SEGURIDAD®
EN AMÉRICA

Especial:

Seguridad en la industria automotriz

Nueva normatividad en hospitales

Reportaje: Guardias intramuros

Año 22 / No.129
Noviembre-Diciembre

www.seguridadenamerica.com.mx

CONTROL

SEGURIDAD PRIVADA INTEGRAL

ÁREAS DE NEGOCIO

- SEGURIDAD Y VIGILANCIA
- CONTECH
- PROTECCIÓN EJECUTIVA
- CONTROL TRUST
- SERVICIOS MÉDICOS
- SERVICIOS DE CONSULTORÍA

20 años

- GENERANDO CONFIANZA
- INNOVANDO
- CERTIFICÁNDONOS
- APORTANDO SEGURIDAD A MÉXICO

SÚPER EMPRESAS EXPANSION 2021 TOP companies

SÚPER EMPRESAS
Desde 2021

México 2021

REPSE
Registro de Prestadoras de Servicios Especializados u Obras Especializadas

REPSE. *Desde 2021*

ESR

EMPRESA SOCIALMENTE RESPONSABLE

ESR. *Desde 2014*

ISO 9001:2015
Organización Certificada
OC-0080/13

ISO 9001:2015
Norma 2008 desde el 2013
Norma 2015 desde el 2018

BASC
Business Alliance for Secure Commerce
CERTIFICADO BASC
USAELP00042-1-2

BASC USA
Capítulo México desde el 2014
Capítulo USA desde el 2018

Superbrands
MEXICO'S CHOICE

SUPERBRANDS
Desde el 2016

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

Socio Fundador. Desde 2013

www.seguridadcontrol.com.mx

@segcontrol

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

(55)5406 5287 • (55)3455 4375

INFO@MULTIPROSEG.COM.MX

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

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

- SERVICIOS DE MONITOREO
- SISTEMAS ELECTRÓNICOS DE SEGURIDAD
- CUSTODIAS DE TRANSPORTE
- GUARDIAS INTRAMUROS

MONTERREY • SINALOA • QUERÉTARO • PUEBLA • EDOMEX • BAJA CALIFORNIA SUR

CORPORATIVO CDMX

SEGURIDAD EN AMÉRICA

Es una publicación con 22 años de presencia en el mercado. Nuestra misión es informar a la industria de seguridad, tecnología de la información (TI) y seguridad privada, así como al sector de la seguridad pública. Distribuidos 40 mil ejemplares bimestrales en más de 15 países de Latinoamérica.

Año 22 / No. 129 / noviembre-diciembre / 2021

Foto de Portada
SEA

Síguenos por

Seguridad-En-América

@Seguridad_En_Am

@seguridad_en_america

SeguridadEnAmerica

revista-seguridad-en-america

@seguridad_en_america

www.seguridadenamerica.com.mx

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
Verónica Romero Contreras
v.romero@seguridadenamerica.com.mx

Arte & Creatividad
Arturo Bobadilla

Diego Idu Julián Sánchez
arte@seguridadenamerica.com.mx

Administración
Oswaldo Roldán
oroldan@seguridadenamerica.com.mx

Ejecutivos de Ventas
Alex Parker, DSE
aparker@seguridadenamerica.com.mx

Pilar Erreguerena
perreguerena@seguridadenamerica.com.mx

Reporteros
Mónica Ramos
redaccion1@seguridadenamerica.com.mx

Erick Martínez Camacho
redaccion2@seguridadenamerica.com.mx

Pablo Romero Navor
redaccion3@seguridadenamerica.com.mx

Elizabet Gómez
redaccion4@seguridadenamerica.com.mx

Medios Digitales
Brenda Chávez Altamirano
mdigital@seguridadenamerica.com.mx

Iván Solís Bustos
mdigital2@seguridadenamerica.com.mx

Jesús Chávez García
mdigital3@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

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

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

Representante en Ecuador
José Echeverría, CPP
Soluciones de Seguridad Corporativa
+593-9920-54008
joseomar90@gmail.com

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

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

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

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

Apoyando a:

Socio de:

COMPARTE ESTA REVISTA
COMPARTIR ES RECICLAR

Conmutador: 5572.6005
www.seguridadenamerica.com.mx

EDITORIAL

Los nombres de empresarios, políticos, líderes mundiales, deportistas y celebridades aparecieron en los *Pandora Papers*, una filtración de casi 12 millones de documentos que revelan riqueza oculta, evasión de impuestos y, en algunos casos, lavado de dinero por parte de algunas de las personas más ricas y poderosas del mundo.

La investigación fue elaborada por el Consorcio Internacional de Periodistas de Investigación (ICIJ, por sus siglas en inglés) e involucró a unos 600 periodistas de 150 medios, incluidos The Washington Post y The Guardian. En México, la investigación fue publicada por Quinto Elemento Lab.

En Latinoamérica se detectaron a tres presidentes en funciones y 11 ex presidentes de América Latina, siendo los presidentes: Sebastián Piñera, presidente de Chile; Guillermo Lasso, presidente de Ecuador; y Luis Abinader, presidente de República Dominicana. En cuanto a los ex presidentes encontramos a César Gaviria Trujillo (con mandato de 1990 a 1994) y el conservador Andrés Pastrana Arango (1998-2002) de Colombia; de Argentina, a Jaime Durán Barba, consultor político que catapultó a la presidencia a Mauricio Macri en 2015; y Zulema Menem, hija del expresidente Carlos Menem (1989-1999); Daniel Muñoz (ya fallecido), ex secretario del ex presidente Néstor Kirchner; en Brasil, el ministro de Economía, Paulo Guedes; y el presidente del Banco Central, Roberto Campos Neto, entre otras figuras más.

En México son más de 3 mil personas vinculadas al caso. La mayoría de estos mexicanos se han inventado sociedades para mantener sus fastuosas vidas y comprar residencias de lujo, jets, yates, pagando menos impuestos y hacer que rinda más la administración de sus fortunas y herencias; gestionar inversiones, abrir cuentas bancarias y ocultarles sus utilidades a sus trabajadores y gobiernos.

Ha dejado al descubierto las riquezas ocultas de los grandes contratistas de Petróleos Mexicanos (Pemex), ya que la última filtración a la que ha tenido acceso el Consorcio Internacional de Periodistas de Investigación revela cómo los dueños de cuatro grandes proveedoras de la petrolera abrieron sociedades en paraísos fiscales y movieron millones de dólares, al mismo tiempo que recibían millones de pesos de las arcas públicas.

De acuerdo con El País, el dueño de Oceanografía y proveedor de buques tanque a Pemex, Amado Yáñez Osuna, creó una empresa para comprarse un lujoso yate en 2012, tras alcanzar su auge empresarial en México. Al igual que el presidente de Grupo R, Ramiro Garza Vargas, que abrió dos empresas en 2001 para comprar dos yates de lujo. Fabián Narváez Tovar, director de Administradores Navieros del Golfo, desplegó una red de entidades entre 2010 y 2018 para adquirir bienes raíces y embarcaciones. O los fundadores del consorcio Blue Marine, que operaron durante el sexenio pasado una compleja estructura que abarcaba desde ahorros personales a inversiones en varios países.

En México, los *Pandora Papers* han servido para reafirmar la deshonestidad y la corrupción en cualquier tendencia política. Lo que sí hace esta filtración es demostrar que el combate a la corrupción va a seguir sin funcionar si la seguimos viendo como un problema nacional. La gran corrupción es un fenómeno transnacional y es en ese ámbito donde deberíamos estar actuando. ■

Seguridad en América *le desea felices fiestas y un próspero año nuevo 2022, lleno de abundancia y seguridad.*

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 Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León, México, 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

Cinthya V. Mayén,

directora de Operaciones en Control y Seguridad Meraki

¿Cuáles considera que serán las consecuencias de quitar a la Seguridad Privada de instalaciones gubernamentales?

Desde mi perspectiva, sacar a la seguridad privada de las instalaciones gubernamentales sólo significa una cosa, llevar a la seguridad pública dentro de las mismas, exponiéndose así a diversos retos, ya que ambas están enfocadas a atender diferentes áreas y conflictos, por tanto, la capacitación de ambos es completamente diferente. Teniendo todo esto en cuenta, llevar a la seguridad pública a cuidar instalaciones gubernamentales implicaría invertir grandes cantidades del erario público en capacitación en áreas para las cuales los policías no están capacitados, tales como: seguridad a instalaciones, control de accesos, protección civil, primeros auxilios como primer respondiente y antimotines, por nombrar solamente algunas áreas, todo esto sin mencionar que por cada policía que metamos a cuidar de las instalaciones, será un policía menos en las calles que cuide de los ciudadanos. ■

GRUPO IPS

GARANTÍA EN SEGURIDAD

10 AÑOS

Best Workplaces for Women
Great Place To Work.
MÉXICO 2021

Síguenos

grupoipsmexico.com

Tel. (55) 5525 3242

VIDEOVIGILANCIA

CONTROL DE ACCESO

TRANSPORTE SEGURO

CONTRA INCENDIOS

CIBERSEGURIDAD Y TI

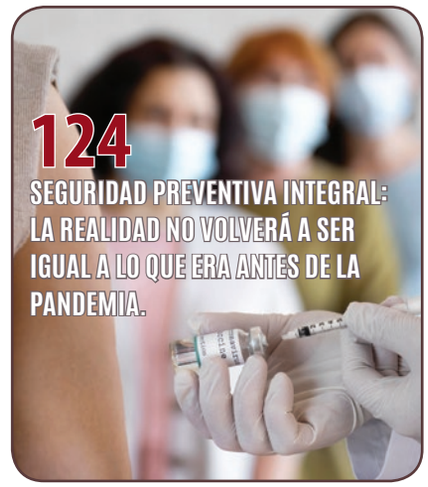
ESPECIAL

ESPECIAL

SEGURIDAD PRIVADA

ADMINISTRACIÓN DE LA SEGURIDAD

SEGURIDAD PÚBLICA



FOROS Y EVENTOS

NOVEDADES DE LA INDUSTRIA

TIPS

COLUMNA ALAS
COMITÉ NACIONAL MÉXICO

Alberto López Flores

Vicepresidente de Membresías en ALAS Comité Nacional México y Sales Manager en México para Eagle Eye Networks.

Más sobre el autor:

CIBERSEGURIDAD EN LOS SISTEMAS DE VIDEOVIGILANCIA: VULNERABILIDADES INMINENTES

Foto: Creativeart - Freepik

MÉXICO

Los sistemas de video de hoy en día se han vuelto importantes tanto para las corporaciones como para los gobiernos por la capacidad de proteger sus personas, instalaciones y activos como por la perspectiva empresarial que proporcionan una importante información que eficientizan sus operaciones.

Dichos sistemas, están cada vez más conectados a Internet, impulsados en gran parte por la demanda del cliente por acceso remoto a video.

Normalmente los sistemas de video suelen ser de tres tipos:

1. **Sistemas tradicionales DVR/VMS/NVRs conectados a Internet.**
2. **Sistemas tradicionales DVR/VMS/NVRs conectados a una red local que a su vez está conectada a Internet.**
3. **Sistemas administrados en la Nube.**

Para maximizar su seguridad, es imprescindible definir mejores prácticas para su propia empresa como parte de la evaluación del sistema de su cámara de seguridad, así como su implementación y mantenimiento.

Es recomendable proteger a su empresa y clientes con medidas de prevención, entonces hablemos de las vulnerabilidades principales y cómo contrarrestarlas.

VULNERABILIDAD DESDE LA CÁMARA

Se estima que uno de cada cinco usuarios de la web todavía usan contraseñas fáciles de vulnerar. Casi todas las cámaras vendidas hoy en día tienen una interfaz de usuario basada en web (GUI), y vienen con un usuario y contraseña por defecto que es publicada en Internet.

Foto: Creativeart - Freepik

Algunos instaladores nunca cambian la contraseña y dejan la misma contraseña por defecto en todas las cámaras. Sólo pocas cámaras tienen una manera de desactivar el GUI, así que la vulnerabilidad de seguridad es que alguien puede intentar acceder a la cámara vía la GUI en línea para adivinar la contraseña. El '*hacker*' necesita acceso a la red para hacer esto, pero las cámaras se encuentran usualmente en una red compartida, no en una red separada físicamente o una VLAN (red de área local virtual).

La práctica ideal es asignar una contraseña única, larga y no obvia para cada cámara. Un proceso meticuloso como tal toma más tiempo en preparar, es más complicado de administrar y muy difícil de seguir. Es por ello que, lamentablemente, muchos instaladores usan una sola contraseña para todas las cámaras en una cuenta.

Para permitir este desafío, una mejor práctica aceptable es:

- Red pública: contraseña fuerte diferente para cada cámara.
- VLAN o red física privada: la misma contraseña fuerte para todas las cámaras.

Las recompensas económicas por robar datos de empresa son lo suficientemente altas como para que los intrusos busquen también acceder a su red mediante un ataque directo a su equipo físico en sus instalaciones

VULNERABILIDAD AL ACCEDER VÍA REMOTA

La mayoría de las compañías o gobiernos ahora demandan y esperan acceso remoto a videos. Esta función es normalmente entregada al exponer el DVR, NVR o servidor a Internet de alguna manera. La exposición típica a Internet de un servidor HTTP es extremadamente peligrosa debido a que existe un gran número de posibilidades maliciosas que pueden ser usadas para obtener acceso. Las máquinas abiertas a Internet son usualmente escaneadas más de 10 mil veces al día.

No conecte su servidor desprotegido a Internet. Si expone su sistema a Internet, entonces "redireccione el puerto" a la menor cantidad de puertos posible y utilice un *firewall* de nueva generación que analice el protocolo y bloquee protocolos incorrectos enviados al puerto equivocado. En una situación ideal, despliegue además un IDS/IPS para mayor protección.

VULNERABILIDADES POR LA TOPOLOGÍA DE RED

Si su sistema de cámaras de seguridad está conectado a su red principal, está creando una puerta para que los *hackers* pueden ingresar a su red principal a través de su sistema de vigilancia, o entrar a su sistema de seguridad física a través de su red principal. Mezclar cámaras en una red estándar sin separación es una receta para el desastre.

Idealmente, ubique su sistema de cámaras de seguridad en una red separada físicamente del resto de su red. Si está integrado con un ambiente informático, no siempre es posible separar los dos sistemas físicamente, entonces debe utilizar una VLAN.

VULNERABILIDAD POR EL SISTEMA OPERATIVO

Su VMS, DVR, NVR o sistema de grabación tendrá un sistema operativo, también las cámaras tienen un sistema operativo. Ahora, todos los sistemas operativos tienen vulnerabilidades, tanto los basados en Windows como los basados en Linux.

