis y seguimiento de ruta en tiempo real 24/7.

https://www.jvplogistica.com/

/jvplogistica

@jvplogistica

55 81 08 05 87
55 25 51 28 17

JVP
LOGÍSTICA

ENCUENTRO DE SEGURIDAD **FARMACÉUTICA 2024**

Más de 100 asistentes, 10 especialistas en seguridad, ocho horas de aprendizaje y networking y más de 20 años de experiencia organizando eventos académicos y comerciales: **SEA**

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Seguridad en América Academy llevó a cabo el "Encuentro de Seguridad Farmacéutica 2024" el 25 de abril en el Hotel Courtyard by Marriott de la Ciudad de México, el evento estuvo dirigido por Samuel Ortiz Coleman, director general de SEA, y contó con la participación de diferentes especialistas en seguridad que han desarrollado sus conocimientos y experiencia en la industria farmacéutica.

Este Encuentro es un foro de aprendizaje y *networking* en el que los más de 100 asistentes pudieron conocer los principales riesgos de seguridad de dicha industria, los retos a los que se enfrenta actualmente y las diferentes tecnologías que coadyuvan en la prevención y reacción ante cualquier incidente de seguridad. También se contó con el el patrocinio de SEPSISA, Protege, Grupo IPS, y Multiproseg; además de la colaboración con la Cámara Nacional de la Industria Farmacéutica (CANIFARMA).

PANEL DE EXPERTOS

El primer panel de especialistas llevó por título "La sinergia de esfuerzos para la protección del paciente" y estuvo integrado por Nery Ayala González, *Head of Investigation* en Laboratorio Merck; Octavio García Peregrina, CPP, gerente de Seguridad y Protección en Farmacéuticos Maypo; Héctor Hernández Castelán, *Head of Security* en Takeda; Eduardo Téllez, CPF, director de Seguridad en Liomont; Jesús Islas, *Country Security Lead* en Novartis, presidente de la Canifarma; y Gerardo Corchado Chávez, asesor de Seguridad Corporativa en Canifarma.

Para dar inicio al panel, Gerardo Corchado bajó del escenario para explicar los diferentes riesgos a los que la industria farmacéutica se enfrenta, uno de ellos y de gravedad, es la falsificación de medicamentos, para ello mostró algunos ejemplos de cómo la delincuencia sustituye o recrea las cajas, las botellas, empaques, sustancias, soluciones y las vende en el mercado negro como medicamento original. Y el problema, como lo recalcó el especialista, el principal problema es que si el medicamento falsificado llega al paciente, éste pone su salud en riesgo y le puede provocar la muerte. De ahí que los integrantes del panel coincidieron en que el objetivo principal de los responsables de Seguridad en esta industria, es la seguridad de los pacientes, que el medicamento llegue al paciente en óptimas condiciones y así contribuya a la salud de cada uno.

Otro de los aspectos que se abordaron en el panel que fue moderado por Nery Ayala, fue la importancia de la creación de una cultura de seguridad tanto al interior de las empresas, como en la sociedad, para comprender la magnitud del daño que ocasiona la producción y venta de medicamento falsificado. Por su parte, Eduardo Téllez, añadió cinco servicios críticos que como seguridad en la industria farmacéutica deben tener siempre cuidando y protegiendo: agua, drenaje, electricidad, gas y telecomunicaciones; además de la reputación e imagen de la marca. Gerardo Corchado invitó a los asistentes a "ser héroes", a contribuir con la salud y la seguridad de los pacientes, a comprender la importancia de su papel en la industria y actuar con responsabilidad, de manera profesional e inteligente cuando se les presente algún incidente.

Otro tema que abordó el mismo panel de especialistas, pero ahora moderado por Samuel Ortiz Coleman, fue el de los retos y desafíos

de la seguridad en el sector farmacéutico. Octavio García Peregrina fue el encargado de dar una introducción sobre la situación de la industria farmacéutica y los retos a los que se enfrenta este sector en la actualidad, los cuales enumeró de la siguiente manera y desarrolló un esquema de acuerdo a sus conocimientos y experiencia:

1) **Cumplimiento normativo y regulaciones.** El sector farmacéutico está sujeto a regulaciones y estándares, tanto a nivel naclonal como internacional. Mantener el cumplimiento de estas normativas es un desafío, especialmente debido a los cambios frecuentes en la legislación y los requisitos regulatorios.
2) **Cadena de suministro/ globalización.** Altamente compleja y globalizada, con múltiples proveedores, fabricantes y distribuidores. Gestionar la seguridada lo largo de esta cadena puede ser difícil debido a la diversidad de procesos que se deben cuidar.
3) **Amenazas cibernéticas y tecnológicas.** En la industria farmacéutica, las amenazas cibernéticas representan un riesgo cada vez mayor. La seguridad de los datos y los sistemas informáticos es crucial para proteger la propiedad intelectual, la informacion del paciente y la integridad de los procesos de fabricación.
4) **Innovación y reducción de costos.** Se debe innovar y desarrollar la seguridad para atender los riesgos. Al mismo tiempo, debemos reducir los costos y mejorar la eficiencia en la distribución, lo que puede afectar negativamente a la inversion en seguridad y calidad.

Ante estos retos, el especialista compartió algunas estrategias de seguridad, por ejemplo, proporcionar información regular sobre seguridad y concienciar al personal sobre los riesgos y la importancia de cumpilir con los protocolos de seguridad establecidos. Así como implementar tecnologías avanzadas de seguridad, como sistemas de gestión de riesgos, sistemas de seguridad de la cadena de suministro y soluciones de ciberseguridad, para proteger los activos y datos de la empresa contra amenazas, entre otras. Los demás participantes del panel, compartieron sus experiencias, casos de éxito y sugerencias para que puedan mejorar la efectividad de las estrategias de seguridad en la industria.

CICLO DE CONFERENCIAS COMERCIALES MULTIPROSEG

La primera conferencia comercial del día, estuvo a cargo de Armando Vega, gerente comercial de Multiproseg quien platicó acerca de los servicios y principales diferenciadores de la empresa de seguridad privada a la que pertenece. Armando realizó un cuestionario a los asistentes que incluyó preguntas acerca de la normatividad, los organismos que interfieren en los diferentes procesos del área de Seguridad, la perspectiva que tienen de la seguridad privada en la industria farmacéutica, entre otros aspectos.

Una vez concluida la encuesta y premiado a la participante con mayor puntuación, el gerente comercial presentó los servicios de Multiproseg, los cuales son:

- Técnico en Seguridad Privada y Vigilancia.
- Custodias de Transporte.
- Sistemas Electrónicos de Seguridad.
- Análisis de Riesgos.
- Monitoreo.

Y recalcó que Multiproseg es un socio comercial que ofrece servicio personalizado, calidad, procesos y control, capacitación constante, experiencia en el mercado de más de 18 años a nivel nacional, y sobre todo, que cuenta con diferentes certificaciones, entre ellas, ISO 50001, y BASC (Business Alliance for Secure Commerce).

PROTEGE

La siguiente ponencia la dirigió el comandante Juan Manuel García Coss, presidente ejecutivo de Grupo Corporativo de Prevención (GCP) y de la empresa de seguridad privada armada, Protege, la cual tiene experiencia en el sector farmacéutico con una transnacional alemana que es la más antigua del mundo, fundada en 1668, con la que colaboró por nueve años; así como una farmacéutica que llegó a México en 2012, la más impórtate en Japon, con presencia en más de 80 paises y regiones, fundada en 1781 y de la que fue responsable de su seguridad por seis años. Durante ambos servicios no hubo quebrantos, y las situaciones de riesgo estuvieron controladas.

El comandante García Coss, presentó tres videos impactantes sobre el ataque de delincuentes a la custodia de transporte, los cuales, gracias a su capacitación, lograron evadir a los agresores, actuando, primero, con alerta telefónica al Centro de monitoreo, y después reaccionando con armas y manejo evasivo. Aquí destacó la importancia de la selección de personal para este servicio armado, así como la ca-

pacitación y los elementos con los que son enviados a custodiar. Explicó las cinco etapas del blindaje, entre ellas, el monitoreo activo y dedicado las 24 horas de los 365 días del año; el mantenimiento preventivo y correctivo de unidades operativas para su correcto funcionamiento; y algunas medidas de prevención.

SEPSISA

La tercera conferencia comercial la dio Mónica Molina, socia y directora comercial de SEPSISA, empresa de seguridad privada que cuenta con más de 20 años de experiencia en el mercado y que logró la Certificación Internacional de Calidad ISO 9001-2015, manteniendo sus procesos bajo los estándares de calidad, mismos que son auditados semestralmente.

Los servicios que SEPSISA ofrece son: guardias de seguridad, Circuito Cerrado de Televisión (CCTV), Cercas electrificadas, alarmas de seguridad, seguridad canina, rastreo satelital GPS, Control de Acceso para Personas y Vehículos, y Custodia de Mercancías.

Algo que caracteriza a Sepsisa es el proceso de selección, capacitación y certificación de cada elemento de seguridad, los cuales están regulados bajo los lineamientos de que marca la Secretaría del Trabajo y Precisión Social (STPS) y registrados ante la Secretaría de Seguridad y Protección Ciudadana (SSPC) federal.

La selección del personal está realizada por psicólogas profesionales nales que aplican diferentes exámenes de personalidad, honestidad e inteligencia, además de otras pruebas y requisitos de contratación.

IPS

La última conferencia comercial la impartió Jorge Uribe Maza, director comercial en Grupo IPS de México, quien expuso el tema "La seguridad y la persona: la integridad dentro de las organizaciones". "La inseguridad es la principal preocupación de muchos mexicanos. Solemos caer en versiones dicotómicas, donde dividimos a la sociedad en buenos (nosotros) y malos (los que ya vienen así y su lugar está en la prisión). También caemos en conclusiones fáciles, como que el crimen organizado es una creación de nuestros gobernantes corruptos. La responsabilidad de proveer seguridad a la sociedad está en las policías y los jueces, pero al no ser confiables, estamos desamparados", indicó.

Jorge Uribe invitó a los asistentes a reflexionar sobre quién tiene en sus manos el cambiar la seguridad, si las organizaciones o los ciudadanos. También recordó cómo han sido los modelos de la fuerza e inteligencia policial y cómo la seguridad privada coadyuva con las autoridades y para la salvaguarda de las personas y los bienes materiales.

Concluyó con éxito el "Encuentro de Seguridad Farmacéutica", esperando que el próximo año mantenga y mejore las expectativas de los asistentes. ■

Fotos: Mónica Ramos / SEA

MEXSEPRO

SEGURIDAD Y PROTECCIÓN DE MÉXICO

Somos tu
[SEGURIDAD | Inteligente]
mexsepro.com

La NUEVA GENERACIÓN en SEGURIDAD PRIVADA

GUARDIAS de Seguridad Privada

CUSTODIA y Patrullaje para de mercancias

SISTEMAS en Seguridad Electrónica

ALARMAS y Monitoreo CCTV

CONSULTORÍA Integral en Seguridad

ISO 9001:2015 · COPARMEX CIUDAD DE MÉXICO · AMESP · ASIS INTERNATIONAL · CÁMARA DE COMERCIO · red conocer · AMEXSI · REPSE

Nuestras nuevas oficinas corporativas SP MEXSEPRO

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

- mexsepro.com
- (55)65854448
- (55)4141 8573
- facebook.com/MEXSEPRO
- instagram.com/mexsepro
- twitter.com/spmexsepro

CONVENCIÓN SEPSISA 2024: 20 AÑOS DE ESFUERZOS Y EVOLUCIÓN

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

SEPSISA, empresa mexicana de Seguridad Privada, llevó a cabo su primera Convención interna en el Hotel Sheraton de Guadalajara, Jalisco, del 12 al 15 de junio, en la que reunió a más de 200 colaboradores de la compañía provenientes de distintas ciudades, entre ellas, Ciudad de México, Ecatepec, León, Cancún, Coahuila, Ciudad Juárez, Puebla, Villa Hermosa, Mérida y, por supuesto, de la Perla Tapatía, entre otras. El objetivo, convertirse en la mejor empresa de seguridad privada del país, en al menos tres años, meta que externó de forma emotiva y con seguridad, Saturnino Soria, director general de SEPSISA.

La Convención inició con una cena de gala, en la que los asistentes fueron recibidos con música y un salón ambientado que denotaba la importancia de que ellos estuvieran ahí, de que son parte de la empresa y que de ellos también depende el rumbo de ésta. Antes de abrir la pista de baile, amenizada por un DJ, Saturnino Soria agradeció a todos los asistentes por formar parte de este momento histórico de la compañía, ya que en el mes de junio celebraron sus primeros veinte años de existencia. "Este evento lo preparamos para todos ustedes, y el objetivo es que, a través de las conferencias, de las charlas que vamos a presenciar estos días, aprendamos nuevas prácticas y mejoremos las que ya sabemos, porque la meta es ser la mejor empresa de seguridad privada de México y lo vamos a lograr".

La Seguridad Privada, destacó Saturnino Soria, representa casi el 2% del Producto Interno Bruto (PIB) de la economía mexicana, también genera más de un millón de empleos directos, de los cuales, 600 mil son oficiales de seguridad, cifra muy por encima del número total de la fuerza policial del país, lo que refleja el grado de importancia de este sector, y que, a través de capacitación, aprendizaje, y dando lo mejor para su empresa, es como se logrará el objetivo.

"En SEPSISA somos una gran familia, y yo lo que quiero es que se queden, que permanezcan en ella, que se sientan parte de ella, que hagan una carrera aquí y que nos propongamos metas y las logremos. La más inmediata, a partir de hoy, contribuir cada uno desde su área para lograr la certificación Great Place to Work (GPTW)", señaló.

SEPSISA cuenta con la certificación ESR (Empresa Socialmente Responsable), así como en ISO 9001 (calidad en el servicio), y BASC (Business Alliance for Secure Commerce–gestión de control en los procesos), y este año comenzará a trabajar para obtener la certificación "Great Place to Work", la cual reconoce que la empresa crea la mejor experiencia para sus colaboradores, y que en México, sólo tres empresas de seguridad privada, tienen esta certificación.

CONFERENCIAS

El primer día estuvo lleno de magia, sí, de la magia de Disney, ya que desde que los asistentes ingresaron al Salón "Patricia Elton", del hotel, en sus sillas los esperaban una diadema de orejas de Mickey Mouse y unas burbujas, esto porque Beatriz Arcos, psicoterapeuta, impartió la charla "La magia del servicio al cliente. El Modelo Disney". Este modelo, explicó la especialista, está basado en la experiencia del servicio al cliente, en los detalles que marcan la diferencia en una persona y personalizan su estadía en el parque, que de por sí, genera infinidad de emociones. Les reiteró la importancia que tiene desde un saludo hasta un servicio de seguridad, con diferentes dinámicas, así como recordar poner su total atención en la otra persona, y tener presente el propósito, los valores y la promesa que ofrece SEPSISA a sus clientes: seguridad y tranquilidad.

El segundo día contó con dos conferencias magistrales y la participación de las diferentes áreas de la empresa. La primera magistral fue impartida por Gildardo Avendaño Osogobio, reconocido conferencista empresarial, que enfocó la atención de los asistentes en la importancia de un líder, de una buena comunicación, actitud positiva, y llevó por nombre: "La maestría

está en los detalles". Una conferencia emotiva, reflexiva y la cual fue bien recibida por sus escuchas.

Para hablar sobre los procesos del área Comercial, fue Mónica Molina, socia y directora comercial de SEPSISA, quien explicó desde la historia de la compañía, hasta los pasos que se deben dar para lograr la venta y ejecución de un servicio de seguridad: Reclutamiento, Selección, Contratación, Capacitación de los oficiales de seguridad, y el cómo cumplir con lo pactado con el cliente y superar sus expectativas. El día continuó con Sonia Montesinos, directora de Capital Humano, quien les informó que la meta de este año es lograr certificarse como Great Place to Work, y la necesaria participación de todos para lograrlo.

Por su parte, Rodolfo Serrano, del área de Operaciones, compartió la importancia de los planes de seguridad, análisis y gestión de riesgos en esta área, explicando que en el año 2017, se realizaban 253 custodias al año, mientras que a finales de diciembre del 2023, fueron 36 mil 768 custodias con un porcentaje de 0.001% de incidencias, es decir, SEPSISA cuenta con un 99.9% de efectividad, gracias a estándares como BASC, y la elaboración de Procesos efectivos, así como el trabajo del Centro de Inteligencia Logística (CIL), que permite dar respuesta inmediata, conocer la trazabilidad de los servicios, y lo único que les pide es más empatía con la base de la empresa: los oficiales de seguridad.

También dentro de esta área se encuentra Desarrollo Organizacional, que son quienes le dan voz a todos los colaboradores de SEPSISA, que comparten su experiencia, y buscan mejores oportunidades de desarrollo profesional, este Departamento está liderado por Isabel Nevares, de la oficina de León, Guanajuato, y quien con su equipo, organizaron parte importante de la Convención, que se pudo ver, precisamente, en los detalles de cada día.

Una parte fundamental para el crecimiento de SEPSISA, es el trabajo que diferentes áreas críticas han realizado, el área de Administración, encabezada por Edmundo Valverde; así como el área de Auditoría y del Centro de Inteligencia y Logística y Control Vehicular, a cargo de Lorenzo Briones; el área Legal, con Max Duarte; y en el área Contable, Héctor Sánchez, quien destacó que en los seis años que tiene formando parte de SEPSISA, ha presenciado un crecimiento de 300%.

La última conferencia estuvo a cargo de Gerardo Corchado, especialista certificado en seguridad y conferencista, con la plática "El camino del héroe", en la que habló sobre qué es seguridad, la actitud que tenemos, la imagen que damos, la calidad en el servicio al cliente y el orgullo de pertenecer a SEPSISA. A través de una gran charla motivacional, respaldada por la experiencia de más de 25 años en el sector, Gerardo Corchado demostró cómo provocar el sentimiento de pertenencia cuando comenzó a desabotonar su camisa y, como súper héroe, apareció en su vestimenta una playera con el logo de SEPSISA: "Siéntanse parte de la mejor empresa de seguridad privada de México", finalizó.

TORNEO INTEROFICINAS SEPSISA 2024

Para cerrar la Convención SEPSISA 2024, se realizó la tercera edición del "Torneo Interoficinas" de futbol en el campo de la fábrica Philip Morris International, en las categorías femenil y varonil, siendo el equipo de "Valquirias" (Barranca del Muerto) quien ganó el primer lugar por parte de las mujeres; en segundo lugar, "Amazonas" (Capital Humano). Por parte de los hombres, el primer lugar se lo llevaron "Los Tlacuaches" (Capital Humano); en segundo lugar, "Real de Cuautitlán" (Cuautitlán Izcalli). En total fueron ocho equipos de hombres y tres de mujeres los que participaron en el torneo.

Después de la esperada premiación, el director general les hizo entrega de unos reconocimientos y un incentivo económico a algunos custodios de blindadas que se encuentran en Guadalajara, por su labor y esfuerzo heroico, también pidió un minuto de silencio para el custodio que lamentablemente falleció en un servicio.

Antes de despedir a los asistentes, Saturnino Soria les informó que el siguiente año se realizará de nuevo la Convención, pero en un destino de playa, así sean los mismos 200 o 500 asistentes, esta convención está planeada para motivar a que todos y todas contribuyan con el objetivo primordial de SEPSISA, que es el de llevar seguridad y tranquilidad a sus clientes, bajo los principios de: confianza, lealtad, respeto y entrega. ■

Fotos: Mónica Ramos / SEA

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

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

MÉXICO | **Hermelindo Rodríguez Sánchez**

Foto: Freepick

CONTROL DE MONITOREO DE VIDEOVIGILANCIA

Objetivo: establecer los lineamientos, responsabilidades y alcance que deben observar los elementos de Seguridad en las instalaciones, en la realización de actividades de videovigilancia mediante el Circuito Cerrado de Televisión.

Alcance: este procedimiento aplica en apoyo a las medidas de Prevención, Seguridad e Higiene de la empresa.

Definiciones:

- **CCTV:** equipo de videovigilancia, denominado circuito cerrado de televisión.
- **Monitor:** el monitor o pantalla de ordenador, aunque también es común llamarlo "pantalla", es un dispositivo de salida que, mediante una interfaz, muestra los resultados del procesamiento de una computadora.
- **Área:** cantidad de espacio en una superficie delimitada.

Lineamientos:

1) Conocer las áreas de vigilancia monitoreadas por el CCTV.
2) Permanecer alerta ante las situaciones que se observan a través de la videovigilancia la actividad de monitoreo.
3) Registrar todas las desviaciones de las normas y procedimientos de seguridad dentro de las instalaciones.
4) La observación por medio del monitor debe realizarse a todas las áreas que cuentan con cámara de CCTV. El área de cobertura se incrementa observando los detalles de fondo de las imágenes.
5) Se debe poner atención a las áreas de mayor riesgo.
6) Es importante que todas las desviaciones a las normas y procedimientos de seguridad sean reportadas de forma inmediata al área correspondiente, solicitar el respaldo de las video grabaciones al personal de Sistemas o de TI.
7) Es importante resaltar la importancia de reportar de forma inmediata situaciones como:
a) Identificar al personal de áreas de producción que no porte de manera correcta o completa el equipo de protección personal EPP en horas de trabajo.
b) Detectar al personal que por estar divagando en sus áreas de trabajo provoquen un accidente.
c) Observar las omisiones a las instrucciones del uso de maquinaria y/o equipo provoquen alteraciones a la producción.
d) Personas sospechosas que deambulen por las zonas perimetrales.
e) Vehículos sospechosos estacionados por largos periodos, cerca de las instalaciones.
f) Situaciones irregulares que representen un riesgo para la seguridad de la empresa y sus colaboradores.
8) El Centro de Monitoreo es un sitio de carácter restringido, por lo tanto, a él pueden ingresar exclusivamente personal autorizado de la empresa, el jefe de Servicio, el jefe de Turno y el Administrador del Sistema.
9) En este Centro de Control se procesa toda la información y reportes del área de Seguridad y Vigilancia. El personal operativo es el responsable de distribuir

Foto: Freepick

y archivar los reportes y la papelería correspondiente a los controles dispuestos por la Dirección y sus colaboradores.

10) Documentar el procedimiento del monitoreo del CCTV sirve de apoyo con las funciones de control y vigilancia en el área de cobertura de los sistemas de seguridad electrónica con el propósito de reforzar la seguridad en las instalaciones.

11) Cuando se presente una novedad que requiera el seguimiento por medio del sistema de videovigilancia, es necesario buscar la evidencia, y el seguimiento en el orden cronológico de la misma. El operador de CCTV será el encargado de generar un informe por escrito, con todos los detalles respectivos de fecha, hora, seguimiento de cámaras, investigación de posiciones de oficiales, etc.

12) Cuando un oficial, de cualquier posición observe una irregularidad, deberá informar inmediatamente al Centro de Monitoreo para ubicar la cámara más cercana y tomar evidencia de la novedad reportada. Al momento, el jefe de Servicio y/o jefe de Turno debe informar vía radio al gerente de Seguridad o a la Dirección para recibir indicaciones y seguimiento.

13) En caso de algún incidente de seguridad que requiera investigación, por indicación directa del director o del gerente de Seguridad, se deberá hacer un respaldo de la porción del video que sustente la investigación en proceso para futuras referencias.

14) Esta información podrá ser mostrada o entregada a las personas afectadas siempre y cuando sea solicitado por escrito y bajo autorización de la Dirección o Gerencia de Seguridad. La información generada por el Centro de Monitoreo se encuentra clasificada como reservada y de acceso restringido.

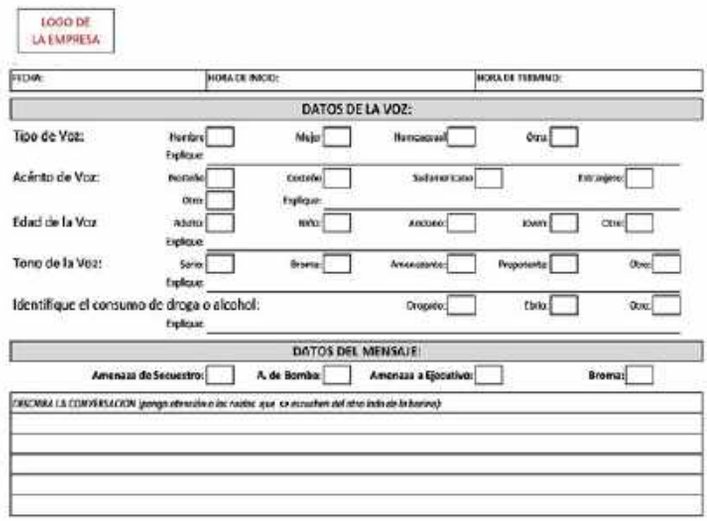
15) Ante cualquier emergencia, el jefe de Servicio y/o jefe de Turno deben actuar oportunamente, enviando a los oficiales necesarios al lugar del incidente, para verificar y brindar apoyo. Los oficiales se movilizarán inmediatamente, lo que permitirá un tiempo de reacción menor, por lo que su pronto arribo favorece a la emergencia reportada.

16) El jefe de Servicio y/o jefe de Turno debe establecer comunicación constante desde el Centro de Monitoreo hacia los puntos estratégicos de vigilancia para alertarlos de cualquier situación sospechosa o ilícita principalmente en horarios de mayor afluencia, asentando las novedades y actividades en la bitácora.

17) En las áreas de mayor afluencia, el jefe de Servicio y/o jefe de Turno debe solicitar efectuar grabación a detalle cualquier objeto o persona sospechosa, así como las actividades de entrada y salida de vehículos. Cuando ocurre alguna eventualidad, el tiempo de respuesta en la identificación de personas y unidades vehiculares relacionadas con actos delictivos debe ser inmediata.

CONSIGNAS ANTE UNA LLAMADA DE EXTORSIÓN

- Reporte enseguida a su jefe inmediato.
- No realice ninguna acción que lo soliciten después del horario de trabajo.
- No abra ni entre en lugares a los que no suele ingresar por ningún motivo.
- Por ningún motivo abra o fuerce oficinas, cajones o lugares y menos fuera de horario.
- No conteste el teléfono fuera de horario laboral a menos que sea su jefe inmediato o el número registrado de la persona responsable del inmueble.
- Utilice el formato de Registro de Llamada Amenazante, el cual es un documento de carácter confidencial, que debe ser utilizado durante la llamada, por parte del elemento de Seguridad.


LOGO DE LA EMPRESA

FECHA: | HORA DE INICIO: | HORA DE TERMINO:

DATOS DE LA VOZ:

Tipo de Voz: Hombre ☐ Mujer ☐ Homosexual ☐ Otra ☐ Explique:

Acento de Voz: Norteño ☐ Costeño ☐ Sudamericano ☐ Extranjero ☐ Otro ☐ Explique:

Edad de la Voz: Adulto ☐ Niño ☐ Anciano ☐ Joven ☐ Otro ☐ Explique:

Tono de la Voz: Serio ☐ Broma ☐ Amenazante ☐ Prepotente ☐ Otro ☐ Explique:

Identifique el consumo de droga o alcohol: Drogado ☐ Ebrio ☐ Otro ☐ Explique:

DATOS DEL MENSAJE

Amenaza de Secuestro ☐ A. de Bomba ☐ Amenaza a Ejecutivo ☐ Broma ☐

ANOTAR LA CONVERSACION (pregunte otra vez o dígale que no escuchan del otro lado de la bocina)

ES IMPORTANTE SEGUIR EL SIGUIENTE PROCEDIMIENTO EN EL LLENADO DE DICHO REGISTRO:

1) Anote la fecha en que se recibe la llamada.

2) Anote la hora en que tomó la llamada. Por ningún motivo se lo diga a otra persona ajena al personal autorizado, ya que solo provocaría situación de pánico y descontrol.

3) Especificar el tipo de voz (identificando si es de hombre, de mujer, de niño) y registre la casilla que corresponda en dicho formato.

4) El acento de la voz (norteño, costeño, extranjero, otro).

5) Edad de la voz, señalando en el registro la edad promedio de acuerdo a las características del timbre durante la modulación de su lenguaje.

6) Señale el tono de la voz, indicando el estado de ánimo que se percibe (serio, en broma, enfadado, prepotente).

7) Identifique si por su voz pudiera percibirse que "arrastra la lengua" al hablar para determinar si pudiera estar drogado o ebrio.

8) Al estar hablando con él, identifique otros datos importantes para el llenado de su Registro de Llamada Amenazante:

- Trate de calcular su edad, pero tenga cuidado, la voz de niño se confunde con la de mujer.


Foto: Freepick

- Ruidos que se escuchen del otro lado de la bocina, esto será de gran ayuda, ya que si se escuchan carcajadas, lo más seguro es que se trate de una broma, pero no se confíe.

9) La llamada amenazante debe ser atendida en todos los casos, ya que no debe descartar una posible venganza de algún ex empleado inconforme y sin escrúpulos, a quien no le importe no sólo el dañar a las instalaciones, sino a las personas.

10) El tomar en cuenta los puntos anteriores, le permitirá atender las acciones mínimas necesarias con eficacia y utilizar los medios que tiene a su disposición, y recibir el apoyo oportuno.

¿QUÉ ES EL CIBERTERRORISMO?

El ciberterrorismo es un tipo de terrorismo que se realiza a través de Internet y otros medios digitales. En este apartado hablaremos sobre cómo puede prevenirse.

El ciberterrorismo es una amenaza real para la seguridad nacional. A medida que más y más funciones críticas de los gobiernos y las empresas se hacen en línea, los ciberdelincuentes tienen más oportunidades de causar daños significativos. Afortunadamente, existen medidas que se pueden tomar para prevenir el ciberterrorismo.

En primer lugar, es importante tener un buen sistema de ciberseguridad en el lugar. Los sistemas de seguridad deben ser capaces de detectar y bloquear intrusiones, y también deben tener un plan de respuesta en caso de un ataque.

En segundo lugar, hay que saber que todos los empleados estén bien informados sobre el ciberterrorismo y la forma en que pueden evitar ser víctimas de un ataque. Los empleados deben saber cómo identificar intentos de *phishing* y otras formas de ciberataques, y también deben saber qué hacer si son víctimas de un ataque.

En tercer lugar, las empresas y los gobiernos tengan un plan de respuesta en caso de un ataque cibernético. Este plan debe incluir una lista de contactos de respuesta, una lista de tareas a realizar en caso de un ataque, y un plan de comunicación para mantener a los empleados y a la opinión pública informados.

El ciberterrorismo es una amenaza real y creciente, pero afortunadamente existen medidas que se pueden tomar para prevenirlo. Si se toman las medidas adecuadas, se puede reducir significativamente el riesgo de que ocurra un ataque cibernético.

PUNTOS IMPORTANTES QUE TENEMOS QUE TOMAR EN CUENTA

- El ciberterrorismo es una amenaza real y creciente.
- Las empresas y los organismos gubernamentales deben tomar medidas para protegerse contra los ataques cibernéticos.
- Los sistemas de información deben estar protegidos contra los ataques.
- Deben estar conscientes de los riesgos y tomar medidas para protegerse.
- Los proveedores de servicios deben estar preparados para responder a los ataques.
- Las leyes y los reguladores deben establecer y hacer cumplir las normas de seguridad.
- Es necesario un esfuerzo coordinado para enfrentar este problema.

El objetivo del ciberterrorismo es provocar el terror y el caos utilizando la tecnología, y puede incluir acciones como el hackeo de sistemas críticos, el robo y divulgación de información privada, o el ataque a redes de computadoras. El ciberterrorismo puede ser utilizado tanto por grupos terroristas tradicionales como por individuos, y puede tener un impacto a nivel local, nacional o internacional.

¿QUÉ HACER PARA PREVENIR UN ATAQUE CIBERNÉTICO?

- Prevenir ataques cibernéticos requiere una estrategia de seguridad en tres niveles: tecnología, procesos y personas. La tecnología es sólo una parte de la ecuación, los procesos y las personas son igualmente importantes.
- Las mejoras en la tecnología de seguridad pueden ayudar a prevenir ataques, pero no pueden proteger por completo a una empresa.
- Los procesos de seguridad deben estar en su lugar para minimizar el riesgo de un ataque exitoso, y las personas deben estar capacitadas para identificar y responder a los intentos de ataque.

¿QUÉ HERRAMIENTAS O APLICACIONES EXISTEN PARA PROTEGERNOS DE UN CIBERATAQUE?

Existen varias herramientas y aplicaciones que podemos utilizar para protegernos de un ciberataque. Algunas de estas herramientas son:

- **Antivirus:** los antivirus son programas diseñados para detectar y eliminar virus informáticos.
- ***Firewall:*** un *firewall* es un sistema que se utiliza para controlar el tráfico de red entrante y saliente, y puede ayudar a prevenir los ciberataques.
- ***Software* de seguridad:** el *software* de seguridad puede ayudar a proteger nuestros dispositivos y sistemas contra ciberataques.
- **Criptografía:** la criptografía es una forma de protección de datos que puede ayudar a prevenir que los ciberdelincuentes accedan a nuestra información. ■

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

CRNOVA SECURITY

Custodia de Mercancía

Guardia Intramuros

Monitoreo y Rastreo

ISO 9001

ISO 28000

BASC

ISO 18788

ISO 37001

AMESP

ESR

ASIS INTERNATIONAL

crnovaoficial

crnovasecurity

www.crnova.com.mx

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

ISIS: SEGURIDAD INTEGRAL, VANGUARDISTA E INNOVADORA

Certificaciones, capacitación y tecnología como factores esenciales para una custodia al transporte efectiva

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Con más de 19 años de trayectoria en el mercado de la Seguridad Privada, ISIS Seguridad Integral se mantiene a la vanguardia para cumplir con el compromiso de brindar seguridad y protección a las personas y sus bienes, a través de la combinación de capital humano altamente capacitado con tecnología de punta en equipamiento de seguridad electrónica.

Actualmente los servicios que ofrece ISIS son:

1) **Guardias Intramuros.** Enfocado a la prevención de robo, daño de bienes, protección física y material, así como auxiliar en caso de siniestros o desastres.
2) **Custodia al Transporte.** Servicio especializado para el acompañamiento del transporte, enfocado en la prevención y reacción en caso de robo de mercancía. Se utilizan procedimientos establecidos *Step by Step*, para el seguimiento en el monitoreo del servicio 24/7, asegurando la trazabilidad de la información desde origen hasta destino en su logística.
3) **Rastreo Satelital GPS y Monitoreo.** El Centro de Control de Monitoreo ISIS ha sido diseñado para brindar una herramienta de localización para unidades empresariales, flotillas, reparto de mercancía, particulares, entre otros.
4) **Seguridad Electrónica.** Integrada por Sistemas de CCTV (Circuito Cerrado de Televisión), Control de Acceso y Alarmas, para poder ver en todo momento lo que sucede en casa, negocio o empresa, desde cualquier parte del mundo.
5) **Control de confianza.** Podrá realizarlo a través de la Certificación ISIS de Control de Confianza, especializada en personal de planta, temporal u ocasional.
6) **Consultoría y capacitación.** ISIS ofrece consultoría en: Análisis de Riesgos, Protección Civil, Monitoreo especializado en CCTV, Control de Acceso, Planes y Programas de Capacitación y Adiestramiento, Seguridad e Higiene en el Trabajo, y BCP (Plan de Continuidad de Negocio).

CUSTODIA AL TRANSPORTE: EFECTIVA Y NECESARIA

De acuerdo con información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), en el primer bimestre del 2024, se contabilizaron mil 381 robos a transporte de carga, concentrándose, principalmente (90%), en cinco estados: Puebla, Estado de México, Morelos, Michoacán y San Luis Potosí; por lo que cada vez más empresas están invirtiendo recursos en estrategias de seguridad que contrarresten esta situación. Una de ellas es la custodia de transporte, servicio que ofrece ISIS Seguridad Integral y que se respalda con personal capacitado, un centro de monitoreo 24/7, y tecnología preventiva, de seguimiento y reactiva.

"La importancia de adquirir un servicio de custodia de transporte tiene dos vertientes. La primera, es que hoy en día las empresas aseguradoras, en la mayoría de los casos, exigen a sus clientes que cuenten con diferentes medidas de seguridad, entre ellas escolta, ya sea con o sin armas. Eso como primera instancia, y, en segundo lugar, debido a la creciente incidencia delictiva del robo al transporte que año con año crece y que hasta el momento, no ha habido manera de que se pueda contener, a pesar de analizar y buscar las mejores rutas y horarios para transitar seguros", comentó en entrevista Raymundo Mancera Sandoval, director general de ISIS Seguridad Integral.

Raymundo Mancera Sandoval, director general de ISIS Seguridad Integral

La selección del personal adecuado y de confianza, así como la capacitación que éste recibe, será pieza fundamental para asegurar al transporte, la carga y el operador, además de la integración de herramientas tecnológicas innovadoras y a la vanguardia.

"En ISIS siempre estamos buscando la actualización de nuestras herramientas tecnológicas para cualquiera de los servicios que ofrecemos, en primera instancia, utilizamos con respecto al factor humano, una selección de personal que cumpla con el perfil del puesto y cumpla con los controles de confianza que le son aplicados, un buen reclutamiento y selección del personal adecuado contribuirá desde un principio a que la custodia sea efectiva. Acto seguido en la capacitación del personal y sobre todo alcanzar una certificación, desde el personal administrativo hasta el operativo. El personal debe conocer las reglas de tránsito, y los protocolos que se establecen en los centros de control, para dar una respuesta adecuada ante situaciones de emergencia. El monitorista a su vez, también debe estar certificado y en constante capacitación, y contar con una telemetría adecuada dentro de los sistemas de GPS para poder tener una serie de patrones de seguimiento muy claros", indicó el especialista.

DIFERENCIADORES QUE GENERAN CONFIANZA

ISIS Seguridad Integral está legalmente registrada y cuenta con el Permiso Federal para operar en toda la República, el Permiso de la Ciudad de México, y Permiso de Estado de Guanajuato; además tiene la certificación BASC (*Business Alliance for Secure Commerce*).

"En ISIS le brindamos un traje hecho a la medida, contamos con tecnología, y un centro de control 24-7; tenemos experiencia en el mercado especializándonos en custodia al transporte de mercancías de todo tipo, y nuestro personal cuenta con la capacitación y el adiestramiento necesario para poder llevar a cabo esa función. Independientemente de la tecnología con la que cuentan nuestras unidades, que son sistemas de GPS, sistemas de circuitos cerrados de televisión, tenemos instaladas cámaras en las unidades que nos permiten, con una tecnología que estamos trabajando de nueva generación, poder tener acceso a las unidades vía *streaming* en tiempo real y de manera oportuna", comentó.

Respecto a la integración de la Inteligencia Artificial en la Seguridad Privada, comentó que en definitiva es una herramienta muy novedosa, pero que en cuanto a seguridad todavía se encuentra en proceso y maduración para integrarla de forma adecuada y benéfica.

LA SEGURIDAD PRIVADA COMO UNA INVERSIÓN

Raymundo Mancera coincide en que los altos índices de inseguridad están propiciando el crecimiento del sector de la seguridad privada, por lo que demanda un reto para esta industria y que requiere especial atención en la parte legal, puesto que operan empresas que no cuentan con los permisos necesarios y generan una competencia desleal que no sólo afecta a la seguridad de sus clientes, sino también al prestigio de empresas como ISIS, que operan con toda la normatividad y requisitos que las autoridades respectivas, solicitan.

"El aumento de robo en carretera está obligando a que cada vez más empresas transportistas inviertan en seguridad, en sistemas de monitoreo, vigilancias virtuales, en adiestramiento de los operadores, etcétera. ISIS es una gran empresa de seguridad, es integral, vanguardista e innovadora, enfocada en cubrir los estándares de calidad de los clientes y trabajar dentro de los marcos legales que establecen las autoridades, recordando que su seguridad es nuestro compromiso", finalizó el CEO. ■

Fotos: Mónica Ramos / SEA

LA MERCADOTECNIA EN LAS EMPRESAS DE SEGURIDAD PRIVADA

Recomendaciones para administrar el área de Mercadotecnia en una empresa

Foto: Freepick

MÉXICO **Adhaf Raúl Hatem López**

Hablar de mercadotecnia y sobre todo enfocada a un sector como el de la seguridad en ocasiones es difícil, debido al desconocimiento de lo que realmente implica y abarca esta área, por ello, hablaremos en resumidas cuentas de lo fundamental y sobre todo daremos unos tips para poder gestionar un área correcta de Mercadotecnia.

Lo primero es saber qué significa, una definición que tiene muchas variantes y la pregunta correcta debe ser: ¿Para qué sirve la mercadotecnia? Y la respuesta es simple, sirve para entregar valor, nos sirve para entender a nuestros clientes y prospectos, para identificar, anticipar y satisfacer las necesidades y deseos de nuestro cliente.

¿La Mercadotecnia vende? La respuesta es no, quien vende es el área comercial, la mercadotecnia te ayuda a presentar de la mejor forma que vende el área comercial y el objetivo principal en seguridad es posicionar a la marca como una marca sólida, confiable y de gran valor.

¿El área Comercial debe tener a cargo el área de Mercadotecnia? No, en mi particular punto de vista la mercadotecnia en una empresa de seguridad privada debe depender del director general directamente, ya que debe estar enfocada a la estrategia y objetivos de la organización, un claro ejemplo es que los precios de los servicios depende de un área de Análisis de Costos, misma que depende el área Comercial y Financiera, bajo la premisas de rentabilidad y viabilidad (también

Foto: Freepick

Lo principal es que sepas y tengas bien definida tu estrategia de negocio, de ahí emana todo, saber por qué tienes este negocio, qué quieres lograr con él y sobre todo para qué lo quieres lograr, una vez contestando esto vendrá sola la estrategia

enfocados a la estrategia de negocio), pero Mercadotecnia no debe, ni puede sugerir precios y costos, ¡su objetivo es otro completamente! (Pero si puede usar esos números para su estrategia).

¿Las redes sociales deben depender de mercadotecnia? Sí, justo son un medio principal de difusión del valor de marca y porque es confiable, junto con medios electrónicos, impresos y otros tradicionales donde se pueda difundir esta estrategia.

¿QUÉ DEBE TENER EN FOCO *MARKETING*?

Los servicios de seguridad privada son complejos de vender, ya que los compradores son selectivos y en su mayoría no tienen conocimiento de lo que abarca toda el área, desde la confianza, naturaleza y reglamentaciones, por ello, ahí es donde Mercadotecnia debe enfocarse con el valor de marca, debe recalcar la importancia de que los servicios deben brindarse bajo ciertas característica técnicas, y justo ahí es donde entra el valor, qué da diferente tu organización frente a otras, qué representas para la sociedad, para tu cliente interno (los guardias), etc. Bajo ese enfoque coadyuvará la estrategia cuando Comercial entre a negociar, le será más fácil cerrar.

¿Debo tener un área de Mercadotecnia? Sí, es fundamental para el crecimiento de una organización y la mayoría no lo contemplan, ni le dan el peso que debería, casi siempre la lleva el área Comercial (ya se explicó por qué no) y no funciona, no importa el tamaño de la empresa, puedes tener un área interna o una empresa externa que te ayude con esto al nivel que requieras.

¿Qué debo tener para hacer un buen *marketing*? Lo principal es que sepas y tengas bien definida tu estrategia de negocio, de ahí emana todo, saber por qué tienes este negocio, que quieres lograr con él y sobre todo para qué lo quieres lograr, una vez contestando esto vendrá sola la estrategia y convencido de la misma, podrás diseñar qué quieres mostrar y qué valor tiene tu marca. Si no tienes esto definido, sólo tirarás el dinero si inicias mercadotecnia en tu negocio, ya que no tendrá función ni objetivo. ■

Adhaf Raúl Hatem López,
CEO de MEXSEPRO S de RL de CV.
Más sobre el autor:

Los servicios de seguridad privada son complejos de vender, ya que los compradores son selectivos y en su mayoría no tienen conocimiento de lo que abarca toda el área, desde la confianza, naturaleza y reglamentaciones, por ello, ahí es donde Mercadotecnia debe enfocarse con el valor de marca

Foto: Freepick

RIESGOS DE SEGURIDAD EN LA INDUSTRIA MAQUILADORA

Crisis energética, robo al transporte de carga, huelgas, competencia desleal, y daño reputacional, son algunos de los riesgos a los que maquiladoras nacionales se enfrentan actualmente

Foto: Freepick

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La maquila nace en los años sesenta en nuestro país, como resultado de la alta demanda de mano de obra económica y calificada, misma que fue desarrollándose con mayor auge en los estados del norte, convirtiéndose en uno de los países con la mejor mano de obra siendo muy competitiva en cuanto a precio-calidad, representando una gran participación en el Producto Interno Bruto (PIB). Con los años, las industrias maquiladora y manufacturera se han convertido en uno de los pilares de la economía mexicana.

De acuerdo con un comunicado publicado en el Diario de la Federación el 29 de mayo de 2020, la industria maquiladora se consideró como esencial, y hasta junio de ese mismo año, se tenían registrados 5 mil 184 establecimientos en activo. En 2021, las maquiladoras representaron el 58% del PIB y el 48% del empleo industrial. México también ha sido uno de los países mejor posicionados para el *nearshoring,* modelo económico que atraerá la inversión de 9 mil 50 millones de dólares en activos fijos para establecer nuevas líneas de producción, plantas y fábricas en este año, de acuerdo a estimaciones del Consejo Nacional de la Industria Maquiladora.

UNA INDUSTRIA ESENCIAL

Para entender la magnitud que la industria maquiladora representa para el país y sus habitantes, Paul Messeguer Lamas, *Country Security Manager* en ZF Group y presidente de ASIS Capítulo Occidente, impartió una conferencia magistral en uno de los *roadshows* que organizó **Seguridad en América** este año, en donde expuso los beneficios que brinda la industria manufacturera al país:

- Crean fuentes de empleo.
- Fortalecen la balanza comercial del país, a través de una mayor aportación neta de divisas.
- Contribuyen a una mayor integración interindustrial y elevan la competitividad internacional de la maquila nacional.
- Elevan la capacitación de los trabajadores e impulsan el desarrollo y la transferencia de tecnología en el país.

En el siguiente esquema se puede visualizar la distribución de la industria maquiladora de acuerdo con su producción, sin embargo, con la llegada del *nearshoring,* y la crisis hídrica que enfrentan algunos estados, así como la inseguridad, las empresas extranjeras han optado por trasladar sus fábricas al sur del país.

AUTOMOTRIZ	AEROESPACIAL	ELECTRÓNICA	MÉDICA
• San Luis Potosí • Aguascalientes • Querétaro • Guanajuato • Puebla • Saltillo • Nuevo León	• Querétaro • Baja California • Guanajuato • Chihuahua • Estado de México	• Jalisco • Aguascalientes • Baja California • Chihuahua • Ciudad de México • Nuevo León	• Baja California • Tijuana

PRINCIPALES RIESGOS DE SEGURIDAD

Para definir los riesgos de seguridad a los que se enfrenta actualmente la industria maquiladora se debe empezar por mantener un enfoque básico de seguridad, es decir, contemplar todos aquellos procesos, herramientas, procedimientos, situaciones, nuevas tecnologías, elementos de seguridad física, políticas, auditorías, todo lo relacionado a la maquila que estemos protegiendo o resguardando. Paul Messeguer dividió los riesgos en dos niveles, los cuales contemplan de manera general y particular todo lo que sucede dentro y fuera de esta industria, que de una manera u otra, se relaciona con la seguridad de ésta:


Foto: Freepick

En 2021, las maquiladoras representaron el 58% del PIB y el 48% del empleo industrial

RIESGOS NIVEL 1

- **Factor documental.** El no contar con políticas y guías establecidas, basadas en los objetivos de la empresa, en donde se identifiquen y registren los riesgos de la maquiladora, eso en sí mismo representa un riesgo para la propia empresa. Es importante, además, que estas políticas sean de conocimiento del personal que está involucrado en cada proceso en conjunto con el área de Seguridad.
- **Factor Recurso Humano.** Una vez que se tienen las políticas y guías, se debe informar a todas las áreas sobre los riesgos conocidos, y solicitar que estas brinden información sobre los riesgos que identifiquen desde sus actividades. Así el responsable de Seguridad o del Departamento de Gestión de Riegos (*Risk Management*) tenga presente todos los riesgos y, a su vez, todos accionen al enfrentarlos: manejarlos, prevenirlos, minimizarlos, asumirlos y transferirlos.

Dentro del Recurso Humano, se encuentra un riesgo latente, que es el de la falta de un proceso de contratación y selección del personal con enfoque en seguridad. Así como la falta de entrenamiento y sensibilización en temas de seguridad a todo el personal, basado en las políticas y guías:

a) Política General de Seguridad Patrimonial.
b) Protección de Activos (tangibles e intangibles).
c) Manejo de emergencias y crisis.
d) Uso de equipos de IT.
e) Uso de armas.
f) Uso de drogas.
g) Violencia en el lugar de trabajo.
h) Antisoborno.
i) Acoso sexual y laboral.
j) Autoprotección como empleado de la organización (cultura de seguridad).

- **Factor Seguridad Física.** El no contar con procesos y recursos para la protección de las personas, activos e instalaciones es un riesgo, por ello es importante contar con:

a) Cámaras de videovigilancia.
b) Control de accesos.
c) Guardias de seguridad.
d) Equipamientos y tecnología para detección de amenazas.
e) Formación del personal: asegurar que todos comprendan y apliquen las medidas de seguridad física.
f) Respuesta ante emergencias: capacitar al personal para actuar en situaciones críticas.

- **Factores IT.** La falta de ciberseguridad hoy en día representa un riesgo importante, que requiere de la capacitación de todo el personal para evitar ser presa de ciberataques o extorsiones y robo de información.

a) Ciberataques.
b) *Phishing, Malware,* virus y *Ransomware*.
c) Fallas en la gestión de contraseñas.
d) Privacidad de datos–robo de identidad.
e) Falta de procesos como BCP/DRP.
f) Falta de certificaciones en ciberseguridad (TISAX).
g) Factores globales.
h) Dependencia de los socios comerciales.
i) Competencia y adaptabilidad.
j) Guerras.
k) Pandemias.
l) Cambios en la Cadena de Suministros (pospandemia).
m) *Nearshoring*. Si no se implementa de manera adecuada y oportuna, se puede convertir en un riesgo de *supply*.
n) Inestabilidad política y cambios en políticas fiscales.
o) Crimen organizado.
p) Extorsión.
q) Cobro de piso.
r) Secuestro físico y virtual.
s) Inserción en el *Supply Chain* e indirectos.

RIESGOS NIVEL 2

- **Factor Recurso Humano.** Las siguientes situaciones representan un nivel de riesgo y consecuencias más complejas y que interfieren con la seguridad de la maquiladora, la materia prima, el personal y los usuarios finales, como son:

a) Huelgas.
b) Espionaje industrial.
c) Falsificación de productos.
d) Sabotajes.


Foto: Freepick

PAUL MESSEGUER, CPP, *SECURITY STRATEGY, RISK & CONTROL ASSURANCE*

Profesional de seguridad con más de 30 años de experiencia, en los que ha adquirido un avanzado conocimiento en temas de seguridad, sin dejar de lado la habilidad que tiene para trabajar con las diferentes áreas de las empresas donde ha colaborado, en industrias de manufactura, logística, seguridad privada y productos de consumo. Como parte de sus roles y responsabilidades con la sociedad, ha colaborado con diversas asociaciones civiles y de gobierno. Es miembro fundador de ASIS México Capítulo 247 y electo como presidente de este Capítulo para el periodo 2024. También es miembro del consejo de OSAC consulado Guadalajara, ex miembro del Consejo Ciudadano de Seguridad Pública prevención y readaptación social del Estado de Jalisco.

Es un riesgo el no contar con políticas y guías establecidas, basadas en los objetivos de la empresa, en donde se identifiquen y registren los riesgos de la maquiladora

e) Extorsión dentro de la maquiladora.
f) Violencia / tiradores activos.
g) Manifestaciones no violentas que pueden llegar a cerrar accesos, vialidades, e interrumpir la operación.
h) Rotación del personal.
i) Salud (enfermedades, epidemias, pandemias).
j) Derechos humanos.
k) Reputacionales, *recall*, denuncias.

- **Factor Cadena de Suministros:**

a) Robo de carga. Tan sólo de enero a mayo de este año fueron reportados mil 410 robos de vehículos en todo el país, de los cuales 700 fueron cometidos a transporte de carga[1].
b) Escasez de materia prima.
c) Materiales y distribución.
d) Amenazas a la Cadena de Suministros.
e) Proveedores.

- **Riesgos gubernamentales:**

a) Falta de energía.
b) Tratados comerciales ventajosos.
c) Competencia desleal.
d) Políticas económicas irregulares.

- **Factores naturales:**

a) Sismos.
b) Inundaciones.
c) Erupciones volcánicas.
d) Tornados.
e) Huracanes.
f) Sequía.
g) Olas de frío, y muy reciente, todo lo que está conllevando las olas de calor en el país.

- **Factor financiero.**

a) Costos de exportación.

- **Factor legal.**

a) Propiedad intelectual.
b) Demandas laborales.
c) *Governance*.

- **Sustentabilidad.**

a) Accidentes ambientales.
b) Falta de espacio, agua y energía.
c) Generación de desechos peligrosos.
d) Contaminación atmosférica. ■


Foto: Freepick

Referencias:

[1] *"Informe mensual de robos al 31 de mayo de 2024", Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV).*

Asistencia Legal

ALES

Gestoría jurídica en materia de Seguridad Privada

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

Asumimos la responsiva de su empresa en los siguientes rubros:

- Obtención de autorizaciones iniciales, revalidaciones y modificaciones, para empresas de seguridad privada en todas las modalidades y en cualquier estado de la República.
- Mantenimiento y asesoría de los permisos de seguridad privada, cumplimiento de obligaciones Municipales, Estatales y Federales.
- Análisis jurídico y atención a cualquier procedimiento administrativo de cada permiso.
- Representación, atención y respuesta a visitas de verificación, supervisión o de inspección.
- Atención a multas y sanciones mediante recursos legales idóneos.
- Juicios de nulidad y amparo administrativo.
- Registro de personal directivo, administrativo y/o técnico-operativo a nivel Federal y Estatal hasta la obtención de CUIP o CIP.
- Alta o registro de agente capacitador interno o externo, planes y programas de capacitación, constancias laborales de capacitación DC-2, DC-3, DC-4 y DC-5,
- Elaboración de manuales operativos o de capacitación.
- Evaluaciones de Perfiles médicos, físicos, psicológicos, toxicológicos, entorno social.
- Permiso para el uso de armas de fuego, así como alta y registro de armamento ante SEDENA.
- Inscripción de Reglamento Interior de Trabajo, ante el Centro Laboral de Conciliación y Registro Laboral, Juntas Locales.

LicDanteGarciaMtz@outlook.com

Cel: +52 477 828 1291

SEGURIDAD EN LOS JUEGOS OLÍMPICOS PARÍS 2024. DESDE UN ANÁLISIS DEPORTIVO

Los Juegos de la XXXIII Olimpiada marcará un parteaguas en su historia con la paridad de género plena, así como un gran reto de seguridad para los especialistas que ya contemplan un plan A, B y C frente a posibles amenazas terroristas

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

El 26 de julio iniciará la trigésima tercera edición de los Juegos Olímpicos, siendo París la ciudad anfitriona y quien tiene planeada una actuación que marcará la historia de los Juegos, no sólo en el aspecto deportivo, sino también en la organización, la equidad de género y la seguridad. Por primera vez la ceremonia inaugural se llevará a cabo fuera de un estadio o recinto deportivo, será el Río Sena, en el corazón de la Ciudad de la Luz, el que se iluminará con la antorcha olímpica y cada delegación nacional lo recorrerá en barcos equipados con cámaras para que los espectadores virtuales puedan ver de cerca las reacciones de los atletas provenientes de todo el mundo. El recorrido abarcará 6 km y se posicionarán frente al Trocadero, para concluir la ceremonia oficial.

Meses de planeación es lo que harán posible esta innovación que promete ser única en la historia de los Juegos, y asombrar a los espectadores y atletas durante esta ceremonia fuera de lo tradicional, lo que también implica un gran reto de seguridad, tanto para la protección de los atletas como de los espectadores, ya que la asistencia no tendrá costo, aproximadamente serán 94 embarcaciones las que saldrán del puente de Austerlitz, con 10 mil 500 atletas representando a 206 países, y con la presencia de al menos 120 jefes de Estado, soberanos y jefes de Estado. Los Juegos Olímpicos París 2024, serán los primeros en lograr paridad de género plena, es decir, que habrá igual representación de hombres y mujeres en los 32 deportes en los que se competirá.

Foto: Freepick

Betty Vázquez, periodista especializada en cobertura de Juegos Olímpicos

RETOS DE SEGURIDAD

La seguridad de los más de 300 mil asistentes a la ceremonia inaugural (104 mil personas en gradas a lo largo del río Sena, y otras 220 mil en caminos elevados a lo largo del tramo de seis kilómetros[1]), más los atletas en los embarcaderos, implica el reto más grande de los Juegos Olímpicos, pues a partir de garantizar la integridad y la vida de los asistentes, es que se podrá disfrutar de estos. Situación que se tiene contemplada a través de diferentes estrategias por parte de las autoridades parisinas, pues es inevitable y necesario tener presente que París lamentablemente ha sido víctima de ataques terroristas, recordando aquel 13 de noviembre de 2015 en el que extremistas bombardearon y asesinaron a 130 personas en diferentes puntos de la Ciudad (Bataclan, seis bares y restaurantes y el perímetro del estadio deportivo Stade de France), dejando más de 400 heridos y una cicatriz en los parisinos y el mundo.

"Si creemos que hay riesgos de seguridad, tendremos el plan B, e incluso el plan C", comentó en una entrevista con BFMTV, Emmanuel Macron, presidente de Francia. Y también se deben tomar en cuenta otros aspectos de seguridad por la ubicación geográfica de Francia y quienes lo rodean.

"No debemos olvidar la tensa situación entre rusos y ucranianos, y ahora tal vez los de Georgia, por un lado, y por el otro los palestinos y los israelitas, cuya presencia, históricamente, siempre representa un punto más de atención y seguridad, la que normalmente corre por su propia cuenta", comentó en entrevista para **Seguridad en América**, Betty Vázquez, periodista especializada en cobertura de Juegos Olímpicos.

La prevención no es sólo un aspecto que países que han tenido ataques terroristas deben contemplar, y las autoridades en París han dejado claro que después de todo un proceso de planeación, el terrorismo y cualquier otro riesgo de seguridad han sido contemplados, de hecho han asegurado que, hasta el momento, no ha habido alguna amenaza que pueda afectar el desarrollo seguro de los JJOO.

"Cuando se llevaron a cabo los Juegos Olímpicos de Múnich 72, nadie sospechaba que en plena Villa Olímpica se viviría una jornada de terror que terminaría con atletas, jueces y entrenadores muertos; ante esta horrible situación, se tuvo que hacer una pausa. Cuando fueron los de Atlanta 1996, hubo un atentado en el Círculo Olímpico, pero no se interrumpieron las pruebas; recuerdo que cuando viajamos a Atenas para la edición de 2004 en el aire flotaba una eventual amenaza de bomba, afortunadamente no pasó absolutamente nada, pero tampoco se detuvo el desarrollo de los Juegos. Siendo, tal vez, optimista, considero que continuar con los Juegos es no permitirle al miedo que gane y continuar con un evento cuyas bases son la paz y la convivencia entre todos los pueblos, la esperanza a partir de la justa competencia deportiva y el deseo de que los conflictos armados se terminen… No aplica ya la antigua Tregua Olímpica, pero ¿quién estaría en contra?", comentó Betty.

LOS JUEGOS OLÍMPICOS CON EL MAYOR RETO

París promete ser innovador desde la ceremonia, y como cada una de las ediciones efectuadas de los Juegos, tiene un gran reto de organización logística, infraestructura, seguridad; sin embargo, y de acuerdo con el análisis de nuestra entrevistada, la edición con el reto más grande en la historia de los JJ.OO., fue Tokio 2020, pues además de todos los aspectos antes mencionados, el anfitrión debió adaptar todo y cuidar mucho más a los atletas, *staff*, organizadores, etcétera, por la crisis sanitaria que provocó el virus SARS-CoV-2 (COVID-19) en ese momento.

"Tokio (2020) enfrentó un gran reto por el peligro mundial de la pandemia lo que obligó a que se hicieran modificaciones nunca antes vistas tanto entre los deportistas como en los representantes de los medios de comunicación y, evidentemente, entre los aficionados, que se vieron impedidos en una escala muy grande de poder estar presentes. Este año las condiciones políticas tienen al mundo entero en vilo, y un escenario como el de los JJ.OO. se vuelve el mejor para poder hacer llegar a todos algún tipo de mensaje, lo que el COI sabe y sobre lo que ha trabajado incansablemente con deportistas, entrenadores y jueces".

El deporte implica disciplina, carácter, pasión; representa un reto personal, trabajo en equipo, orgullo nacional, pero no está alejado de la política, la influencia hacia la sociedad está ligado a la economía, es por ello que se han dado diferentes ataques terroristas en estos eventos porque ellos entienden todo lo que implican para un país. "Recordemos el Maratón de Boston, en su edición de 2013 fue objeto de un atentado que dejó muertos y heridos de gravedad, ¿por qué decidieron hacerlo ahí? Porque todo el mundo se enteraría".

UN RIESGO ANUNCIADO

La ciberseguridad también es algo que actualmente se debe tener en cuenta en cualquier organización, empresa, evento, y los JJ.OO. no deben ser la excepción. Sin embargo, en febrero de este año, le fue robada en un tren una computadora portátil y dos llaves de memoria con información sensible sobre la seguridad de los JJ.OO. a un ingeniero del Ayuntamiento de la ciudad, no obstante, las autoridades informaron que los aparatos robados no contenían los datos de seguridad críticos, y se han repetido estos sucesos.

"Informes y documentos del Comité Organizador de París, particularmente de la sede de Lille, fueron ya extraídos de sus oficinas, esto ocurrió a principios de mayo, equipos completos de cómputo fueron robados, evidentemente la noticia alarma porque ahí están todos los planes, los sistemas, los protocolos y demás, que garantizan la seguridad. Se informó que todos los datos estaban encriptados


Foto: Freepick

La ciberseguridad también es algo que actualmente se debe tener en cuenta en cualquier organización, empresa, evento, y los JJ.OO. no deben ser la excepción

y que los equipos fueron bloqueados de manera remota, sin embargo, es una muestra del grado de vulnerabilidad que se tiene y de la enorme necesidad de contar con seguridad en todos lados", recalcó Betty Vázquez.

UN BUEN ANFITRIÓN

¿Qué se requiere para ser un buen anfitrión de los Juegos Olímpicos? "Cubrir con todas y cada una de las exigencias del Comité Olímpico Internacional en todos los rubros: instalaciones (nuevas o rehabilitadas), oferta hotelera, seguridad, movilidad, conectividad, logística; contar con el apoyo del gobierno local y nacional, participación de iniciativa privada y convencer al Comité correspondiente del COI que se encarga de designar a la ciudad sede". ¿Actualmente México podría ser un buen anfitrión?

Bien dicen que no se puede tapar el sol con un dedo, y cada país en donde se han desarrollado los JJ.OO. tienen sus problemas de seguridad internos, unos más radicales que otros, pero los tienen. En París, el prefecto de Policía local, Laurent Nuñez, anunció que se extenderá el perímetro de seguridad antiterrorista a todos los edificios que dan al río Sena durante la ceremonia inaugural y durante el desarrollo de los JJ.OO. "Hay un perímetro antiterrorista que tiene una serie de controles y lo hemos querido ahora extender a todos los edificios que tienen una vista al río Sena, más allá de lo establecido por los organizadores", señaló Nuñez, en una conferencia de prensa en París[2].