Las vulnerabilidades de Windows están tan bien aceptadas que los equipos de TI las monitorizan regularmente. Recientemente, se ha vuelto más y más

Sólo pocas cámaras tienen una manera de desactivar el GUI, así que la vulnerabilidad de seguridad es que alguien puede intentar acceder a la cámara vía la GUI en línea para adivinar la contraseña

Foto: Eagle Eye Networks

aparente que Linux tiene también muchas vulnerabilidades, como Shellshock (2014) y Ghost (2015), lo cual ha hecho vulnerables a millones de sistemas.

En teoría, su fabricante de sistema tendrá un equipo de seguridad de alta gama que esté disponible para ofrecerle actualizaciones de seguridad. La realidad es que muchos proveedores no hacen esto de una manera predecible.

Si es un sistema basado en Windows, existen muchas vulnerabilidades y muchas actualizaciones a ser aplicadas. Aunque son menos frecuentes, las vulnerabilidades de Linux deben también ser rastreadas y atendidas rápidamente. También puede contactar con su proveedor de DVR/NVR para averiguar qué sistema operativo usa su NVR/DVR (Linux, Windows) y también qué versiones de sistema y módulos adicionales están implementados (por ejemplo, el servidor de páginas web Microsoft ISS) para que pueda entender qué vulnerabilidades de seguridad van a impactarle.

Además, asegúrese de que su proveedor de cámara ofrezca parches para problemas de seguridad y que esté actualizando el *firmware* de su cámara en cuanto las nuevas versiones estén disponibles.

VULNERABILIDAD POR CONEXIONES SIN CIFRADO SSL O EQUIVALENTE

Un número sorprendente de DVR/NVR/VMS's usan conexiones que no están cifradas con SSL o equivalentes. Este riesgo es idéntico al de iniciar sesión en un banco o realizar compras en líneas sin HTTPS. Crea una vulnerabilidad de contraseña y abre la posibilidad a brechas de privacidad y espionaje.

Es imprescindible que su conexión sea cifrada con SSL o equivalente. Pregunte a su proveedor cómo manejar esto y sólo elija proveedores que cifren sus conexiones.

Si el sistema está gestionado en la Nube, confirme con su proveedor cómo su sistema maneja esto, la gran mayoría lo maneja, pero no hay que darlo por hecho.

VULNERABILIDAD POR VIDEO NO CIFRADO

El cifrado es el proceso de cambiar datos para que no se puedan leer (encriptación), de manera que al volver a cambiarlos a su forma original, se puedan volver a leer (descifrado). Incluso la forma más sencilla de cifrado utiliza un único set de caracteres (números, letras y/o símbolos) como clave de cifrado para hacer ambas operaciones.

Además de conexiones inseguras debido a una falta de cifrado, los mismos riesgos de privacidad se aplican cuando el video no es cifrado al ser guardado en un disco o en tránsito si se almacena en la Nube.

ACCESO FÍSICO AL EQUIPO Y ALMACENAMIENTO

Las recompensas económicas por robar datos de empresa son lo suficientemente altas como para que los intrusos busquen también acceder a su red mediante un ataque directo a su equipo físico en sus instalaciones. Por eso mantenga seguro sus gabinetes, cables y la habitación donde guarda los DVR/NVR/VMS, interruptores y servidores de almacenamiento de video. Proporcione un control de acceso seguro a la habitación, incluyendo videos de seguridad para monitorizarlo. Esta práctica no sólo protege su red, sino que también previene robos violentos en sus instalaciones, aquellos donde el DVR/NVR de grabación es robado junto a otros artículos.

Aunque los mismos principios claramente se aplican a un sistema basado en la Nube, existen menos equipos en las instalaciones que proteger. La grabación inmediata en la Nube también protege ante ataques violentos al equipo de grabación en sitio. Es importante preguntar a su integrador o proveedor por medidas de seguridad generales que toman para sus servidores en la Nube.

CONCLUSIÓN

No existe seguridad física sólida, si no se tiene la seguridad informática como pilar, sin embargo, la gran mayoría de los ataques se gestan por descuido, por circunstancias prevenibles, muchos de éstos a través de accesos por inicio de sesiones a través de contraseñas vulnerables.

La mayoría de los ataques cibernéticos funcionan obteniendo acceso mediante credenciales de inicio de sesión del usuario y después utilizando las vulnerabilidades de dispositivos y sistemas para obtener un alto nivel de acceso que permita a los atacantes un control completo. ■

EL LÍDER DEL MERCADO PROBADO INTRODUCE EL **SPEEDLANE COMPACT.**

EL TORNIQUETE ÓPTICO **MÁS CORTO DE SEGURIDAD**

La última incorporación a la gama premium de Boon Edam resuelve el problema de introducir la seguridad en áreas pequeñas y valiosas de espacios inmobiliarios.

Para obtener más información, vaya a:
www.boonedam.mx/compact

BOON EDAM
YOUR **ENTRY** EXPERTS.

OPTIMIZANDO LA SEGURIDAD EN HOSPITALES CON SOLUCIONES DE VIDEOVIGILANCIA AVANZADAS

Contar con sistemas tecnológicos de última generación en hospitales, en condiciones normales logrará mejorar sus operaciones, maximizar sus recursos y obtener soluciones para simplificar su administración, lo que permitirá una mejor atención para los pacientes

ESPAÑA | Alberto Pérez Aparicio

En la actualidad, nuestros hospitales se encuentran viviendo una vorágine muy pocas veces vista con anterioridad y cuando se trata de seguridad física, los hospitales y las instalaciones sanitarias se enfrentan a una serie de desafíos únicos.

La gran cantidad de flujos de personas transitando, el refuerzo de los protocolos de auto-protección de los trabajadores (personal sanitario, auxiliares, celadores, administrativos, etc.), la utilización de medios materiales y productos de gran valor económico junto a la necesidad de seguir prestando una buena atención a los pacientes, hacen que los centros hospitalarios necesiten dotarse de recursos tecnológicos y procedimentales, que les permitan disponer de un entorno mucho más seguro y con herramientas que les faciliten la toma de decisiones en los momentos clave. Y todo esto deben hacerlo cumpliendo al mismo tiempo con una serie de estándares, códigos, reglas y regulaciones.

La naturaleza 24/7/365 de los hospitales requiere una atención adicional cuando se trata de las medidas de seguridad más apropiadas. En las instalaciones sanitarias, la videovigilancia es una herramienta eficaz no sólo para aumentar la seguridad, sino también para conseguir un control efectivo de los costos, así como supervisar y perfeccionar los protocolos de actuación, haciendo uso de los datos que los diferentes componentes del sistema pueden proporcionar a los responsables para una mejor toma de decisiones.

CUIDADO Y VIGILANCIA REMOTA DE PACIENTES

Uno de los escenarios más extendidos es la utilización de cámaras para el cuidado y vigilancia de pacientes, estando más extendidas en las áreas de psiquiatría o en las UCIs, para que los pacientes puedan ser monitorizados en tiempo real desde el puesto de control y el personal sanitario pueda gestionar su tiempo de una forma mucho más eficiente.

Con capacidades que van más allá de la simple videovigilancia hacia sistemas con analíticos basados en inteligencia artificial, control de accesos, administración de visitantes o incluso la mejora de la atención al paciente; las estrategias de videovigilancia modernas están ayudando a los centros de salud a satisfacer estas demandas tan complejas.

JUMI-MKT
MERCADOTECNIA Y PUBLICIDAD

NUESTROS SERVICIOS

MARKETING DIGITAL

MANEJO Y GESTIÓN DE REDES SOCIALES

DISEÑO DE CONTENIDO

SOMOS LA AGENCIA DE PUBLICIDAD Y MERCADOTECNIA ESPECIALIZADA EN EMPRESAS DE SEGURIDAD PRIVADA

(55) 5406 5287

@JUMIMKT

JUMIMKT@GMAIL.COM

JUMI MKT

Esa combinación del CCTV dando cobertura al binomio seguridad-operativa en la instalación, se fundamenta en el uso de herramientas de videoanálisis basadas en la inteligencia artificial o en la integración con sistemas de posicionamiento, y pueden desagregarse en los siguientes aspectos:

- Realización de un **control de los accesos mediante el reconocimiento facial**, y de esta forma responder de forma proactiva ante intrusiones de personas no autorizadas en áreas restringidas o para autorizar accesos a determinadas áreas a aquellas personas que sí lo tengan permitido, usando la biometría facial como sustitutiva de las tradicionales tarjetas, códigos numéricos o huellas dactilares.

- **Supervisión e identificación de bienes u objetos** que hayan podido ser **abandonados** de forma negligente y que pueden suponer un riesgo para las personas o las instalaciones.

- Apoyo en la gestión de emergencias, como por ejemplo en evacuaciones, usando el sistema para saber mediante el **control de aforos** cuántas personas hay en las instalaciones y poder tener una herramienta más, que ayude a la hora de gestionar y coordinar todos los protocolos necesarios.

- **Control de los estacionamientos**, permitiendo conocer en todo momento cuántos vehículos se encuentran en su interior y tenerlos identificados mediante la lectura de sus matrículas.

  Estas prestaciones permiten informar a los visitantes de si el *parking* dispone de plazas libres y, al área de Seguridad del centro hospitalario, poder autorizar accesos a vehículos de trabajadores previamente registrados o verificar posibles vehículos sospechosos que permanezcan más del tiempo habitual.

- **Seguimiento de equipos médicos y de bienes**. En los últimos meses, se ha venido produciendo un aumento en la preocupación por proteger tanto los activos físicos (equipos médicos y de diagnóstico de alta tecnología) como aquellos productos (medicamentos o vacunas) de alto valor económico y que puedan ser objeto de robos o hurtos.

  Los **sistemas de videovigilancia** permiten realizar **integraciones con sistemas de posicionamiento** que, mediante *tags* acoplados a los activos o productos señalizan en todo momento dónde se encuentran ubicados y es posible visualizar en tiempo real la cámara que se encuentre más cercana a donde se encuentre ubicado el *tag*.

  Adicionalmente, y con motivo de pesquisas forenses, sería posible reconstruir en video todo el recorrido del *tag* asociado al activo o producto en un intervalo temporal determinado dentro del hospital. De esta forma, los elevados costos por reposición de dichos bienes pueden verse reducidos considerablemente.

Esa combinación del CCTV dando cobertura al binomio seguridad-operativa en la instalación, se fundamenta en el uso de herramientas de videoanálisis basadas en la inteligencia artificial o en la integración con sistemas de posicionamiento

Todas las posibilidades anteriores que se abren con los sistemas de videovigilancia generan a su vez datos de interés que pueden ser interpretados por sistemas especializados de *business intelligence*, y presentarse a los gestores de los centros hospitalarios en forma de cuadros de mando que sirvan de apoyo a la hora de supervisar, valorar y optimizar los procedimientos internos, la calidad en la atención al paciente y la utilización de los recursos humanos y materiales. Estos cuadros de mando resultan muy eficaces para asegurar el éxito de la gestión hospitalaria.

Sin duda, los sistemas de videovigilancia inteligente consiguen aportar valor a toda la organización, y no únicamente al departamento de Seguridad a la hora de contar con la evidencia. Permiten la mejora continua de procedimientos internos, ahorro en costos operacionales y administrativos, ofreciendo un auténtico *big data* de información para tomar decisiones relacionadas con el propio negocio. Bienvenidos al negocio. ■

Fotos: SCATI

Alberto Pérez Aparicio,
director comercial de SCATI para Latinoamérica.

Más sobre el autor:

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA

EVOLUCIONA la SEGURIDAD de tu HOGAR y NEGOCIO al SIGUIENTE NIVEL

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

222 141 12 30

WWW.PEM-SA.COM

gerenciacomer@pem-sa.com

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

No. CERTIFICADO: SG20211485

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD ALAS

SOCIO ACTIVO

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

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

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

VIDEOVIGILANCIA Y CIUDADES INTELIGENTES EN AMÉRICA LATINA

Tres casos de éxito

MÉXICO | Leopoldo Ruíz Alfaro

Uno de los temas emergentes de cara a la nueva normalidad es el de las ciudades inteligentes, en el cual la mayoría de los especialistas comulgan con la definición de desarrollo tecnológico para mejorar la calidad de vida de sus habitantes y garantizar un retorno seguro para todos. No obstante, se pueden encontrar muchas definiciones centradas en la integración de infraestructuras, innovación y tecnología para mejorar la eficiencia en los servicios, gestionar la movilidad, hacerlas más seguras, resilientes y sostenibles.

Empresas como Axis se han enfrentado a múltiples desafíos en la región latinoamericana, sin embargo, los principales retos están centrados en la utilización de la tecnología para mejorar la calidad de vida dentro de las ciudades, pues la Comisión Económica para América Latina y el Caribe estima que aproximadamente el 80% de la población se concentra en zonas urbanas. América Latina representa uno de los territorios más grandes del mundo, y con ello, uno de los principales retos en temas de seguridad debido a su creciente urbanización, en este sentido, la videovigilancia se ha posicionado como una piedra angular para mejorar la seguridad y, sobre todo, para el desarrollo de las urbes.

TRES CIUDADES INTELIGENTES EN AMÉRICA LATINA

La videovigilancia con analíticas y audio IP (Internet Protocol) ha marcado un antes y un después en la reducción de tiempos en el trabajo de monitoreo, lo que ha permitido ofrecer soluciones basadas en la visión, sonido y análisis para mejorar la seguridad, optimizar el rendimiento de las ciudades y cumplir con las normas de sanidad. En Latinoamérica, los proyectos de Ciudades Inteligentes ya son una realidad:

Vicente López, Argentina

Vicente López está situado en la sección norte del área del Gran Buenos Aires, con una población de aproximadamente 300 mil en un área cercana a 13 millas cuadradas. Esta gran ciudad se enfrentó a la necesidad de procurar la seguridad de miles de ciudadanos que diariamente viajan a diversos puntos de la ciudad, ya sea en transporte público o en auto privado, por lo que el Gobierno tuvo que modernizar y expandir el sistema de videovigilancia de la ciudad, con el fin de lograr un monitoreo constante y crear un entorno seguro para los ciudadanos.

De esta forma las autoridades pusieron en marcha un proyecto de Ciudad Inteligente con ayuda de la videovigilancia. Logrando instalar más de 800 cámaras de alta tecnología para la vigilancia en edificios gubernamentales, a lo largo de la vía pública, servicio de transporte, así como en coches patrulla, dando como resultado la creación de uno de los proyectos urbanos más completos y de vanguardia de toda América del Sur.

León, Guanajuato (México)

León es una ciudad con aproximadamente 1,4 millones de habitantes y debido a los riesgos de seguridad, además de la falta de personal para cubrir los lugares con altos índices de delincuencia, el gobierno municipal decidió modernizar el sistema de vigilancia por cámaras IP para dar respuesta a las necesidades de seguridad en la zona. Se determinaron las ubicaciones de las cámaras mapeando las llamadas de emergencia realizadas a la policía y seleccionaron una combinación de cámaras de última generación para generar una red de videovigilancia robusta y escalable.

Este proyecto de Ciudad Inteligente logró que León pudiera capturar una amplia variedad de incidentes, desde infracciones administrativas hasta asaltos. La evidencia captada por las cámaras ha ayudado al municipio a resolver estos incidentes gracias a la

disminución de los tiempos de respuesta del personal de seguridad y aumentar la calidad de vida de sus habitantes debido a la sensación de seguridad que las cámaras proporcionan. Hoy el sistema es monitoreado por operadores ubicados en el Centro de Comando C4, pero también de forma remota desde otros edificios del Ministerio de Seguridad.

Concón, Chile

Los desastres naturales son situaciones que no se pueden evitar, sin embargo, sí es posible mitigar sus impactos. En 2015 un terremoto que alcanzó una magnitud de 8.4 grados y el posterior tsunami provocaron daños en la costa chilena, principalmente en Concón. Ante los futuros riesgos, el ayuntamiento decidió dar respuesta a las necesidades de los habitantes y realizó una solicitud pública para iniciar un proyecto de Ciudad Inteligente, basado en un sistema de cámaras y altavoces IP que se convertirían en parte de la solución a los problemas de vandalismo, además de brindar asistencia ante desastres.

La instalación constó de más de 23 cámaras y 28 altavoces que tenían el objetivo de aumentar el nivel de comunicación entre autoridades públicas y residentes. Gracias a esta iniciativa Concón ahora es una ciudad preparada para alertar a las personas a través del sistema de altavoces y se ha convertido en un modelo de ciudad para toda la costa de Chile.

De esta forma nos ha sido posible contribuir al concepto de "Ciudades Seguras", combinando recursos humanos y administración para crear un enfoque intuitivo a través de la observación, comunicación y gestión de la información mediante la tecnología de video en red, la cual ha experimentado una demanda exponencial después de la crisis sanitaria. Hoy las posibilidades que ofrece un sistema de videovigilancia son innegables y estos ejemplos de proyectos con visión a futuro, son la antesala para la generación de ciudades preparadas para los retos de hoy y mañana. ■

Fotos: Axis Communications

Si quiere conocer más acerca de cómo la videovigilancia puede ayudar a mejorar la seguridad ciudadana, escaneé el código QR:

Leopoldo Ruiz Alfaro,
director regional para Latinoamérica en Axis Communications.

Más sobre el autor:

REPENSANDO CON SERIEDAD **EL CONCEPTO DE ALARMAS DE SEGURIDAD** PARA RESIDENCIAS

Foto: Creativeart - Freepik

Hoy existen las soluciones tecnológicas a costos accesibles y es necesario lograr tener un concepto integral de seguridad para residencias, que nos permita diferenciar entre una alarma falsa y una alarma relevante

ALEMANIA | Hans Klein

Los principios de detección de intrusión y las pautas básicas de seguridad se deben considerar y aplicar para todos los "verticales". Me refiero, a que los principios en relación con la detección de intrusión no cambian, si se trata de la protección de un sitio con infraestructura crítica o si se trata de proteger una casa de familia, además, a nivel personal, no hay un sitio más "crítico" que la casa donde vivimos con nuestra familia.

Sin embargo, en la práctica vemos que, en la gran mayoría, no se están aplicando las mismas pautas. La solución "clásica" para la protección de residencias es el sistema de alarmas "interiores", que conceptualmente, fue diseñado para que no nos roben cuando no estemos en casa. Un sistema que alarma, hasta cuando los intrusos están dentro de la casa, es de poca ayuda, e incluso, puede ser hasta contraproducente. Pero hoy día, cuando toda la familia está en casa, nuestra preocupación es otra, y es mucho más grande: ¡Una intrusión o asalto a la casa con la familia dentro!

El sector residencial es uno de los más rezagados en cuanto a los elementos básicos de seguridad y, posiblemente, una buena parte de la industria (alarmas de residencias, monitoreo, etc.), todavía no conoce las oportunidades y soluciones que, por fortuna, están al alcance para proteger mejor y con más eficiencia las residencias y a sus familias. Es tiempo de adaptar el concepto residencial de seguridad a la situación que se vive y mirar el espectro de amenazas y exposición en el que estamos.

PARA TOMAR EN CUENTA

Los principales criterios que tenemos que reconocer como los más relevantes para una eficiente detección de amenazas o intrusiones en residencias son:

- **La detección de un intruso tiene que ser lo más temprano posible,** ojalá antes de que suceda algún daño, pero lo más importante, **antes de que pueda lastimar a las personas dentro de la residencia.** Sensores de detección en el perímetro, sensores de detección entre perímetro y casa, detectar en el jardín, patio, detección de la fachada. Son algunas alternativas para detectar al adversario, antes de que esté dentro de la propiedad, y así ganar un tiempo muy valioso.

Foto: Creativeart - Freepik

- Que la detección de una intrusión o amenaza sea confiable y que el sensor cumpla su función, aún en condiciones adversas (por ejemplo: vegetación, mascotas, animales pequeños silvestres, lluvia, neblina, etc.). Cabe destacar la importancia de la selección de la tecnología correcta. Por un lado, respondiendo a las condiciones que demanda un sitio en particular, pero también teniendo en cuenta la calidad de la tecnología y la marca.

Nunca habías amado más a tu tablet

DoorKing. Administrador de Cuenta en la Nube. Programa desde cualquier lugar al Toque de un Botón.

Desde 1948, DKS ha desarrollado una línea completa de dispositivos de acceso confiables diseñados para trabajar juntos sin problemas desde el portón hasta la puerta, el ascensor y más allá. Ahora, el nuevo Administrador de cuentas en la nube permite a los administradores del sistema de acceso personalizar la configuración de su sistema de entrada desde cualquier computadora, tableta o teléfono inteligente con conexión a Internet. La nube es perfecta para los equipos de administración remota, y nunca más te verás atrapado por problemas de PC o sobreescritura de datos. DKS: Te da la libertad de controlar tu acceso como quieras y donde quieras.

DKS DOORKING

HECHO EN EE.UU

OBTENGA MÁS INFORMACIÓN SOBRE CÓMO CREAR SU SOLUCIÓN

doorking.com/freedom

800-673-3299 • info@doorking.com

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Es tiempo de adaptar el concepto residencial de seguridad a la situación que se vive y mirar el espectro de amenazas y exposición en el que estamos

Especialmente en el mercado residencial, donde la cuestión del costo es muy sensible, el mercado tiende a orientarse más por cantidad (costo) y no por calidad (eficiencia), a pesar de que, muchas veces, la diferencia entre lo bueno y malo es muy poco.

Un sistema de detección y el concepto moderno y eficiente de protección para residencias, también tiene que **contemplar la verificación de las alarmas, en vivo.** Es decir, cuando se detecta un movimiento en una zona exterior determinada de interés, entonces es preciso poder ver y evaluar, simultáneamente, el lugar donde se detectó.

El área de detección debe coincidir con la perspectiva de la cámara, para que el operador/receptor del video o imágenes del evento pueda evaluar fácilmente y reconocer la naturaleza de la alarma en el instante. Incluso, puede obtener imágenes memorizadas desde segundos antes del instante de la detección.

Eso se puede lograr de manera sencilla —pero con un grado limitado de confiabilidad—, con cámaras y video analíticos, —probablemente con un índice alto de alarmas no deseadas—, y, por ende, un *streaming* de videos elevado y distracciones innecesarias de recursos. Con poco esfuerzo adicional, se puede evitar eso y lograr mucho mayor confiabilidad. Por ejemplo: agregando a la cámara un sensor físico de alto rendimiento para exteriores como el PIR (Passive Infrared), AIR (Active Infrared), Láser, etc., aumentando así, la probabilidad de detección de un evento real y, al mismo tiempo, minimizando el índice de falsas alarmas y las transmisiones de "alarmas innecesarias".

Hoy existen las soluciones tecnológicas a costos accesibles y es necesario lograr tener un concepto integral de seguridad para residencias, que nos permita diferenciar entre una alarma falsa y una alarma —o amenaza— relevante. Sea para monitoreo profesional y a gran escala o '*standalone*' (el usuario opera su sistema, ej. con aplicación *smartphone*, servicio en Nube, etc.).

- Para el bien de la industria y de los usuarios, es importante considerar que las falsas alarmas son una carga y un obstáculo importante para nuestra causa y para un sistema (social) funcionando. Sea para las fuerzas del orden o bien, para el sector privado de seguridad, "alarmas que no son" significan un costo muy alto, pero poco visible para la sociedad y/o los particulares. Los costos no contados en términos de horas-hombre deben correr a cargo de alguien, cuando en realidad son distraídos para prevenir y resolver delitos reales y, en vez de ello, responden a falsas "llamadas de robo" de los sistemas de alarma residenciales, comerciales o industriales.

SENSORES PARA LA DETECCIÓN DE INTRUSIÓN

Mediante el uso de sensores inteligentes para detectar al intruso y activar el video para verificar el evento, unimos la potencia de dos tecnologías importantes. Cualquiera que sea el tamaño y la complejidad del sitio para proteger, y el sistema de seguridad en este lugar, en OPTEX tenemos los sensores para encontrar la aplicación y la solución perfecta con verificación visual dirigida por sensores confiables.

OPTEX es uno de los fabricantes líderes con la más amplia gama de tecnologías de sensores para la detección de intrusión y detección temprana de amenazas. Los sensores para exteriores (inalámbricos o cableados) de OPTEX, han demostrado ser tan exitosos en el campo, que muchos expertos que especifican e instalan equipos de seguridad, han cambiado la forma de diseñar los sistemas de seguridad en sus proyectos residenciales, para enfrentar mejor la inseguridad en el sector.

Todos los sensores exteriores están equipados con la última programación de análisis de OPTEX que incluye tolerancia a animales pequeños, no-detección de vegetación y protección meteorológica mejorada, para garantizar que se eviten falsas alarmas de cualquier índole. Los sensores son a prueba de manipulaciones y los sensores inalámbricos tienen una duración de la batería de tres años a cinco años. Los sensores fabricados por OPTEX presentan especificaciones con los índices más bajos de falsas alarmas y las tasas de detección confiable más altas de la industria. ■

Para más información visite www.optexamerica.com, www.fibersensys.com y www.raytecctv.com.

Hans Klein,
presidente para Latinoamérica de Optex

Más sobre el autor:

La nueva

DECISIÓN INTELIGENTE

GARRETT SmartScan THERMAL SCREENING SYSTEM

SmartScan™ Ventajas

- Rentabilidad, detección de temperatura rápida tomada durante la operación normal de detección
- No ralentiza el proceso de chequeo existente
- Funciona con baterías para facilitar su uso
- Actualizable en campo para cualquier PD 6500i o Multi Zone con conexiones simples

MADE IN THE USA

GARRETT®
METAL DETECTORS

Email: security@garrett.com
Toll Free (U.S. and Canada) **800.234.6151**
Tel: **1.972.494.6151**

Para más información: https://info.garrett.com/garrett-metal-detectors-smartscan

¿CÓMO REDUCIR LOS RIESGOS EN EL SECTOR SALUD MEDIANTE LA GESTIÓN DE LLAVES Y ACTIVOS?

EUA | Danny Garrido

Los hospitales que cuentan con sistemas de gestión de llaves y activos físicos obtienen grandes beneficios: mejoran la seguridad, fortalecen la rendición de cuentas por parte del personal y reducen los riesgos y las demandas por responsabilidad civil

Los sistemas de salud de todo el mundo buscan permanentemente formas de preservar la seguridad de sus pacientes, empleados y miembros de la comunidad, así como hacer más eficientes sus operaciones. La gestión de llaves y activos desempeña un papel fundamental en este esfuerzo; tanto si se trata de mejorar el control del ingreso a las salas de pacientes de alto riesgo (como los pacientes con COVID-19), auditar el uso de las llaves de los casilleros de dispensación de medicamentos o tener mejor control de los activos asociados a la gestión de la infraestructura de la organización.

REDUCIR LOS RIESGOS DE LA SEGURIDAD PERIMETRAL

La capacidad de un hospital de brindar cuidado constante y de alta calidad depende de los edificios y la infraestructura con los que funciona. Los centros hospitalarios entienden que la gestión de llaves incide en la salud, la seguridad y la productividad de su organización.

Los avances en tecnología y equipos, tales como cámaras de videovigilancia, programas de reconocimiento de matrículas de vehículos (LPR, por sus siglas en inglés) y soluciones biométricas de control de acceso, ayudan a reducir las vulneraciones y los riesgos de seguridad.

Foto: Creativeart - Freepik

Pero, ¿cómo están almacenando sus instalaciones las tarjetas de acceso o protegiendo los vehículos y las personas que ingresan y salen de ellas? La gestión de llaves físicas añade otro nivel de seguridad a la red perimetral externa.

Los sistemas inteligentes de gestión de llaves hacen seguimiento de la ubicación y el uso de las llaves por parte de los empleados que ingresan y salen de la propiedad. Mejoran la rendición de cuentas de los empleados y el cumplimiento de los planes de mantenimiento. Asimismo, fortalecen la seguridad al impedir que el personal retire llaves y bienes de las instalaciones.

Foto: Creativeart - Freepik

LA GESTIÓN CONVENCIONAL FRENTE A LA GESTIÓN INTELIGENTE DE LLAVES

La gestión convencional de llaves puede consistir simplemente en que el usuario retira y sustituye una llave de un tablero perforado o de un cajón.

Este método no permite controlar quién puede acceder a las llaves o a los vehículos, ni avisa a la administración de la organización cuando, por ejemplo, sean retirados y devueltos los vehículos. Tampoco lleva registro de los problemas de funcionamiento que estos puedan presentar.

Los sistemas inteligentes de gestión de llaves restringen los permisos de acceso a las mismas, y el desplazamiento de los activos, envían alertas cuando una llave no es devuelta o cuando se produce un intento de acceso no autorizado.

Además, si un vehículo necesita una revisión de mantenimiento o una reparación, el usuario puede registrar un desperfecto en el momento de devolver la llave al gabinete. Una vez ingresado el registro, el sistema impedirá en el futuro el acceso a la llave hasta tanto no se solucione el problema y este quede marcado como resuelto. Esta función permite ahorrar tiempo y dinero, pues garantiza que la flota esté en buenas condiciones y tenga un mantenimiento adecuado.

MEJORAR LA ADMINISTRACIÓN Y EL TIEMPO DE RESPUESTA A LOS PACIENTES

Con más frecuencia de la deseada, es sólo hasta que ocurre una emergencia que nos damos cuenta de la importancia que tienen las llaves y los equipos para nuestras organizaciones. La pérdida de una llave maestra en un hospital puede llegar a costar cientos de miles de dólares, pues es necesario cambiar las cerraduras de los puntos de acceso.