Betty Vázquez tiene una gran trayectoria como periodista deportiva, especializándose en la cobertura de Juegos Olímpicos y conociendo de cerca el desarrollo de estos en diferentes países, respecto a alguna situación de riesgo que haya sufrido en alguna cobertura, ella comentó que, hasta el momento, y esperando así continúe, no ha sufrido incidente alguno, sin embargo, en Atenas, durante los JJOO de 2004, un colega de un periódico fue asaltado. "Le robaron su mochila con su equipo de cómputo, sus identificaciones y su dinero; y de lo más grave que yo escuché no fue en Olímpicos sino en la Copa del Mundo de Futbol de Sudáfrica, en donde a varios les dieron cristalazos y otros sufrieron robos en sus habitaciones de hotel, cabe aclarar que lamentablemente mis compañeros fueron hospedados en una de las zonas más inseguras de Johannesburgo, algo que tanto las empresas como los mismos reporteros deben evitar".

PANORAMA DEPORTIVO

Sin lugar a dudas, los Juegos Olímpicos son un evento mundialmente aclamado, en el que cada país quiere ver ondear su bandera, escuchar su himno, mirar a sus atletas subirse al pódium, un evento único del deporte. Este año veremos coronarse a países que a lo largo de la historia han trabajado por estar ahí, atletas que dedican su vida para ese momento, y seguramente veremos algunas sorpresas deportivas. Para el análisis y panorama deportivo, Betty nos compartió lo siguientes:

"Históricamente EEUU ha dominado este evento con un total que supera las dos mil preseas y el primer lugar en el medallero de manera consecutiva en Tokio 2020, Río 2016 y Londres 2012, y con la promesa de asistir con otro *Dream Team* de Basquetbol, se anticipan partidos espectaculares y el oro para ellos, como se espera ocurra en muchas otras disciplinas; sin embargo, en cada edición, los anfitriones no desean quedarse atrás así que Francia presentará también a sus mejores cartas entre las que se encuentra quien ha sido señalado como el posible sucesor de Phelps, o al menos quien será la estrella de la natación en estos Juegos: Leon Marchand".

Respecto a la Delegación Mexicana, Betty señaló que hasta el momento tiene poco más de 80 integrantes, los cuales tendrán una participación digna. "Si bien es cierto la polémica por los apoyos ha sido una constante este ciclo olímpico, eso no ha sido suficiente para que los deportistas busquen sus mejores resultados porque nos debe quedar claro algo, son mexicanos, pero el lugar que ocupen al final será de ellos, del país por añadidura, pero el esfuerzo es completamente de ellos, el objetivo es de ellos, el sueño es de ellos y lo comparten con el resto de los mexicanos".

Algunas de las preseas que tentativamente los deportistas mexicanos podrían colgarse, serían en clavados, tiro con arco, taekwondo, en pentatlón moderno, y aunque no hay nada escrito ni descartable, en natación artística, gimnasia rítmica y artística, tiro deportivo y ciclismo. ■

Referencias:

1 *"Emmanuel Macron dice que la ceremonia de apertura de París 2024 podría cambiarse en caso de amenaza terrorista", Dalal Mawad. CNN en Español 16/04/2024 https://cnnespanol.cnn.com/2024/04/16/emmanuel-macron-dice-ceremonia-apertura-paris-2024-cambiarse-en-caso-de-amenaza-terrorista-trax/#:~:text=(CNN)%20%2D%2D%20El%20presidente%20de,de%20Verano%20de%20Par%C3%ADs%202024.*

2 *"París aumenta seguridad en apertura de los JJOO ante riesgo de ataque terrorista", Forbes staff abril 25, 2024 https://www.forbes.com.mx/paris-aumenta-seguridad-en-apertura-de-los-jjoo-ante-riesgo-de-ataque-terrorista/*

LA TECNOLOGÍA
Y EL SOPORTE TÉCNICO
APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA




SEGURIDAD ELECTRÓNICA:

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

REGISTRO FEDERAL DGSP/303-16/3302 PERMISO SSP PUEBLA
SSP/SUBCOP/DGSP/506-23/460
REPSE ARR3280/2024

ALAS · SISTEMA DE GESTIÓN ISO 9001:2015 BICERT, S.C. · Achilles No. 329,814 · COPARMEX

222 141 12 30 gerenciacomer@pem-sa.com

WWW.PEM-SA.COM

FALSIFICACIÓN DE MEDICAMENTOS: UN RIESGO DE SEGURIDAD NACIONAL

El sector salud en México se ha incrementado a un TCAC de 6.68%, lo que significa una participación activa en la economía del país, pero sobre todo en el bienestar de sus habitantes, a menos que peligre su autenticidad

Foto: Freepick

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Este año el *nearshoring* fue el centro de atención de las compañías que tienen como meta mejorar y expandir su producción y economía, México fue uno de los destinos mejor calificado para este modelo económico, debido a su posición geográfica, infraestructura y la disponibilidad y costo de la mano de obra, aunque la escasez de agua está siendo punto de discusión tanto para sus habitantes como para los inversionistas nacionales e internacionales. Una de las industrias que se ve beneficiada ante este modelo es la manufacturera, y de ahí la farmacéutica, misma que a raíz de la pandemia por COVID-19, incrementó su presencia y representación económica en el país.

De acuerdo a un informe realizado por KPMG, firma global especializada en servicios de auditoría, asesoramiento legal, fiscal, financiero y de negocio, "el producto interno bruto (PIB) del sector salud en México se ha incrementado a una tasa de crecimiento anual compuesto (TCAC) de 6.68% de 2014 a 2022, incluso por encima del PIB nacional"[1], lo que significa que es una de las industrias con mejor rendimiento para la economía nacional. También es uno de los sectores con necesidades específicas para su desarrollo, ya que directamente, quienes se ven beneficiados por este, son las propias vidas de las personas.

"Nuestro país representa el segundo mercado farmacéutico más grande en América Latina, después de Brasil. Los ingresos generados por esta industria, por concepto de ventas, han crecido a una TCAC (tasa de crecimiento anual compuesto) de 3.3% de 2016 a 2020, con un valor de 688 mil millones de pesos al cierre de 2020, superando las ventas totales de las tiendas de autoservicio por 17%. Sin embargo, se espera que siga creciendo aceleradamente a una TCAC de 4.7% de 2020 a 2025, llegando a los 911 mil millones de pesos"[2].

Pero ¿cómo se puede lograr que esta industria continúe creciendo? Para empezar, y como en cada sector, lo primero es lograr preservar sus bienes y activos, así como a su personal, y a su vez lograr que se cumpla con el objetivo principal de esta industria: que el medicamento o el dispositivo médico lleguen a la persona que lo necesita, y así contribuya a mejorar su salud, a continuar con vida.

PRINCIPAL PROBLEMA DE SEGURIDAD

Con base en el mismo informe de KPMG, los principales productos con mayor demanda de la industria farmacéutica, son los analgésicos, seguidos de las vacunas, los medicamentos de cardiología, y enfermedades infecciosas. Esta industria, así como las demás y de forma general, enfrenta diferentes riesgos y retos de seguridad: robo interno, robo en la cadena de suministro, pero la diferencia está en las consecuencias que pueden surgir a raíz del robo de medicamentos, o peor, de la falsificación de estos, ya que le pueden causar la muerte a quien compra un medicamento robado extraído y transportado sin las características necesarias


Foto: Freepick

Gerardo Corchado Chávez *es egresado de la Licenciatura en Comunicación y Periodismo por la Escuela Carlos Septién. Fue subdelegado de la Policía Judicial Federal, director de Inteligencia en la Procuraduría del Distrito Federal, y fue director de Seguridad durante 20 años en Novartis. Es CPP (Certified Protection Professional), y CFE (Examinador Profesional de Fraude). También fue docente en la Escuela de Periodismo Carlos Septién. Fue presidente de la Comisión de Seguridad en Canifarma por cinco años y Coordinador del Comité de Seguridad en la Cámara de Comercio suizo-mexicana durante tres años. Actualmente es asesor de seguridad para la CANIFARMA y consultor privado en temas del desarrollo de programas antifalsificación de productos, Seguridad Corporativa, Investigaciones y Compliance.*

para su cuidado, o bien, consumiendo algo que no lo va a beneficiar en nada y por el contrario va a contribuir con el deterioro de su salud.

La falsificación y robo de medicamentos es entonces el problema de seguridad más grave que esta industria enfrenta, es por ello que entrevistamos a uno de los especialistas del sector para conocer el panorama general de seguridad de la industria farmacéutica en México y más específicamente, la falsificación de medicamentos.

Seguridad en América (SEA): ¿Cuáles son los principales riesgos de seguridad en la industria farmacéutica?

Gerardo Corchado (GC): si bien es cierto que la industria farmacéutica está igualmente afectada que las demás por la delincuencia, el peligro para las personas y el riesgo para los pacientes que genera, por ejemplo, en el robo de medicamento, ya que es totalmente diferente. Los medicamentos pueden, en un evento así, perder su cadena fría, sus condiciones de higiene o almacenamiento y desconfigurarse perdiendo sus efectos terapéuticos.

Los medicamentos robados también son una fuente importante para la falsificación ya que son rellenados o manipulados para hacer más dosis, alterar su fecha de caducidad, etcétera. Cualquier atentado de seguridad contra los medicamentos en fábricas, traslados, almacenes, hospitales, farmacias, etcétera, puede tener efectos dañinos en los pacientes o simplemente agravar su enfermedad porque el medicamento que requiere está en desabasto porque fue robado, alterado o falsificado. El principal riesgo en esta industria es el daño a los pacientes.

SEA: ¿Qué es la falsificación de medicamentos y cuál es la situación en México?

GC: es cuando se fabrican, envasan o venden productos farmacéuticos usando una autorización otorgada legalmente a otro y se imita al producto legalmente fabricado y registrado. Los falsificadores utilizan la necesidad de los pacientes por los medicamentos para curarse y envasan sustancias desconocidas en envases parecidos y estuches que aparentan ser los originales, todo con la intención de engañar al usuario sin importarles la afectación de la salud o integridad física de los pacientes.

Hasta hoy no existe una medición real del problema, hay mucho trabajo que hacer en el flujo de la información y la actuación en conjunto con la autoridad para generar una estadística confiable. La Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS) tiene un acumulado histórico de 163 alertas sanitarias por falsificación de medicamentos emitidas desde 2013 hasta el 28 de diciembre de 2023. En México, según datos de la Unión Nacional de Empresarios de Farmacias (UNEFARM), se estima un incremento del mercado ilegal de medicinas que superó los 32 millones de pesos, al cierre de 2022. En 2020 hubo en COFEPRIS 13 alertas sanitarias por falsificación, en 2022 hubo 44. Apenas el 22 de mayo de este año, CANIFARMA y el PSI, quien dirige Eddie Agrait, confirmaron la necesidad de generar información más fidedigna y completa sobre los casos de productos farmacéuticos falsificados en México y Latinoamérica, todo se perfila hacia un acuerdo formal de colaboración entre ambas entidades por el bien de los pacientes.

SEA: ¿Cuáles son las consecuencias de la falsificación de medicamentos?

GC: el más importante y potencialmente peligroso es la seguridad del paciente, también el fracaso terapéutico del producto, la morbilidad, las complicaciones de la enfermedad y finalmente en el peor de los casos la muerte. Luego la afectación en la salud pública, que puede generar resistencia a los antibióticos e interrupción de la confianza en los sistemas de atención médica social, principalmente. Hay daño también a la reputación del fabricante y la interrupción de la confianza en marcas y compañías que la construyeron en décadas.

Y por ende esto genera un impacto económico y pérdida de ingresos en empresas, que a su vez impactan la innovación y el empleo. Los ingresos por pérdida de impuestos para las autoridades fiscales nacionales, hay un impacto general en la economía local y global.

SEA: ¿Cómo distinguir un medicamento falsificado de uno original?

GC: la industria farmacéutica también se unió a la venta en línea, al famoso *e-commerce,* sin embargo, es importante que ante lo delicado de su producción y consumo, las compras de medicamentos sean directamente con los proveedores autorizados, en sus páginas oficiales, y aun así, verificar que el medicamento cumpla con los lineamientos de la COFEPRIS.

"Los medicamentos originales se venden en las farmacias, que son puntos de venta reconocidos y autorizados. Los medicamentos sospechosos de falsificación pueden ser vendidos en mercados informales, tianguis, abarroteras, Internet, en la vía pública, etcétera", explicó Gerardo Corchado.

El especialista también indicó que las cajas de los medicamentos originales son perfectas, mientras que en las falsificadas se pueden encontrar posibles faltas de ortografía, errores de alineación que hacen que se vean chuecas y sin márgenes adecuados, falta de barniz que hace que las cajas se ven opacas y desgastadas, defectos en el suaje y armado de las cajas, etiquetas mal pegadas, falta del registro sanitario, otros idiomas diferentes al castellano, errores en la impresión como tintas corridas o escurridas en los *blisters*, diferente color, forma y tamaño de los medicamentos al que usa comúnmente, un precio más bajo que el usual, entre otros.


Foto: Freepick

La industria farmacéutica también se unió a la venta en línea, al famoso e-commerce, sin embargo, es importante que ante lo delicado de su producción y consumo, las compras de medicamentos sean directamente con los proveedores autorizados, en sus páginas oficiales

"Es importante destacar que, frente a la duda, la recomendación es que el medicamento no sea administrado y se busque ayuda de inmediato, en el estuche de cualquier medicamento está el correo del departamento de Farmacovigilancia del laboratorio fabricante y también el correo de COFEPRIS; otra opción es llamar a la Canifarma quien en su sitio web ofrece los detalles de estos asuntos en una campaña contra los medicamentos falsificados. También existe un entrenamiento completo y detallado para la detección y manejo de producto farmacéutico falsificado que se puede otorgar a autoridades o grupos de interés", concluyó el especialista. ■

Referencias:
1 y 2 "Contribución económica de la industria farmacéutica en México", KPMG. 2024 https://kpmg.com/mx/es/home/tendencias/2022/04/contribucion-economica-industria-farmaceutica-en-mexico.html

5 CASOS DE MEDICAMENTO FALSIFICADO (CONOCIDOS POR GERARDO CORCHADO)

1. Los falsificadores utilizaban lentejas capeadas con concreto para fabricar tabletas de un medicamento contra el cáncer, las empacaban en tableteadoras artesanales.
2. Los falsificadores fabricaban un jarabe para niños contra la tos simplemente mezclando agua con colorantes y grenetina, el proceso se hacía con utensilios sucios y dentro de un baño junto al inodoro.
3. Los falsificadores inventaron una versión en talco de un medicamento original en tabletas orales contra los hongos en las uñas, afortunadamente era talco y no se les ocurrió poner cal u otro material peligroso.
4. Los falsificadores usaron un medicamento para el dolor, envasado en un frasco de vidrio, con un costo de 150 pesos, para "vestirlo" con etiquetas y un empaque secundario de otro producto contra el cáncer, pero este con un costo de 13 mil pesos, en un envase idéntico, pero de plástico. Ambos medicamentos eran de administración intravenosa.
5. Los falsificadores fabricaron un tarro de ungüento con materiales desconocidos que se vende en los vagones del metro de la CDMX con el nombre de una famosa marca, pero cambiando la letra V por B.

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

TOTAL ACCESO
Consulta a reportes de estadísticas de robos

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

SOCIOS ACTIVOS

Tracking Systems · si4tel · Holkan · skyguardian · skymeduza · ADS LOGIC · SECUREWITNESS · INFO TRAX · TECNO LOGISTIK · RAINDE · seguridad.com · ATLANTIDA · TTC · ISIS · GEOTRUCKS · GRUPO ALFIL · SOLUCIONES · GPSMonitor · GRUPO PRYSE · DUMAX · PROTECCLONE

SOCIOS ADHERENTES

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

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

COMUNÍCATE
55 3334 4707

GESTIÓN DE RIESGOS EN CENTROS EDUCATIVOS

Depresión, ansiedad y trastornos mentales, como los principales problemas de salud y seguridad en estudiantes de todo el mundo

Foto: Freepick

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Hace diez años, la Organización Mundial de la Salud (OMS) emitió un informe titulado *'Health for the world's adolescents'*, en el que arrojó resultados alarmantes, por ejemplo, que la depresión es la principal causa de enfermedad y discapacidad entre los adolescentes de ambos sexos de edades comprendidas entre los 10 y los 19 años, y el suicidio ocupó el tercer lugar entre las causas de mortalidad, presentando los primeros síntomas de trastornos mentales a los 14 años de edad.

En noviembre de 2019, a través de un comunicado de prensa, UNICEF (Fondo de las Naciones Unidas para la Infancia, por sus siglas en inglés) y la OMS (Organización Mundial de la Salud) compartieron la importancia de incluir programas de ayuda emocional en las escuelas, principalmente para las y los adolescentes, ya que, informaron, más del 20% de los adolescentes de todo el mundo sufren trastornos mentales; alrededor del 15% de los adolescentes de países de ingresos medios y bajos se ha planteado el suicidio, mismo que se convirtió, en ese año, en la segunda causa de muerte entre los jóvenes de 15 a 19 años.

La salud mental ha sido poco priorizada en el mundo, sin embargo, las afectaciones a ésta muestran una tasa relevante de muerte al año, siendo la depresión un factor clave y tratable para evitar ese trágico desenlace. La pandemia por COVID-19 cambió totalmente la vida de las personas y contribuyó a que sectores de la sociedad, como niños y adolescentes, sufrieran de violencia y presentaran problemas de ansiedad, depresión y suicidio.

En el informe de la Organización para la Cooperación y el Desarrollo Económico (OCDE), 'Health at a Glance 2023', comunicó que, en el año 2020, en plena crisis sanitaria, los índices de depresión en México crecieron un 71%, en comparación con los niveles de 2019[1], y la ansiedad se presentó en cinco de cada 10 personas, de hecho, hasta el año 2022, todavía dos de cada diez personas presentan ansiedad y depresión a raíz de la pandemia, y lo más alarmante es que, en ese mismo año, "el suicidio fue la cuarta causa de muerte más común en niños y adolescentes de 10 a 14 años y la tercera en el grupo de jóvenes de 15 a 24 años".

Queda claro que la salud mental debe priorizarse en las políticas públicas, sin embargo y pese a los datos presentados, pocas son aquellas instituciones que lo tienen presente y llevan a cabo programas que supervisen y apoyen a los adolescentes que presentan situaciones de riesgo. Una estrategia para esta problemática, es contar con un Plan de Gestión de Riesgos de Trastornos mentales en estudiantes, dirigido por personas capacitadas y profesionales.

CRISIS MENTALES POSPANDEMIA

A cuatro años y medio de que inició la pandemia por COVID-19, y a un año de que en México pone fin a la emergencia sanitaria, los estragos físicos, sociales, económicos y mentales siguen presentándose en las personas. Los niños que nacieron en 2020, los llamados *'pandemials'*, los niños que interrumpieron su educación preescolar presencial para adaptarse a clases virtuales, y los niños que ahora son adolescentes y se integran a las secundarias y preparatorias, son quienes presentan retos significativos ante estos cambios de socialización y comportamiento.

"Las crisis emocionales no tratadas en los jóvenes pueden manifestarse en problemas de conducta, bajo rendimiento académico e incluso situaciones de violencia. De ahí la importancia de crear programas de Prevención de riesgos, salud, seguridad y bienestar de las organizaciones estudiantiles. De ahí la importancia de implementar programas de salud y apoyo

Antonio Bellorín actualmente es el *Chief Security Officer* del Sistema del Tecnológico de Monterrey, y su misión es garantizar que se definan e implementen modelos y programas efectivos de gestión de riesgos de seguridad a nivel estratégico, táctico y operativo de sus Universidades, Preparatorias, Hospitales, y SorteosTec. Es un profesional de las Ciencias Criminológicas y Delito, especialista en Manejo de Crisis y Continuidad del Negocio, posee una amplia experiencia con más de 30 años de trabajo en complejas operaciones de seguridad al servicio tanto de empresas multinacionales como de gobierno. Ha tenido la oportunidad de desarrollar su carrera internacional viviendo en cuatro países con entornos culturalmente diversos, políticamente sensibles y estratégicamente desafiantes.

Desde 2013 al 2019 ocupó el cargo de director regional de Seguridad para América Latina de Reckitt Benckiser (antes Mead Johnson Nutrition), ejecutando varios proyectos de seguridad de alta visibilidad en mercados como Argentina, Colombia, Venezuela, El Salvador, Ecuador, Trinidad y Tobago, Brasil, Panamá, Perú, países del Caribe y México. Antes formó parte del equipo de liderazgo de Seguridad de British American Tobacco en Venezuela y México, haciéndose acreedor de una gran reputación de liderazgo global en Latinoamérica, Europa, Medio Oriente y África.

Egresó como Licenciado en Ciencias y Artes Militares, mención Aeronáutica de la Academia de la Fuerza Aérea Venezolana y cuenta en su *background* con más de 12 años de exitosa carrera militar y de aviación. Tiene una maestría en Ciencias de la Criminología y obtuvo con méritos la Certificación de Continuidad de Negocios del Instituto BCI, así como en Gestión de Riesgos bajo la norma ISO-31000. Es miembro de varias organizaciones profesionales y formó parte del Capítulo de América Latina y México de OSAC.

Foto: Freepick

que aborden estas crisis mentales. Es nuestra responsabilidad crear ambientes seguros, inclusivos, a través de la prevención de riesgos, que contemplen la salud, seguridad y bienestar de las organizaciones estudiantiles", comentó en el *roadshow* organizado por **Seguridad en América**, Antonio Bellorín, *Chief Security Officer* en el Tecnológico de Monterrey.

Los responsables de la Seguridad en los Centros Educativos, ahora, no sólo están comprometidos con la seguridad física de la comunidad estudiantil y de las instalaciones, sino que también conllevan en sus responsabilidades, preservar la integridad psicológica de estos, reto al que desde hace muchos años se enfrentan, no sólo a raíz de la pandemia por COVID-19.

"Hay tres principales causas de gravedad entre los adolescentes: la depresión, ansiedad y los trastornos de comportamiento como principales causas de enfermedad y discapacidad entre adolescentes, de acuerdo a información de la OMS. Mientras que, localmente, estamos frente a un reto global, en donde el bienestar mental y emocional de quienes protegemos a las comunidades educativas cambió de rol y de posición; ahora ante este escenario, nuestras herramientas más poderosas, no sólo son las que nos brindan los sistemas de seguridad física, sino que ahora la empatía y la comprensión, son las armas que nos van a apoyar para brindar espacios de seguridad y certeza para los miembros de nuestra comunidad", destacó el especialista.

NUEVOS RETOS DE LA GESTIÓN DE RIESGOS DE SEGURIDAD

En Seguridad cada día es diferente, los retos van cambiando de acuerdo al entorno, al contexto, la geografía, el sector, para ello la actualización constante del análisis de riesgos es fundamental para preservar la seguridad e integridad de quienes protegen y son protegidos. Para lograr un entorno de aprendizaje y positivo en los centros educativos, es necesario generar protocolos de prevención, detección y respuesta, que contemplen la integridad psicológica de la comunidad.

"Estamos comprometidos junto con las otras áreas funcionales que tienen parte de esta responsabilidad, a preservar la integridad psicológica de quienes confían en nosotros. Somos la primera línea de defensa, somos la ayuda visible para los elementos de seguridad o protección que la comunidad tiene a su disposición, desde los oficiales de seguridad hasta nuestras líneas de atención o canales de emergencia para comunicar incidentes o situaciones que puedan afectar el bienestar integral de cualquier miembro de la comunidad", señaló Antonio Bellorín.

Los nuevos retos de la Gestión de Riesgos de Seguridad en Centros Educativos, fueron enumerados en tres por el especialista: uno, mayor conocimiento sobre la salud mental; dos, erradicación de la estigmatización, y tres, identificación temprana de problemas de salud mental.

RIESGOS EN INSTITUCIONES EDUCATIVAS

Además de la situación psicológica a la que se enfrentan actualmente los adolescentes y los responsables de Seguridad, existen otros riesgos persistentes, como es el robo, secuestro, feminicidios, venta y compra de drogas y estupefacientes, o asalto a los estudiantes en transporte público como se ha visto recientemente en municipios como Naucalpan, en el Estado de México.

"Debemos tener presente los riesgos de seguridad en los centros educativos, contemplando a todos los integrantes de la comunidad: estudiantes, el personal docente, administrativo y de servicios, las familias, los voluntarios y los visitantes".


Foto: Freepick

Bellorín explicó que algunos de los principales riesgos específicos en constante evolución son:

- **Violencia.** Existencia de conflictos y agresión física o verbal entre estudiantes o personal.
- **Acoso escolar.** Comportamientos intimidatorios, burlas o exclusión que afectan negativamente a otros estudiantes.
- **Riesgos de Suicidio.** Sentimientos de desesperanza y aislamiento que aumentan el riesgo de autolesiones o suicidio.
- **Abuso de sustancias.** La presencia de consumo de drogas o alcohol que afecta la salud y seguridad de los estudiantes.
- **Intimidación.** Comportamientos amenazantes y coercitivos que generan temor y estrés en los estudiantes.
- **Crisis emocionales y conflictos interpersonales.** Situaciones que generan comportamientos disruptivos y perjudiciales para el ambiente escolar.

ESTRATEGIAS DE GESTIÓN Y PREVENCIÓN: PLANES DE MITIGACIÓN

Una vez que se tienen visibles los riesgos a los que se enfrentan actualmente los miembros de la comunidad educativa, existen diferentes estrategias que se pueden implementar de manera colaborativa con las demás áreas que tienen que ver con la salud y bienestar de los estudiantes, Antonio Bellorín recomendó las siguientes:

- **Implementar Programas de Prevención de Situaciones de Vulnerabilidad.** Por ejemplo, el método RULER, el cual "se centra en el desarrollo personal y profesional de los profesores y las familias para que puedan ser modelos y competentes para educar emocional y socialmente a los alumnos". También se puede aplicar el modelo QPR (por sus siglas en inglés: Question, Persuade, Refer), el cual es un entrenamiento práctico de primeros auxilios para la prevención del suicidio. Así como el Testigo Activo, aquí participan todos los miembros de la comunidad estudiantil, para detectar conductas de riesgo, por lo que es importante capacitar al personal para reconocer estas señales no verbales que pueden significar una alerta de una persona que está teniendo ansiedad, depresión o estrés.
- **Programa de bienestar integral.** Es importante brindar una capacitación constante y específica al personal, sobre estos trastornos mentales para la identificación de riesgos psicosociales y apoyo a personas afectadas antes, durante y después de una crisis emocional, fomentando la confianza en la toma de decisiones seguras en situaciones difíciles.
- **Programa de Prevención y Respuesta ante Suicidio.** Capacitación para observar y reconocer los gestos y señales no verbales que pueden indicar angustia emocional. Procedimientos de respuesta y las mejores prácticas en la intervención en caso de suicidio.
- **Programas de Prevención del Acoso Escolar.** Capacitación para estudiantes y personal escolar, políticas de tolerancia cero y mecanismos de reporte y respuesta rápida a incidentes de acoso.
- **Programas de apoyo a padres.** Vinculación y comunicación directa con los padres.
- **Uso de sistemas y tecnologías de seguridad.** Inteligencia Artificial y Análisis de Datos.
- **Programa de Formación para Formadores.** Dirigido a profesores, tutores y estudiantes mentores.
- **Programas de Contención.** Recursos y apoyo psicológico para manejar el estrés y el impacto emocional del trabajo, dirigido a primeros respondientes y personal de consejería.
- **Programa de Postvención.** Acciones de apoyo y asistencia que se implementan luego de una muerte por suicidio, dirigido a familiares y testigos.
- **Programa de Promoción de Conductas Adecuadas.** Introducción de contenidos vinculados con la seguridad en el currículo escolar, como parte de la formación permanente.

"Los retos del mundo en el que vivimos, nos reclaman concebir a la Gestión de Riesgos de Seguridad como un componente integral de la Gestión Institucional. Hoy asumimos el compromiso con el bienestar y la seguridad emocional de quienes confían en nosotros, con ello, creamos un entorno en el que las personas puedan sentirse valoradas y protegidas; lo que también ayuda a mejorar la productividad, la moral y la reputación de la institución en su conjunto", concluyó el especialista.

Las estadísticas no mienten, y ante esta alarmante situación entre los niños y adolescentes, todo el apoyo posible, capacitación, implementación de programas y estrategias para los trastornos mentales, el estrés y la ansiedad, contribuirán en la mejora de la seguridad e integridad de la comunidad educativa. ■

Referencias:

[1] *"Depresión", OMS, marzo 31 de 2023. https://www.who.int/es/news-room/fact-sheets/detail/depression*

- Otras fuentes consultadas: UNISEF, WHO (World Health Organization- Organización Mundial de la Salud). "La salud mental no se recupera de la pandemia: 2 de cada 10 mexicanos tienen depresión", Ana Karen García, El Economista, noviembre 20/2023 https://www.eleconomista.com.mx/arteseideas/La-salud-mental-no-se-recupera-de-la-pandemia-2-de-cada-10-mexicanos-tienen-depresion-20231120-0014.html


Tracking® Systems de México S.A. de C.V.
LÍDERES EN SOLUCIONES DE
RASTREO SATELITAL
24/365 DÍAS Monitoreo de equipos
WEB
Desarrollo de WEB y APP
Telemetría e inteligencia Artificial (IA)
Tecnología 3G/4G/Satelital
Contamos con puntos estratégicos en todo el país
amazon web services
Azure
Infraestructura sustentada por AWS y Azure
Más Información:
Contáctanos
55-5374-9320
+ de 52,500 equipos instalados
26 años DE EXPERIENCIA
Recuperación 98.5%
Aviso en menos de 30 minutos*
VALIDACIÓN DE IDENTIDAD CON IA
REVISIÓN A NIVEL MUNDIAL EN MÁS DE 1,100 LISTAS RFL
ANÁLISIS POR FRECUENCIA DE VOZ
TRUST ID
VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL
LA FORMA MÁS PODEROSA E INNOVADORA DE CERTIFICAR A TU PERSONAL
UNA SOLUCIÓN DE Grupo UDA Tracking Systems
TRUSTID.MX
Contáctanos
55·4447·0231
5374-9320 · EXT 159
atencionaclientes@trustid.mx

EXPO SEGURIDAD MÉXICO 2024

El 16, 17 y 18 de abril se llevó a cabo la vigésima primera edición de Expo Seguridad México, evento que reunió a más de 17 mil visitantes y un sinfín de tecnología e innovaciones en esta industria

MÉXICO

Tania G. Rojo Chávez / *Staff* Seguridad en América

Expo Seguridad México, el principal evento en Latinoamérica que se enfoca en mostrar productos, servicios y soluciones para la protección de personas, bienes y activos, cumplió con su objetivo de dar a conocer la tecnología de última generación e innovaciones presentadas por más de 360 empresas expositoras, al mismo tiempo de contribuir a la actualización profesional de los especialistas de seguridad de los sectores público y privado.

En esta ocasión la empresa organizadora, RX México, ocupó más de veinticuatro mil metros cuadrados de piso de exhibición para albergar la 21 edición de Expo Seguridad México (ESM) y la 16 edición de Expo Seguridad Industrial (ESI), en el Centro Banamex de la Ciudad de México, con la asistencia de cerca de 17 mil 500 profesionales que visitaron del 16 al 18 de abril los pabellones internacionales, muestras y prácticas de capacitación preparadas para este evento anual.

"Superamos las expectativas de visitantes, logrando un crecimiento de más del 15% en ESM y un 20% en ESI, ambos en comparación con el año anterior. El área de exposición aumentó un 15%, y observamos una mayor participación internacional en esta ocasión. Además, gracias a nuestra oferta de productos digitales, generamos 110 mil prospectos para nuestros expositores. Esta edición destacó por su enfoque innovador, alcanzando un potencial de negocio de 338.7 millones de dólares, lo que reafirma nuestro compromiso con la excelencia y el avance en la industria de seguridad", explicó Laura Barrera, directora de ambos eventos.

La directiva resaltó la participación de los visitantes que atendieron el programa académico, diseñado casi en su totalidad por SIA, quienes se mostraron dispuestos a actualizarse profesionalmente con más de 50 ponentes especializados. Igualmente, resaltó la aceptación que tuvieron las áreas de demostración y el espacio destinado para el vuelo de drones, como parte de las soluciones de seguridad que se exhibieron.

"Observamos complacidos que el SIA Education Program fue un éxito, y lo fortaleceremos aún más en la siguiente edición. Igualmente, vimos que las nuevas áreas y distintos pabellones estuvieron sumamente concurridos, lo que habla de una comunidad activa y con deseos de hacer negocios y *'networking'*. Recordemos que la colaboración y la pasión por la excelencia nos llevan a crear un futuro brillante", puntualizó Laura Barrera.

Por su parte, Luiz Bellini, director general de RX México, dijo que ESM y ESI son eventos cruciales para entender y atender el cambiante panorama de los negocios y las innovaciones que se presentan. Igualmente, señaló que el compromiso de todos los participantes es evolucionar "junto con las necesidades de nuestros clientes, hacia la transformación digital de las operaciones, y asegurarnos que las interacciones 'cara a cara' sigan siendo el corazón de lo que hacemos; aprovechamos nuestra experiencia como líderes globales en exposiciones y eventos de negocios para crear conexiones y ecosistemas que fomenten el crecimiento empresarial".

Por su parte, Don Erickson, *Chief Executive Officer of* Security Industry Association (SIA), externó que tienen una confianza sólida en la industria mexicana de la seguridad, ya que casi tres de cada cuatro encuestados en el informe de investigación del Índice de Mercado de Seguridad (SMI) de marzo-abril de 2024 calificaron las condiciones comerciales actuales como positivas, y casi un tercio las describió como "excelentes". "Este sector está evolucionando y múltiples factores disruptivos están impulsando cambios sistémicos", concluyó Erickson.

"Para nuestra próxima edición, anticipamos un crecimiento de más del 10% tanto en el número de empresas participantes como en los metros cuadrados del espacio de exhibición. La capacitación jugará un papel fundamental en nuestros eventos, ya que seguiremos impulsando programas educativos de alto nivel junto con la segunda edición del Programa de Educación SIA. Gracias a los resultados exitosos de esta edición, hemos confirmado a las principales asociaciones del sector, y estamos en proceso de establecer nuevas alianzas que enriquecerán y crecerán verticales de como *'Safety & Fire'*, segmentos industriales y fuerzas del orden", finalizó Laura Barrera.

UNA EXPOSICIÓN CON CAUSA

Este año además, se llevó a cabo el primer Pabellón y Mascota con Causa, que fue recibido con entusiasmo por parte de los visitantes, ya que todas las piezas de la mascota se vendieron, lo que refleja el éxito de la iniciativa. Las ganancias obtenidas fueron destinadas íntegramente a la Red Nacional de Refugios, que difundió su labor durante el evento. Además, se establecieron alianzas con empresas del sector de seguridad, con el objetivo de colaborar en la protección de mujeres, niñas y niños en situaciones de vulnerabilidad.

"Al unirnos con la Red Nacional de Refugios, estamos fortaleciendo nuestro compromiso con la seguridad y protección de quienes más lo necesitan. Juntos, trabajamos para construir un futuro más seguro y justo para todos", finalizó Laura Barrera.

A continuación, les compartimos las entrevistas con algunos de los expositores más importantes de este año:

Manuel Aguilar, director de Ingeniería y Soporte de FF Videosistemas Geutebrück; y Alejandro Navarro, director comercial de Cuentas Estratégicas en FF Videosistemas Geutebrück

ALEJANDRO NAVARRO, DIRECTOR COMERCIAL DE CUENTAS ESTRATÉGICAS EN FF VIDEOSISTEMAS GEUTEBRÜCK; Y MANUEL AGUILAR, DIRECTOR DE INGENIERÍA Y SOPORTE DE FF VIDEOSISTEMAS GEUTEBRÜCK

¿Qué vienen presentando este año?

El tema de Inteligencia Artificial, analíticos basados en IA, algunas analíticas especializadas enfocadas a las características de personas o de objetos que van pasando por una escena para poder filtrar todos esos procesamientos. Esto nos ayuda como forma de prevención en ciertas situaciones de riesgo y es lo que se busca impulsar al día de hoy. Además de estas cámaras con IA ofrecemos VMS, la plataforma que nos va a dar esa gestión y robustez para poder filtrar toda esa información y actuar de manera preventiva ante situaciones diarias.

Producto estrella

La plataforma y gestión VMS Geutebrück es muy potente, se pueden centralizar multisitios, auditar, centralizar alertamientos y eventos, aunque se detecten a través de las analíticas de las cámaras.

¿Para qué verticales de negocio están dirigidos?

Estamos dirigidos a todas las verticales de negocio. Es decir, podemos tener clientes del segmento de banca, industrial, logística, incluso soluciones de movilidad en el transporte.

Bruno Camacho, encargado de Desarrollo de Negocios en SYSCOM para Huawei

BRUNO CAMACHO, ENCARGADO DE DESARROLLO DE NEGOCIOS EN SYSCOM PARA HUAWEI

¿Qué presentan este año en la expo?

Soluciones de ciberseguridad, soluciones de *Routing & Switching* con Datacom, que es la línea de MiniFTTO (Mini Fiber To The Office), que es la nueva tecnología de Huawei. Traemos también la parte del GPON (Gigabit-capable Passive Optical) con OLT y la IDEAHUB, que es la parte de colaboración inteligente con pantallas interactivas.

¿Qué beneficios tienen estas soluciones?

En el caso de ciberseguridad, traemos una plataforma que está basada en Inteligencia Artificial que nos permite tener en la Nube todas las soluciones y que podemos observar todos los dispositivos en tiempo real, así como los ataques. En la parte de Datacom, traemos la línea de MiniFTTO, que funciona a través de tecnología PON (Passive Optical Network), que energiza el dispositivo, en este caso el *access point*, a través de un cable especial de fibra y puede llegar a alcanzar hasta 150 metros, único en el mercado realmente.

La línea de OLT con GPON, traemos tecnologías en las cuales podemos expandirnos para los ISP y comenzar a hacer migraciones, desde muy pequeñas hasta grandes *carriers*, con soluciones Carrier Class. Y en la parte de colaboración inteligente, es poder cambiar la forma en la que se trabaja con las reuniones interactivas, pero también para hacerles saber a los expositores esas diferencias.

¿Para qué verticales de negocios van dirigidas?

Son soluciones SMB, sin embargo también pueden llegar a línea Enterprise con la parte de GPON o con la de ciberseguridad.

César Figueroa, Manager Entrance Systems Mexico, Central America & Caribbean de dormakaba

CÉSAR FIGUEROA, *MANAGER ENTRANCE SYSTEMS MEXICO, CENTRAL AMERICA & CARIBBEAN DE DORMAKABA*

¿Qué están presentando este año en la Expo?

En dormakaba, nuestro propósito refleja la contribución que hacemos con nuestros productos a la sociedad, brindamos seguridad, protección y sostenibilidad, permitiendo a las personas moverse

sin problemas y dar forma a sus vidas de la manera que deseen: "*For every place that matters*".

Este año en Expo Seguridad, estamos realizando el lanzamiento de nuestra nueva generación de carriles Serie V60, diseñado para proyectos con espacio limitado pero que requieren una solución de control de acceso como parte de sus procedimientos de seguridad.

La avanzada tecnología de sensores del carril V60 permite contar con un equipo compacto y eficiente, preservando el mismo lenguaje de diseño de la línea de carriles de dormakaba Serie 40 /60/80, además en este modelo se puede instalar un lector de proximidad, así como lectores de código de barras, dentro del carril para una solución estética.

La línea de carriles de dormakaba puede integrarse a cualquier marca de sistemas de control de acceso del mercado gracias a su arquitectura abierta, siendo una solución para los integradores de seguridad, clientes finales y arquitectos.

Producto estrella

Definitivamente, la línea de carriles de dormakaba es un producto estrella de la división de negocios de Access Automation Solutions. Las empresas están interesadas en la arquitectura y el diseño de sus oficinas, saben que el diseño de interiores en un valor en el que vale la pena invertir. La identidad de una compañía es visible y palpable en detalles como la fachada del edificio, el vestíbulo y sus oficinas interiores, por lo que la demanda de diseño también está aumentando en términos de equipamiento técnico.

Los carriles de dormakaba Serie 40 /60/80 crean una sorprendente "primera impresión" al entrar en un vestíbulo. Juntos con la zona de recepción, los carriles se convierten en una parte representativa del edificio.

¿Para que verticales de negocios están dirigidos?

dormakaba diseña y desarrolla productos, soluciones y servicios para una amplia gana de mercados, como por ejemplo:

Edificios Corporativos y Oficinas: nuestra gama completa de soluciones de control de acceso, *door hardware*, torniquetes de acceso, carriles, puertas automáticas, le ayudan a garantizar que su espacio de trabajo sea eficiente y seguro, además contamos con soluciones libres de contacto como operadores automáticos de puertas que brindan una sensación de comodidad e higiene en los espacios compartidos.

Aeropuertos: nuestras soluciones y servicios de acceso automatizados y confiables permiten un flujo fluido de pasajeros, mejoran la seguridad y respaldan la eficiencia y aceleración de los procesos de operaciones aeroportuarias. Los pasillos antirretorno, y nuestras puertas e-Gates para temas de auto-embarque, migración y puntos de seguridad son un ejemplo de estas soluciones.

Hotelería: nuestra amplia gama de sistemas de alojamiento y soluciones de acceso garantizará que un hotel sea seguro y conveniente, de una manera que se ajuste a los requisitos operativos y estilo únicos.

Otras verticales de negocio a los cuales estamos dirigidos son: espacios educativos, *healthcare*, (hospitales), industria y manufactura, *vacational rent* y hospitalidad, *retail*, espacios recreativos y culturales, centros logísticos así como infraestructura crítica y sector financiero.

CHESUS MIGUEL GAY GRAO, *COUNTRY MANAGER* DE SCATI MÉXICO

¿Qué es lo que están presentando este año?

Presentamos el sistema de SCATI Access, que es control de acceso, y SCATI Centry, que es una plataforma integral de todos los subelementos de seguridad electrónica.

SCATI Access viene manejando el análisis biométrico y reconocimiento facial compatible con el uso de las tarjetas de proximidad, pero lo principal es la herramienta de exploración, que es propia, con controladores de puertas, controladoras maestras, etc., que nos permite un crecimiento en cuanto a clientes, sus capacidades y control de puertas, y de usuarios de forma ilimitada, además del desarrollo que se pueda necesitar por parte del cliente, y SCATI Centry, como plataforma de integración.

¿Para qué verticales de negocio está dirigido?

Prácticamente para cualquier inmueble, aunque nuestro nicho principal en México es la banca, pues nosotros lo impulsamos para este sector, pero puede ser para cualquier vertical como industria, donde el cliente quiera soluciones muy adaptadas, muy potentes.

CONCHA MARTÍNEZ CANO, DIRECTORA GENERAL DE LANACCESS EN LATINOAMÉRICA

¿Qué están presentando este año en la expo?

Una solución en la Nube llamada Cloud Vision. Somos fabricantes de CCTV, desarrollamos *hardware* y *software*, todo hecho en España.

Producto estrella

Potenciando VMS con analíticos, intentando no sólo enfocarlo en seguridad electrónica, sino también en la línea de negocios, *marketing*, *retailer*, para estudios de mercado, reconocimiento y detección facial, toda la parte de perímetros, para proteger infraestructuras críticas, estamos en verticales importantes como son la banca, celdas fotovoltaicas, hospitales, transporte, etc.

GEORGI PANDEV, ENCARGADO DEL ÁREA COMERCIAL DE OLSEK TECHNOLOGIES

¿Qué están presentando este año en la expo?

Traemos lo último en tecnología de *hardware* para apoyar al ecosistema de integradores de seguridad en cuanto a videovigilancia con todo lo que consiste en equipos de cómputo, grabación, almacenamiento y visualización de video, junto con el lanzamiento de una plataforma basada en Inteligencia Artificial con videoanalítica y grabación híbrida en la Nube o también en el lugar del proyecto. Es parte del portafolio de Olsek Technologies, lo tradicional es todo el portafolio de *hardware* que tenemos de grabación y almacenamiento que puede escalar hasta una docena de *pegabytes* de almacenamiento.

¿Para qué vertical de negocios está dirigido?

Son soluciones multivertical basadas en tecnología del mundo del TI, nuestro enfoque abarca desde el mundo del *retail*, también la parte de transporte, gobierno, tenemos mucho proyecto en la industria, así como sitios industriales; cualquier sitio que requiere cámaras puede usar nuestros servidores.

GUILLERMO SANDOVAL, DIRECTOR DE VENTAS PARA GENETEC MÉXICO

¿Qué presentan este año?

Mostramos los últimos avances en la plataforma de unificación de Genetec, que está teniendo una evolución con toda la experiencia que tenemos de recopilar proyectos y experiencias de seguridad física en los últimos 27 años, logramos desarrollar una plataforma de unificación de seguridad sobre la Nube, es nuestra solución llamada Security Center SaaS, es una oferta disponible para toda nuestra cadena de integradores certificados de Genetec que ayuda a recortar la brecha de adopción de la Nube en la tecnología de seguridad física.

¿Cuáles son las expectativas para el mercado latinoamericano este 2024?

Tenemos una expectativa muy alta desde un par de años, Genetec ha tomado una relevancia más grande con todo el público de Sudamérica y percibimos un potencial bastante grande de crecimiento con nuestros clientes, en particular en la región andina, en México con toda la extensión de seguridad en las empresas de *nearshoring*. Brasil también presenta bastante potencial.

¿Cuáles son las tendencias que se observan en el mercado para este año?

Notamos una tendencia de varios fabricantes siguiendo el mismo camino que nosotros tenemos desde hace muchos años de unificación, es un concepto único que tiene Genetec, pero algunos otros fabricantes lo resuelven con una integración especializada entre un sistema de control de acceso con un sistema de videovigilancia, analíticos, integración de diversos sensores, audio y videos. Observamos que esta es una tendencia que están tomando más compañías que van similares al concepto de unificación que tenemos como Genetec, que es algo que ya tenemos bastante bien elaborado.

También notamos que el público de Latinoamérica cada vez tiene más sensibilidad por la ciberseguridad, notamos que mantener su sistema de seguridad física protegida, sin vulnerabilidades, cada vez les llama más la atención, porque cada vez es más real que pueda haber ataques a sus compañías o a sus activos a través de los sensores de seguridad que tienen conectados a la red, es algo que vemos que está tomando auge.

HUMBERTO VILLEGAS RIZO, DIRECTOR GENERAL DE ALSE MEXICANA

¿Qué están presentando en la expo este año?

Nuestra empresa se dedica a importar productos de especialidad en diferentes áreas, este año estamos mostrando muchos productos que ya hemos instalado en México desde hace tiempo, como los portones vehiculares de alta velocidad, alta eficiencia, barreras vehiculares antichoque, sistemas de control de llaves para tener una auditoría sobre las llaves que tiene una empresa o una agencia de carros, sistemas para el control de seguridad en centros penitenciarios tanto para cerraduras como muebles de baño antivandálicos y con ahorro de energía, en fin que es una amplia gama de productos con un nivel de especialidad alto y de marcas líderes a nivel mundial.

¿Para qué vertical de negocio van dirigidos, principalmente?

Industrias, centros penitenciarios, agencias de automóviles, instituciones bancarias, instituciones financieras, toda empresa que tiene un requerimiento de seguridad de un nivel alto.

JOSEPH REISS, INGENIERO PREVENTA EN EL ÁREA DE CONTROL DE ACCESO PARA HID GLOBAL

¿Qué están presentando este año en la expo?

Varias novedades, en primer lugar el lanzamiento de HID Identity Positioning, que es una solución que nos permite rastrear o conocer en tiempo real la ubicación de las personas dentro de sus instalaciones. Tenemos también toda la línea de lectores Signo, paneles de control Aero, y paneles de control Mercury.

Producto estrella

Para este año estamos dando énfasis en HID Identity Positioning, ya que es un lanzamiento nuevo y queremos darlo a conocer con todos nuestros clientes.

¿Para qué vertical de negocios va dirigido?

Esto aplica para muchísimas verticales, tiene muchísima utilidad en *Commercial Real Estate*, en el sector salud, en el sector universitario; lo bueno es que esta plataforma es muy versátil, muy fácil de personalizar y se puede adaptar a las necesidades de cada tipo de cliente.

MARCELO ORSI, DIRECTOR DE VENTAS PARA QUECLINK EN LATINOAMÉRICA

Estamos en Argentina, Brasil, hasta México y vendemos productos para todos los niveles de telemetría que necesiten, desde el mas económico hasta el más fuerte con telemetría avanzada, video con información de fatiga del conductor, si está comiendo. Hay varios productos que se pueden utilizar todo dependiendo de su operación y lo que se necesite. Tenemos una solución que va justamente a combinar con su negocio.

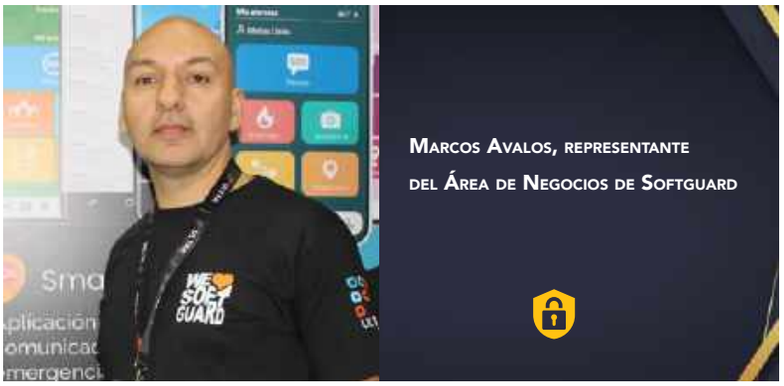
Producto estrella

Me gustaría resaltar la CV200, que es una cámara que se puede utilizar para varios tipos de negocios relacionados a imagen, se puede observar lo que está ocurriendo en la calle y automáticamente mandar esto a la Nube, y se tienen varios recursos de rastreador. Un acelerómetro de 3x, que si se sufre un accidente, por ejemplo, y se choca con mucha fuerza el aparato es capaz de identificar que es un accidente, grabar 10 segundos antes y 10 segundos después de lo ocurrido y hacer recopilado de la información para su operación, esto es lo más económico.

Pero si quiero agregar aquí, por ejemplo, con el modelo DM100 se podría identificar si el conductor está cansado, si está comiendo, fumando durante la conducción del vehículo e identifica para poder mantenerlo en el portafolio, guarda todo aquí y funciona como una cámara. Se puede combinar lo que quiera con este tipo de cámara y montar su solución, hay varios productos que hacen la diferencia para el cliente.

El modelo GV350CEU es el nivel más alto de telemetría que tenemos, este producto puede leer la CANBus del vehículo con todo las informaciones que hay ahí, puede dar información de combustible, de consumo, temperatura del motor, se puede monitorear como el conductor está manejando el vehículo y tiene *driver behavior*.

GV57CG es más económico, se puede utilizar éste o el básico para monitoreo, rastreo y bloqueo del vehículo. Esto ayuda a reducir el índice de delincuencia en carreteras.



MARCOS AVALOS, REPRESENTANTE DEL ÁREA DE NEGOCIOS DE SOFTGUARD

¿Qué están presentando este año en la expo?

Venimos a traer soluciones para aplicaciones de celulares, entendemos que el mercado está pasando por una transición, empezando a complementar lo que es el servicio de monitoreo de alarmas con productos que tienen relación con la domótica, el IoT y todo ese mercado que se gestiona a través de soluciones *mobile* para poder darle un servicio mucho más rápido y de demanda espontánea a cualquiera de los usuarios, así que nuestro nicho de mercado este año está muy enfocado en el desarrollo de aplicaciones de celular para soluciones de seguridad.

Producto estrella

La solución SmartPanics, que es altamente versátil, permite que las empresas prestadoras puedan ofrecerla en diferentes mercados. No está acotado al mercado de la seguridad exclusivamente, sino que se puede vender en el área de gobierno, educativa, de seguridad corporativa, realmente tiene muchas aplicaciones posibles.

¿Para qué vertical de negocios va dirigido?

Principalmente, el más importante es el mercado de seguridad de las empresas de seguridad privada, sin embargo tenemos una incursión bastante interesante en el área de gobierno, venimos desarrollando aplicaciones para seguridad ciudadana que nos ha permitido ingresar al sector de gobierno con soluciones apuntadas al ciudadano común o específicamente al área de violencia de género, dándole opciones de seguridad a las mujeres.

MAURICIO SWAIN, DIRECTOR DE VENTAS PARA MILESTONE EN LATINOAMÉRICA

¿Qué están presentando este año?

Los tres mensajes importantes que tenemos este año es inteligencia artificial, la Nube y, por supuesto, tecnología responsable, además de todo lo que ya conocen nuestros clientes sobre usos tecnológicos y *partners* que es obviamente la mejor plataforma de videovigilancia basadas en datos y que además es abierta.

Producto estrella

Es XProtect, de hecho es nuestro único producto además de nuestros servidores, con cinco variaciones que son diferentes productos dependiendo del tamaño y el enfoque que requieren los clientes; desde XProtect Essential+, que es incluso gratuito porque tiene la limitante de sólo tener seis a ocho cámaras en el mercado, hasta Corporate que ya puede ser una plataforma, por ejemplo, para videovigilancia urbana de varios países, varios estados o incluso a nivel *enterprise* en las empresas y obviamente tener un *headquarter* con muchísimas sucursales y demás, en este no hay límite de dispositivos.

Hoy estamos hablando de IA que es lo que todo mundo quiere conocer y está en boga. Milestone trae la Inteligencia Artificial como parte estructural del *backbone* que estamos desarrollando no solamente para lo actual sino también para el futuro, actualmente estamos trabajando con usos tecnológicos donde ellos trabajan con IA en el borde, están tomando información para poder analizarla y darle información a nuestros clientes, desde la parte de seguridad que es lo básico y lo que todo mundo espera, pero adicional a eso en la parte administrativa, operativa, logística, experiencia con el cliente, esa es la parte de la Inteligencia Artificial.

También, que muchos clientes ya están buscando opciones hacia la Nube, entonces hacia allá va el mundo, se va moviendo desde la seguridad y en el ámbito de día a día, y basado en eso estamos lanzando nuestra solución Milestone Kite, lo estaremos lanzando aquí en Latinoamérica durante el 2024.

Finalmente, la parte de tecnología responsable; esto significa que al estar usando mucho la IA la gente está preocupada con respecto a cómo va a utilizarla para ser éticamente responsable, si esos datos van a ser utilizados de forma adecuada, van a discriminar a las personas. Milestone está muy preocupado de empezar a trabajar para que nuestra solución sea tecnológicamente responsable, es decir, no discrimine a las personas, usar los datos para buenas causas, que la información que sea utilizada sea implementada para solucionar cosas que sean éticamente responsables.

Ya firmamos un acuerdo con la Unión Europea, estamos en desarrollo de trabajar también con otras organizaciones a nivel mundial, ya que nosotros queremos que nuestros clientes sepan que toda la información que esté siendo utilizada y procesada dentro de nuestra plataforma, va a ser usada de forma responsable. Se busca usar la tecnología con buenos fines.

PEDRO SIMOES, *CORPORATE VICEPRESIDENT* DE MERCADOS INTERNACIONALES DE MOTOROLA SOLUTIONS PARA VIDEO ACCESS CONTROL

¿Qué están presentando este año en la expo?

Varias cosas nuevas, principalmente enfocar en la parte de *Cloud* con la presentación de la última adquisición que hemos hecho de una compañía americana llamada IPVideo Corporation, que traza una tecnología única de sensores que pueden detectar desde sonidos, humo, contaje de personas que le permiten a lugares donde no se puede aplicar equipos de imagen visibles y a través de sensores obtenemos la información necesaria para tomar las decisiones requeridas.

Otro tema que traemos es un Avigilon Unity, que es la parte de detección de armas de fuego a través de *video analytics* que nos permite tener una presencia única en el mercado con una posición de continuar desarrollando analíticas que consideramos responsables que permiten ser utilizadas de forma responsable para dar protección de acceso a personas.

Por parte de Pelco, que representa la parte de cámaras de nuestro portafolio, que son cámaras hechas para comunicarse con cualquier VMS de mercado, estamos por introducir Pelco Elevate, basado en *Clouds* y que permite utilizar distintas analíticas en el mercado, como web y detección. Le permite tener toda la capacidad analítica de Motorola, misma a trabajar en un *software* que no sea de Motorola; este es un componente muy fuerte porque permite integraciones con distintos VMS.

Producto estrella

Todo lo que se comentó se han presentado en ferias, venimos a acoger México-Brasil; esto tiene una amplitud tremendamente grande, porque con *Cloud* nos da la capacidad para mercados desde infraestructuras críticas donde tenemos componentes de cámaras especializadas para *oil & gas* o para *retail*, donde necesitamos soluciones sin tener un servidor dentro de una tienda de *retail*. El portafolio de Motorola abarca desde la tienda más pequeña a la situación de infraestructura crítica mayor que puedas imaginar.

DARÍO ANDRÉS MÓJICA, DIRECTOR DE INGENIERÍA DE PREVENTA PARA LATINOAMÉRICA DE MOTOROLA SOLUTIONS EN VIDEOSEGURIDAD Y ANALÍTICA

¿Qué están presentando en la expo?

Presentamos soluciones en la Nube tanto de video como de acceso, así como las soluciones *on-premise* de video y acceso, igualmente todo integrado con radios, y estamos mostrando una herramienta llamada Orchestrate, que es una herramienta que le va a servir a los usuarios para integrar diferentes soluciones de Motorola a través de un servicio en la Nube de manera gratuita. Entonces, si se tienen ciertos componentes del ecosistema que vendemos, podemos hacer que acciones o eventos en un sistema hagan reaccionar al otro.

Producto estrella

Esta es una de las herramientas, porque realmente está en toda la parte de soluciones de Nube que, de control de acceso y video, tiene una tendencia cada vez mayor en el mercado; en Latinoamérica todavía hay cierto recelo, pero es una tendencia donde se nota que muchos clientes, sobre todo corporativos, ven ventaja en delegar esa tarea de tener servidores y tener que mantenerlos en sitio, a un servicio en la Nube.

RODRIGO ESCAMILLA, DIRECTOR DE DESARROLLO DE NEGOCIO PARA MERCADOS VERTICALES DE NEGOCIOS DE DAHUA TECHNOLOGY; Y SERGIO SOUZA, DIRECTOR DE LA DIVISIÓN DE PANTALLAS COMERCIALES PARA DAHUA MÉXICO

¿Qué están presentando este año en la Expo?

Para nosotros el participar en esta edición de Expo Seguridad, sabemos que es donde es el punto de encuentro para todo lo que es la innovación de las grandes tecnologías, es un honor y nos da mucha felicidad estar mostrando nuestras soluciones, entre ellas, el *display* que han podido apreciar hoy que aplican para todo tipo de mercados que estamos manejando, tanto en el sector privado como en el público, tanto para la parte de centros de monitoreo, como de *display*.

Ha sido muy interesante, si bien el segmento de seguridad por el cual surge la necesidad de traer pantallas a México y llevamos ya muchos años vendiendo el clásico *videowall* de LCD en el que armas un Lego, pero hoy estamos presentando tres cosas muy interesantes: pantalla inmersiva 3D, más o menos pesa como 28 kg por m^2, es una pantalla muy ligera para el tamaño que tiene, es muy bueno para los espacios públicos y abiertos. Como México es un país sísmico, pues aguanta muy bien.

Estamos viendo una oportunidad muy grande, porque la Copa del Mundo se aproxima y es cuando se disparan las ventas de pantallas y estamos viendo que en pantallas profesionales y el centro de comando que tenemos de excelente calidad, se nos van a disparar las ventas significativamente y es un excelente tiempo con la Copa del Mundo, los restaurantes están agotando eso, los monitoristas por todas partes están consumiendo pantallas para estar checando el estatus de las cámaras, todos los reportes e incidentes que suceden del medio logístico. Tenemos aplicación prácticamente en el 100% de las verticales que atacamos, como gobierno, *retail*, entretenimiento, la industria restaurantera, etc. Estamos muy emocionados por traer a ustedes este tipo de innovación, ya que el *display* de alta gama viene a complementar toda nuestra oferta de soluciones que tenemos.

RONALD DAVID ZÚÑIGA SÁNCHEZ, *PRODUCT MARKETING MANAGER* PARA LATINOAMÉRICA DE HANWHA VISION

¿Qué están presentando este año en la expo?

Innovación en dos sentidos: *hardware* y *software*. Hanwha Vision es una empresa coreana que trae excelencia en aparte de procesamiento de video, cámaras de seguridad y audio, entonces traemos innovación en ambos sentidos, en *hardware* con la tendencia de tener cámaras con más capacidad de procesamiento en borde, maximizar el procesamiento en borde, lo estamos haciendo con *partnerships*, con NVIDIA o con nuestra propia tecnología para que las cámaras sean cada vez más capaces y poder generar más información útil para el cliente, no sólo cosas de seguridad. Y en *software* estamos trayendo nuevas analíticas para nuevos tipos de objetos, carritos de compras, carritos olvidados o robados, protecciones personalizadas, como el ejemplo que tenemos con WiseDetector.

Traemos de *software* y *hardware*, dos opciones para personalizar el uso de videovigilancia hacia la necesidad del cliente.

Producto estrella

La solución estrella es la cámara multisensor con NVIDIA, el cual conocemos como un líder en el mercado en procesamiento GPU, procesamiento gráfico, etc. Y el *partnership* que es primero en la industria de tener la tecnología de procesamiento dentro de la cámara y que esté funcionando en borde, potenciar o maximizar el procesamiento en borde. Tiene cuatro canales con procesamiento de NVIDIA.

¿Para qué vertical de negocios va dirigido?

Principalmente para seguridad ciudadana y de industria, pero abre la flexibilidad para cualquier caso de uso que necesite correr modelos de Inteligencia Artificial fuertes en borde, lo hemos hecho principalmente para videovigilancia urbana, donde hay múltiples aplicaciones como reconocimiento facial u otros partners que hayan desarrollado sobre NVIDIA pueden correr sobre la cámara. En la industria lo están utilizando mucho para casos muy específicos de seguridad industrial, por ejemplo, un fabricante de vehículos lo planeaba utilizar para alertar cuando los operadores ponen planchas de aluminio y evitar que quede una mano en la maquinaria antes de que prensen el aluminio, y así poder evitar un accidente industrial; eso es posible hacerlo con servidores y gastar mucho en servidores y cámaras normales o con nuestro producto estrella, que es traer la potencia de procesamiento NVIDIA dentro de la cámara, es por eso uno de los productos principales. ■

Fotos: Tania G. Rojo Chávez / **SEA**

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:

CLAVES PARA UN LIDERAZGO EXITOSO

MÉXICO

Foto: Freepick

En la actualidad, las empresas se enfrentan a desafíos cada vez más complejos en su búsqueda de competitividad y éxito sostenible. En este contexto, es crucial comprender cómo es el liderazgo hoy en día.

De acuerdo con un estudio de Gallup, los equipos liderados por personas centradas en los individuos experimentan un 70% menos de rotación de personal, un 21% más de rentabilidad y un 41% menos de ausentismo laboral. Por lo tanto, es importante conocer cómo adoptar un enfoque de liderazgo orientado a las personas para generar un impacto positivo tanto en los colaboradores como en los resultados empresariales.

¿CÓMO HA IDO EVOLUCIONANDO EL LIDERAZGO?

A lo largo de la historia, el liderazgo se ha transformado para adaptarse a las necesidades cambiantes de la sociedad. En sus inicios, estaba ligado al poder y la autoridad, con dirigentes que imponían su voluntad mediante el miedo y la presión. Sin embargo, con la complejidad creciente de las sociedades, surgió la necesidad de gerentes más efectivos en la guía de sus seguidores.