Eso sin contar con la pérdida de tiempo y el daño a la reputación. Una tarjeta de acceso extraviada o mal utilizada puede poner a una organización en una situación de mayor vulnerabilidad frente al daño o robo de sus bienes, e incluso poner a las personas en riesgo de ser asaltadas, o de que les ocurra algo peor.

Las soluciones para la gestión de llaves reducen el riesgo de demandas por responsabilidad civil, pues brindan una cadena de custodia completa para todas las llaves, 24 horas al día, siete días a la semana. Los hospitales que utilizan sistemas inteligentes de gestión de llaves están al tanto de dónde se utilizan sus llaves y activos, la hora en que estos elementos se utilizaron por última vez y la última persona que accedió a ellos.

Esta información permite al personal responder con confianza y de manera adecuada a una serie de problemas frecuentes relacionados con las llaves. La gestión de llaves también puede reducir el tiempo requerido para la administración del equipo de seguridad del hospital e incluso definir restricciones de acceso específicas a las llaves de las instalaciones y a las áreas críticas, a fin de mejorar la seguridad.

Mientras los hospitales siguen enfrentando desafíos cada vez mayores por cuenta de la pandemia, el empleo de métodos de control de acceso (entre los que se cuenta la gestión de llaves) puede garantizar una plena rendición de cuentas y un mayor control sobre objetos protegidos, generar un proceso más seguro para la transferencia de elementos delicados —como los medicamentos y los registros clínicos— y permitir un registro de auditoría de todas las actividades.

Al implementar tecnologías que aumentan la eficiencia de las operaciones diarias, el personal hospitalario de primera línea contará con las herramientas necesarias para prestar sus servicios con más agilidad y capacidad de respuesta, así como para satisfacer las nuevas demandas y cada vez mayores expectativas de los pacientes.

MEJORAR LA RENDICIÓN DE CUENTAS DE LOS EMPLEADOS Y CONTRATISTAS

¿Sabía que los registros clínicos hurtados de pacientes de instituciones de salud se venden cada uno entre 250 y 500 dólares estadounidenses en la red oscura (Dark Web), lo cual supone para el sector de la salud un costo mayor por registro robado que para cualquier otro sector?

Peor aún, los registros clínicos robados contribuyen al hurto de identidad, a los diagnósticos erróneos y al trato injusto de las víctimas de fraude. Según información suministrada por el sitio web *Safeatlast.co* en su blog "14 Gripping Medical ID Theft Statistics to Ponder on in 2021" (14 estadísticas sobrecogedoras sobre robo de registros clínicos para reflexionar en 2021), en 2019 la seguridad de casi 4.5 millones de pacientes se vio comprometida debido al acceso no autorizado a sus registros médicos, ya fuera debido a vulneraciones a la seguridad informática o a la sustracción física de registros físicos.

Para preservar la seguridad de los empleados y los pacientes es necesario saber dónde se encuentran en todo momento no sólo ellos, sino además las llaves y los activos. Las instituciones

de salud que emplean gabinetes de llaves y sistemas de casilleros tienen un control de acceso de primer nivel, pues pueden supervisar y auditar el tiempo durante el cual se ha retirado una llave o un activo, determinar quién los retiró o está autorizado a hacerlo, y recibir una alerta si un objeto no ha sido devuelto en el plazo asignado.

Los profesionales de la salud por lo general tienen que fijar diferentes niveles de acceso para el personal y los contratistas. Un sistema inteligente para la gestión de llaves permite asignar y restringir este acceso según las funciones, necesidades y permisos de cada persona.

Las instituciones de salud que utilizan gabinetes de llaves y casilleros inteligentes disminuyen la probabilidad de que ocurran violaciones a la confidencialidad de los pacientes, reducen la exposición de los empleados a enfermedades y previenen vulneraciones a la seguridad informática por robo de equipos médicos.

Foto: Creativeart - Freepik

> Los sistemas inteligentes de gestión de llaves restringen los permisos de acceso a las mismas, y el desplazamiento de los activos, envían alertas cuando una llave no es devuelta o cuando se produce un intento de acceso no autorizado

REDUCIR EL RIESGO DE ROBO DE EQUIPOS CON CASILLEROS INTELIGENTES

Los casilleros inteligentes protegen sus activos de alto valor: desde los equipos hasta los medicamentos. Cuando su institución de salud está en capacidad de controlar, monitorear y registrar el uso de los equipos en sus instalaciones, se fortalece la seguridad de los empleados, los equipos de alto valor, los medicamentos y las áreas de acceso restringido. Los casilleros inteligentes protegen los objetos de alto valor sin sacrificar el acceso a ellos ni la comodidad.

El robo de equipos médicos es, por desgracia, frecuente. Esto no sólo supone un costo millonario para las organizaciones de salud, sino que además encarece los servicios médicos, puesto que las organizaciones tienen que transferir los costos a los pacientes. Además, los estudios calculan que los costos por el abuso de medicamentos de venta con prescripción y su desvío a aseguradoras médicas tanto públicas como privadas ascienden aproximadamente a 72 mil 500 millones de dólares al año, sólo en Estados Unidos.

Una de las formas en que los profesionales de la salud que trabajan en los hospitales pueden mejorar el tiempo de respuesta a los pacientes y reducir el riesgo de demandas por responsabilidad civil es utilizando casilleros de dispensación de medicamentos. Estos casilleros permiten al personal de enfermería ubicar dentro los medicamentos de los pacientes, protegerlos con una clave o un código y utilizar una autenticación de dos niveles para garantizar su administración en dosis adecuadas.

Este innovador uso de los casilleros se implementó por primera vez en las prisiones como una solución para que los presos accedieran a sus medicamentos sin tener que hacer filas, las cuales planteaban desafíos en materia de seguridad y recursos.

Gracias a los casilleros de dispensación, el personal hospitalario puede tener mayor confianza en que los medicamentos no caerán en manos equivocadas; entre otras, las de trabajadores sin la debida capacitación ni la correspondiente autorización. Esta solución también disminuye la molestia y el riesgo que implica el hecho de intentar localizar las llaves cuando un paciente necesita medicación rápidamente.

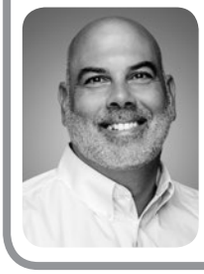
Por último, la función de generación de informes con la que cuentan los casilleros permite a los administradores saber quién y cuándo ha tenido acceso a cada casillero, reduciendo así las discrepancias en el inventario de medicamentos.

CONCLUSIÓN

Una reducción del riesgo de la seguridad perimetral, un tiempo de respuesta más rápido a los pacientes, un mejoramiento de la rendición de cuentas del personal y un menor riesgo de robo de equipos o prescripciones de medicamentos. Estas son sólo algunas de las ventajas que obtendrá su organización con un sistema inteligente de gestión de llaves y activos.

Los pacientes, empleados y miembros de la comunidad esperan el funcionamiento seguro y eficiente de los centros hospitalarios. Un sistema inteligente para la gestión de llaves contribuirá en gran medida a alcanzar sus objetivos de seguridad y eficiencia operativa. ■

Danny Garrido,
presidente de Traka (Las Américas), una compañía del Grupo ASSA ABLOY.



Más sobre el autor:

MÁS QUE UNA LLAVE

La entrada a sus puntos más vulnerables

Proteja sus instalaciones, sus bienes y a su personal con Traka.

Si no cuenta con un método para gestionar y supervisar adecuadamente el uso de las llaves, estas pueden convertirse rápidamente en una fuente de problemas que pone en riesgo sus instalaciones, sus bienes y a sus empleados.

Descubra hoy mismo una manera inteligente de proteger, gestionar y auditar las llaves y los activos más valiosos para su negocio. Envíe un correo electrónico a nuestros expertos a **sales@traka.com** o visite nuestro sitio web y obtenga más información.

traka
ASSA ABLOY

traka.com | 877-34TRAKA

PREVENCIÓN DE PÉRDIDAS DE AUTOPARTES EN PROCESOS DE **"LOGÍSTICA INVERSA"**

Seguridad en plantas automotrices

Foto: Creativeart - Freepik

ARGENTINA | Gustavo David Clara Clara

La Seguridad Corporativa es transversal en todos los procesos de una compañía. En el caso particular de la industria automotriz no es la excepción, sobre todo cuando la fabricación de un vehículo requiere de más de 4 mil 500 componentes para su adecuado ensamble, abarcando éstos, una amplia variedad de dimensiones y composición con un alto costo como común denominador. Hablamos de más de 2.7 millones de partes diarias que participan en la cadena de suministros.

Estos componentes son activos que tienen un alto valor de reventa en el mercado informal, y como tales se transforman en un riesgo que se llevan la mayor parte de gestión en prevención de pérdidas del departamento de Seguridad Corporativa, y esta actividad se vuelve más desafiante todavía, cuando el sistema de gestión de procesos logísticos se basa en el *Just in Time* (JIT), tal como ocurre en Toyota Argentina.

Por lo mencionado comparto algunas de las exigencias diarias, en relación con el proceso descripto, para luego poder desarrollar escuetamente parte de nuestra experiencia en la mitigación de los riesgos mencionados, evitando las pérdidas internas.

- **Alto flujo continuo y sincronizado de transportes, permitiendo el abastecimiento de las piezas de forma directa a la línea de producción (800 controles de camiones diarios por seis accesos durante 18 horas).**

- **Mínimo tiempo de control (3/5min) de los camiones al egreso de planta debido a que los mismos deben regresar a los proveedores para volver a abastecer a la producción a tiempo.**

- **Abastecimiento de autopartes por método de "logística inversa", es decir, los envases en que llegan las autopartes deben ser devueltas al proveedor vacíos.**

- **Amplias y variadas zonas de descargas para los transportes, donde se trasfieren las piezas hacia el interior de la nave industrial (zonas críticas).**

KEY PERFORMANCE INDICATOR

Habiendo hecho una simplificada descripción del contexto, podemos determinar que uno de los principales desafíos de la seguridad corporativa es evitar las pérdidas de activos en el proceso de logística inversa, al momento de la devolución de los envases vacíos, sea por descuidos en el proceso de devolución, o depositados intencionalmente dentro.

Esto se sustenta en los indicadores de seguridad o *Key Performance Indicator* (KPI) y es aquí, donde llegamos primeramente a concluir que es fundamental en la gestión de seguridad contar con indicadores, midiendo todos los desvíos, sus características y analizándolos en referencia a distintas variables. Por lo tanto, es imprescindible saber qué y cómo queremos medir, fijando estándares y parámetros del proceso de medición.

La experiencia marca la importancia de realizar una lista de las piezas críticas de mayor reventa en el mercado ilegal y

hacer un seguimiento interno, cruzando los datos de las unidades producidas contra las órdenes de compras de esas mismas autopartes, teniendo en cuenta que, de acuerdo con el target de cada compañía existe un porcentaje de autopartes que se dañan y se descartan en el proceso de ensamble.

Cuando buscamos mitigar los efectos de la pérdida de autopartes, debemos llegar a una solución eficiente, con economía de Recursos Humanos y de gastos; y logrando que las inversiones tengan un Retorno de la Inversión (ROI) no más allá de dos años. Dicho retorno, lo podemos cuantificar valorizando los desvíos por perdidas evitadas en el proceso de logística inversa (otro punto importante por el cual debemos llevar (KPIs).

Pero antes de abordar la búsqueda de la solución, es elemental conocer todo el proceso logístico y productivo, los cuales sufren un constante cambio de *layout* interno, lo que requiere un permanente monitoreo y buena comunicación con todos los sectores de producción.

Y es aquí, donde revindicamos las transversalidad del departamento Seguridad Corporativa a toda la organización, conociendo minuciosamente todo el proceso que transitan las autopartes, para lo cual, aplicando el concepto de la cultura japonesa '*genchi genbutsu*', "ver y observar en el lugar de los hechos", es necesario coordinar una recorrida con los referentes de todas las áreas industriales involucradas. De esta forma, podremos determinar cuáles serán los puntos claves del proceso que debemos supervisar.

PLAN DE CONTRAMEDIDAS

Una vez que visualizamos en el lugar, valorizamos los desvíos (utilizando los KPIs) y conocemos detalladamente el proceso y sus puntos más vulnerables, podemos diseñar un plan de las contramedidas.

Usualmente, la mejor acción para atenuar estas pérdidas está dada por la combinación de procedimientos, tecnología y seguridad física, como los primeros son los adaptados y aplicados en general a todo proceso industrial, tales como la colocación de cámaras HD en procesos críticos y uso de escáneres de rayos X para la revisión de equipajes en los accesos peatonales a la planta industrial, en este caso particular haré referencia a los procesos de seguridad física.

Cuando buscamos mitigar los efectos de la pérdida de autopartes, debemos llegar a una solución eficiente, con economía de Recursos Humanos y de gastos; y logrando que las inversiones tengan un Retorno de la Inversión no más allá de dos años

Nuestra intención es transmitir la experiencia en cuanto a las medidas de seguridad física que implementamos como parte del conjunto de la contramedida, entre ellas la creación de un equipo de guardias de "Prevención y Pérdidas" (P&P), conformado por un jefe de equipo de igual jerarquía que el encargado del servicio de Seguridad Física y vigilantes las 24 horas del día los 365 días del año, los cuales fueron seleccionados por su rendimiento y fidelidad hacia la compañía.

El equipo depende directamente de la Gerencia de Seguridad Corporativa. Entre sus principales funciones están: supervisar los procesos de logística inversa en los puntos vulnerables, supervisar sectores críticos de descarga, pesaje y transferencia de partes de forma aleatoria y sorpresivas. Auditar los procesos de control que se realizan en los diferentes accesos, investigaciones internas y generación de reportes a la Gerencia de Seguridad Corporativa.

Con la conformación de "P&P", se busca mitigar los desvíos en el proceso de vacíos y elevar la eficiencia de los vigilantes que realizan los controles en los diferentes accesos, ya que producto de la actividad repetitiva y rutinaria suelen descuidar los estándares de los procesos de control.

Otro aspecto positivo que nos brinda este equipo es que se ha incrementado notablemente la disuasión en la organización producto de sus visitas sorpresivas y aleatorias en sectores críticos. Y además nos permite obtener información de forma precisa y oportuna, aspecto muy valioso si de prevención de pérdidas hablamos. ■

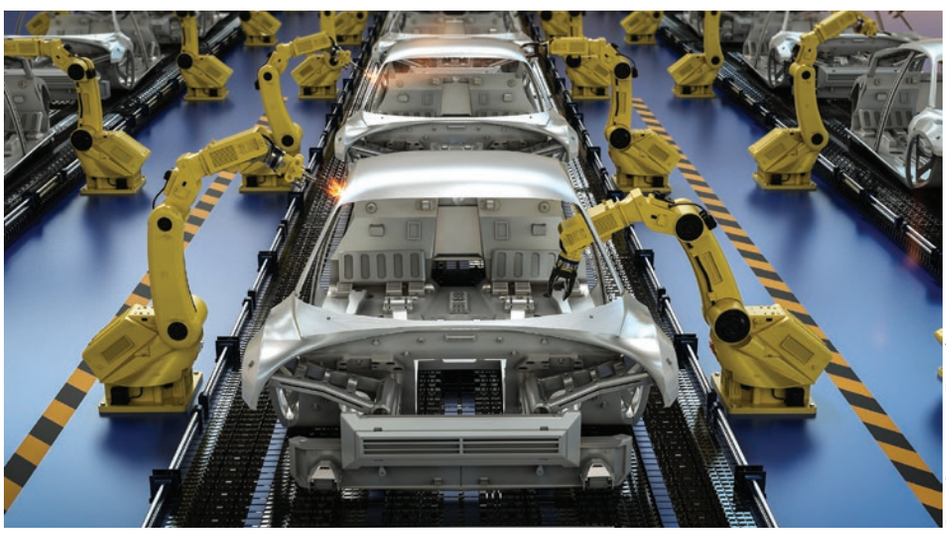


Foto: Creativeart - Freepik

Gustavo David Clara Clara,
Oficial (R) del Ejército Argentino y analista *senior* de Seguridad Corporativa en Toyota Argentina.

Más sobre el autor:

CÓDIGO PBIP: PROTECCIÓN Y SEGURIDAD MARÍTIMA

Obliga a gestionar los riesgos a la protección marítima, de una forma profesional, que incluye realizar análisis de riesgos y planes de protección, considerando las amenazas, vulnerabilidades y las consecuencias

Foto: Creativeart - Freepik

PANAMÁ | Jairo Rondón Torres

INTRODUCCIÓN

Desde su creación la Organización Marítima Internacional – OMI (IMO, por sus siglas en inglés) ha tenido como uno de sus dos objetivos principales el lograr una navegación más segura y salvaguardar la vida. En este sentido, ha impulsado un conjunto de Convenios Internacionales dirigidos a lograr tal objetivo, dentro de los cuales merece especial atención el Convenio Internacional para la Seguridad de la Vida Humana en el Mar, 1974 (SOLAS, por sus siglas en inglés).

No obstante, a raíz de los trágicos sucesos acaecidos el día 11 de septiembre de 2001 en las ciudades de Nueva York y Washington, en Estados Unidos, así como el aumento de la piratería y actos de terrorismo marítimo sucedidos en el estrecho de Malasia, Mar de China y las costas de África, entre 2000 y 2001.

La comunidad marítima internacional se vio forzada a mirar el tema de la seguridad marítima desde un nuevo ángulo, ya no exclusivamente ligada a las causas tradicionales que atentan contra la seguridad marítima como los riesgos naturales implícitos en la aventura marítima o en el error humano de la gente de mar, sino a una causa distinta: el terrorismo; de hecho ello generó "un nuevo enfoque de la OMI en materia de Protección Marítima".

Es así como en el mes de diciembre de 2002, en el marco de la Asamblea General de la OMI, se acordó por unanimidad, enmendar el Convenio SOLAS, la cual concluyó en la renumeración del Capítulo XI en XI-1 sobre las "Medidas Especiales para Incrementar la Seguridad Marítima" y un nuevo Capítulo XI-2 sobre "Medidas Especiales para Incrementar la Protección Marítima" y donde se menciona que para su cumplimiento se deberá adoptar de forma obligatoria la parte A del Código PBIP (Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias) a partir del 1 de julio de 2004.

> El adoptar estas "mejoras prácticas" en materia de protección marítima y portuaria, no nos garantizan un 100% de que estemos exentos de ataques o de que se cometan actos ilícitos, sin embargo, nos permiten estar mejor preparados

ANTECEDENTES Y APLICACIÓN DEL CÓDIGO PBIP

Este año 2021 arribamos a los 17 años de la implementación del Código PBIP (ISPS Code, conocido por sus siglas en inglés), el cual consta de dos partes, la primera denominada Parte A contiene requerimientos de carácter obligatorio en torno a las previsiones del nuevo Capítulo XI-2 del Convenio SOLAS; en tanto que la segunda de ellas identificada como Parte B establece los lineamientos, a manera de recomendaciones, del propio Código PBIP y el Capítulo XI-2 del SOLAS.

Es importante destacar que este Código conjuntamente con las enmiendas al Convenio SOLAS están dirigidas a incrementar la protección marítima, según lo señala la regla 2 del Capítulo XI-2 del Convenio y lo reafirma toda la Parte A del Código con las disposiciones y prescripciones obligatorias, las cuales se aplican a buques de pasaje y de carga de arqueo bruto igual o superior a 500 toneladas gruesas, así como a las unidades móviles de perforación costa afuera, siempre que todos ellos realicen navegación internacional. También se aplican estas normas a las instalaciones portuarias que atiendan buques que hagan tráfico marítimo internacional, lo cual constituye uno de los puntos más interesantes de esta novedosa normativa. Es decir, por primera vez la OMI coloca un pie en tierra y se crea así un "Anillo Global Anti-Terrorista para el comercio marítimo internacional".

El principal objetivo del Código es la protección marítima de los buques y de las instalaciones portuarias, contra los actos de terrorismo y otros actos ilícitos, mediante la implementación de un sistema de gestión de la protección marítima basada en la gestión de riesgos.

Si bien es cierto el Código PBIP es extenso y posee 19 secciones con sus diferentes reglas y recomendaciones; un aspecto importante es que se obliga a gestionar los riesgos a la protección marítima, de una forma profesional, que incluye realizar análisis de riesgos y luego los planes de protección, considerando los tres aspectos medulares, como lo son: las amenazas; las vulnerabilidades tanto de las instalaciones portuarias como de los propios buques y la criticidad o consecuencia, es decir el impacto que tendría el que se materializara uno u otro escenario de amenaza, que debe ser objeto de análisis y evaluación.

El principal objetivo del Código es la protección marítima de los buques y de las instalaciones portuarias, contra los actos de terrorismo y otros actos ilícitos, mediante la implementación de un sistema de gestión de la protección marítima basada en la gestión de riesgos

Además, esta normativa establece Tres Niveles de Protección Marítima, que podemos definirlos de manera simple como unos niveles de "alerta" por la información o presunción de un aumento en el nivel de riesgo. En el interactúan de manera dinámica y muy activa, tres organizaciones, a saber:

1) **La administración o autoridad marítima de cada país que representa al gobierno contratante.**
2) **Las compañías navieras u armadores de buques o sus representantes (agencias navieras).**
3) **Las instalaciones portuarias que estén dentro del ámbito de aplicación de este código.**

Por otra parte, no existe textualmente ninguna regla que obligue a implementar un sistema de gestión de calidad y protección marítima tipo ISM Code – Código IGS; sin embargo, cuando se analiza el código en todo su contexto no es necesario ello, ya que efectiva-

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

> Los sistemas de transporte tradicionalmente han sido y seguirán siendo blancos de ataques, para lo cual es sumamente importante la concienciación de todas las partes involucradas en el negocio marítimo y el comercio internacional

mente lo exigido en la parte A del Código PBIP busca que tantos las compañías que operan buques como las que funcionan y administran facilidades portuarias con atención de buques en tráfico internacional, deben establecer un "Sistema de Gestión de Riesgos de Protección Marítima" y ello perfectamente encuadra en el enfoque de gerencia por procesos, conocido como ciclo PHVA, el cual consiste en Planificar, Hacer, Verificar y Actuar en un ciclo permanente y dinámico que permitirá a la organización la mejora continua de todo el proceso en sí.

El cumplir eficazmente este ciclo PHVA bajo la óptica del Código PBIP es un trabajo arduo, que requiere tiempo, esfuerzo, dedicación, análisis, inversión de recursos y lo más importante el compromiso de la dirección de cada organización en planificar, implementar, mantener, auditar y adoptar las acciones correctivas a sus propios planes de protección, que deberán estar previamente aprobados por la autoridad marítima de cada administración en cada caso particular.

CONCLUSIONES

Finalmente podemos concluir que el auge de la piratería y el terrorismo global no va a cesar y por el contrario expertos en seguridad, aseguran que se van a incrementar. Los sistemas de transporte tradicionalmente han sido y seguirán siendo blancos de ataques, para lo cual es sumamente importante la concienciación de todas las partes involucradas en el negocio marítimo y el comercio internacional. Particularmente en este período de la pandemia global del COVID-19, los buques y varias empresas navieras han sufrido ataques cibernéticos o "ciberataques", combinados con ataques de piratería tradicional, especialmente en el Mar Mediterráneo, Mar Negro y el Mar Rojo, respectivamente.

El Código PBIP y el nuevo enfoque de la OMI son una excelente herramienta gerencial para gestionar los riesgos de protección marítima de una manera profesional y definitivamente se han elevado los niveles de seguridad y protección tanto a nivel de buques, como de las instalaciones portuarias.

El adoptar estas "mejoras prácticas" en materia de protección marítima y portuaria, no nos garantizan un 100% de que estemos exentos de ataques o de que se cometan actos ilícitos, sin embargo, nos permiten estar mejor preparados, contamos ahora con procedimientos, protocolos y planes evaluados y con un personal idóneo y entrenado que pueda enfrentar y responder ante un posible escenario de ataque. Es por ello, por lo que la prevención, la protección constante y la investigación deben ser vistas de forma integral y no se debe escatimar esfuerzos y recursos para la gestión de los riesgos de intencionalidad.

No podemos seguir viendo a la seguridad como un gasto, sino como una buena y saludable inversión que permitirá reducir pérdidas y mantener una operación y gestión portuaria, marítima y de logística en niveles aceptables de riesgos de protección y que al final redundarán en mejores beneficios para todas las partes involucradas, además de fortalecer la imagen corporativa de las empresas.

Desde el Centro de Formación Marítima e Industrial – MITC, S.A., y los campus universitarios de la Universidad Marítima Internacional de Panamá (UMIP), y la Universidad Metropolitana de Educación Ciencia y Tecnología (UMECIT) Panamá, yo como docente de algunas cátedras en temas de especialidad y gerencia de riesgos, pongo día a día nuestro granito de arena en la formación de los nuevos profesionales del campo de la ingeniería naval y gente de mar.

Así mismo, desde MSRAM, S.A., queremos poner a disposición de la comunidad portuaria, de logística y de compañías / agencias navieras y de la autoridades competentes, léase AMP (Autoridad Marítima de Panamá), ACP (Autoridad del Canal de Panamá) y el Comité de Protección Portuaria nuestra modesta experiencia internacional de más de 25 años en temas de gerencia de riesgos y particularmente en gestión de protección marítima y portuaria en general; tanto a nivel de servicios, consultoría y entrenamiento en materia de PBIP y Código IGS. ■

Jairo Rondón Torres,
presidente de MITC, S.A., director del Centro de Formación Marítima e Industrial (CFMI) y presidente fundador de MSRAM, S.A.

Más sobre el autor:

Protectio

Seguridad Logística

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

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

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

ESR EMPRESA SOCIALMENTE RESPONSABLE

Nuestros Ejecutivos son miembros activos de:
ASIS INTERNATIONAL CAPÍTULO MÉXICO 217
* ASIS no avala empresas, únicamente a Profesionales de la Seguridad

COPARMEX CIUDAD DE MÉXICO

CONSEJO NACIONAL CNSP SEGURIDAD PRIVADA A.C.
MR
EMPRESAS DE CALIDAD DESDE 1996

Columna de Jaime A. Moncada

jam@ifsc.us

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

Más sobre el autor:

EUA

¿DÓNDE INSTALAR ROCIADORES AUTOMÁTICOS?

Aunque países como Colombia, Costa Rica, Ecuador, Panamá, Perú, Puerto Rico y la República Dominicana ya requieren, en muchas edificaciones, protección con rociadores automáticos, otros países como Argentina, Bolivia, Chile, Guatemala, El Salvador, Honduras, México, Nicaragua, Paraguay, Uruguay y Venezuela no los requieren.

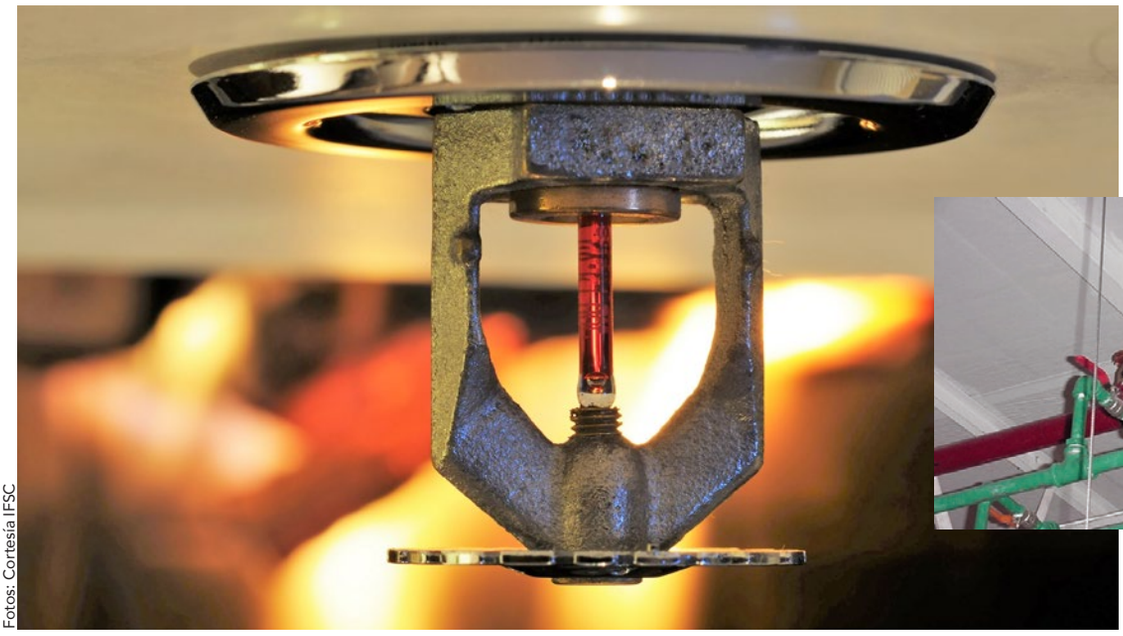
Desafortunadamente la mayoría de la población de la Latinoamérica hispanoparlante vive en ciudades donde los códigos de construcción no requieren este tipo de protección. Digo desafortunadamente, porque "los sistemas de rociadores automáticos son considerados por la NFPA (National Fire Protection Association) y la comunidad de ingeniería de protección contra incendios como el sistema más eficaz y efectivo de supresión de incendios en existencia.