En el liderazgo clásico, que abarcó desde tiempos antiguos hasta el siglo XIX, se valoraban cualidades como valentía, fortaleza, riqueza o astucia; estos líderes ofrecían seguridad a cambio de lealtad. Durante el siglo XX, experimentó cambios significativos debido a los avances tecnológicos y la rápida difusión de la información. Los dirigentes debían adaptarse a los cambios rápidos y comprender su importancia.

En el siglo XXI, el liderazgo enfrenta nuevos desafíos en los ámbitos empresarial y social. Se requieren líderes capaces de manejar la incertidumbre, los cambios constantes, la flexibilidad organizativa y la responsabilidad social.

El enfoque se ha desplazado hacia un liderazgo centrado en la persona, en el que el individuo se convierte en el centro de los procesos en una organización, comunidad o sociedad. Estas demandas se extienden más allá del ámbito organizacional y afectan a todo el entorno social.

¿QUÉ ES EL LIDERAZGO CENTRADO EN LA PERSONA?

Se basa en la premisa de que el talento humano es el activo más valioso de una organización. Reconoce la importancia de comprender y atender las necesidades, motivaciones y aspiraciones de los colaboradores,

y fomenta su crecimiento personal y profesional. Este enfoque no sólo se preocupa por la productividad y los resultados económicos, sino que también busca crear un entorno de trabajo saludable, motivador y enriquecedor para todos.

BIENESTAR Y SALUD: CLAVE PARA EL ÉXITO EMPRESARIAL

Para entender cómo es el liderazgo hoy en día debemos hablar sobre el bienestar y la salud, ya que un estilo de vida saludable no sólo beneficia al equipo humano individualmente, sino que también puede tener un impacto significativo en los resultados empresariales.

Cuando adoptamos el liderazgo orientado en la persona, el bienestar de los colaboradores es crucial, al estar sanos y equilibrados, son más felices, comprometidos y motivados, lo que se traduce en una mayor productividad y un mejor desempeño laboral. Además, un enfoque en el bienestar y la salud puede reducir los costos asociados con la atención médica y el ausentismo laboral, mejorando así la rentabilidad de la empresa.

En la actualidad, las habilidades únicas del ser humano para la creación de tecnología han cambiado la forma en que las empresas operan. Las relaciones humanas juegan un papel clave, tanto con los clientes como con los colaboradores. Es necesario colocar al ser humano en el centro, lo que resulta en colaboradores más comprometidos y alineados con los valores de la empresa.

Comprendiendo las necesidades de los colaboradores, fomentando su crecimiento personal y profesional, y promoviendo programas de bienestar, las organizaciones pueden lograr un mayor compromiso, productividad y satisfacción laboral. Esto también permite comprender mejor al cliente y adaptarse a sus necesidades, generando un impacto positivo en los resultados empresariales y en la experiencia del cliente.

Invertir en el bienestar y desarrollo de los colaboradores es una inversión estratégica que conduce al éxito sostenible de la organización.

En el mundo militar y en la empresa privada existen ejemplos claros de buen liderazgo, pero en el mundo político y especialmente en los últimos años observamos precisamente lo contrario, la falta de un líder que en tiempos de incertidumbre pueda servir de referente por sus virtudes para guiar una nación.

Prestancia, comunicación, imagen, dedicación, son atributos que no son ajenos a la figura del líder político, pero, ahora bien, ¿cuáles son las características que definirían el liderazgo político de nuestro tiempo? ¿Cuáles son los rasgos por los que reconoceremos, indubitadamente, a un líder político?

1) **La credibilidad.** En nuestros días es la cualidad más importante para un líder. El descrédito actual que vive la clase política sólo podrá superarse gracias a ella. En Norteamérica, Barack Obama consiguió crear esta credibilidad haciendo del *'yes, we can'* toda una declaración de Estado. Haciendo a los americanos conscientes de que si algo se proponían podría hacerse realidad. Si hoy en día preguntásemos si el presidente americano es un líder nato, la respuesta estaría condicionada, como no, por los resultados, pero la perspectiva histórica debe servir para juzgar las conductas en cada momento y en 2008 Obama, sin duda, era el líder, el reflejo de toda una Nación bajo un patrón común.
2) **La firmeza.** La política no es terreno para pusilánimes y mucho menos en tiempos de crisis. Ver dudar a un oficial en el campo de batalla es un anticipo de un fracaso seguro y en un espacio, el de la política, en el que valores son el combustible de una máquina diseñada para gobernar, la firmeza, y la resolución son cualidades que proporcionan seguridad a los ciudadanos. Esta cualidad, como ya se ha señalado, esencial en tiempos de crisis, está precisamente ausente del discurso y del relato político occidental actual. Winston Churchill es, quizá, el principal representante de este valor. Su determinación en la lucha de un pueblo contra la barbarie le llevó precisamente a ejercer su liderazgo desde la firmeza.
3) **La autoridad.** Distingámoslo de la firmeza, puesto que, mientras que la primera se refiere a la imposición y la previsibilidad del yo, la autoridad se ejerce frente al resto. También es conveniente diferenciarla del autoritarismo que convierte al líder político en un caudillo local, en una persona que pierde la referencia del partido para convertir la política en él mismo. En este caso, la gran mayoría de caudillos políticos se dan en el ámbito local donde confluyen la cercanía de la acción política con la comunicación directa con el ciudadano. Rudolph Giuliani, el emérito alcalde de Nueva York que lideró la recuperación de la ciudad frente al vandalismo, supo marcar la distinción entre el líder y el caudillo preservando en todo momento la búsqueda del bien común.
4) **La honestidad.** El líder político necesita, al igual que el mando en el Ejército, ser honesto con sus votantes, con los ciudadanos. Cuando el 9 de mayo de 1950, Robert Schuman, el político francés [?]de origen luxemburgués[?], declaró como se construiría la futura Unión Europea no ocultó en su mensaje el esfuerzo y el sacrificio a realizar. Sería, precisamente, a través de las realizaciones concretas, del paso a paso, como se configuraría el mayor espacio de democracia política y económica en la historia de nuestro continente.
5) **La convicción.** El líder político actúa conforme al diálogo, no a la imposición. Su autoridad en este sentido es más moral que ejecutiva porque realmente convence tanto a sus seguidores como incluso a sus adversarios. Muhatma Gandhi es el símbolo perfecto de esta cualidad. Su simple influencia moral le bastó para derrotar a un imperio basando su victoria en principios irreductibles frente al autoritarismo.
6) **La empatía.** Vital en el siglo XXI. A menudo observamos cómo los políticos se asemejan cada vez más actores del Club de la Comedia en sus mítines. No se trata de eso, ni de ser simplemente gracioso. Se trata de empatizar con aquellos ciudadanos que, a pesar de no estar pasando por una buena situación, consiguen llamar su atención y visualizarse como la solución a ese problema. Esta característica es quizá la más etérea del liderazgo político, pero, sin duda, es la más importante en el siglo de lo audiovisual, de lo inmediato, de lo intangible. A John Fitzgerald Kennedy simplemente le bastaba un gesto, una mirada para transmitir una idea, pero también era capaz de captar los sentimientos de sus ciudadanos y convertirlos en su trabajo: la política.

Estas seis características no son, por supuesto, excluyentes de otras muchas que conforman al líder político, pero sí son las principales razones por las que un líder puede ser percibido como tal en nuestro siglo. Quizá sea sólo una casualidad, pero son seis líderes políticos masculinos con seis virtudes en femenino. Los tiempos, incluso para los líderes, están cambiando. ■

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

Columna de
GEMARC

paulina.bustos@dhl.com

PAULINA BUSTOS, DIRECTORA DE SEGURIDAD PATRIMONIAL EN DHL SUPPLY CHAIN.

Más sobre la autora:

LA IMPORTANCIA DE REAPRENDER

MÉXICO

Hablamos constantemente del aprendizaje, de seguirnos preparando, de conocer cosas nuevas. Al menos en seguridad siempre hay mucha oferta de cursos, conferencias, congresos, pero los temas que ya damos como aprendidos los catalogamos como cerrados y creo que por eso algunas veces podemos ser confrontativos en cuanto a ese conocimiento, se vuelve un tipo de ley personal pensar que las entrevistas se tienen que realizar con X estructura, o que mi metodología de análisis de riesgo es la que más aspectos abarca, es difícil no pensarlo así, lo has hecho un montón de veces, te has enfrentado a diferentes retos y has ido perfeccionando ese conocimiento. Pero les voy a platicar cómo me he confrontado con este tema poniendo de ejemplo algo que no sea seguridad, para poder darme algunos permisos.

Una de las cosas que más me enorgullece decir es que soy bailarina de tango. Hace poco más de 15 años empecé a tomar clases con mi esposo, se volvió algo muy representativo nuestro, incluso con nuestra compañía de tango hicimos varias presentaciones en teatros. Siempre bailamos con el mismo maestro y llegamos a conocer muy bien cómo bailaban nuestros compañeros. Ahora viviendo en Guadalajara, Jalisco, encontramos nuevas clases y esto me ha dado mucha perspectiva respecto al aprendizaje.

Foto: Freepick

Foto: Freepick

El orgullo muchas veces nos puede jugar en contra, sobre todo cuando somos líderes o llevamos mucho tiempo haciendo algo, da pánico, no sólo miedo, aceptar que no sabemos algo o que no lo hacemos del todo bien y es lógico, porque con los años te pagan por saber más, por demostrar tus resultados

Lo que provoca moverte a un espacio nuevo con distintas personas te da, lo que considero el regalo más importante, la perspectiva. Es humano que cada maestro se enfoque en lo que le parezca más importante, para alguno será la postura y el abrazo, para otro el caminado y los pivotes, incluso cada uno tendrá sus pasos favoritos y los repetirá más veces.

Yo, en esta primera clase del nuevo ciclo, noté en mí un cierto caminado de pavorreal tratando de demostrar que no soy principiante, como me estaban poniendo ejercicios muy básicos quería ir más allá y darme a notar, pero la realidad es que lo que me conviene es regresar a los básicos, pulir mi caminado, mi postura, y todas las cosas que ya daba por sentadas, pero no lo estaba viendo como una oportunidad, sino como un retroceso.

ABRIRSE AL CONOCIMIENTO

El orgullo muchas veces nos puede jugar en contra, sobre todo cuando somos líderes o llevamos mucho tiempo haciendo algo, da pánico, no sólo miedo, aceptar que no sabemos algo o que no lo hacemos del todo bien y es lógico, porque con los años te pagan por saber más, por demostrar tus resultados. Se necesitan varios *shots* de humildad para estar receptivo al aprendizaje, y no ir a tomar el curso pensando que ya lo sé todo, o dejar pasar la oportunidad para hacer un comentario que contenga todo mi conocimiento y los demás noten que soy relevante.

Aquí es donde creo que decimos que estamos abiertos al conocimiento, pero la realidad es que sólo queremos ir a demostrar qué tanto sabemos del tema, deberíamos (debería) no tener esta lucha mental durante todo el curso pensando si lo está diciendo de manera correcta y mejor abrir la mente para asimilar otro enfoque diferente al nuestro.

En mi trabajo y en mi vida, soy promotora de que las cosas avancen sin ser perfectas para que sí sucedan, y en el camino se van mejorando, y justo eso sucede cuando, por ejemplo, estás montando una coreografía, primero debes tener la estructura, aunque no salga tan artístico, y conforme vayas dominando los pasos le puedes ir metiendo emoción, estrionismo, estirar más las puntas, mejorar la postura.

Y así es como muchas veces tenemos que aprender; sobre la marcha, porque ya está sucediendo un problema o un proyecto, lo hacemos sin la mayor estructura técnica mientras funcione, y lo que deberíamos hacer con los años es perfeccionarlo, aceptar las correcciones de nuestra metodología, porque por más que lo sepamos hacer siempre hay áreas de mejora.

Así que en mi tercer clase de tango y después de este constante debate interno decidí aflojar el cuerpo y volver a aprender todo lo que yo ya daba por sentado, confieso que el hecho de ser todas personas nuevas hace este proceso más sencillo, también ayudó que no gritáramos a los cuatro vientos que nos considerábamos bailarines expertos, pero creo que de todos el factor más importante es tener un buen maestro, que sepa identificar por qué estás poniendo mal la postura, que te quieres adelantar al paso o que llevas tantos años bailando con tu pareja que ya sabes qué te quiere decir sin que el cuerpo haga la indicación correcta.

Un buen maestro es alguien con talento que sabe analizar y sabe comunicar la manera correcta de hacerlo, que cuando te lo explica todo tiene sentido. Y esto también implica a tus maestros anteriores, que ya te contagiaron su pasión por la música y te hicieron desarrollar habilidades que ahora consideras únicas, pero así hay que seguir en el camino del reaprendizaje, teniendo más maestros e incrementando tu perspectiva, para que un día seamos de esos maestros a los que les quieres dedicar un artículo. ■

Foto: Freepick

Muchas veces tenemos que aprender sobre la marcha, porque ya está sucediendo un problema o un proyecto, lo hacemos sin la mayor estructura técnica mientras funcione, y lo que deberíamos hacer con los años es perfeccionarlo, aceptar las correcciones de nuestra metodología, porque siempre hay áreas de mejora

MEJORES PRÁCTICAS PARA LA SEGURIDAD EN MAQUILADORAS

Las medidas de seguridad adecuadas pueden reducir el riesgo de pérdidas financieras debido a robos, accidentes o incumplimiento normativo, así como mejorar la confianza de los empleados y la comunidad en la empresa

MÉXICO

José Luis Sánchez Gutiérrez

Foto: Freepick

Nuevamente estimados lectores, realmente muy emocionado y agradecido por su acostumbrada preferencia; y en esta ocasión tocaremos el tema de la seguridad en las maquiladoras.

Recordemos que las maquiladoras, son entornos industriales donde se producen bienes para la exportación. Estas instalaciones enfrentan una serie de desafíos únicos en términos de seguridad. Les detallo algunas de las mejores prácticas de seguridad que pueden implementarse en éstas:

A) Control de Acceso.
B) Vigilancia y Monitoreo.
C) Iluminación Adecuada.
D) Seguridad Perimetral.
E) Formación del Personal.
F) Control de Inventarios.
G) Respuesta a Emergencias.
H) Colaboración con Autoridades Locales.

A) CONTROL DE ACCESO EN MAQUILADORAS

Es un aspecto fundamental de la seguridad corporativa. Aquí te detallo algunas prácticas clave para implementar un control de acceso efectivo en estas instalaciones:

1.- Sistemas de Identificación:

1.1- Utilización de tarjetas de identificación o credenciales de acceso para todos los empleados y visitantes.

1.2.- Empleo de tecnología de proximidad, tarjetas inteligentes o biometría para mejorar la seguridad y evitar la falsificación por propios o terceros.

2.- Puntos de Acceso Designados:

2.1- Establecimiento de puntos de acceso claramente definidos en las instalaciones con los cuales determinas y centras tu atención en el ingreso de propios y terceros.

2.2- Limitación del número de entradas y salidas para facilitar un mejor control y monitoreo.

3.- Control de Puertas y Entradas:

3.1- Instalación de dispositivos de control de acceso en puertas y entradas principales.

3.2- Uso de cerraduras electrónicas (con su respectiva batería de respaldo), lectores de tarjetas o sistemas de reconocimiento biométrico para autorizar la entrada y salida de las instalaciones.

4.- Sistemas de Registro y Monitoreo:

4.1- Implementación de sistemas de registro y monitoreo para registrar la entrada y salida de todas las personas (empleados, proveedores, visitantes, autoridades, etc.).

4.2- Utilización de *software* de gestión de acceso para mantener un registro preciso de quién ingresa y sale de las instalaciones.

5.- Integración con otros sistemas:

5.1- Integración del sistema de control de acceso con otros sistemas de seguridad, como sistemas de videovigilancia, radares y alarmas.

5.2- Establecimiento de alertas automáticas en caso de intentos de acceso no autorizados o violaciones de seguridad dentro de la instalación y fuera del perímetro de la maquiladora.

6.- Políticas de Acceso:

6.1- Desarrollo de políticas claras y procedimientos para el acceso de empleados, contratistas y visitantes.

6.2.- Establecimiento de criterios de autorización basados en roles y responsabilidades específicas de cada uno.

7.- Constante formación del Personal:

7.1- Mantener una formación y capacitación regular a todos los empleados y personal de seguridad sobre el uso adecuado de los sistemas de control de acceso.

7.2.- Promover la concientización sobre la importancia de la seguridad y la responsabilidad en el manejo de credenciales de acceso de cada uno de los usuarios.

8.- Respaldo y Recuperación de Datos:

8.1- Implementación de medidas de respaldo remoto y recuperación de datos para garantizar la integridad y disponibilidad de la información de acceso.

8.2- Establecimiento de protocolos de seguridad para proteger la información confidencial relacionada con el control de acceso.

B) VIGILANCIA Y MONITOREO

La vigilancia y el monitoreo son aspectos esenciales de la seguridad corporativa en las maquiladoras. Aquí te detallo al-

gunas prácticas clave para implementar un sistema efectivo de vigilancia y monitoreo en estas instalaciones:

1.- Instalación de Cámaras de Vigilancia:

1.1- Colocación estratégica de cámaras de vigilancia en áreas críticas dentro y fuera de las instalaciones.

1.2- Utilización de cámaras de alta resolución con capacidad de visión nocturna para garantizar una supervisión efectiva en todo momento (en algunos casos dependiendo del ambiente exterior -con niebla, por ejemplo- se deberán utilizar cámaras termográficas o incluso algunos drones).

2.- Monitoreo en Tiempo Real:

2.1- Implementación de sistemas de monitoreo en tiempo real para supervisar activamente las imágenes de las cámaras.

2.2- Uso de *software* de gestión de video que permita a los operadores del Centro de Mando, detectar y responder rápidamente ante cualquier incidente o actividad sospechosa identificada.

3.- Almacenamiento y Archivo de Grabaciones:

3.1- Utilización de sistemas de almacenamiento de video robustos y seguros para almacenar grabaciones de cámaras de manera eficiente (preferentemente con respaldo de manera remota).

3.2- Establecimiento de políticas de "retención de datos" para garantizar que las grabaciones estén disponibles para su revisión durante un periodo de tiempo adecuado.

4.- Monitoreo de Perímetros y Áreas Exteriores:

4.1- Colocación de cámaras de vigilancia en los perímetros y áreas exteriores de la planta para detectar intrusiones y actividades sospechosas.

4.2- Utilización de cámaras con capacidades de panorámica, inclinación y *zoom* (PTZ), termográficas y drones, para una cobertura amplia y flexible.

5.- Auditorías de Seguridad y Revisión de Grabaciones:

5.1- Realización de auditorías periódicas de seguridad utilizando grabaciones de video para identificar áreas de mejora y detectar posibles vulnerabilidades.

5.2- Revisión regular de grabaciones de video en respuesta a incidentes o para investigaciones de seguridad posteriores.

Foto: Freepick

C) ILUMINACIÓN ADECUADA

La iluminación adecuada es un aspecto crucial de la seguridad corporativa en las maquiladoras. Aquí te detallo algunas prácticas clave para garantizar una iluminación adecuada en estas instalaciones:

1.-Iluminación Exterior:

1.1- Instalación de luces exteriores potentes en áreas perimetrales, estacionamientos y zonas de acceso para disuadir la intrusión y mejorar la visibilidad durante la noche.

1.2- Utilización de luces de inundación o proyectores para iluminar áreas amplias y reducir los puntos ciegos.

2.- Iluminación Interior:

2.1- Colocación estratégica de luces interiores en pasillos, áreas de trabajo y zonas de almacenamiento para proporcionar una iluminación uniforme y reducir los riesgos de tropiezos y caídas.

2.2- Uso de iluminación dirigida en estaciones de trabajo y áreas de producción para mejorar la visibilidad y la seguridad de los empleados.

3.- Luces de Emergencia:

3.1- Instalación de luces de emergencia en áreas críticas y salidas de emergencia para garantizar una iluminación adecuada durante cortes de energía o situaciones de emergencia.

3.2- Pruebas regulares de las luces de emergencia para asegurar su funcionamiento correcto en caso de necesidad por medio de simulacros programados.

4.- Sensores de Movimiento:

4.1.- Implementación de luces con sensores de movimiento en áreas poco transitadas o exteriores para activar la iluminación cuando se detecte movimiento, lo que puede disuadir la actividad delictiva y reducir el consumo de energía.

5.- Tecnología de Iluminación Eficiente:

5.1.- Utilización de tecnología de iluminación eficiente, como luces LED, que ofrecen una mayor durabilidad, menor consumo de energía y una iluminación más brillante y uniforme en comparación con las fuentes de luz tradicionales.

6.- Mantenimiento Regular:

6.1- Programación de un programa de mantenimiento regular para inspeccionar y mantener todas las luces en óptimas condiciones de funcionamiento.

6.2.- Reemplazo o reparación inmediata de luces defectuosas o fundidas para evitar áreas oscuras que puedan ser aprovechadas por intrusos.

7.- Iluminación de Señalización:

7.1- Instalación de luces de señalización en áreas de riesgo, como escaleras, rampas y salidas de emergencia, para facilitar la evacuación y la navegación en situaciones de emergencia.

D) SEGURIDAD PERIMETRAL

La seguridad perimetral en maquiladoras es esencial para proteger las instalaciones y sus activos contra intrusiones no autorizadas. Aquí te detallo algunas prácticas


Foto: Freepick

clave para garantizar una seguridad perimetral efectiva en estas instalaciones:

1.- Cercado Perimetral:

1.1- Instalación de cercas perimetrales robustas y de altura adecuada para delimitar claramente los límites de la propiedad.

1.2- Utilización de materiales resistentes y difíciles de escalar, como malla metálica o alambre de púas, para disuadir a los intrusos.

2.- Control de Acceso:

2.1- Establecimiento de puntos de acceso controlados y vigilados en las entradas y salidas de la planta.

2.2.- Implementación de sistemas de control de acceso, como tarjetas de identificación o lectores biométricos, para autorizar la entrada de personas autorizadas y registrar la actividad de los visitantes.

3.- Vigilancia Electrónica:

3.1- Instalación de sensores de movimiento y sistemas de detección de intrusos a lo largo del perímetro para alertar sobre cualquier intento de intrusión.

3.2.- Utilización de tecnología de videovigilancia con cámaras de alta resolución y visión nocturna para monitorear continuamente el perímetro y registrar cualquier actividad sospechosa.

4.- Iluminación Exterior:

4.1- Implementación de iluminación exterior adecuada en todo el perímetro de la planta para disuadir la intrusión durante la noche.

4.2.- Utilización de luces de inundación o proyectores con sensores de movimiento para activarse automáticamente ante la detección de actividad no autorizada.

5.- Patrullaje y Vigilancia Humana:

5.1.- Realización de patrullas regulares por parte de personal de seguridad a lo largo del perímetro para detectar y responder rápidamente a cualquier intrusión.

5.2.- Implementación de torres de vigilancia elevadas para proporcionar una vista panorámica del área perimetral y aumentar la visibilidad del personal de seguridad.

E) FORMACIÓN DEL PERSONAL

La formación del personal en maquiladoras es fundamental para garantizar la seguridad y el bienestar de todos los empleados, así como para proteger los activos de la empresa. Aquí te detallo algunas prácticas clave para llevar a cabo una formación y capacitación efectiva en estas instalaciones:

1.- Entrenamiento en Seguridad Laboral:

1.1- Proporcionar formación en seguridad laboral para todos los empleados, incluyendo temas como prevención de accidentes, manejo de productos químicos y procedimientos de emergencia.

1.2.- Enseñanza de prácticas seguras de trabajo y el uso adecuado de equipo de protección personal (EPP) específico para cada tarea.

2.- Concientización sobre Seguridad:

2.1.- Realización de sesiones de concientización regular para destacar la importancia de la seguridad en el lugar de trabajo y fomentar una real cultura de seguridad.

2.2.- Promoción de la participación activa, de los empleados en la identificación y reporte de riesgos potenciales.

3.- Capacitación en Manejo de Maquinaria:

3.1.- Entrenamiento especializado en el manejo seguro de la maquinaria utilizada en la producción, incluyendo operación, mantenimiento y procedimientos de apagado de emergencia.

3.2.- Certificación de los empleados que operan equipos especializados después de completar con éxito la capacitación correspondiente.

4.- Prevención de Incendios y Evacuación:

4.1.- Realización de simulacros periódicos de incendio y evacuación para familiarizar a los empleados con los procedimientos de emergencia y las rutas de evacuación.

4.2.- Capacitación en el uso adecuado de extintores de incendio y otros equipos de lucha contra incendios.

5.- Seguridad en el Manejo de Materiales:

5.1- Entrenamiento en el manejo seguro de materiales y productos, incluyendo técnicas adecuadas de levantamiento y transporte.

5.2.- Instrucción sobre el almacenamiento seguro de productos químicos y materiales inflamables, así como la manipulación adecuada de desechos y residuos.

6.- Seguridad en la Cadena de Suministro:

6.1.- Capacitación en seguridad para empleados involucrados en la recepción, almacenamiento y distribución de materiales y productos en la cadena de suministro.

6.2.- Educación sobre la importancia de la verificación de identidad y la inspección de cargas para prevenir la intrusión de productos no autorizados.

7.- Actualización Continua:

7.1.- Programación de sesiones regulares de capacitación y actualización para mantener a los empleados al tanto de los cambios en los procedimientos de seguridad y las regulaciones gubernamentales.

7.2.- Fomento de una cultura de aprendizaje continuo y mejora en materia de seguridad entre todos los empleados.

F) CONTROL DE INVENTARIOS

El control de inventarios en maquiladoras es fundamental para garantizar la eficiencia operativa, la transparencia y la seguridad de los activos de la empresa. Aquí te detallo algunas prácticas clave para llevar a cabo un control efectivo de inventarios en estas instalaciones:

1.- Sistema de Gestión de Inventarios:

1.1.- Implementación de un sistema de gestión de inventarios automatizado y centralizado que permita el seguimiento en tiempo real de los movimientos de inventario.

1.2.- Utilización de *software* especializado que facilite la identificación, conteo y registro de todos los productos y materiales almacenados en la maquiladora.

2.- Etiquetado y Codificación:

2.1.- Etiquetado y codificación de todos los productos y materiales con información detallada, como número de serie, código de barras o RFID, para facilitar la identificación y el seguimiento individual de cada ítem.

2.2.- Utilización de etiquetas y códigos de identificación únicos para cada producto para evitar confusiones y errores en el registro y control de inventarios.

3.- Inventarios Periódicos:

3.1.- Realización de inventarios físicos periódicos para verificar la precisión de los registros del sistema y detectar posibles discrepancias o pérdidas de inventario.

3.2.- Programación de auditorías internas regulares para revisar y validar la exactitud de los datos de inventario y garantizar el cumplimiento de los procedimientos establecidos.

4.- Control de Entradas y Salidas:

4.1.- Registro detallado de todas las entradas y salidas de productos y materiales de la maquiladora, incluyendo fechas, cantidades y responsables.

4.2.- Implementación de procedimientos de autorización y verificación para garantizar que sólo personal autorizado pueda acceder y manipular el inventario.

5.- Seguridad Física:

5.1.- Almacenamiento seguro de los inventarios en áreas designadas y protegidas, como almacenes cerrados con acceso restringido y sistemas de seguridad perimetral.

5.2.- Utilización de cerraduras electrónicas y de alta seguridad, cámaras de vigilancia y sistemas de alarma para proteger contra robos e intrusiones no autorizadas.

Foto: Freepick

6.- Rotación de *Stock*:

6.1.- Implementación de prácticas de rotación de *stock* para garantizar que los productos más antiguos se utilicen primero y se minimicen las pérdidas por obsolescencia o caducidad.

6.2.- Monitoreo continuo de los niveles de inventario y ajuste de las cantidades almacenadas según la demanda y las proyecciones de ventas.

G) RESPUESTA A EMERGENCIAS

La respuesta a emergencias en maquiladoras es crucial para garantizar la seguridad y el bienestar de los empleados, así como para proteger los activos y la continuidad operativa de la empresa. Aquí te detallo algunas prácticas clave para llevar a cabo una respuesta efectiva a emergencias en estas instalaciones:

1.- Planificación de Emergencias:

1.1.- Desarrollo de un plan de emergencias detallado que incluya procedimientos claros y específicos para diferentes tipos de emergencias, como incendios, accidentes químicos, evacuaciones y amenazas de seguridad.

1.2.- Identificación de roles y responsabilidades del personal en caso de emergencia, incluyendo líderes de equipo, brigadistas de emergencia y coordinadores de evacuación.

2.- Simulacros y Entrenamiento:

2.1.- Realización regular de simulacros de emergencia para familiarizar a los empleados con los procedimientos de respuesta y practicar la evacuación de manera segura y ordenada.

2.2.- Capacitación del personal en primeros auxilios, manejo de extintores de incendio y otras habilidades básicas de respuesta a emergencias.

3.- Comunicación y Alerta:

3.1.- Establecimiento de un sistema de comunicación efectivo para alertar rápidamente a todos los empleados sobre una emergencia y proporcionar instrucciones claras sobre cómo responder.

3.2.- Utilización de alarmas audibles, sistemas de megafonía y mensajes de texto o correos electrónicos para notificar a los empleados sobre la situación de emergencia y las acciones a tomar.

4.- Evacuación Segura:

4.1.- Definición de rutas de evacuación claramente marcadas y salida de emergencia en todas las áreas de la maquiladora, con señalización adecuada y luces de emergencia.

4.2.- Designación de puntos de encuentro fuera de las instalaciones para garantizar la contabilidad de todos los empleados durante una evacuación.

5.- Coordinación con Autoridades Locales:

5.1.- Establecimiento de relaciones de colaboración con los servicios


Foto: Freepick

de emergencia locales, como bomberos, policía y servicios médicos de emergencia, para facilitar una respuesta coordinada y eficiente a situaciones de crisis.
5.2.- Participación en ejercicios de respuesta conjunta con las autoridades locales para mejorar la coordinación y la capacidad de respuesta en caso de emergencia.

6.- Equipamiento de Emergencia:
6.1.- Mantenimiento regular de equipos de emergencia, como extintores de incendio, botiquines de primeros auxilios, kits de derrames químicos y equipos de protección personal (EPP).
6.2.- Disponibilidad de recursos adicionales, como camillas, mantas térmicas y equipos de rescate, para responder a situaciones de emergencia de manera efectiva.

H) COLABORACIÓN CON AUTORIDADES LOCALES

La colaboración con las autoridades locales en maquiladoras es esencial para garantizar la seguridad y el cumplimiento de las regulaciones en el lugar de trabajo. Aquí detallo algunas prácticas clave para establecer y mantener una colaboración efectiva con las autoridades locales:

1.- Establecimiento de Relaciones:
1.1.- Iniciar y mantener una relación proactiva con las autoridades locales pertinentes, como la policía, el cuerpo de bomberos, los servicios médicos de emergencia, protección civil, y las agencias gubernamentales de regulación.
1.2.- Designar un punto de contacto principal dentro de la maquiladora para facilitar la comunicación y la coordinación con las autoridades locales.

2.- Participación en Reuniones y Foros:
2.1.- Asistir a reuniones y foros de seguridad locales donde se discutan temas relevantes para la comunidad y la industria, y donde se puedan establecer vínculos con las autoridades locales.
2.2.- Contribuir activamente en la planificación de la seguridad pública y las iniciativas de prevención del delito en el área circundante a la maquiladora.

3.- Compartir Información:
3.1.- Compartir información relevante con las autoridades locales, como planes de emergencia, datos sobre incidentes de seguridad, y cambios en las operaciones que puedan afectar la seguridad pública.
3.2.- Colaborar en la identificación y mitigación de riesgos de seguridad en la comunidad, como puntos vulnerables en las rutas de transporte de carga o áreas propensas a la delincuencia.

4.- Coordinación de Ejercicios y Simulacros:
4.1.- Coordinar y participar en ejercicios y simulacros conjuntos con las autoridades locales para mejorar la preparación y la capacidad de respuesta ante situaciones de emergencia.
4.2.- Practicar la coordinación y la comunicación entre la maquiladora y las autoridades locales durante estos ejercicios para garantizar una respuesta efectiva en caso de crisis.