No existe otro sistema que conjugue el mismo nivel de confiabilidad (más de un 90% efectivo), con un ciclo de vida largo y un mantenimiento relativamente sencillo y de bajo costo"[1]. Sencillamente es el sistema más utilizado a nivel mundial para la protección contra incendios de los edificios e industrias.

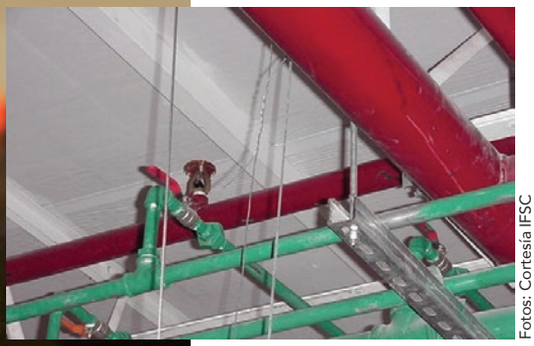
LOS CÓDIGOS DE LA NFPA

Para obviar este problema, la mayoría de los latinoamericanos miramos a los códigos de la NFPA. Desde esta óptica, el código que debería ser el punto de partida para definir cuándo y dónde se debe proteger un edificio o industria con rociadores automáticos es la NFPA 1, el Código de Prevención de Incendios.

Debo recalcar que la NFPA 101®, Código de Seguridad Humana, aunque más conocido que la NFPA 1, enfrenta la seguridad contra incendios de una manera singular. Es decir, NFPA 101 sólo fiscaliza la seguridad humana de los ocupantes del edificio, y no hace referencia a objetivos como la prevención de incendios, protección a la propiedad o características constructivas de los edificios[2]. La NFPA 1 tiene unos objetivos de protección más completos y es por eso que yo he sido un proponente de que éste sea el código que nosotros en Latinoamérica deberíamos adoptar o adaptar.



Fotos: Cortesía IFSC



Fotos: Cortesía IFSC

Foto: Creativeart - Freepik

Todas las prisiones y cárceles en general deben estar protegidas por rociadores, excepto en prisiones "Uso Condición I - Egreso Libre", donde los prisioneros pueden salir libremente al exterior

¿DÓNDE SE REQUIERE PROTECCIÓN CON ROCIADORES?

A continuación se incluye un resumen simple y rápido basado principalmente en los requerimientos de la NFPA 1, edición 2021. En este texto la palabra "debe" o "deben", indica un requisito obligatorio. Estos resúmenes son para edificios nuevos. La protección con sistemas de rociadores automáticos es expresada a continuación simplemente como "rociadores". Esta protección implica un fiel cumplimiento de la NFPA 13.

1. **General:** cualquier edificio, no importa su ocupación, debe ser protegido con rociadores si cumple cualquiera de las siguientes condiciones:
   a. Tiene tres pisos o más, excepto aparcamientos abiertos que no sean parte de otra ocupación.
   b. Sótanos que tengan más de 232m² de área construida.
   c. Edificios que alberguen servicios de bomberos, emergencia o ambulancia.
2. **Aeropuertos:** los requerimientos de rociadores están basados en la NFPA 415, donde se indica que estos edificios deben ser protegidos con rociadores cuando tengan áreas de asamblea de más de 1,115 m².
3. **Aparcamientos abiertos:** edificios que cumplan con la NFPA 88A no deben ser protegidos por rociadores.
4. **Aparcamientos cerrados:** áreas de aparcamiento debajo de edificios que requieran rociadores o cuando tengan más de 1,115 m² de área construida deben estar protegidos por rociadores.
5. **Apartamentos residenciales:** los edificios de apartamentos residenciales deben estar protegidos por rociadores. Los edificios de hasta cuatro pisos y 18.3 m de altura pueden ser protegidos con rociadores diseñados de acuerdo con la NFPA 13R.
6. **Bares y discotecas:** sitios como bares, clubes nocturnos, discotecas y pistas de baile deben estar protegidos por rociadores.
7. **Bodegas de almacenamiento:** deben estar protegidos con rociadores:
   a. Bodegas con estanterías con un área construida mayor a 232 m².
   b. Bodegas de almacenamiento general con un área construida mayor a 1,115 m².
   c. Bodegas conteniendo mercancías clasificadas como plásticos Clase A con una altura de almacenamiento superior a 1.5 m sobre un área construida mayor a 232 m².
8. **Centros comerciales:** los centros comerciales, incluyendo las tiendas ancla, deben estar protegidos por rociadores. Cada tienda o espacio arrendado se debe poder sacar de operación, por ejemplo en una renovación, sin afectar la protección de las otras porciones del centro comercial.
9. **Cuartos de cómputo:** según la NFPA 75, los cuartos y áreas con equipos de tecnología de información localizados en un edificio que requiera protección con rociadores deben contar, en el cuarto de cómputo, con rociadores automáticos. Si el edificio no requiere protección con rociadores, entonces el cuarto o área con equipos de tecnología de información deben ser protegidos con rociadores, o con un sistema de extinción de agente limpio, o con ambos.
10. **Edificios de gran altura:** todos los edificios de gran altura deben estar protegidos por rociadores, no importa cuál sea su ocupación. Un edificio de gran altura está definido como cualquier edificio que tiene más de 23 m de altura medidos desde el piso ocupado más alto hasta el nivel más bajo de acceso para bomberos.
11. **Escuelas:** de acuerdo con NFPA, las ocupaciones educacionales incluyen escuelas, colegios, academias y jardines infantiles, pero excluyen universidades, las cuales están catalogadas como usos de negocios. Todas las ocupaciones educacionales que tengan un área que exceda 93 m², o cuyas porciones estén debajo del nivel de descarga al exterior, deben estar protegidos por rociadores.
12. **Hospitales:** todos los hospitales o edificios utilizados para propósitos de atención o tratamiento médico simultáneamente a cuatro o más pacientes con internación deben estar protegidos por rociadores automáticos, incluyendo áreas de quirófanos.

Foto: Creativeart - Freepik

Los centros comerciales deben estar protegidos por rociadores. Cada tienda o espacio arrendado se debe poder sacar de operación, sin afectar la protección de las otras porciones del centro comercial

13. **Hoteles y moteles:** todos los hoteles, moteles y dormitorios que bajo la misma administración provean acomodación para más de 16 personas deben estar protegidos por rociadores. Las habitaciones deben estar protegidas con rociadores de respuesta rápida. Los hoteles de hasta cuatro pisos y 18.3 m de altura pueden ser protegidos con rociadores diseñados de acuerdo con la NFPA 13R.

14. **Industrias:** toda ocupación industrial, excepto si está clasificada como una de riesgo bajo, debe estar protegida por rociadores sí cumple cualquiera de las siguientes condiciones:

    a. Tres o más pisos de altura.

    b. Un área en exceso de 1,115 m^2.

    c. Si la suma del área de todos los pisos supera los 2,230 m^2.

15. **Negocios:** oficinas en general, universidades, edificios institucionales y judiciales, oficinas médicas y de dentistería y clínicas ambulatorias son todas catalogadas como ocupaciones de negocios por NFPA. Estos usos requieren protección por rociadores cuando tengan tres o más pisos de altura y excedan los 232 m^2 de área debajo del nivel de descarga a la calle.

16. **Prisiones:** todas las prisiones y cárceles en general deben estar protegidas por rociadores, excepto en prisiones "Uso Condición I – Egreso Libre", donde los prisioneros pueden salir libremente al exterior. Los rociadores que protegen estas ocupaciones deben ser del tipo institucional, para así ofrecer una protección más segura.

17. **Residencias uni y bifamiliares:** el cambio más importante de la última década en lo que tiene que ver con los requerimientos de protección con rociadores ocurrió en la protección de la residencia. En ese sentido, de acuerdo con la NFPA, todas las residencias uni y bifamiliares deben estar protegidas con sistemas de rociadores diseñados de acuerdo con NFPA 13D.

18. **Reuniones públicas:** sitios de reunión, de exhibición, bibliotecas, teatros y cinemas, museos, restaurantes, salas de conferencias, auditorios y de usos similares que tengan una ocupación mayor a 300 personas (ya sea en una o en varias partes en un mismo edificio) deben estar protegidas por rociadores, como sigue:

    a. En el piso que contenga la ocupación de reunión pública.

    b. En ocupaciones de reunión pública debajo del nivel de descarga a la calle, en todos los niveles entre este nivel y el nivel de descarga a la calle.

    c. En todos los pisos debajo de la ocupación de reunión pública.

    d. Existen excepciones a estos criterios, bajo ciertas circunstancias, para cuartos multipropósito de menos de 1,115 m^2 de área, gimnasios, piscinas, y estadios, entre otros.

19. **Tiendas mercantiles:** ocupaciones mercantiles deben estar protegidas por rociadores, cuando se cumpla cualquiera de las siguientes condiciones:

    a. Tengan tres pisos o más de altura.

    b. Tengan más de 1,115 m^2 de área por piso.

    c. Tengan pisos debajo del nivel de descarga a la calle, que tengan un área superior a 232 m^2 y que se utilicen para la venta, manejo o almacenamiento de mercancía combustible.

CONCLUSIONES

Reitero que el resumen anterior es sólo eso, un extracto de lo que requiere NFPA. Para definir efectivamente dónde y cómo proteger un edificio, se debe analizar más detenidamente la normativa de la NFPA, ojalá con la asistencia de un ingeniero de incendios competente.

Finalmente, un tema que ha tenido poca difusión en nuestra región es la definición del tipo de construcción, la cual es definida no sólo por la ocupación, área y la altura de un edificio, sino también si el edificio está o no protegido por rociadores. Es decir, la resistencia al fuego y la compartimentación interna de un edificio puede variar si el edificio está protegido con rociadores automáticos o no. ■

REFERENCIAS

[1] *Moncada, J. & Moncada, J.A. (Eds.), Manual de Protección Contra Incendios, Quinta Edición en Español, NFPA, Pag 8.1.*

[2] *Este tema está mejor desarrollado en el International Building Code (IBC) o en la NFPA 5000, Código de Construcción y Seguridad en Edificios.*

GSI
SEGURIDAD PRIVADA

GSI Seguridad Privada SA de CV

Profesionales en Seguridad Privada

Oficiales de Seguridad Intramuros

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

SOMOS GRUPO GSI, Orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx

atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

CERTIFICADO ISO-9001:2015 GSI SEGURIDAD PRIVADA

ESR EMPRESA SOCIALMENTE RESPONSABLE

redconocer de prestadores de servicios Centro de Evaluación

TYPE OF CERTIFICATION MARK DNV·GL STANDARD

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

EMPRESAS DE GSI GRUPO SEGURIDAD INTEGRAL

LA IMPORTANCIA DEL *PENETRATION TESTING*

Foto: Creativeart - Freepik

Las pruebas de penetración brindan mayor seguridad y certidumbre a las organizaciones

MÉXICO | Víctor Díaz Bañales

¿QUÉ ES UN *PENETRATION TESTING*?

Últimamente podemos llegar a escuchar con mayor frecuencia los términos de pruebas de penetración, análisis de vulnerabilidades, *pentest* y demás términos que engloban la prevención de ciberataques en las organizaciones.

Las pruebas de penetración tienen como objetivo validar la factibilidad que una vulnerabilidad tiene de ser explotada. Aquí me detendré un poco a explicarlo en un término más sencillo y amplio, una vulnerabilidad es considerada una debilidad, por ejemplo supongamos que tenemos conectada a nuestra red corporativa una PC de usuario que tiene un sistema operativo Windows XP®, el cual ya no cuenta con ningún soporte ni parches de seguridad, el cual puede ser vulnerado y a través de dicho equipo un atacante puede acceder a nuestra red, al explotarse dicha vulnerabilidad el riesgo se materializa y la empresa queda expuesta a diversos ataques, es ahí donde nace la importancia de contar con pruebas de penetración que nos permitan prevenir, medir y ejecutar controles de remediación ante dichos eventos.

¿EN QUÉ INTERVALOS DE TIEMPO DEBERÍAMOS EJECUTARLOS?

El tiempo es un factor determinante, dado el mundo tecnológico e hiperconectado en el que nos encontramos, día con día cambian los escenarios y aumentan las vulnerabilidades, tomando como ejemplo la pandemia global, los límites y perímetros que las empresas tenían se han vuelto vulnerables por diferentes

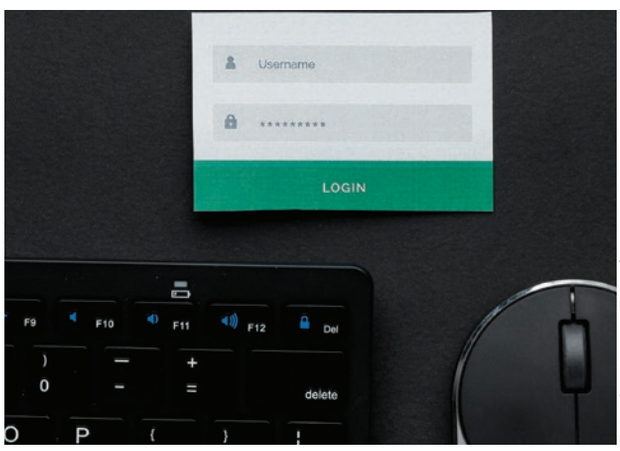


Foto: Creativeart - Freepik

Muchas organizaciones en verdad les temen a estas pruebas y la realidad es que de cierta manera tienen razón, las pruebas de penetración tradicionales involucran conceder el ingreso o permitir a personal ajeno tener o ganar acceso a los recursos empresariales como redes, servidores, información, acceso físico y demás

factores, los principales pueden ser el uso de equipos fuera de la compañía, uso de redes públicas, uso de equipos personales para fines laborales, equipos desprotegidos, entre otros.

Lo importante a señalar es que hoy en día existen herramientas automatizadas para realizar estas tareas y para los casos tradicionales de pruebas de penetración realizadas por terceros, se recomienda que se haga al menos uno por año, lo deseable serían dos por año y que se documente todo lo necesario, desde los hallazgos hasta los impactos que dichos eventos podrían ocasionar en la organización.

¿ES UN GASTO QUE SE DEBERÍA HACER?

Sí, la realidad es que no debería verse o tratarse como un gasto, sino como una inversión, ya que una organización que es vulnerada puede sufrir múltiples pérdidas, desde reputacionales hasta económicas y legales graves, hay muchos ejemplos públicos de empresas que han sufrido secuestro de información (*ransomware*) y que han tenido que cerrar operaciones o dejar de producir debido a que no cuentan con respaldo de información, tema que pudo haber sido detectado y resuelto posteriormente a la ejecución de una prueba de penetración, el costo de las pruebas de penetración está ligado al tipo de prueba, su alcance y la cantidad de personal que estará involucrado.

¿QUÉ CUIDADOS DEBO TENER?