5.- Apoyo Mutuo en Emergencias:
5.1.- Establecer protocolos claros para la comunicación y la coordinación durante situaciones de emergencia, incluyendo la activación de recursos de emergencia y la prestación de asistencia mutua según sea necesario.
5.2.- Brindar apoyo logístico y operativo a las autoridades locales durante emergencias, como acceso a instalaciones, equipos de seguridad y recursos humanos capacitados.

6.- Cumplimiento Normativo:
6.1.- Trabajar en estrecha colaboración con las autoridades locales para garantizar el cumplimiento de las regulaciones de seguridad, medio ambiente y salud ocupacional en la maquiladora.
6.2.- Proveer acceso a instalaciones y registros para inspecciones regulatorias y colaborar en la resolución de cualquier hallazgo o requerimiento regulatorio.

También, desde mi observador, les comparto los pros y contras para la seguridad en maquiladoras.

PROS DE LA SEGURIDAD EN MAQUILADORAS

a) **Protección del personal:** la implementación de medidas de seguridad en maquiladoras ayuda a proteger la integridad física y el bienestar de los empleados, reduciendo el riesgo de accidentes laborales y lesiones.
a) **Prevención de pérdidas:** la seguridad adecuada en las maquiladoras ayuda a prevenir robos, vandalismo y otros tipos de pérdidas, lo que a su vez contribuye a mantener la rentabilidad del negocio.
a) **Cumplimiento normativo:** el establecimiento de protocolos de seguridad garantiza el cumplimiento de regulaciones y normativas locales e internacionales, evitando sanciones y multas por incumplimiento.
a) **Continuidad operativa:** la implementación de medidas de seguridad contribuye a mantener la continuidad de las operaciones al reducir el impacto de eventos adversos, como desastres naturales o emergencias.
a) **Mejora de la imagen corporativa:** una buena gestión de seguridad en las maquiladoras puede mejorar la reputación de la empresa, tanto entre los empleados como entre los clientes y la comunidad en general.

CONTRAS DE LA SEGURIDAD EN MAQUILADORAS

a) **Costos financieros:** la implementación y mantenimiento de sistemas de seguridad puede implicar costos significativos, incluyendo la inversión

en tecnología, equipos y capacitación del personal.

a) **Complejidad operativa:** la gestión de la seguridad en entornos industriales puede ser compleja debido a la naturaleza de las operaciones y a la diversidad de riesgos asociados, lo que requiere una planificación cuidadosa y recursos adecuados.
a) **Resistencia del personal:** algunos empleados pueden percibir las medidas de seguridad como restrictivas o intrusivas, lo que puede generar resistencia y afectar la moral y la productividad.
a) **Vulnerabilidad ante la corrupción:** en algunos casos, la corrupción o la colusión interna pueden comprometer la efectividad de las medidas de seguridad, especialmente si no se implementan controles adecuados.
a) **Posible impacto en la productividad:** algunas medidas de seguridad, como controles de acceso o procedimientos de registro, pueden ralentizar los procesos operativos y afectar la eficiencia y la productividad.

NOVELTY, FEASIBILITY, SPECIFICITY, IMPACT Y WORKABILITY

Una vez más, no quiero dejar pasar mí ya tradicional análisis *Novelty, Feasibility, Specificity, Impact* y *Workability* en esta ocasión, aplicado a la seguridad en maquiladoras:

- ***Novelty* (Novedad):** la seguridad en maquiladoras ha sido una preocupación constante, pero su enfoque ha evolucionado con el tiempo para adaptarse a las cambiantes amenazas y tecnologías. La novedad radica en la implementación de soluciones de seguridad más avanzadas, como sistemas de vigilancia inteligente, tecnología biométrica y análisis predictivo de datos para prevenir riesgos y proteger a los empleados y activos
- ***Feasibility* (Viabilidad):** la viabilidad de implementar medidas de seguridad en maquiladoras es alta, dado el acceso a tecnologías avanzadas y la disponibilidad de recursos financieros para inversiones en seguridad. Sin embargo, también es importante considerar la viabilidad operativa y logística, así como el tiempo y los recursos necesarios para la implementación efectiva de las medidas de seguridad.

Foto: Freepick

- ***Specificity* (Especificidad):** las medidas de seguridad en maquiladoras deben ser específicas y adaptadas a las necesidades y riesgos específicos de cada instalación. Esto incluye la identificación de áreas de vulnerabilidad, como accesos no autorizados, robo de mercancías o riesgos laborales, y la implementación de soluciones específicas para abordar estos problemas de manera efectiva; como siempre se los he comentado, "hay que hacer un traje a medida" de cada instalación.
- ***Impact* (Impacto):** el impacto de la seguridad en maquiladoras es significativo tanto en términos de protección de empleados y activos como en la continuidad operativa y la reputación de la empresa. Las medidas de seguridad adecuadas pueden reducir el riesgo de pérdidas financieras debido a robos, accidentes o incumplimiento normativo, así como mejorar la confianza de los empleados y la comunidad en la empresa.
- ***Workability* (Viabilidad Operativa):** la viabilidad operativa de las medidas de seguridad en maquiladoras se refiere a su capacidad para integrarse de manera efectiva en los procesos y operaciones existentes sin afectar negativamente la eficiencia y la productividad. Es importante asegurarse de que las medidas de seguridad no obstaculicen el flujo de trabajo o generen una carga adicional para el personal, sino que complementen las actividades diarias y mejoren el ambiente laboral.

Tomar en cuenta que siempre como seguridad corporativa tenemos en todo momento como objetivo, el cuidado de las personas, de los activos físicos y biológicos, el cuidado de la reputación (imagen y marca), así como realmente apoyar la rentabilidad del negocio con todas las actividades realizadas en el área.

Una vez más, gracias por permitirme compartir contigo este artículo, esperando sea de tu interés y nos leemos en la siguiente edición. ■

José Luis Sánchez Gutiérrez, director de Seguridad Patrimonial en la Industria Cárnica. *Más sobre el autor:*

SEGURIDAD INTEGRAL EN PARQUES INDUSTRIALES

La implementación de medidas preventivas, la capacitación continua y la innovación tecnológica son fundamentales para garantizar un entorno industrial seguro y sostenible

COSTA RICA | **Juan Luis Parra Acosta**

La seguridad en los parques industriales, y en general en todas las organizaciones, constituye un elemento crítico para asegurar un entorno laboral saludable, salvaguardar la integridad de los trabajadores y resguardar los activos corporativos. La gestión de la seguridad no admite aproximaciones superficiales; más bien, exige un compromiso total por parte de todos los integrantes de la comunidad y un análisis detenido de las medidas esenciales y las mejores prácticas destinadas a potenciar la seguridad en los parques industriales.

En el ámbito ejecutivo, la seguridad se perfila como una prioridad estratégica que impacta directamente en la continuidad operativa y el rendimiento de la empresa. Asegurar un ambiente de trabajo exento de riesgos no sólo cumple con normativas regulatorias, sino que también responde a la responsabilidad de preservar el bienestar de los empleados y salvaguardar los recursos esenciales de la organización.

La adopción de medidas proactivas en seguridad implica una implicación activa y consciente de cada individuo dentro de la comunidad empresarial. Desde los niveles ejecutivos hasta el personal operativo, todos desempeñan un papel vital en el fortalecimiento de una cultura de seguridad sólida. Esta cultura no sólo se limita a cumplir con protocolos; va más allá, fomentando la concientización y la responsabilidad compartida en la prevención de riesgos.

Foto: Freepick

En términos prácticos, la seguridad como un todo implica la implementación de estrategias integrales que aborden las distintas dimensiones del entorno laboral. Esto incluye inversiones en tecnologías de seguridad avanzadas, capacitación continua para los empleados, protocolos de respuesta ante emergencias y una constante evaluación de riesgos. Además, se enfatiza la importancia de colaborar activamente con organismos regulatorios y fuerzas de seguridad para mantenerse actualizado sobre las mejores prácticas y normativas vigentes.

ASPECTOS A CONSIDERAR

Desde una perspectiva ejecutiva, la seguridad no sólo se concibe como una exigencia legal, sino como un componente integral para garantizar la sostenibilidad y reputación de la empresa. La gestión proactiva de riesgos y la promoción de una cultura de seguridad robusta son esenciales para proteger el capital humano y los activos corporativos, contribuyendo así al éxito sostenible de la organización en el entorno empresarial actual. Algunos puntos importantes a tomar en cuenta cuando hablamos de seguridad en los parques industriales son:

- **Gestión de Riesgos:** la evaluación periódica de riesgos se convierte en un aspecto crítico para identificar potenciales peligros en el parque industrial. Se enfatiza la importancia de realizar evaluaciones cuantitativas, preferiblemente mediante la metodología de juicio de expertos, para garantizar una evaluación precisa. Se recomienda la revisión continua de riesgos y la auditoría regular de los sistemas de seguridad.
- **Planes de Emergencia:** la elaboración de planes de emergencia en colaboración con los responsables de HSE de las empresas del parque es esencial. Estos planes deben abordar diversas situaciones, desde incendios hasta amenazas de bombas. La realización periódica de simulacros garantiza una respuesta efectiva en casos de emergencia.
- **Capacitación Continua:** se destaca la importancia de proporcionar capacitación regular a los empleados sobre prácticas seguras de trabajo y manejo de emergencias. La formación debe incluir información específica sobre los riesgos presentes en el parque industrial para mejorar la conciencia situacional.
- **Equipamiento de Seguridad:** asegurar que los trabajadores dispongan del equipo de protección personal necesario es fundamental. La revisión constante de equipos de seguridad, como extintores y sistemas contra incendios, es esencial para mantener su eficacia.
- **Coordinación entre Empresas:** fomentar asociaciones de ayuda mutua entre las empresas del parque y externas para fortalecer la colaboración y coordinación en materia de seguridad. El intercambio de mejores prácticas y experiencias contribuye a robustecer las medidas de seguridad en conjunto.
- **Vigilancia y Monitoreo:** implementar sistemas avanzados de vigilancia y monitoreo en áreas críticas del parque industrial es crucial. Se resalta la importancia de capacitar regularmente al personal de monitoreo sobre procedimientos y responsabilidades. La incorporación de tecnologías como videovigilancia con inteligencia artificial y sensores potencia la detección temprana de posibles riesgos.

En sí, la seguridad en los parques industriales es un esfuerzo colectivo que requiere la colaboración activa de todas las empresas presentes. La implementación de medidas preventivas, la capacitación continua y la innovación tecnológica son fundamentales para garantizar un entorno industrial seguro y sostenible. ■

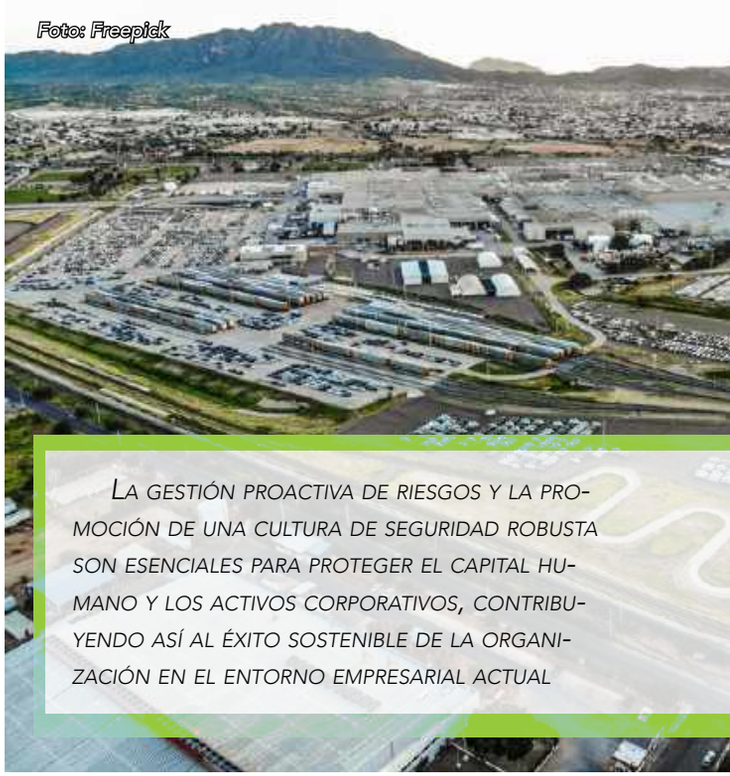


Foto: Freepick

La gestión proactiva de riesgos y la promoción de una cultura de seguridad robusta son esenciales para proteger el capital humano y los activos corporativos, contribuyendo así al éxito sostenible de la organización en el entorno empresarial actual


Foto: Freepick

La incorporación de tecnologías como videovigilancia con inteligencia artificial y sensores potencia la detección temprana de posibles riesgos

Juan Luis Parra Acosta, CPP, gestor de riesgos con más de 20 años de experiencia en el área de la Seguridad Corporativa. *Más sobre el autor:*

PARA LOS GESTORES DE RIESGO: CUANDO EL RIESGO ERES TÚ MISMO

Los impactos de un buen o mal líder en la empresa

Foto: Freepick

PERÚ

Herbert Calderón

En primer término, es necesario revisar la figura del gerente en una empresa que desempeña un papel crucial en la dinámica y el éxito de un equipo de trabajo, siempre y cuando este pueda motivar, inspirar y potenciar a sus empleados, mientras que si es un mal gerente puede tener un efecto destructivo en el ambiente laboral y en la productividad del equipo.

Sus peores errores usualmente son: la agresividad, la manipulación, el egoísmo, el no saber escuchar, la mala comunicación, la falta de empatía, la poca flexibilidad, el pensar que siempre tienen la razón, el llevarse los créditos por el trabajo de otros.

Por lo tanto, un mal jefe y un consiguiente mal plan afectan la operación y el objetivo fundamental, que son los clientes, ante los problemas con la baja de la calidad de los servicios y la baja de calidad de atención del personal, pues un empleado psicológicamente afectado transmite eso a los clientes o presionado por las metas descuida la posventa.

Los profesionales en general tienen aptitudes y actitudes relacionadas con las funciones a realizar, todas ellas acordes con la misión y visión de la empresa. Por ello la empresa debería llevar un proceso de selección, evaluación con base en los objetivos trazados, así como la experiencia en manejo de crisis, inteligencia emocional, habilidades en comunicación, habilidades técnicas, necesarias e imprescindibles. En nuestro caso, en cuanto a la conducción de riesgos, podrían estar en manos adecuadas o inadecuadas, y ello repercute en la solución de problemas en la organización.

Tal es el caso en la conducción de riesgos, si hay una actitud irresponsable, desordenada, inadecuada, incoherente el resultado va a hacer una total ausencia de resultados adecuados, en donde posiblemente se afecte la operación.

Es más, si el gestor de riesgos es una profesional con poco sentido de responsabilidad podría desmembrar su posición, eludir funciones, evitar responsabilidades y contratar profesionales incompetentes también.

La gran responsable de toda esta situación es la misma empresa, la cual es la responsable de captar el recurso humano adecuado para cada necesidad, sobre todo con condiciones especiales para los responsables de riesgos. La situación empeora cuando no se hace seguimiento a la gestión del funcionario, dado que puedan existir situaciones de ausencia de apoyo, involucramiento, seguimiento, los denominados riesgos propios de la función, y que a la larga crearán o agravarán situaciones inseguras en general.

RIESGOS FUNCIONALES

Son los riesgos referidos a la gestión, el apoyo de la organización hacia los responsables de seguridad, así como de la percepción, el grado de responsabilidad percibida por todos los colaboradores. Este viene a ser uno de los aspectos más relevantes en el proceso, dado que de no tener resultados positivos en las varibales de análisis, es muy probable que impacte a los riesgos operacionales, en la forma de:

1) Eludir responsabilidades.
2) Culpar y no asumir faltas propias.
3) No liderar en su proceso sobre la protección de su patrimonio.
4) No reaccionar correctamente ante crisis operacionales como: incendios, desastres naturales, fraudes, sabotajes, extorsiones, acoso, huelgas, etc.
5) Ser cómplice o autor de un ilícito.
6) No apoyar y obstaculizar la gestión del proceso de protección.
7) Maltratar y genera un clima laboral inadecuado.
8) Seleccionar a personas inadecuadas para desarrollar gestión en el proceso.
9) No tomar acciones concretas y de acuerdo a recomendaciones para la protección del patrimonio.
10) Ausencia de apoyo y presupuestos para el proceso de proteccion.
11) Inversiones y gastos del proceso de protección no salen de las áreas de operación.
12) Ocultar, no informar, participar en ilícitos.
13) Desestimar, obstaculizar proyectos relacionados con la mejora de la protección, equipos de respuesta a contigencias, planes de continuidad del negocio.
14) Obstaculizar, postergar, aminorar y maquillar los hallazgos o el proceso de las auditorías internas.

Variables para medir los riesgos funcionales:

1) Apoyo gerencial.
2) Conciencia operacional.
3) Involucramiento de los dueños en los procesos. ■

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

ESS+®

FERIA INTERNACIONAL DE SEGURIDAD

30+ AÑOS

Generando oportunidades para la industria de la seguridad en Latinoamérica

Exhibición tecnológica *en tiempo real*

Showcase *de innovación*

Pabellón *safety*

Conferencias *y talleres*

Rueda de *negocios*

21-23 AGOSTO 2024

Bogotá, Colombia

EXPERIENCIA · NEGOCIOS · PROGRESO

- Seguridad Electrónica
- Seguridad Industrial
- Seguridad Contra Incendios
- Ciberseguridad

REGÍSTRESE COMO VISITANTE

Escanee el código QR para asistir sin costo todos los días de la feria

Visite una feria madura, con trayectoria y un propósito superior:

ser parte de la solución

GREMIOS ALIADOS

ORGANIZAN

MEDIOS ALIADOS

securityfaircolombia.com

DESARROLLO PROFESIONAL:
UNA GUÍA PARA PROFESIONALES DE GESTIÓN DE RIESGOS

Los profesionales bien informados y calificados están mejor equipados para identificar, evaluar y mitigar riesgos de forma efectiva, protegiendo así los intereses de la organización

Foto: t-RisK

BRASIL **Tácito Augusto Silva Leite**

El manejo de riesgos es una disciplina vital que ha evolucionado significativamente a lo largo de las últimas décadas. En un mundo empresarial cada vez más complejo e interconectado, la capacidad de identificar, evaluar y mitigar riesgos es crucial para la sostenibilidad y el éxito de cualquier organización. Con la evolución de las amenazas y la creciente presión por transparencia y cumplimiento, los profesionales de manejo de riesgos enfrentan desafíos constantes y la necesidad de adaptación y aprendizaje continuo.

En el entorno actual, caracterizado por la rápida evolución tecnológica, cambios regulatorios y un panorama de riesgos cada vez más complejo, los profesionales del sector deben mantenerse actualizados con las últimas herramientas, técnicas y mejores prácticas en manejo de riesgos. La actualización continua es fundamental no sólo para el desarrollo individual, sino también para el fortalecimiento y la resiliencia de las organizaciones ante los desafíos presentes y futuros.

Este artículo ofrece una exploración de estrategias esenciales para profesionales que desean mantener su relevancia y eficacia en el campo del manejo de riesgos. Abordaremos la importancia de la lectura continua de publicaciones del sector, de la asociación a organizaciones profesionales, de la participación en cursos en línea, del uso de herramientas de *software* avanzadas y de la presencia en conferencias y eventos relevantes. Además, discutiremos cómo estas prácticas pueden integrarse en un plan de desarrollo profesional estructurado, orientado al crecimiento continuo y la excelencia en el área de manejo de riesgos.

Al final de la lectura, los profesionales estarán mejor equipados para navegar en el dinámico campo del manejo de riesgos, con perspectivas sobre cómo mantenerse actualizados y continuar contribuyendo significativamente a sus organizaciones y a la disciplina en su conjunto.

LEA PUBLICACIONES DEL SECTOR

En el dinámico campo de la gestión de riesgos, mantenerse actualizado con las últimas tendencias, investigaciones y mejores prácticas es crucial. Una manera efectiva de permanecer informado es a través de la lectura regular de publicaciones relevantes del sector. Estas publicaciones pueden incluir revistas académicas, revistas especializadas, boletines informativos, y reportes de investigación y análisis.

Los profesionales de gestión de riesgos deben entender que el sector está en constante evolución, con nuevas amenazas emergiendo y estrategias de mitigación siendo desarrolladas. La lectura continua permite a los profesionales anticiparse a tendencias, adaptarse a nuevas regulaciones y aplicar las mejores prácticas en sus operaciones.

Es esencial elegir publicaciones que sean reconocidas por su calidad, relevancia y contribución al campo de la gestión de riesgos. Esto puede incluir material específico de la industria, además de publicaciones académicas que traten teorías y metodologías avanzadas.

Además de adquirir conocimiento, los profesionales deben ser capaces de traducir la información obtenida en acciones prácticas dentro de sus organizaciones. Esto significa identificar *insights* aplicables, tendencias emergentes y estudios de caso relevantes que puedan informar estrategias de gestión de riesgos más efectivas.

La dedicación a la lectura y al estudio demuestra un compromiso con la excelencia y el desarrollo profesional continuo. Este compromiso no sólo beneficia al individuo en su carrera, sino también contribuye a la resiliencia y el éxito de la organización en la que trabaja.

Además de las revistas académicas y especializadas, es importante reconocer el valor de formatos variados, como boletines informativos, blogs, *podcasts* y hasta canales de video. Cada uno de estos formatos puede ofrecer perspectivas únicas e *insights* en tiempo real, haciendo el aprendizaje más dinámico y adaptable a las preferencias individuales de consumo de información.

Animar a los profesionales a personalizar sus suscripciones y seguir publicaciones que se alineen directamente con sus áreas de especialización eleva la relevancia y la aplicabilidad de los conocimientos adquiridos. Como en el ejemplo dado, un profesional enfocado en riesgos de seguridad cibernética se beneficiaría inmensamente de seguir fuentes especializadas como CSO Online, Dark Reading, The Hacker News, entre otros.

Es útil también destacar estrategias para integrar estas lecturas al día a día profesional. Esto puede incluir la asignación de horarios específicos para la actualización, la participación en discusiones internas sobre artículos recientes o la organización de grupos de estudio con colegas para debatir sobre las novedades y aplicaciones prácticas de los *insights* adquiridos.

Al diversificar las fuentes de información, el profesional no sólo se mantiene actualizado con los desarrollos del sector, sino también enriquece su base de conocimiento, volviéndose más versátil y capaz de anticipar riesgos emergentes y aplicar soluciones innovadoras.

ASOCIACIONES Y GRUPOS PROFESIONALES

La afiliación a asociaciones profesionales es una estrategia valiosa para profesionales de la gestión de riesgos que desean expandir su red de contactos, acceder a recursos educativos exclusivos y participar en iniciativas que promueven el desarrollo del área. Las asociaciones profesionales ofrecen oportunidades únicas de *networking*, permitiendo que los miembros interactúen con colegas, líderes del sector y expertos. Estas relaciones pueden ser fundamentales para el intercambio de conocimientos, experiencias y para la formación de colaboraciones significativas.

Muchas asociaciones proporcionan acceso a una amplia gama de recursos educativos, incluyendo talleres, seminarios, *webinars* y publicaciones exclusivas. Además, algunas asociaciones ofrecen programas de certificación que pueden enriquecer el currículo del profesional y reconocer formalmente sus competencias en el campo de la gestión de riesgos.

Asociarse a una organización profesional también permite que los individuos contribuyan activamente al avance del campo de la gestión de riesgos. Esto puede incluir la participación en comités, contribuciones a publicaciones del sector e involucramiento en investigaciones.

Las asociaciones frecuentemente organizan conferencias y eventos que destacan las últimas tendencias, investigaciones y mejores prácticas en gestión de riesgos. Participar en estos eventos puede proporcionar *insights* valiosos y actualizados, además de inspirar nuevas aproximaciones y estrategias.

Al elegir una asociación para afiliarse, es importante evaluar su relevancia para el área de especialización del profesional, la calidad de los recursos ofrecidos y el potencial para *networking* y desarrollo profesional.

La participación en foros en línea y grupos de discusión, como mencionado en el texto, es una excelente forma de complementar la experiencia proporcionada por las asociaciones profesionales. Plataformas como LinkedIn o foros especializados permiten que los profesionales compartan experiencias, intercambien ideas y discutan las últimas novedades en herramientas y técnicas de gestión de riesgos. Este intercambio fomenta un ambiente de aprendizaje colaborativo y expone a los miembros a una amplia variedad de perspectivas dentro de la comunidad de gestión de riesgos.

Además de los recursos tradicionales, puedes buscar conocimiento en informes globales de riesgo, como el Global Risk Report del World Economic Forum, y actualizaciones de consultorías renombradas. Estos recursos complementan el aprendizaje y la actualización profesional, ofreciendo *insights* sobre las tendencias globales y mejores prácticas en auditoría y gestión de riesgos.

Ejemplos de asociaciones profesionales incluyen el Project Management Institute (PMI), el Institute of Risk Management (IRM), el Institute of Strategic Risk Management (ISRM), la International Association of Risk and Compliance Professionals (IARCP), la Associação Brasileira de Profissionais de Segurança (ABSEG), entre otras. Esta información puede ser útil para dirigir a los profesionales a las organizaciones más relevantes y reconocidas en gestión de riesgos, donde pueden encontrar oportunidades de *networking*, educación y certificación.

FORMACIÓN Y CURSOS EN LÍNEA

Las plataformas de cursos en línea ofrecen una variedad de módulos que cubren diferentes aspectos de la gestión de riesgos. Esto incluye análisis de riesgo, evaluación de riesgo, comunicación de riesgo, mitigación de riesgo y reportes de riesgo. Esta variedad permite que los profesionales profundicen conocimientos en áreas específicas, según sus necesidades e intereses.

Los cursos en línea ofrecen la oportunidad de personalizar la trayectoria de aprendizaje de acuerdo con el nivel de experiencia, objetivos y disponibilidad de tiempo del profesional. Esta personalización es crucial para maximizar la relevancia y la eficacia del aprendizaje, permitiendo que los profesionales elijan cursos que mejor se alineen con sus metas de desarrollo.

Al actualizarse y adquirir nuevas habilidades a través de cursos en línea, los profesionales no sólo expanden sus conocimientos, sino que también pueden mejorar significativamente su desempeño en el trabajo. Esto se traduce en mayor confianza en la toma de decisiones y en la implementación de estrategias de gestión de riesgos.

La selección de cursos debe considerar también el reconocimiento y la credibilidad de las plataformas y los instructores, asegurando que la inversión en tiempo y recursos traiga retornos significativos en términos de aprendizaje de calidad.

UTILICE HERRAMIENTAS Y *SOFTWARE* PARA GANAR EXPERIENCIA

En el entorno actual de gestión de riesgos, la tecnología juega un papel fundamental. Las herramientas de *software* especializadas pueden aumentar significativamente la eficiencia y eficacia en la identificación, evaluación, monitoreo y mitigación de riesgos.

Las herramientas de *software* modernas para la gestión de riesgos ofrecen capacidades avanzadas de integración de datos, permitiendo que las organizaciones agreguen información de múltiples fuentes. Esto facilita una visión holística de los riesgos y ayuda en la toma de decisiones basadas en datos.

La automatización proporcionada por estas herramientas puede reducir significativamente el tiempo dedicado a tareas manuales, permitiendo que los profesionales se enfoquen en aspectos más estratégicos de la gestión de riesgos. Procesos como la evaluación y el monitoreo de riesgos pueden ser optimizados, aumentando la precisión y la eficiencia.

Los *softwares* de gestión de riesgos a menudo incluyen funcionalidades que ayudan en la conformidad con regulaciones y estándares del sector. Pueden generar informes detallados que facilitan la comunicación con *stakeholders* y la documentación de acciones de mitigación de riesgos.

La selección de una herramienta de *software* debe considerar las necesidades específicas de la organización, el nivel de madurez de los usuarios, el soporte, mantenimiento, compatibilidad con sistemas existentes y la facilidad de uso. Buscar referencias con otros clientes de la empresa de *software* es una buena práctica. Es crucial elegir soluciones que se alineen con los objetivos de gestión de riesgos de la empresa y que puedan adaptarse a cambios organizacionales o de mercado.

Para maximizar el beneficio de las herramientas de *software*, es esencial que los profesionales reciban capacitación adecuada y se mantengan actualizados sobre nuevas funcionalidades y mejores prácticas en la utilización de estos sistemas.

La automatización proporcionada por *softwares* de gestión de riesgos puede reducir significativamente (hasta un 80%) el tiempo dedicado a tareas manuales, permitiendo que los profesionales se concentren en aspectos más estratégicos de la gestión de riesgos.

PARTICIPE EN CONGRESOS, CONFERENCIAS Y EVENTOS PRESENCIALES Y REMOTOS

La participación en conferencias y eventos es una manera excelente de mantenerse informado sobre las últimas tendencias, herramientas y técnicas en gestión de riesgos. Estas oportunidades permiten que los profesionales se actualicen, se conecten con colegas y expertos de la industria y adquieran conocimientos valiosos para aplicar en sus prácticas profesionales.

Conferencias y eventos a menudo presentan charlas, talleres y paneles sobre los últimos desarrollos en el campo de la gestión de riesgos. Participar en estas sesiones puede proporcionar conocimiento profundo y actualizado, que es vital para mantener la relevancia profesional.

Estos eventos son puntos de encuentro para profesionales de diversas áreas y especializaciones dentro

de la gestión de riesgos, ofreciendo una plataforma excelente para el *networking*. Construir una red de contactos puede abrir puertas a oportunidades de carrera, alianzas y colaboración en proyectos.

Muchas conferencias incluyen ferias o exposiciones donde las empresas presentan las últimas tecnologías, herramientas y soluciones en gestión de riesgos. Explorar estos espacios puede ofrecer a los profesionales una visión práctica de las innovaciones en el mercado.

Además de los eventos presenciales, muchas conferencias y seminarios se ofrecen en formatos virtuales, proporcionando acceso a un público más amplio. Estos eventos virtuales pueden ofrecer la flexibilidad de participar desde cualquier lugar, maximizando la inclusión y el acceso a contenido de calidad.

Hay que destacar la participación en eventos específicos, como el Risk Management Summit, el Global Risk Forum o la International Conference on Risk Analysis and Crisis Response, ofrece a los lectores ejemplos concretos de dónde pueden buscar aprendizaje y *networking*. Esta información específica ayuda a ilustrar el tipo de oportunidades disponibles y anima a los profesionales a buscar eventos que se alineen con sus intereses y necesidades de desarrollo.

La mención de que estos eventos cubren una variedad de temas relacionados con la gestión de riesgos subraya la riqueza de conocimiento disponible. Esta variedad asegura que los profesionales puedan encontrar contenido relevante que esté alineado con sus áreas de especialización e intereses de aprendizaje.

La participación en conferencias y eventos permite el descubrimiento de nuevas tendencias, innovaciones, tecnologías y ayuda a ilustrar el valor práctico de tales compromisos. Los profesionales pueden aprender sobre las investigaciones más recientes, tecnologías emergentes y estrategias avanzadas en gestión de riesgos, lo que puede ser directamente aplicable en sus funciones.

Construir una red de contactos puede abrir puertas a oportunidades de carrera, alianzas y colaboración en proyectos.

BENEFICIOS Y CREACIÓN DEL PLAN DE DESARROLLO PROFESIONAL

La trayectoria de un profesional en gestión de riesgos está marcada por un aprendizaje continuo y por la adaptación a un entorno que está siempre evolucionando. Las sesiones abordadas en este artículo destacan las diversas maneras en las que los profesionales pueden mantenerse actualizados y mejorar sus habilidades y conocimientos.

Mantenerse actualizado con las últimas herramientas, técnicas y sistemas de apoyo en gestión de riesgos no sólo potencia la eficacia individual, sino que también contribuye significativamente al éxito y la resiliencia de las organizaciones. Los profesionales bien informados y calificados están mejor equipados para identificar, evaluar y mitigar riesgos de forma efectiva, protegiendo así los intereses de la organización.