Muchas organizaciones en verdad les temen a estas pruebas y la realidad es que de cierta manera tienen razón, las pruebas de penetración tradicionales involucran conceder el ingreso o permitir a personal ajeno tener o ganar acceso a los recursos empresariales como redes, servidores, información, acceso físico y demás, por lo cual es un tema complejo y delicado, siempre se recomienda firmar NDA's (Acuerdos de Confidencialidad) para mitigar la exposición de la información, de igual forma se recomienda que los resultados se entreguen a un único contacto de la organización en el nivel más alto posible y que dicho contacto divulgue lo que considere pertinente entre sus subordinados.

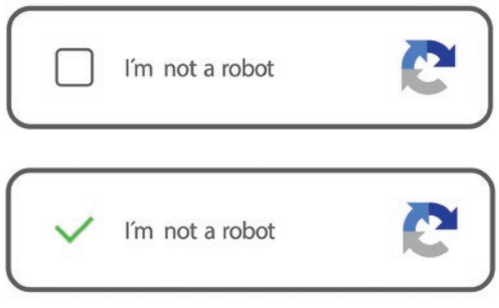


Foto: Creativeart - Freepik

> Hay muchos ejemplos públicos de empresas que han sufrido secuestro de información (*ransomware*) y que han tenido que cerrar operaciones o dejar de producir debido a que no cuentan con respaldo de información, tema que pudo haber sido detectado y resuelto posteriormente a la ejecución de una prueba de penetración

¿CUÁL ES LA TENDENCIA FUTURA?

Como lo sabemos la automatización ha llegado para quedarse y las pruebas de penetración también cambiarán para brindar mayor seguridad y certidumbre a las organizaciones, hoy en día existen herramientas que tienen la capacidad de ejecutar de forma automatizada y centralizada las pruebas de penetración más comunes que existen en el mercado y esto permite a la organización no exponer sus vulnerabilidades con terceros ajenos a la organización y que podrían ejecutarlas en su contra, lo cual es una excelente opción en estos tiempos de desconfianza total, a su vez dichas herramientas cuentan con módulos de Inteligencia Artificial (AI), lo cual les permite estar actualizadas sobre los ataques que suceden en el mundo. ■

Víctor Díaz Bañales,
socio director de Ramdia.

Más sobre el autor:

Las soluciones de automatización, además de ser fundamentales, aportan un gran valor a los procesos productivos del sector automotriz

CONVERGENCIA DE TI: TENDENCIA CLAVE EN LA REESTRUCTURACIÓN AUTOMOTRIZ

MÉXICO | Joel Alejandro Camacho Cortés

La industria automotriz mundial siempre se ha caracterizado por encontrarse en un constante proceso de reestructuración, el cual se ha intensificado durante las dos últimas décadas. Es por ello que la industria automotriz se ha convertido en una de las industrias más dinámicas de la actualidad, habiendo impulsado múltiples e importantes avances en temas de productividad, desarrollo tecnológico y competitividad.

Por ejemplo, la manera en que se utilizan las nuevas tecnologías para la producción de vehículos híbridos nos hace pensar que no falta mucho tiempo para que este tipo de tecnología se globalice y sea aplicada en todos los autos y todas las marcas del planeta.

BREVE ANÁLISIS DE LA REESTRUCTURACIÓN AUTOMOTRIZ

En este sentido, la reestructuración del sector automotriz puede ser analizada desde dos ópticas diferentes: 1) la innovación tecnológica en los procesos productivos y de organización laboral, y 2) la reconfiguración del mercado.

Las empresas que se están consolidando como las más importantes del sector automotriz son aquellas que están implementando los mayores adelantos tecnológicos del momento en sus procesos de producción, al igual que están adoptando los mejores esquemas de relación con sus proveedores.

De acuerdo con datos sobre la producción de vehículos en el mundo, la estructura del sector automotriz ha cambiado de manera significativa durante las últimas décadas. Países como Estados Unidos y Alemania han perdido participación en esta industria, mientras que países como Japón, China, España, Corea del Sur, la India, Brasil y México han ganado liderazgo al incrementar su producción de manera considerable.

Entre los países mencionados, China merece una mención especial, ya que ha logrado avances espectaculares en el sector automotriz durante los últimos años al grado de posicionarse como el principal productor de vehículos a nivel mundial, contando con uno de los mercados más importantes en la industria (junto con Estados Unidos y Japón). Es por ello que la participación de este país en el sector automotriz resulta fundamental.

En la industria automotriz, cada día se requiere una mayor integración de los procesos de manufactura en plataformas de gestión de datos e interfaces con diferentes roles de operación y manejo de la producción

CONOCE NUESTRA GAMA DE EQUIPOS DE UNIFORMES O

CREA TU PROPIA IMAGEN

- CORTE Y CONFECCIÓN
- BORDADOS
- DISEÑO UNIFORMES

www.uniformesjr.com.mx

Palmira 14
Francisco Villa
54059 Tlalnepantla, Méx.

INFORMACIÓN :
(55) 5082-9568
(55) 2873-0771

ventas@uniformesjr.com.mx

La industria automotriz es una de las más amplias y diversificadas del mundo, razón por la cual también es una de las más difíciles de analizar respecto a las relaciones que existen entre las empresas ensambladoras y las proveedoras de autopartes, ya que la cadena de suministro de autopartes de este sector es una de las más complejas debido al gran tamaño que puede alcanzar.

Sin duda, el análisis de las empresas proveedoras de autopartes es de suma importancia, sobre todo cuando éstas también se han visto afectadas por el actual y constante proceso de reestructuración del sector automotriz, teniendo que transformarse para adecuarse a las nuevas necesidades y requerimientos de la industria terminal.

TENDENCIA DE AUTOMATIZACIÓN Y CONTROL

Como en todas las industrias de hoy en día, las soluciones de automatización además de ser fundamentales aportan un gran valor a los procesos productivos del sector automotriz, cuyos beneficios y resultados dependerán de la identificación y adopción de las principales tendencias del mercado y su correcta implementación y operación por parte del personal correspondiente.

Una tendencia muy clara en el sector de la automatización y control es la convergencia de las tecnologías de la información en el área industrial. Cada día se requiere una mayor integración de los procesos de manufactura en plataformas de gestión de datos e interfaces con diferentes roles de operación y manejo de la producción.

Por ejemplo, actualmente se requiere comunicar una mayor cantidad de controladores lógicos programables (PLCs) distribuidos en una planta. Estos equipos, destinados a controlar procesos específicos, necesitan interactuar con un cuarto de control central y, en algunos casos, con uno de control local, lo cual se lleva a cabo a través de una red de comunicación digital, usualmente una red industrial TCP/IP, que se ha vuelto el estándar por preferencia de fabricantes, integradores y usuarios finales.

SISTEMAS SCADA

Si hablamos de sistemas SCADA (Supervisory Control and Data Acquisition), el más usado y difundido a nivel global es Wonderware, sistema que utilizamos en SISSA como plataforma de integración y desarrollo de soluciones gracias a las múltiples ventajas que ofrece, incluyendo su capacidad para integrar una enorme gama de equipos, dispositivos y PLCs de diferentes marcas, además de que permite un desarrollo sumamente versátil y flexible, y cuenta con una suite de drivers de comunicación para infinidad de protocolos de comunicación.

Lo anterior, sumado a las tecnologías de servidores hiperconvergentes y al poder de virtualización con un ESNXi de VMware o Hyper V (entre otros), genera un potencial y nivel de escalabilidad tan elevado que permite adaptar dichas soluciones en diferentes campos de automatización y control de procesos.

PROTOCOLOS DE COMUNICACIÓN

En la industria manufacturera, hablando específicamente de sus procesos, existe una inmensa variedad de protocolos de comunicación. Es por esta razón que en SISSA hemos seleccionado la System Platform de Archestra como nuestra plataforma de desarrollo, la cual tiene la capacidad de establecer comunicación desde el IO Server con un amplio portafolio de *drivers* de comunicación para PLCs específicos, facilitando así la integración de gestores y permitiendo una fácil integración de tecnologías .Net de Microsoft.

LAS SOLUCIONES DE AUTOMATIZACIÓN Y CONTROL DE SISSA

En SISSA implementamos un desarrollo en C#, el cual implica conexiones con bases de datos como SQL Server y APIs (Application Programming Interface) propietarias de equipos en específicos, permitiendo el monitoreo, automatización y control de los sistemas electrónicos de seguridad, sistemas de tecnologías de la información y sistemas de soporte a la operación de cualquier infraestructura, siendo una solución ideal para la industria automotriz. ■

Fotos: SISSA Monitoring Integral

Joel Alejandro Camacho Cortés,
Business Development Director en SISSA Monitoring Integral.

Más sobre el autor:

MSPV
SEGURIDAD PRIVADA

Protegerte, nuestro Compromiso

27
Años de
EXPERIENCIA

HONESTIDAD

DISCIPLINA

EFICACIA

RESPONSABILIDAD

PERTENENCIA

LEALTAD

MSPVSeguridad

MSPVCiudaddeMéxico

ventas@mspv.com.mx

55 5399 9937 ext. 846
800 253 0717

www.mspv.com.mx

Lago Superior No.25, Col. Tacuba,
Alc. De Miguel Hidalgo, C.P. 11410 CDMX

ESR EMPRESA SOCIALMENTE RESPONSABLE

ISO 9001:2015

BASC

ALAS

CNSP EMPRESAS DE CALIDAD DESDE 1996

El ciberespionaje tiene una amplia gama de objetivos claves, que muchas veces logran concretar dado que no se reconocen como material clave que puede terminar comprometiendo la dinámica de una organización o la gobernabilidad de un Estado

CIBERESPIONAJE, NUEVO MODELO DE NEGOCIOS INTERNACIONALES

COLOMBIA | Jeimy Cano

Recientemente las noticias globales anuncian aperturas avanzadas en países desarrollados con ocasión del proceso de vacunación masiva. Estos titulares crean sensaciones e imaginarios que afectan a los inversionistas globales, motivando el movimiento de transacciones a nivel internacional y tendencias alcistas en los diferentes mercados accionarios. No obstante estos titulares internacionales, crecen de forma equivalente las noticias falsas, la desinformación y la creación de inciertos alrededor de la efectividad de los agentes biológicos como una nueva batalla geopolítica que configura una nueva ciberofensiva de poder y control sobre nuevos intereses nacionales basados en la propiedad intelectual y posicionamiento científico (Reys, 2021).

Antes de la creación de Internet y su despliegue a nivel internacional, las agencias de inteligencia y espionaje de las diferentes potencias luchaban en medio de la penumbra y la sorpresa para concretar sus acciones y tener acceso a información sensible de su enemigo, bien para debilitar sus centros de poder, deteriorar la calidad de la información de inteligencia, inhabilitar sus funciones de contrainteligencia o motivar la deserción de los agentes enemigos. El espionaje como fuente natural de búsqueda y consolidación de ventajas estratégicas hoy se configura como una herramienta clave en el contexto de un mundo más interconectado (Libicki, 2017).

Hoy el espionaje, si bien utiliza técnicas similares del pasado como el engaño, la suplantación, la infiltración, la extracción, la implantación de dispositivos de escucha y los canales de comunicación encubiertos y seguros, entre otros, ha evolucionado haciéndose más silencioso y más digitalizado, como quiera que el reto de pasar desapercibidos en una infraestructura de comunicaciones, de tecnología o de Internet de las cosas, es ahora menos complejo con la ayuda de equipos especializados en penetrar y tomar control de estos componentes.

> El ciberespionaje como un nuevo modelo de negocios internacionales reinventa y expande las prácticas de la guerra regular, para crear presiones, tendencias, inestabilidades y afectaciones económicas, que pueden partir de engaños, fallos técnicos, campañas de desinformación, entre otros

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

> Hoy el espionaje, si bien utiliza técnicas similares del pasado como el engaño, la suplantación, la infiltración, la extracción, la implantación de dispositivos de escucha y los canales de comunicación encubiertos y seguros, entre otros, ha evolucionado haciéndose más silencioso y más digitalizado

Las películas sorprendentes del agente británico 007, en sus últimas ediciones, muestran los avances tecnológicos que terminan apoyando la labor del funcionario encubierto. Explosivos, dispositivos de intervención de comunicaciones, armas compactas y vehículos modificados, establecen la base sobre la cual el espionaje moderno concreta sus actividades. Sin perjuicio de lo anterior, se advierte un renovado espionaje basado en el contexto cibernético, donde los límites y capacidad de penetración retan cualquier capacidad defensiva o disuasiva que se pueda tener.

LOS OBJETIVOS DEL CIBERESPIONAJE

En el ciberespacio los intereses nacionales cambian y se transforman de acuerdo con las posturas dinámicas que se generan con ocasión de tensiones globales que afectan las posiciones dominantes de los países. En este contexto el ciberespionaje es un ejercicio convergente entre la guerra la información, el cibercrimen y las operaciones cibernéticas, donde se tiene como objetivo obtener información sensible, secretos o propiedad intelectual relevante sin el consentimiento de la contraparte, generalmente con fines económicos, otras veces políticos o estratégicos que puedan cambiar el balance de control y poder en el orden internacional (Merrick, Hardhienata, Shafi & Hu, 2016).

El ciberespionaje es un arte que implica el desarrollo de habilidades sociales, técnicas, políticas y diplomáticas. Es un ejercicio que inicia con la identificación de aquella información relevante para crear la inestabilidad deseada. Luego, establecer con la ayuda de la inteligencia la mejor forma de configurar una distracción y un engaño, con el fin de situar aquellas vulnerabilidades que pueden ser susceptibles de ser aprovechadas para ubicar el pivote para el acceso. Hecho lo anterior, se adelanta la penetración (preferiblemente encubierta) donde el agente externo se ubica si ser detectado, para luego acceder a la información clave que es de interés (Schwartz, 2020).

Surtido el proceso anterior, se hace necesario desplegar un código malicioso bien para distraer o movilizar la atención a otros sitio, o para concretar una brecha necesaria para obtener los datos claves. Acto seguido, disfrazar las acciones que se adelantan para engañar a los sensores tecnológicos o físicos sobre lo que ocurre y dirigir sus alertas a lugares distintos, donde la atención estará concentrada para mitigar los efectos creados por el malware o estrategia de entretención (Schwartz, 2020). Con este escenario, el agente encubierto puede adelantar sus acciones bajo el velo de las penumbras informáticas, incluso a la luz del mismo evento creado para entretener, sin que sea percibido, haciendo más complejo sacar a los analistas de los eventos que más "visibilidad" tienen.

Una lista incompleta de objetivos interesantes para el ciberespionaje dirigido a empresas y naciones puede ser (Koehler, 2018):

- La ubicación actual y futura de los miembros de la alta dirección y de los especialistas.
- Los protocolos del consejo de supervisión y de la dirección.
- Las licitaciones, los documentos de identidad y la información sobre el control de acceso.
- Los planes de construcción y de uso del suelo.
- Las plantillas de diseño.
- Los precios de compra.
- Los inventos.
- Los informes de fallos, de auditoría y de calidad.
- Los detalles de fabricación.
- Los sueldos y las primas de los empleados.
- Los cálculos de los beneficios y de la facturación.