CREACIÓN DE UN PLAN DE DESARROLLO PROFESIONAL

Para garantizar el crecimiento continuo en la carrera de gestión de riesgos, es esencial que los profesionales desarrollen un plan de desarrollo profesional. Este plan debe contemplar al menos las siguientes etapas:

1) Establecer objetivos claros y medibles para el corto, medio y largo plazo.
2) Incluir una estrategia para la actualización constante de conocimientos, ya sea a través de lectura, cursos, certificaciones o participación en eventos y conferencias.
3) Prever la adopción y el dominio de nuevas herramientas y tecnologías relevantes para el sector.
4) Fomentar la construcción y expansión de una red de contactos profesionales.
5) Incentivar la contribución al campo de la gestión de riesgos, ya sea a través de investigación, publicaciones o participación activa en asociaciones profesionales.

Al implementar y seguir un plan de desarrollo profesional, los individuos no sólo aseguran su crecimiento y relevancia en el área, sino que también contribuyen activamente a la evolución y fortalecimiento del campo de la gestión de riesgos.

CONCLUSIÓN

La dedicación al desarrollo profesional continuo es una inversión que trae retornos significativos, tanto para el individuo como para la organización y la sociedad. Al comprometerse con el aprendizaje y la actualización constantes, los profesionales de gestión de riesgos se posicionan como líderes e innovadores en su área, listos para enfrentar los desafíos de hoy y de mañana. ■

Fotos: t-Risk

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

REVOLUCIONANDO LA INDUSTRIA EXTRACTIVA:

LA CLAVE ESTÁ EN LA SEGURIDAD Y PLANIFICACIÓN ESTRATÉGICA

¿Cuál es el perfil más apropiado de un especialista de seguridad?

Foto: Freepick

ARGENTINA

Martín López

¿Sabías que el 75% de los proyectos en la industria extractiva enfrentan desafíos significativos en seguridad y eficiencia debido a una planificación inadecuada? Este dato destaca la importancia crítica de adoptar estrategias de planificación y seguridad robustas desde las fases iniciales de cualquier proyecto.

Esto no es ficción. Son datos arrojados por CESCO, organización que en junio de 2023 publicó el análisis de Capex iniciales y finales de 80 proyectos mineros[1]. A lo largo de más de 20 años de ejercicio de mi profesión, fui testigo de realidades semejantes en varias operaciones de *Oil & Gas* y Minería en Argentina, México, entre otros países de América Latina.

Ver repetidas veces que los proyectos se extiendan y surjan sobre sobrecostos parece algo que podemos aceptar o justificar en estas industrias desde el Excel o la Planificación del Proyecto. Sin embargo, consideramos que dichos tiempos extra y sobre costos podrían haberse prevenido, que en gran parte de los casos afectan a los inversionistas, equipos de diseños y/o generan riesgos en la operación futura, me motivó a compartir parte de los aprendizajes que capitalicé en diversas experiencias, y realizar algunas sugerencias para trabajar de forma proactiva sobre aquellos desvíos que no deberían existir.

Ya sea como consultor de riesgos externo o como responsable *inhouse* de la gerencia, la primera recomendación básica y contundente: es conveniente que equipos de ingeniería de operadoras y constructoras, integren desde el inicio de los proyectos a especialistas de seguridad y riesgos estratégicos, en particular haciéndolos partícipes del planeamiento de los estudios de pre y factibilidad. Esta sinergia resulta determinante en el mediano y largo plazo, ya que una correcta gestión de riesgos optimiza los potenciales desvíos de tiempos y presupuestos. Los proyectos de *Oil&Gas* y Minería, sean de gran o mediana escala, no están exentos de las prácticas clave de la Planificación Estratégica y Gestión de Riesgos, donde la mirada diversa y multifuncional es clave de éxito.

Cuando referimos a especialistas de seguridad y riesgos estratégicos: ¿Cuál es el perfil más apropiado? En nuestra profesión, basado en la terminología ASIS[2], nos referimos al perfil del SSE (*Senior Security Executive* o *Senior Security Manager*), y vale tanto para un responsable interno como para un consultor externo. En lo que respecta a conocimientos, capacidades y habilidades, tanto *hard* como *soft*, destacaría las siguientes:

- Contar con inteligencia emocional.
- Gestión de personas y *Coaching*.
- Comunicación asertiva.
- Capacidad de analizar datos en contextos complejos, multidisciplinarios y bajo presión.
- Conocimiento de los procesos del negocio a asesorar.
- Desarrollar un ambiente de honestidad e integridad con el equipo de trabajo.

FALLAS QUE PUEDEN SURGIR EN LOS DIFERENTES NIVELES DE LA PLANIFICACIÓN: ESTRATÉGICO, PROGRAMÁTICO Y OPERATIVO

Fallas comunes que podemos evitar al integrar un especialista en seguridad corporativa SSE (*Senior Security Executive* o *Manager*–ASIS) o la consultoría externa para asesorar en los estudios de prefactibilidad y factibilidad junto a los equipos multidisciplinarios de diseño.

Nos referimos a la etapa previa a la implementación de la guía ASIS Internacional – *Enterprise Security Risk Management* en la fase construcción y producción del proyecto. A continuación, detallo las 11 fallas más importantes que observé en diferentes experiencias:

a) Desconocimiento y falta de análisis de la situación de la región o zona en la que se planea invertir.
b) Información insuficiente, interpretación pobre y un débil de expectativas sobre la licencia social.
c) Falta de tiempo asignado a la planificación y análisis. Hoy todo se centra en el resultado u objetivo económico del proyecto a desarrollar y no en el alcance en primera instancia.
d) No tener objetivos claros y medibles (SMART).
e) Ser reactivos *versus* ser proactivos.
f) Carencia de visión a largo plazo de los equipos de trabajo.
g) No realizar un monitoreo y ajustes de avances constantes en la etapa de planificación.
h) Fallas en la comunicación de la estrategia (todos los empleados deben conocerla).
i) No contar con indicadores de seguimiento en la planificación estratégica.

Falta de tiempo asignado a la planificación y análisis. Hoy todo se centra en el resultado u objetivo económico del proyecto a desarrollar y no en el alcance en primera instancia

Foto: Freepick

j) Presupuestos generalistas lo que conlleva a desvíos importantes en los resultados financieros del proyecto.
k) Misión incongruente o no es funcional a la visión del negocio.

7 *BEST PRACTICES* PARA CONTRARRESTAR ESTA DISOCIACIÓN ENTRE LAS GERENCIAS EN ESTOS ESTADIOS

1) La Planificación debe ser permanente y eficiente por parte del equipo de diseño.
2) En primera instancia de debe planificar el alcance y luego los costos del proyecto.
3) Estimar la línea base, la cual está alineada con los riesgos del negocio (ERM-ASIS).
4) El SSE es un socio estratégico del nuevo proyecto en la estimación de la línea base junto al equipo multidisciplinario. Además, participa en los estudios de prefactibilidad y factibilidad.
5) El equipo multidisciplinario debe tener interacción y capacidad de negociación para alcanzar una planificación realista.
6) Lograr un estudio de prefactibilidad donde el sector financiero no alinee el alcance a la curva de costos, lo cual es un error común en grandes proyectos, sino a la inversa.
7) Siempre existe un componente de incertidumbre y método prueba / error en los estudios preliminares, ya que son líneas base sin llegar a niveles de detalles.

Además, les dejo algunas consideraciones para resaltar en proyectos que se encuentran en las fases de construcción y producción:

- Automatización de la mayor cantidad de procesos para transformar a Seguridad en un *Business Enabler* o facilitador clave del negocio.
- Generar planes de Seguridad con marcado retorno de inversión (ROI).
- Acompañar desde Seguridad el cambio cultural y procesos de transformación digital de la compañía.

Llegando al final de nuestro artículo tal vez te hayas preguntado: ¿Cuál es el "entregable" que debería pedirle al SSE (*Senior Security Executive* o *Manager*) en fase prefactibilidad y factibilidad? Este debe ser un SRVA (por sus siglas en inglés, *Security Risk Vulnerability Assessment*). Se trata de un análisis y evaluación sobre los riesgos del negocio según guías internacionales de ERM (*Enterprise Risk Management* – ASIS), que contempla al menos los siguientes ocho puntos:

1) Situación Regional y local del proyecto (social, económica y política).
2) Reconocimiento del sitio o proyecto y su cadena logística.
3) Realizar *benchmarking* de otros proyectos vecinos sobre el estatus de la licencia social.
4) Mapear *stakeholders* del futuro proyecto.
5) Mapear de riesgos y amenazas iniciales del negocio.
6) Evaluar cadena de suministros.
7) Evaluar sistemas de transporte de personal (Aéreo-Terrestre-Marítimo).
8) Recursos humanos especializados en la zona del proyecto y adyacencias.

Si llegaste a esta parte de la nota, primero quiero agradecerte. Para cerrar, me gusta invitar a pensar que los equipos multidisciplinarios son los que planifican, no las herramientas de *software* que solamente pintan los caminos críticos o cronogramas.

Los equipos de diseño tendrán más probabilidad de éxito y una mejor gestión de los riesgos al incorporar un especialista en riesgos o seguridad corporativa, y promover la interacción entre ellos, capacidad de negociación y consenso, sobre todo transparencia al momento de evaluar los *Milestones* del proyecto. ■

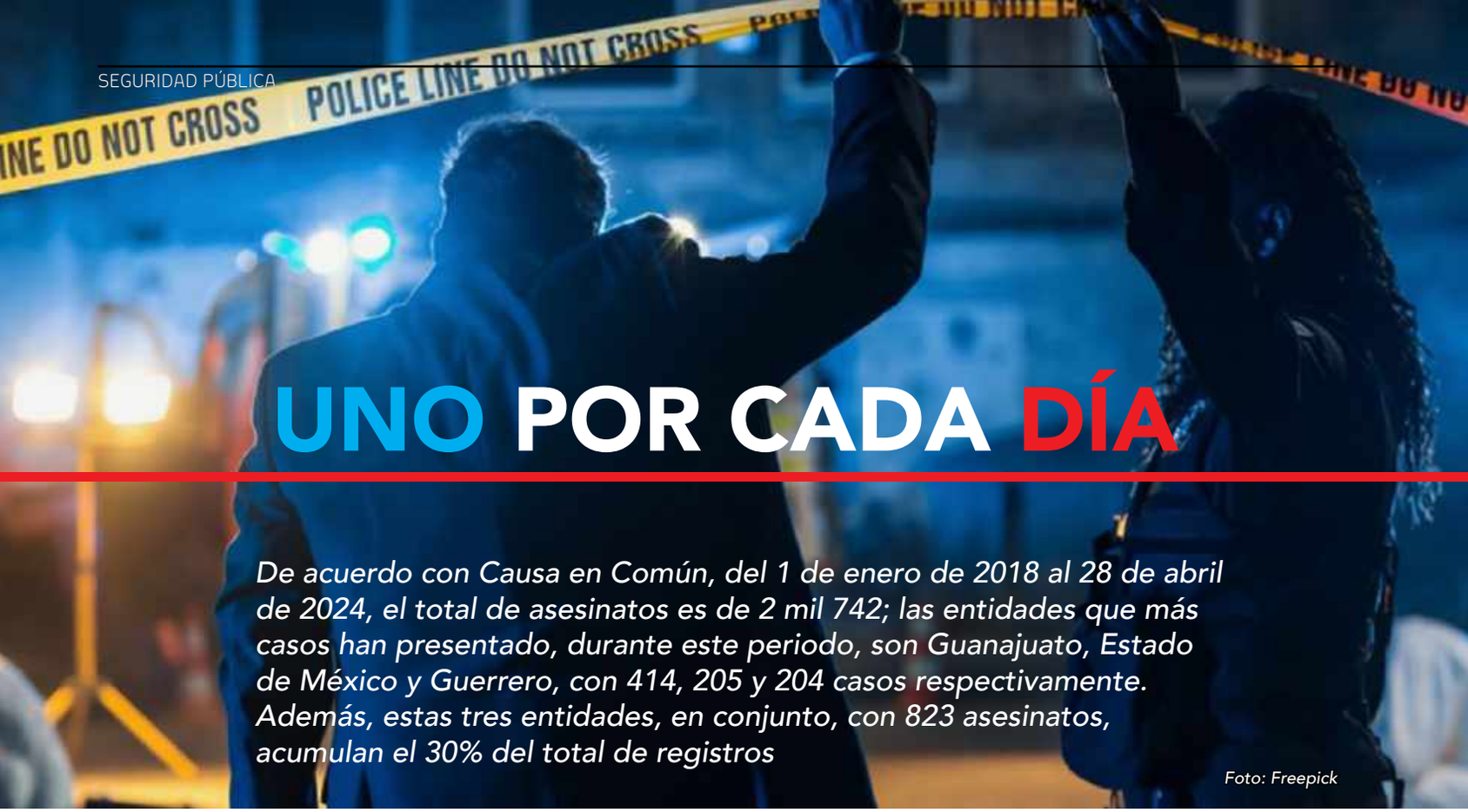
"Los planes no son nada; la planificación lo es todo", Dwight D. Eisenhower

"Un buen plan es como un mapa de carreteras: muestra el destino final y normalmente la mejor forma de llegar a él", H. Stanley Judd

Referencias:

1 https://www.cesco.cl/2023/06/12/cesco-identifica-los-factores-que-han-afectado-el-desarrollo-de-proyectos-mineros-en-chile/
2 ASIS (Sociedad Americana de Seguridad Industrial).

Martín López, Licenciado en Seguridad IUPFA por la Universidad de la Policía Federal Argentina y Magister en Administración del Derecho y Seguridad Pública por la USAL.
Más sobre el autor:



UNO POR CADA DÍA

De acuerdo con Causa en Común, del 1 de enero de 2018 al 28 de abril de 2024, el total de asesinatos es de 2 mil 742; las entidades que más casos han presentado, durante este periodo, son Guanajuato, Estado de México y Guerrero, con 414, 205 y 204 casos respectivamente. Además, estas tres entidades, en conjunto, con 823 asesinatos, acumulan el 30% del total de registros

Foto: Freepick

Edgar Jesús Arriaga Osorio

La seguridad es un tema importante, ya que como sabemos nos ayuda a la reducción de factores preparantes, o predisponentes, así evitando la criminalidad, es una actividad integral, importante en la sociedad, porque tiene un impacto en las esferas económicas, educativas, sociales, culturales, etc.

Por tal motivo se busca que las personas encargadas de esas funciones las lleven a cabo al pie de la letra, al grado de caer en la exigencia a los policías, pero si aplicamos la empatía, que como coloquialmente se dice, "ponernos en los zapatos de los otros", nos haríamos las siguientes preguntas: ¿Respiran? ¿Comen? ¿Tendrán familia?

De acuerdo con el portal Causa en Común, indica que hubo un total de 412 homicidios de policías en el año 2023, esto quiere decir que en promedio fue asesinado un policía por día. Estando como primer lugar el estado de Guanajuato con 60 homicidios de policías, seguido de Guerrero con 40 y, por último, Zacatecas con la cifra de 32, siendo las policías municipales las más afectadas, teniendo un 53.7%. Estas son cifras alarmantes, ya que son precisamente el primer círculo de protección que tenemos para la prevención de los delitos.

¿POR QUÉ SON VÍCTIMAS DE HOMICIDIO?

De acuerdo con el Instituto Nacional de Estadística y Geografía (2021), señala que hay cuatro teorías, las cuales indican por qué los policías son presa de este delito en específico:

1) Es por las necesidades del servicio que se traduce en actividades rutinarias y por sus actividades.
2) La falta de presupuesto a sus operaciones, esto se traduce en menos inversión en materiales y capacitación, más abatimientos.
3) Por sus características físicas, esto quiere decir que hay un rango de edades que van de los 30 a 39 años, y que en su mayoría son hombres.
4) La relación que hay entre la sociedad y autoridad, sumando la ineficiencia y la percepción de corrupción, da la confianza de que no va a pasar nada si abaten a un policía.

Este tema es poco estudiado, o analizado, ya que como todos sabemos los policías son los encargados de procurar el orden público, y si son vulnerados, pues qué nos espera para conseguir la paz que tanto anhelamos. ■

Referencias:

- *Instituto Nacional de Estadística y Geografía. (2021). En Números. Documentos de Análisis y Estadísticas. Policías abatidos: el riesgo de servir a la seguridad pública en México. www.inegi.org.mx. https://www.inegi.org.mx/app/biblioteca/ficha.html?upc=889463901884*
- *Registro de policías asesinados 2023. (s/f). Causa en común. Recuperado el 22 de febrero de 2024, de https://causaencomun.org.mx/beta/registro-de-policias-asesinados-2023/*
- *Suman en sexenio 2,381 policías asesinados en el país. El Economista. Recuperado el 03 de mayo de 2024, de https://www.eleconomista.com.mx/politica/Suman-en-sexenio-2381-policias-asesinados-en-el-pais-20240503-0015.html*

Edgar Jesús Arriaga Osorio, criminólogo y criminalista con experiencia en seguridad hotelera y *retail. Más sobre el autor:*

BUSINESS ALLIANCE FOR SECURE COMMERCE

SISTEMATIZA TU GESTIÓN DE RIESGOS

JUAN AHUMADA

Presidente del Consejo Ejecutivo
BASC OCCIDENTE MÉXICO

"La certificación en la norma internacional BASC ofrece prestigio, confianza ante autoridades nacionales e internacionales, y facilita el comercio internacional al evitar fraudes y riesgos aduaneros."

www.bascoccidente.com.mx
BASCoccidenteMexico
basc_mexico
basc-occidente-méxico

La inseguridad en nuestro país y región es una preocupación constante para expertos, quienes señalan que obstaculiza el desarrollo económico, especialmente para las empresas. Robos, asaltos y homicidios son conductas delictivas comunes, llegando a niveles preocupantes, como los 15,082 homicidios registrados en México en el primer semestre de 2023, según el INEGI. Esta situación se refleja en una alta percepción de inseguridad entre la población y una desconfianza en las instituciones de seguridad pública.

El Foro Económico Mundial reconoce el impacto directo de la inseguridad en la inversión y el desarrollo empresarial en México. Ante este contexto, las empresas se ven obligadas a enfrentar desafíos adicionales en seguridad, lo que requiere acciones estratégicas para protegerse y garantizar la continuidad de sus operaciones.

El Sistema de Gestión de Seguridad de BASC proporciona beneficios significativos para las empresas que lo implementan. Desde la estandarización de procesos hasta la generación de confianza y credibilidad en la gestión de la seguridad, pasando por la reducción de costos y riesgos, este sistema mejora la seguridad integral de la empresa y su cadena de suministro.

La certificación en la norma internacional BASC ofrece prestigio, confianza ante autoridades nacionales e internacionales, y facilita el comercio internacional al evitar fraudes y riesgos aduaneros. Además, promueve la colaboración entre el sector privado y público, fortaleciendo el papel de la empresa en la seguridad y vigilancia privada.

En conclusión, la implementación de normas como BASC fortalece integralmente a las empresas, independientemente de su sector, al mejorar la eficiencia y relevancia de su sistema de gestión de seguridad. Invitando a participar en eventos como el Congreso Mundial BASC, se promueve el intercambio de conocimientos y experiencias para enfrentar los desafíos actuales en seguridad y comercio internacional.

Esperando haber conseguido su interés y sembrado en usted esta iniciativa como alternativa solución para su organización, me complaceré invitarle al 11° Congreso Mundial BASC 2024, el encuentro donde nos reuniremos líderes gubernamentales, organismos de control, empresarios y expertos del comercio y seguridad global. Este importante evento se llevará a cabo los días 25 y 26 de septiembre en la vibrante ciudad del sol y puerta a las Américas, Miami, Florida, donde tendrá la oportunidad de conocer los retos y tendencias actuales que impactan las operaciones comerciales, así como fortalecer sus procesos a través de paneles de discusión, expositores de talla mundial, análisis de tendencias y mejores prácticas de seguridad.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESING (CPTED): PREVENCIÓN DEL CRIMEN A TRAVÉS DEL DISEÑO AMBIENTAL

El concepto CPTED fue tomado de la teoría del "Síndrome de la Ventana Rota", expuesta en el libro "El espacio defendible" de Oscar Newman

COLOMBIA

Javier Nery Rojas Benjumea

La planeación física del espacio a través del diseño adecuado del medio ambiente y el entorno permite actuar como disuasivo en el sentido que delimita áreas reduciendo la oportunidad delictiva.

OBJETIVOS DE CPTED

Su primer gran objetivo es influir en las decisiones de los infractores potenciales para evitar la delincuencia y la actividad criminal, diseñando un mejor entorno urbano e interviniendo sobre sus características para reforzar aspectos como el aumento de la vigilancia natural, la apropiación territorial y la ampliación de la coexistencia en espacios colectivos.

Además, provee una manera de integrar al individuo con su espacio público de entorno, vinculando a las comunidades, haciéndolas partícipes del proceso para que sean vigilantes naturales y activos y de esa manera colaboren en las estrategias de seguridad pública.

Estas intervenciones suelen involucrar desde la implementación de diseños de calles que organicen las posibilidades de flujo, hasta la mejora de plazas y espacios públicos, el diseño de condominios y grandes proyectos de mejoramiento urbano.

Los objetivos específicos de este sistema podrían ser, entre otros: controlar accesos, vigilar a través del diseño físico, diseñar la construcción, administrar el uso del suelo, optimizar los dispositivos mecánicos de vigilancia, elaborar recomendaciones para gerentes y constructores para proteger los usuarios, generar

Su primer gran objetivo es influir en las decisiones de los infractores potenciales para evitar la delincuencia y la actividad criminal, diseñando un mejor entorno urbano e interviniendo sobre sus características para reforzar aspectos como el aumento de la vigilancia natural, la apropiación territorial y la ampliación de la coexistencia en espacios colectivos

Foto: Freepick

vida urbana e interacción social, aprovechar los servicios de seguridad privada, mejorar la relación con la comunidad y las fuerzas de policía, apropiar el territorio y mejorar la imagen del entorno.

En tal sentido el concepto permite desarrollar las siguientes categorías:

- **Territorialidad:** arraigo y apropiación del espacio generando sentido de pertenencia.
- **Vigilancia natural:** ausencia de sistemas electrónicos, la claridad y la limpieza minimalista de los espacios genera comunicación visual.
- **Imagen:** el estado de limpieza y mantenimiento de áreas, así como la iluminación generan percepción de confianza y tranquilidad.
- **Área segura:** el deterioro de lo construido es el ambiente perfecto para los focos de delincuencia.

BENEFICIOS Y ESTRATEGIAS

Su implementación genera varias ventajas:

- **Retardo en la intrusión:** búsqueda y análisis de vulnerabilidades por parte del agresor.
- **Facilita la detección:** la distribución espacial de la facilidad en cada una de las capas de seguridad física facilita la identificación de personas extrañas al entorno.
- **Reducción en el tiempo de respuesta:** la territorialidad y la vigilancia natural facilitan la acción de la fuerza de seguridad.

Son varias las estrategias que se pueden desarrollar en el diseño e implementación del proyecto:

- **Definición fronteriza clara de espacio controlado:** física o simbólicamente entre el espacio público y el espacio privado por medio de placas, pinturas en ambientes, ubicación de muebles, etc.
- **Zonas de transición claramente marcadas:** reconocer inconscientemente las áreas publicas y privadas con iluminación texturas o cambio de nivel.
- **Reubicación de áreas de ingreso:** designar entradas formalmente o áreas de reunión con vigilancia natural y control de accesos.
- **El uso de espacio para proporcionar barreras naturales:** las actividades pueden separarse por el terreno natural u otras funciones para evitar conflicto.
- **Horario para el uso de espacio:** el uso adecuado de los espacios reduce el riesgo para los usuarios.
- **Espacio para aumentar la percepción de vigilancia natural:** la percepción de la vigilancia es más poderosa que su realidad. "Las cámaras ocultas hacen poco para hacer a los usuarios normales sentirse más seguros".
- **Distancia y aislamiento:** mejorando comunicaciones y aumentando eficacias de la percepción de vigilancia natural y control.

El ámbito de aplicación es muy variado, por ejemplo:

- Áreas externas de permanencia.
- Ágoras y plazas.
- Bulevares y alamedas.
- Parqueaderos.
- Oficinas.
- Edificios de oficinas.
- Centros comerciales.
- Bancos.
- Conjuntos residenciales.
- Colegios.
- Centros de convenciones. ■


Foto: Freepick


Foto: Freepick

Los objetivos específicos de este sistema podrían ser, entre otros: controlar accesos, vigilar a través del diseño físico, diseñar la construcción, administrar el uso del suelo, optimizar los dispositivos mecánicos de vigilancia, elaborar recomendaciones para gerentes y constructores para proteger los usuarios, etc.

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

PREVENCIÓN Y REACCIÓN ANTE EL ROBO Y SUSTRACCIÓN PARENTAL DE MENORES

Foto: Freepick

MÉXICO | **Ricardo Nava Rueda**

Recomendaciones para prevenir el robo de niños y niñas

Durante la trayectoria de 34 años en la búsqueda de personas desaparecidas y particularmente en menores, así como mi participación en la Asociación Mexicana de Niños Robados y Desaparecidos, A.C, hago las siguientes recomendaciones:

MEDIDAS PREVENTIVAS CONTRA EL ROBO DE MENORES

1) Retrate a su hijo desde el primer día de nacido y posteriormente cada seis meses.
2) Registre a su hijo lo mas pronto posible.
3) Tome y conserve la huellas dactilares de sus hijos.
4) Enseñe a sus hijos su nombre completo, el de sus padres, domicilio, teléfono y otro dato que considere importante.

EN CASA

1) No permita que sus hijos abran la puerta.
2) Cuando una enfermera, trabajadora social o algún otro servidor se presente en su casa, pídale siempre su identificación y teléfono, verifique datos.
3) Si contrata a una empleada doméstica, retrátela y solicite referencias.
4) Fíjese con quien chatean sus hijos.

EN LA CALLE

1) Acompañe siempre a sus hijos a la escuela y fíjese que nadie los siga.
2) No mande a sus hijos a la tienda.
3) Si tiene varios hijos evite salir con todos a la vez.
4) Tome a sus hijos siempre de la mano.
5) Si algún automóvil en circulación les pide información, no se acerquen a él.
6) Si se dedica al comercio ambulante no pierda de vista ni tampoco permita que sus hijos se alejen de usted.
7) No permita que extraños fotografíen a sus hijos.
8) Nunca deje solos a sus hijos en el coche.

EN OTROS LUGARES

1) Cuando vaya al parque, a una fiesta, al deportivo u otro centro recreativo no pierda de vista a sus hijos.
2) Por ningún motivo confíe a sus hijos a extraños ni a personas que no conozca lo suficiente.
3) Enseñe a sus hijos a no hablar con desconocidos.
4) Siempre esté al pendiente de los niños y con quien juegan sus hijos.

Es importante señalar que estas medidas fueron elaboradas por la Asociación Mexicana de Niños Robados y Desaparecidos, A.C. (AMNRDAC), de acuerdo con un esquema de casos reales en la que fueron robados varios menores.

Enseñe a sus hijos su nombre completo, el de sus padres, domicilio, teléfono y otro dato que considere importante

Foto: Freepick

En el número 141 de esta revista **Seguridad en América**, también comenté el caso de varios niños y niñas que han sido separados por el padre o la madre en contra de la voluntad de la esposa, esposo o pareja, aún en contra de los hijos, porque no se les toma en cuenta. Uno de los proyectos que envié a la PGR (Procuraduría General de la República) y de igual manera a la Cámara de Diputados en el año 2002.

He considerado que los niños y niñas deben estar protegidos por una cédula de identidad o credencial tipo INE (Instituto Nacional Electoral), donde lleven todos sus datos.

- Nombre completo.
- Fecha de nacimiento.
- Tipo de sangre.
- CURP (Clave Única de Registro de Población).
- Huellas dactilares.
- Así como datos importantes que quedaran de manera oculta en la misma.

Esta credencial tendría que ser desde el día de nacimiento y cambiar cada tres años y únicamente ser presentada para trámites generales, para inscripción en escuelas, servicios médicos, así como para viajar.

Con esta credencial se evitaría principalmente que un menor robado o sustraído pueda ser trasladado a cualquier parte de la república mexicana; es muy fácil viajar con menores por cualquier vía, terrestre o por avión, ya que pocas veces se solicita un documento para vender boletos y se verifica el parentesco.

Quizá en un momento pueda ser molesto al impedir cualquier trámite sin la credencial, pero esto sería un gran candado para evitar cualquier ilícito, y por el contrario, daría mayor seguridad y confianza. Lo anterior, reitero, es por la experiencia y casos de los cuales he tenido conocimiento.

En 2001 un par de niñas fueron sustraídas de la frontera sur de México por el padre de las mismas, viajó vía aérea al entonces llamado Distrito Federal (ahora Ciudad de México), después en autobús al interior de la república mexicana y posteriormente a la frontera norte para ingresar de manera ilegal a los Estados Unidos de Norteamérica. Otro caso fue de una menor robada en el Estado de México, trasladada por la frontera sur y llegar hasta república de El Salvador, en Centroamérica.

En ambos casos las menores fueron reintegradas con sus madres a través de difusión por diversos medios de comunicación y con el apoyo de las autoridades correspondientes, pero se pudo evitar si hubiera las medidas preventivas (credenciales de las menores). No obstante, hoy en día siguen siendo trasladados sin verificar quiénes son los menores y con quiénes viajan, ya que también hay líneas de autobuses que salen de distintos destinos y no necesariamente de centrales.

He considerado que los niños y niñas deben estar protegidos por una cédula de identidad o credencial tipo INE, donde lleven todos sus datos

También es cierto que actualmente a través de las terminales de autobuses hay cierto protocolos o filtros para confirmar, de igual manera en aeropuertos cuando existe alguna duda, pero reitero que será mejor si se credencialita a los menores para realmente tener un candado y confirmar su identidad.

"Los niños no son el futuro del mundo, son el presente y hay que cuidarlos hoy". ■

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:*

¿POR QUÉ UN PERITO HABRÍA DE ESTUDIAR UN POSGRADO DE INVESTIGACIÓN PARA LA MEJOR ELABORACIÓN DE SU DICTAMEN PERICIAL?

Además de las habilidades que un posgrado en investigación aportaría al desempeño laboral pericial, contribuye a la formación competente ante los problemas que hay que afrontar en la sociedad (Murillo Campuzano, 2019)

Foto: Freepick

MÉXICO

Wael Sarwat Hikal Carreón y Rubí Sánchez Noriega

INTRODUCCIÓN

Uno de los retos fundamentales en la investigación de los delitos, es la pericia, el cuidado y sigilo que se le aplica a la verdadera búsqueda de indicios, detalles, datos que den luz en el camino a la verdad. Para ello se obliga a la necesidad de desarrollar el sentido estricto de no sólo la profesionalización en la ciencia a fin o en la especialidad, arte u oficio del que se denota se es el indicado para opinar, sino que esto va más allá, de dominar lo que se practica, se refiere pues, a plasmar en líneas la experiencia y la experticia, palabras que den respuesta a los interrogantes que surgen de los hechos fácticos que se presentan como resultados de diversas conductas.

El cargo de "perito", demanda alto compromiso, sobre todo al momento de materializar el producto de su conocimiento, labor, generar sus hipótesis, analizarlas para establecer sus conclusiones, y más aún, por ello la objetividad es un principio pilar en la confección de un dictamen pericial. Pero, ¿qué es en sí un dictamen pericial? ¿Acaso es sólo una opinión del perito? Si bien es cierto la doctrina nos regala infinidad de definiciones que intentan escudriñar en la explicación acertada sobre el término que se analiza, por ello no nos encuadramos en una u otra definición, todas expresan el objetivo principal del concepto.

Así que la descripción juega de la mano de la redacción un papel imprescindible para la elaboración del dictamen, desde el planteamiento del problema, así como la fundamentación y su procedimiento, el método, el análisis o estudio, los resultados, las consideraciones y no se diga, las afamadas conclusiones, según sea el caso, serán piezas clave en la argumentación del mismo, esto es, que se pretende crear un documento que ofrezca la ilustración detallada para dar luz a la parte interesada, siempre apegado a la verdad.

Para lograrlo, además de los elementos descritos, es necesario tener claro, que el ser un especialista en una determinada área, no es sinónimo de saber elaborar un dictamen pericial completo, útil y objetivo, estas cualidades se adquieren alimentándose de herramientas que con el paso del tiempo auxiliarán a la construcción idónea del instrumento. Ya que el éxito resulta, de la constante preparación en ambas esferas, la primera, la del dominio y actualización del tema, así como de la segunda, el conocimiento para elaborar de manera compleja pero precisa el dictamen, con un lenguaje técnico en su contenido pero un lenguaje sencillo en sus conclusiones; esto se debe a que el cuerpo del dictamen puede ser técnico o experimental si la especialidad lo demanda, pero conforme se van obteniendo resultados, las conclusiones se esperan en un lenguaje sencillo y claro.

SIMILITUDES EN EL TRABAJO DE ELABORACIÓN DE UN PERITAJE Y UNA TESIS

En este apartado no se abordan los temas referentes a cadena de custodia, tampoco de los procedimientos del abordaje en la escena o los diferentes tipos de escenas con las que el perito se encuentre según el hecho, no se específica una rama especial sino de manera general se listan las características de un informe pericial en cuanto a su estructura. Por la parte de las características de una tesis de posgrado, igualmente se consideran los protocolos generales, sin profundizar en procedimientos, técnicas específicas. La Tabla

1 muestra un comparativo a similitud entre las estructuras de un peritaje y una tesis.

Antes de listar la estructura del peritaje y la tesis, se precisa aclarar que la secuencia de aparición o jerarquía de temas, así como el contenido, no es de orden universal, dado que según la materia sobre la cual se realice el dictamen pericial, así como la tesis, los elementos que contendrá dependerán del objeto/sujeto de estudio; por ejemplo, no será la misma estructura de un peritaje de accidentes marítimos a un peritaje aeronáutico, tampoco será igual una tesis en ciencias sociales que en Biología, igualmente hay variantes por los enfoques cualitativos y cuantitativos. Por ende, cada fiscalía o procuraduría establecen sus estándares de formato de peritaje, también de acuerdo a cada rama. Por otra parte, cada centro de educación superior señala sus protocolos de tesis. Pero de manera general, se pueden apreciar la siguiente lista como un bastimento.

Tabla 1. Características y similitudes entre un peritaje y una tesis de posgrado.

Peritaje	Tesis de posgrado
Datos generales del proceso, caso, hecho	Título, objeto de estudio
Antecedentes, fundamentación, argumentación, diseño	Antecedentes, fundamentación, objetivos, justificación
Planteamiento del problema	Preguntas de investigación, planteamiento del problema.
Metodología, consideraciones técnicas de estudio, recogida de información	Tipo de investigación, muestra, hipótesis
Análisis, estudio de la información	Metodología
Información adicional	Triangulación
Elaboración del informe, dictamen, resultados	Documento
Conclusiones	Resultados, discusión, conclusiones
Referencias bibliográficas	Referencias bibliográficas
Firma, sello	Firma, sello
Presentación escrita	Presentación escrita
Exposición oral	Exposición oral
Extensión de alrededor de 10 a 20 páginas o más según el caso de estudio. El tiempo de elaboración también depende del peritaje, pero comúnmente debe tomar unas semanas.	La extensión va de entre 100 a 500 páginas según el estudio. El tiempo es de entre un año a cuatro o más según el área de conocimiento.

Nota: Elaboración propia con base en las fuentes consultadas.

En la Tabla 2, se describen los componentes del peritaje.

Tabla 2. Descripción de las características de la estructura del peritaje.

Peritaje	Descripción
Datos generales del proceso, caso, hecho	Para identificar el asunto que se está tratando a investigar. Esto lo solicitan los particulares, el juez u otros intervinientes autorizados para tal efecto (Honores Ortega y Quizhpe Oviedo, 2019).
Antecedentes, fundamentación, argumentación, diseño	Se realizará una construcción teórica sobre el caso de estudio, información que contribuya a entender el fenómeno, casos similares, etcétera. Será la partida para el diseño metodológico y las técnicas que aplicará con objeto del peritaje.
Planteamiento del problema del peritaje	El perito resolverá los planteamientos solicitados y contestará las preguntas planteadas, aquellos cuestionamientos que requieran una opinión técnico científico determinada.
Metodología, consideraciones técnicas de estudio, recogida de información	El perito aplicará sistemáticamente el método que haya determinado para su investigación. Ello le permitirá tener un ordenamiento en la recogida de la información e interpretación de la misma. La diversidad de técnicas le dará la posibilidad de triangular la información y que llegue al mismo resultado o proximal a tal (Kvitko, 2012).
Análisis, estudio de la información	Aplicar en todos los casos el juicio crítico, lo que significa, tener la facultad para distinguir lo cierto de lo falso, aplicando el entendimiento, comparando, estableciendo relaciones y concluyendo, siempre con fundamento científico, informando con total apego a la lógica, sin incurrir en interpretaciones ambiguas (Kvitko, 2012, p. 15).
Información adicional	Podrá valerse de técnicas adicionales para la "aproximación diagnóstica a la situación a investigar, observación científica, observación clínica y participante, visita domiciliaria, entrevistas en profundidad o semiestructurada, cuestionarios" (Honores Ortega y Quizhpe Oviedo, 2019, p. 271), entre otros según el objeto de peritaje.
Elaboración del informe, dictamen, resultados	"Es el paso donde se resume toda la investigación realizada; en este proceso comunicativo se da cuenta de todas las evidencias obtenidas; este informe es el depositario de la interpretación del fenómeno estudiado, que sirve de testimonio como parte de la prueba requerida para la toma de decisión" (Honores Ortega y Quizhpe Oviedo, 2019, p. 272).
Conclusiones	Es la revelación de los hallazgos a los que se llegó. El resumen de lo visto o presentado en el informe o estudio.
Referencias bibliográficas	Importante es valerse de otras fuentes de conocimiento que se aproximen al estudio que se está realizando para darle soporte y argumentación al estudio. Fuentes confiables de bases de información formales.
Firma, sello	Se sostiene en el autor/investigador que ha realizado y concluido el estudio, avalado por la institución que le represente o respalde.
Presentación escrita	Se redactará cada parte de manera clara para facilitar su revisión, consulta, análisis, debe llevar un orden secuencial entre las diferentes partes, que estén conectadas y que la que sigue sea derivada de la anterior, estarán conectadas o hiladas desde el inicio al final.
Exposición oral	Es la declaración y defensa con base en los argumentos, método y resultados ante la autoridad ante la cual se deba exponer o defender el caso.

Nota: Elaboración propia con base en las fuentes consultadas.

Su importancia como medio de prueba ha tomado bastante fuerza en los últimos años, la credibilidad que ostenta por apegarse a una metodología que sustenta, lleva a que se optimice y perfeccione

aún más su confección, con los insumos empleados y los laboratorios acreditados, ya que se exigen requisitos de validación de índole nacional e internacional, así como procesos de certificación, cuyo fin es el esclarecimiento que tenga el testimonio pericial una vez que sea desahogado en juicio por el propio perito, por medio de un interrogatorio, donde defenderá su postura por medio de la explicación oral y proyectiva de su labor en la dictaminación pericial, y se le cuestionará en el contrainterrogatorio para desacreditar su dicho, o bien, en "evidenciar contradicción" (Fernández Romo, Peña Aguirre y Huertas Díaz, 2020; Duce, 2018; Vázquez Rojas, 2017).

En la Tabla 3, se describen las características de la tesis.

Tabla 3. Descripción de la estructura de la tesis de posgrado.

Tesis de posgrado	Descripción
Título, objeto de estudio	Identificará el estudio específico que se está realizando, el cual indica de manera sintética el objetivo
Antecedentes, fundamentación, objetivos, justificación	Se construye con base en anteriores datos que se tengan. Difícil sería iniciar una investigación de ceros, suele tener antecedentes, teorías, historia, etcétera, lo que conducirá a saber qué se quiere estudiar-descubrir y los objetivos que persigue la investigación.
Preguntas de investigación	Son cuestionamientos o interrogantes que se hace el investigador con relación al problema de interés, que al no dar respuesta al mismo realiza un proceso de investigación a fin de fundamentar las respuestas al problema planteado (Carrillo Mayorga, 2020, p.100).
Tipo de investigación, muestra, hipótesis	Según el objeto/sujeto de estudio y de acuerdo a las necesidades que se vayan planteando será el tipo de investigación, sus enfoques, la población de estudio, y el supuesto previo de explicación o de ruta para la investigación.
Metodología	Los objetos/sujetos de estudio determinarán el proceso metodológico, estructurar las técnicas que permitirán revelar la información.
Triangulación	Valiéndose de diferentes técnicas para de diversas formas explicar el mismo fenómeno o aproximarse a la explicación requerida.
Documento	Es el manuscrito original que contiene todos los elementos anteriores. Bien organizada, sistematizada.
Resultados, discusión, conclusiones	Luego del análisis de la información que derivaron los hallazgos de la metodología, se redacta el análisis e interpretación de resultados.
Referencias bibliográficas	Son aquellas fuentes que respaldan el trabajo, la doctrina, teorías, ideas, pensamientos, normatividades que avalen o sustenten la investigación.
Firma, sello	La investigación se respalda o encabeza por una institución de investigación, dirigida por investigadores.
Presentación escrita	Sigue siendo aquel documento formal bien redactado y estructurado.
Exposición oral	Es la exposición de toda la investigación y defensa de la metodología y resultados.

Nota: Elaboración propia con base en las fuentes consultadas.

En las tablas 2 y 3 se puede notar la similitud en las estructuras, contenidos y finalidades entre el dictamen pericial y la investigación de la tesis. En ambas existe un título, introducción, argumentación, teorías explicativas, desarrollo metodológico, estudio de caso, análisis de resultados, conclusiones, presentaciones escrita y oral para sus sistematización, organización y exposición. En el siguiente apartado se reflexionará si el contar con estudios de posgrado facilitaría la construcción de un peritaje teniendo como premisa que precisamente en el posgrado de investigación es donde se aboca enteramente a enseñar sobre argumentación, metodología, análisis de resultados y exposición.

¿TENER POSGRADO EN INVESTIGACIÓN AYUDARÍA A LA MEJOR CONSTRUCCIÓN DE UN DICTAMEN PERICIAL? ENFOQUE ACADÉMICO

Explica Bailey Moreno: "En este sentido, la educación en el posgrado debe ser congruente con las necesidades del contexto nacional y su relevancia científica, así como funcionar con una visión que integre los ámbitos de la docencia, la investigación y la actividad laboral. Bajo el supuesto anterior, los estudios de doctorado debían responder a las demandas de la sociedad del conocimiento a través de investigaciones que permitan solucionar los problemas derivados de los cambios constantes de la sociedad actual (2021, p. 2)".

Aquí no se sugerirá cuál posgrado o en qué área, eso dependerá del interés del lector o estudiante así como de los recursos, instituciones, equipamiento, personal con el que se cuente en el área a donde llegue este trabajo, no se emite juicio sobre algún centro escolar público o privado nacional o internacional, pero si se tiene desarrollado el tema de las acreditaciones de los posgrados por parte del Consejo Nacional de Ciencia y Tecnología, el cual está abierto a toda institución para que postule a evaluación sus posgrados y sea un proceso de mejora continua, donde se encamine la infraestructura, personal y programa educativo a la investigación.

La investigación está inmersa en las universidades, se pasa de un proceso de formación al de especialización y de investigación. Se puede acumular mucha experiencia laboral, pero si no se transmite a otras generaciones se pierde, su paso a los alumnos en formación ayuda a saber hacer y mejorar los procesos que ya se tenían, por ello el sistematizar y divulgar la experiencia es de suma importancia para la evolución de las profesiones y las sociedades (Ramírez García, 2020). Ello permite conocer la realidad conforme los nuevos contextos que se van presentando, esto suele realizarse a través de las tesis, que luego se convierten en artículos para revistas, capítulos en libro o libros, así como conferencias, clases, cursos, talleres, etcétera.

Las tesis de posgrado son un trabajo de largo proceso cuya elaboración es el resultado de la formación en un proceso de saber investigar, desarrollo de habilidades para la identificación de un problema que requiere atención, estudiar sus antecedentes, encontrar teorías que se hayan desarrollado para fenómenos similares, hacer convergencia para interpretar lo que se está estudiando, destacar los objetos del estudio, determinar un supuesto de explicación/solución, saber elaborar el proceso metodológico que permita encontrar y recoger la información, revelar resultados, sistematizarlos y presentarlos a manera de defensa de lo que se ha averiguado. Los resultados deben perseguir

Foto: Freepick

el ser de investigación propia, originales e innovadores, que expliquen algo o mejoren los procesos de comprensión Hernández Márquez; Ojeda Chacón; Torres Paz, y Arizmendi Jaime, 2020).

Ahora bien, ¿en qué beneficiaria tener un posgrado en investigación para la mejor realización de un dictamen pericial? Como se mostró en las tablas *supra*, existen totales similitudes entre un documento de tesis y otro de peritaje, se componen estructuralmente de las mismas partes, la diferencia es la extensión de páginas y el tiempo de elaboración. Cuando se egresa de la licenciatura, los conocimientos sobre argumentación, metodología y exposición son mínimamente básicos apenas para las tareas y proyectos.

En un posgrado, la ventaja es la total dedicación a aprender sobre argumentación, metodología y exposición. Además de las habilidades que un posgrado en investigación aportaría al desempeño laboral pericial, contribuye a la formación competente ante los problemas que hay que afrontar en la sociedad (Murillo Campuzano, 2019), si el perito egresado de un posgrado, además decide publica los resultados de sus investigaciones, contribuirá al desarrollo del conocimiento.

Hasta no hace mucho, los principales autores tradicionales o clásicos del Derecho, Criminalística, Psicología u otras ciencias, eran escritores en primera línea de ejercicio profesional, quienes sistematizaban sus experiencias laborales y las redactaban en formato de libro, algunas ocasiones en artículos producto de conferencias donde hablaban de su praxis. El perito puede ser ese investigador de su propia práctica profesional y sistematizarlo para sus dictámenes, presentaciones, exposiciones, conferencias, artículos, libros, cátedras.

Si se observa el plan de estudios de un programa de posgrado, este suele estar formado por algunas materias para la formación en conocimientos generales del tema del posgrado, para luego especializarse en argumentación, metodología e investigación sobre el área de estudio. El estudiante/investigador será experto sobre el tema que está desarrollando. Esto no es limitante a un objeto/sujeto de estudio, puesto que el posgrado aporta las bases necesarias para extender las investigaciones a otros rubros, por ello que el investigador es conocido como el experto de expertos o perito de peritos en su ámbito, pero también con capacidad de autocuestionarse y redefinir sus rutas de investigación para mejorar, abierto al aprendizaje continuo. ■

Referencias:

- *Bailey Moreno, J. (2021). Aportaciones de los estudios de posgrado en la formación de profesores universitarios. Revista de Investigación Educativa de la REDIECH, (12), 1-14. https://www.rediech.org/ojs/2017/index.php/ie_rie_rediech/article/view/1253/1337*
- *Carrillo Mayorga, J. (2020). Metodología de la Investigación Jurídica. Flores Editor y Distribuidor.*
- *Duce J., M. (2018). Prueba pericial y su impacto en los errores del sistema de justicia penal: antecedentes comparados y locales para iniciar el debate. Ius Et Praxis, 24(2), s.p. https://www.redalyc.org/jatsRepo/197/19758438007/19758438007.pdf*
- *Fernández Romo, R.M.; Peña Aguirre, J.A. y Huertas Díaz, O. (2020). La inspección del lugar del hecho y la valoración legal de la huella o evidencia. Revista Logos, Ciencia & Tecnología, 12(3), 115-27. https://www.redalyc.org/journal/5177/517765273010/html/*
- *Honores Ortega, B.A. y Quizhpe Oviedo, J.M. (2019). El peritaje desde la perspectiva del Trabajo Social. Revista Conrado, 15(68), 267-274. http://scielo.sld.cu/pdf/rc/v15n68/1990-8644-rc-15-68-267.pdf*
- *Kvitko, L.A. (2012). Medicina Legal, peritos y peritaciones. Medicina Legal de Costa Rica. 29(1), 7-16. https://www.scielo.sa.cr/pdf/mlcr/v29n1/art2.pdf*
- *Murillo Campuzano, G.P. (2019). La investigación científica y el posgrado, una herramienta indispensable en la Universidad del Siglo XXI. 15(69), 35-40. http://scielo.sld.cu/pdf/rc/v15n69/1990-8644-rc-15-69-35.pdf*
- *Ramírez García, A.G. (2020). Estudios de posgrado y elaboración de artículos científicos. Utopía y Praxis Latinoamericana, 25(11), 300-313. https://www.redalyc.org/journal/279/27964922021/27964922021.pdf*
- *Vázquez Rojas, C. (2017). Los retos de las pruebas periciales a partir del nuevo Código Nacional de Procedimientos Penales. Apuntes desde la epistemología jurídica. Problema: Anuario de Filosofía y Teoría del Derecho, 11, 341-378. https://www.redalyc.org/pdf/4219/421950524011.pdf*

Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología capítulo Nuevo León y Doctor en Educación por la Universidad Autónoma de Nuevo León. *Más sobre el autor:*

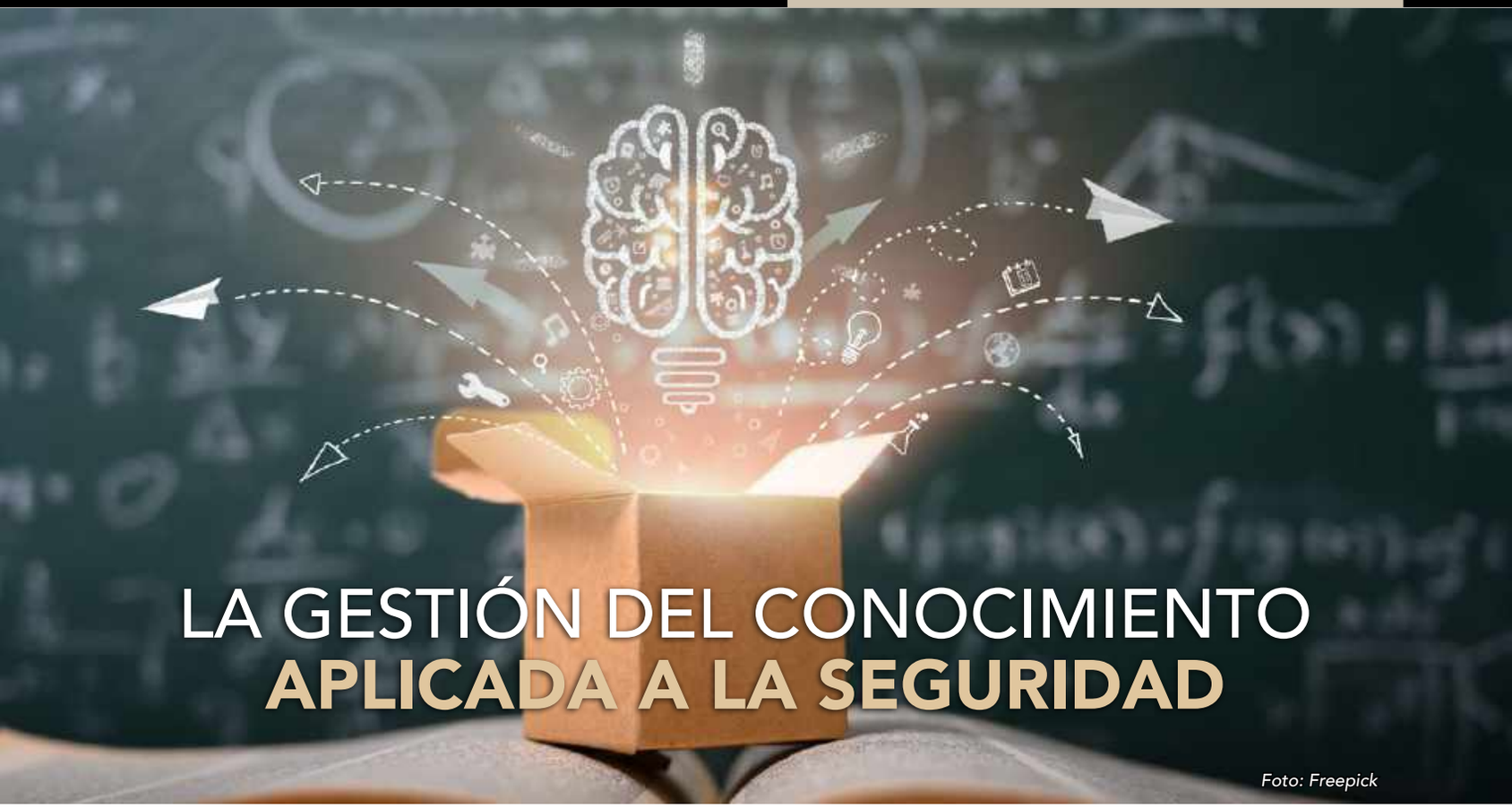
Rubí Sánchez Noriega, docente en la Universidad Autónoma de Durango campus Zacatecas y Doctoranda en Derecho Constitucional, Penal y Amparo. *Más sobre la autora:*

CULTIVANDO COMPETENCIAS

ariyacianci@gmail.com

ARI YACIANCI, SRMP, PROFESIONAL EN GESTIÓN DE RIESGOS Y SEGURIDAD DE ARGENTINA.

Más sobre el autor:



LA GESTIÓN DEL CONOCIMIENTO APLICADA A LA SEGURIDAD

Foto: Freepick

ARGENTINA

¿Cuántas veces has dicho o escuchado que "una cosa es la teoría y otra muy diferente es la práctica"? Esta frase, tal vez algo fatalista, es utilizada para valorar a la experiencia como algo superior a la formación, y en muchos casos es indiscutiblemente cierta. El sector de la seguridad no es la excepción.

Pero… ¿Es necesario que siempre sea así? ¿No se puede modificar la teoría para que se ajuste mejor a la realidad de la práctica? ¿O no podemos mejorar nuestra práctica para adaptarnos mejor a lo que indica la teoría?

Por suerte, existe un concepto que tiene la respuesta a estas preguntas, que es la Gestión del Conocimiento.

¿QUÉ ES LA GESTIÓN DEL CONOCIMIENTO?

Es el proceso de construir, transformar, organizar, implementar y utilizar activos de conocimiento de manera efectiva en las organizaciones, para lograr sus objetivos.

De esto se deduce que los activos de conocimiento son los impulsores del éxito de una organización de seguridad. Estos se dividen en tres grupos.

1) Conocimiento Explícito

Se trata de saberes estructurados que se pueden articular, organizar, documentar y almacenar fácilmente. Siempre está escrito y comunicado. Se le llama *'know-what'*. Por ejemplo:

- Una política de prevención de la violencia en una farmacia.
- Un curso sobre investigaciones internas en una herrería.
- El procedimiento de cierre y apertura segura de un centro comercial.
- Cada vez que hablamos de "teoría", nos estamos refiriendo al conocimiento explícito.

2) Conocimiento Implícito

Es el conocimiento obtenido tras la aplicación del conocimiento explícito en una situación específica. No está escrito y comunicado, pero sí se puede verbalizar (ponerlo en palabras). Se le llama *'know-how'*. Por ejemplo:

- Mariana conoce la política de prevención de la violencia de la farmacia en la que trabaja. Cuando detectó un caso de comportamiento sospechoso que no estaba contemplado por la política, utilizó la línea de informes anónimos igualmente, lo que permitió conseguir ayuda oportuna para un compañero de trabajo que estaba lidiando con pensamientos suicidas.
- Manuel gestiona la seguridad de una herrería, y recuerda que en un curso sobre investigaciones internas recomendaron que haya un testigo en las entrevistas investigativas que realice. Como esto no fue explicado de forma detallada en el curso, ha aprendido a través de largas pruebas y errores cómo solicitar un testigo de forma empática y generando confianza.
- El equipo de guardias de seguridad de un centro comercial aplica fielmente el procedimiento de cierre y apertura, aunque saben que deben interpretarlo de diferentes formas según el turno correspondiente. Si se encuentran puertas abiertas durante el turno de noche, las cerrarán con un candado. Si lo mismo ocurre durante el turno de día, las cerrarán con un precinto descartable.

Cuando hablamos de "práctica", "experiencia", o de "llevar la teoría a la práctica", estamos hablando de conocimiento implícito.

3) Conocimiento Tácito

Son aquellos conocimientos y habilidades que sólo pueden ser adquiridos a través de años o incluso décadas de experiencia en un trabajo. Se extienden más allá del conocimiento implícito, y son difíciles de documentar o transferir verbalmente a otra persona, ya que incluye sabiduría propia o intuición personal. Por ejemplo:

- Luego de 15 años en la farmacia, cuando Mariana recibe informes anónimos se da cuenta rápidamente de qué información es real o falsa, y cuáles informes requieren respuesta inmediata y cuáles no. Este discernimiento no está mencionado ni explicado en la política de prevención de violencia y nadie más de la farmacia lo sabe hacer, por lo que Mariana ha terminado gestionando todos los informes anónimos ella misma, aunque ésa no es una de las funciones de su puesto.
- Manuel ya ha realizado más de 100 investigaciones internas diferentes, y ha construido lentamente una lista de empleados de la herrería que suelen estar dispuestos a prestarse como testigos durante las entrevistas investigativas.
- Nunca ha compartido esta lista al resto de los investigadores de su equipo, por lo que cada vez que deben solicitar un testigo le preguntan primero a Manuel quién podría serlo, lo cual les hace perder tiempo valioso.
- En el centro comercial, la empresa que proveía el equipo de guardias de seguridad ha sido reemplazada por otra. El nuevo equipo ha estudiado a fondo el procedimiento de cierre y apertura, pero como éste no aclara cómo cerrar temporalmente las puertas que se encuentren abiertas, lo han hecho de forma opuesta al equipo anterior.

Foto: Freepick

- Esto ha generado que se impida y demore el ingreso a ciertos usuarios legítimos por haber cerrado puertas con candado durante el turno de día. Y a su vez ha disminuido el nivel de protección física, ya que han cerrado puertas con precinto durante el turno de noche. El cliente, que es el gerente del centro comercial, está muy insatisfecho y molesto con la nueva empresa de seguridad.

¿SE PUEDEN PREVENIR ESTAS SITUACIONES?

Es evidente que para evitar estos problemas causados por la asimetría de información, debemos trabajar para generar, mejorar y difundir el conocimiento organizacional. Esto lo haremos verbalizando y documentando el conocimiento implícito y tácito, para convertirlo en conocimiento explícito.

¿CÓMO PODREMOS LOGRARLO?

A nivel personal, he realizado tres principales tareas en mi trabajo de consultoría para ampliar el conocimiento explícito en seguridad:

1) He realizado sesiones de revisión luego de un incidente, en donde nos preguntamos si el manejo exitoso o fallido de la situación fue gracias a los procedimientos, a pesar de los procedimientos, o por culpa de los procedimientos.

2) He facilitado talleres colaborativos y ejercicios de simulación para poner a prueba y encontrar brechas en los procedimientos actuales, para poder abordarlas antes de que ocurra un incidente.

3) He usado mis conocimientos como diseñador instruccional y editor técnico para ayudar a mis colegas a que se conviertan en nuevos capacitadores y autores. De esta forma, grandes expertos han escrito su primer libro o impartido su primera capacitación, logrando así transmitir sus conocimientos únicos no sólo a sus propios equipos, sino también a la próxima generación de profesionales de seguridad.

Y tú, ¿seguirás quejándote de que la teoría y la práctica están enfrentadas, o trabajarás para mejorar la gestión del conocimiento en el sector de la seguridad? ■

Referencias:

- Sheila Harkatz (2024). Especialización en Gestión del Conocimiento–IFPYGP.

¿CÓMO EVITAR SER VÍCTIMA DE ROBO EN GASOLINERÍAS?

La delincuencia ha incrementado a tal grado sus actividades, que la carga de combustible se ha convertido en un posible riesgo de sufrir desde el robo de gasolina, fraude al momento de pagar el consumo, clonación de tarjetas de crédito, diagnósticos falsos de falta de aditivos o aceites, hasta el robo de autopartes de vehículo, asaltos e incluso, secuestros y homicidios. Es por ello que David Lee, a través del su Blog del "Manual de Seguridad para la Prevención de Delitos", comparte los siguientes tips para prevenir un robo en las estaciones de carga de combustible.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Prevención.** Conozca la capacidad del tanque de combustible de su vehículo y acostúmbrese a cargar gasolina al bajar el nivel medio del tanque, familiarizándote, así, con la cantidad necesaria y el cobro correcto. Procure hacerlo durante el día y en estaciones de servicio perfectamente establecidas, que tengan buena afluencia vehicular. No deje joyas, *laptops*, cartera a la vista. Y evite manipular el teléfono celular durante su estancia ahí, evite distracciones.
2) **En la estación de servicio.** Seleccione una bomba despachadora ubicada al centro de la estación de servicio, evitando quedar cerca de la calle o avenidas y a merced de otro tipo de delincuentes. Estacione a manera que el tapón de gasolina quede cerca de la manguera de suministro y así pueda observar la manguera de gasolina y la pantalla indicadora de cobro.
3) **Al cargar combustible.** Considere bajar del vehículo para verificar que la carga está siendo correcta. Si requiere pagar con tarjeta, cerciórese que sea aceptada en el lugar y que no tengan problemas para efectuar el cobro. Pida al despachador el suministro en litros y no de una cantidad de dinero, ya que, al efectuar la orden a la máquina, en caso de estar alterada o truqueada, existe una menor posibilidad de que lo defrauden.
4) **Productos y servicios adicionales.** Realice un mantenimiento adecuado de su vehículo, así no tendrá la necesidad de pedir revisiones de aceite y anticongelante, y así evitará un diagnóstico falso sólo para adquirir productos innecesarios.
5) **Al efectuar el pago.** Si paga con efectivo, entregue el o los billetes al operador, uno por uno, indicando en voz alta el pago efectuado. Si recibe cambio, observe bien las características de los billetes y monedas recibidos; si paga con tarjeta de crédito, no la pierda de vista en ningún momento. Revise que el *ticket* de cobro coincida con la cantidad indicada en la máquina despachadora, y consérvelo por si hay algún inconveniente. ■

FOMENTE LA CULTURA DE LA SEGURIDAD

SEGURIDAD EN AMERICA

Consulte la revista digital en
www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

ÍNDICE DE ANUNCIANTES

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

30 AÑOS PROFESIONALIZANDO

PROGRAMA LATINOAMERICANO DE PREPARACIÓN PARA EL EXAMEN DE CERTIFICACIÓN INTERNACIONAL COMO:

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

COORDINADOR
Lic. J. Rubén Fajardo, CPP, PSP, PCI

26 SESIONES
Martes y jueves
17 -21 hrs.

MODALIDAD
Presencial y aula virtual

REPASO
Retiro intensivo
32 hrs.

PARTICIPANTE	COSTO
Socio ASIS	$24,000 M.N. + IVA $1,500 USD + IVA
No socio	$28,000 M.N. + IVA $1,750 USD + IVA

INICIO

08 DE AGOSTO 2024

MAYOR INFORMACIÓN
(55 1321 1289
socios@asis.org.mx

incluye gastos de envío

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. **(Marque así X)**

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en Banco Barnorte, SEA MEDIA GROUP, S. de R. L. de C. V. Cuenta: 1095 5437 37

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe: 0721 8001 0955 4373 78

_____
Firma

DATOS DEL CLIENTE (para el envío de la revista):

Nombre: _____

Compañía: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envío de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato vía: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2024

ALLIED UNIVERSAL®
SECURITY SERVICES

There for you.

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/**


2 ANIVERSARIO
2004 - 2024
SEPSISA®
SEGURIDAD PRIVADA
"Somos gente cuidando a la gente y lo más valioso para ti"
Guardias, guardias armados, custodias, custodias blindadas y custodias armadas.
Cobertura a nivel nacional.
www.sepsisa.com.mx
comercial@sepsisa.com.mx
55 5351 0402
REPSE
AMESP
COPARMEX