- Las ideas innovadoras de los talleres o los concursos internos de la empresa.
- Los cálculos financieros.
- Los proyectos de ley preliminares.
- Las estrategias militares de combate.
- Las intenciones de compra de todo tipo.
- Los planos de distribución.
- Las existencias de los almacenes.
- Las listas de proveedores.
- Los contratos de proveedores y de servicios.
- La información logística.
- Las muestras de material.
- Las estrategias de las ferias comerciales.
- Las contraseñas y datos de acceso.
- Las solicitudes de patentes.
- Las historias clínicas.
- Los datos personales de los empleados (especialmente los de la dirección).
- Los proyectos piloto y experimentos.
- Las inversiones de puesta en marcha.
- Los componentes de productos.
- Los planes de viaje y visitas a congresos.
- Las hojas de ruta para variantes de productos o actividades de *marketing*.
- Los sistemas de seguridad.
- Los conceptos de estrategia.
- Los resultados de estudios estratégicos.
- Los registros de conocimientos técnicos detallados.
- Los números de teléfono directos y móviles privados.
- Las disposiciones y resultados de pruebas.
- Las rutas y tiempos de transporte.
- La estrategia de enrutamiento de tráfico de red privado.
- Los análisis e informes de accidentes.
- Las intenciones de venta.
- Los detalles de contratos.
- Las estrategias de venta.
- Las muestras de mercancías.
- Los datos de pagos y cuentas.
- Las facilidades de acceso a través de Internet o VPN (Virtual Private Network).

Como se puede observar el ciberespionaje tiene una amplia gama de objetivos claves, que muchas veces logran concretar dado que no se reconocen como material clave que puede terminar comprometiendo la dinámica de una organización o la gobernabilidad de un Estado. Por tanto, es necesario reconocer esta nueva amenaza en medio de los retos del ciberespacio, ya que es un recurso estratégico de un ciberconflicto, para crear los patrones necesarios de inestabilidad, mediante el "poder suave" o acciones por debajo del "uso de la fuerza", las cuales crean en una zona gris donde no es posible movilizar acciones concretas de disuación, ni efectuar reclamos por intromisiones, ni mucho menos establecer una atribución particular (Rosenbach & Mansted, 2019).

Así las cosas, el ciberespionaje como un nuevo modelo de negocios internacionales reinventa y expande las prácticas de la guerra regular, para crear presiones, tendencias, inestabilidades y afectaciones económicas, que pueden partir de engaños, fallos técnicos, campañas de desinformación, entre otros, como parte natural de un juego que se practica al margen de la diplomacia internacional, para mantener o crear un estatus de liderazgo y control, que no es otra cosa que el encuentro de intereses estratégicos donde el que menor exposiciones y errores genere, será el que mejor posición logre en el tablero de jugadas globales. ■

Foto: Creativeart - Freepik

REFERENCIAS

- *Koehler, T. (2018). Understanding Cyber Risk. Protecting Your Corporate Assets. Londres, UK: Routledge.*
- *Merrick, K.; Hardhienata, M.; Shafi, K. & Hu, J. (2016). A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios. Future Internet. 8(34). https://doi.org/10.3390/fi8030034*
- *Reys, N. (2021). Digital acceleration hits emerging threats. Top five risk. Control Risk. https://www.controlrisks.com/riskmap/top-5-risks/04-digital-acceleration-hits-emerging-threats*
- *Rosenbach, E. & Mansted, K. (2019) The geopolitics of information. Paper. Belfer Center for Science and International Affairs. Harvard University. https://www.belfercenter.org/sites/default/files/2019-08/GeopoliticsInformation.pdf*
- *Schwartz, M. (2020). RedCurl Cyber Espionage Gang Targets Corporate Secrets. Bank Infosecurity. De: https://www.bankinfosecurity.com/redcurl-cyber-espionage-gang-targets-corporate-secrets-a-14819*
- *Libicki, M. (2017). The Coming of Cyber Espionage Norms. 2017 9th International Conference on Cyber Conflict. https://www.ccdcoe.org/uploads/2018/10/Art-01-The-Coming-of-Cyber-Espionage-Norms.pdf*

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:

SEGURIDAD® EN AMÉRICA

Suscripción Anual (6 ejemplares)

México: **$650 pesos**

Extranjero: **$270 dls.**

(incluye gastos de envío)

SEA

¡SUSCRÍBETE YA!

(55) 55726005

telemarketing@seguridadenamerica.com.mx

www.seguridadenamerica.com.mx

SEGURIDAD EN LA INDUSTRIA AUTOMOTRIZ

Las grandes extensiones de territorio de una planta automotriz tienen gran demanda en servicios de seguridad, sin embargo, la seguridad no sólo se limita a cuidar los perímetros de una planta, sino también todo lo que ocurre dentro de una planta automotriz está ligado con las diferentes áreas de seguridad, e incluso resulta un aliado estratégico para la continuidad de negocio

Foto: Creativeart - Freepik

MÉXICO

Erick Martínez / *Staff* Seguridad en América

La industria automotriz en México representa el 3.8% del Producto Interno Bruto (PIB) nacional y el 20.5% del PIB manufacturero, colocándose como el 4° exportador de vehículos a nivel mundial. De esta industria dependen mas de dos millones de familias mexicanas consideradas en áreas como fabricación de automóviles, camiones, autopartes, comercio automotriz, servicio, reparación, mantenimiento entre otras. Alrededor de 24 entidades de país tienen presencia de empresas proveedoras de autopartes.

"México es el mayor fabricante de vehículos de motor de América Latina. En 2020 produjo aproximadamente 3.2 millones de vehículos, de los cuales alrededor del 65% se clasificaron como vehículos comerciales ligeros"[1].

Seguridad en América platicó con dos grandes expertos en este sector: Darío Preza, *Security Officer* México de Daimler Trucks North America; y Erik Navarro, director de Seguridad y Prevención de Incendios de Stellantis México.

LA SEGURIDAD COMO ELEMENTO DE VALOR

Las operaciones de seguridad dentro de una planta automotriz son muchas y muy variadas, sin embargo, la principal función es establecer estrategias a corto mediano y largo plazo con el fin de preservar la seguridad e integridad de los empleados, de los activos tangibles e intangibles y la reputación de la empresa. Asegurando que la función de seguridad se asocie con todas las estrategias para mitigar el riesgo y pérdidas en todos los niveles, las operaciones principales son: manejo de crisis y continuidad de negocio, prevención de incendios, seguridad en las instalaciones, seguridad en la cadena de suministro, prevención de pérdidas, seguridad del personal, investigaciones e innovaciones tecnológicas. La seguridad interactúa de manera constante en todas las áreas antes mencionadas.

"La seguridad en este sector está ligada directamente a la eficiencia de su operación, una planta automotriz opera con procesos '*just in time*', por lo que la seguridad tiene que estar acorde a estos procedimientos para evitar un paro de planta que podría ser muy costoso", afirmó Erik Navarro.

La seguridad en este sector no sólo es un área soporte, sino también un verdadero aliado de negocios, por ejemplo, en el cumplimiento de normatividad nacional e internacional, sin esa injerencia, sin planes de protección civil no puede operar una planta, la seguridad se encarga de cumplir con los requerimientos de la Secretaría de Trabajo y Previsión Social, velando también por programas aduanales, los cuales son pieza fundamental para la exportación e importación como son C-TPAT (Customs-Trade Partnership against

Terrorism), OEA (Operador Económico Autorizado), ISO (Internacional Organization for Standardization). Además, debe contar con una buena comunicación con autoridades para la recuperación de materiales y unidades en caso de robo.

5 AFIRMACIONES DE LA SEGURIDAD COMO ALIADO DE NEGOCIO

Estas cinco afirmaciones por las que el área de Seguridad apoya en el desarrollo y continuidad de negocio de acuerdo con Erik Navarro:

1. Durante la pandemia, la seguridad fue y ha sido fundamental para la incorporación de actividades, pues apoyaron en los procedimientos requeridos por la Secretaría de Salud para evitar los contagios de COVID-19.

2. La continuidad de negocio, área fundamental para la elaboración en los planes de continuidad de negocio y recuperación de desastres.

3. Opimizacion de recursos y apoyo a las metas financieras, apoyando en la identificación de fallas del proceso productivo que ponen en riesgo los bienes de la compañía y la recuperación de materiales productivos y no productivos, ayuda en la prevención de pérdidas.

4. Soporte en los procesos de calidad, como soporte de sistemas de videovigilancia robustos que apoyan en la identificación de alguna deficiencia de calidad en la línea de producción. Además, también para la misma operación y eficiencia de los trabajadores en la línea productiva.

5. Un aliado en cualquier evento fuera de lo ordinario. La seguridad siempre está dispuesta para atender cualquier evento.

RETOS Y FACTORES DE RIESGO = OPORTUNIDADES

Las responsabilidades que realiza el área de seguridad conllevan enfrentarse a diferentes retos en una planta automotriz, sin embargo, cada riesgo o reto que pueda enfrentar seguramente

> "Una planta automotriz opera con procesos 'just in time', por lo que la seguridad tiene que estar acorde a estos procedimientos", **Erik Navarro**

permea en un segundo, y a su vez ese segundo en un tercero, por ejemplo, la pronta identificación de todos los retos y riesgos marcará una gran diferencia en el impacto que pudieran tener en la compañía, sus objetivos, metas y sobre todo la continuidad de negocio.

Darío Preza mencionó que la globalización es uno de los retos más importantes que enfrenta la industria automotriz, actualmente las fronteras son más chicas, pero los mercados globales cada vez más interactúan entre sí, por lo mismo, lo que ocurre en alguna parte del mundo afecta a todo el mundo y en distintas esferas sociopolíticas, económicas y culturales, la pandemia de COVID-19 es el claro ejemplo de ello.

- **Factor humano:** si bien el factor humano para muchos especialistas es la parte más importante en los planes de continuidad de negocio, también es cierto que representa riesgos, retos y grandes inversiones, en diferentes encuestas se ha observado que el mayor riesgo está dentro de la propia instalación con el personal. Se debe capacitar y especializar al personal para que sea capaz de adquirir habilidades y conocimientos tecnológicos además de idiomas o cédulas profesionales, aprender nuevas herramientas de comunicación, usos de tecnologías con IA, el uso de drones, vehículos autónomos, requiere una capacitación especial, de no ser así, estaría posicionando a la empresa fuera de los nuevos mercados y competencias.

  En la actualidad toda empresa debe velar por las necesidades e integridad de cada trabajador y trabajadora, por lo cual se han implementado normas como la NOM 035-STP. "Una reglamentación emitida por la Secretaría del Trabajo y Previsión Social que tiene como objetivo establecer los elementos para identificar, analizar y prevenir los factores de riesgo psicosocial, la violencia laboral, así como para promover un entorno organizacional favorable en los centros de trabajo"[2].

  Diseñar un plan de capacitación, identidad y crecimiento del personal hará también que la rotación del personal disminuya considerablemente, pues es otro de los grandes factores que afecta esta industria.

- **Tecnológicos y cibernéticos:** están asociados con todo el mundo que nos rodea, las comunicaciones, los transportes, la información, la banca, etc., a su vez relacionado con riesgos inherentes a la tecnología, la IA, los ciberataques, el *ransomware*, secuestro de información, entre otros.

  La IA está siendo sin duda lo que esperábamos hace algunas décadas como "futuro", va mucho más allá de dispositivos que hacen funcional una casa, en la industria automotriz tiene un impacto significativo, en programas y mecanismos. Los riesgos tecnológicos también están relacionados con los del trabajo. "Los coches autónomos pueden reemplazar el trabajo de muchas personas dedicadas al transporte, también se están construyendo en fábricas autónomas que pueden reemplazar al humano",

mencionó Darío Preza. Además, la implementación de IA traerá consigo impacto que puede ser un riesgo tanto financiero y político como social en disturbios civiles y de todo orden social relacionado con IA, por lo que se debe incluir en futuros planes de respuesta de emergencia y manejo de crisis, estar preparados y no ser víctimas de riesgos asociados a esa industria. Darío Preza recomendó estar preparados con correctas pólizas de seguros, personas entrenadas en el uso de esas nuevas IA, flotilla que distribuye y vende productos perecederos.

Los ciberataques están asociados al robo de información sensible. Los ciberejércitos no son fuerzas armadas que dependen de habilidades físicas, sino de ingenieros especializados con habilidades que permitan la defensa de una nación, una industria, un pequeño comercio y cualquiera que esté interconectado con la información. "Los riesgos representan una oportunidad para aprender, aplicar nuevos conocimientos, ejecutar diferentes medidas y controles para poder evitarlos, como el secuestro de información, el fin es desestabilizar gobiernos, compañías, empresarios y personas de poder, etc., a través de la inmediatez con la que viaja la información, así poder influir en la percepción de los ciudadanos incluso en elecciones", comentó Darío Preza.

- **Sistemas contra incendios:** el desgaste de los sistemas contra incendio, la supervisión y mantenimiento del mismo, pues al ser una parte muy importante para el desarrollo de esta industria, ya que representa un alto costo, además, la obsolescencia de los sistemas electrónicos, la tecnología que se utiliza en los planes estratégicos de seguridad está en constante evolución, por la cual algunos desarrollos se vuelven inservibles para la demanda actual. Los estragos que trajo la pandemia son las principales afectaciones económicas que afectan la operación en esta industria, la reducción de personal y plantillas completas, afectó muchísimo al área de seguridad, por lo que debe haber un balance adecuado en la seguridad, mejoramiento de la tecnología, selección de personal en constante mantenimiento y actualización.

"Los riesgos representan una oportunidad para aprender, aplicar nuevos conocimientos, ejecutar diferentes medidas y controles para poder evitarlos", **Darío Preza**

LO QUE VIENE A FUTURO

Ambos especialistas, tanto Darío Preza como Erik Navarro, concluyen y coinciden en que se debe diseñar un plan estratégico y consolidar los avances tecnológicos, los cuales están abriendo nuevas y muy grandes oportunidades de crecimiento. Los drones aéreos y terrestres van a crecer y cobrar mucha importancia, son muy costosos aún, pero llegará el punto donde la balanza se equilibre entre el costo-beneficio dejando más actividades a los drones.

Capacitar al personal y especializarlo en las nuevas tecnologías, formas de comunicación y desarrollar el negocio.

"Las operaciones y estrategias en cuestión de seguridad en las empresas y compañías de manufactura de automóviles, es imposible ser exitosos sin un recurso humano adecuado por lo que se debe de consolidar un equipo fuerte, coordinado y con confianza", afirmó Erik Navarro.

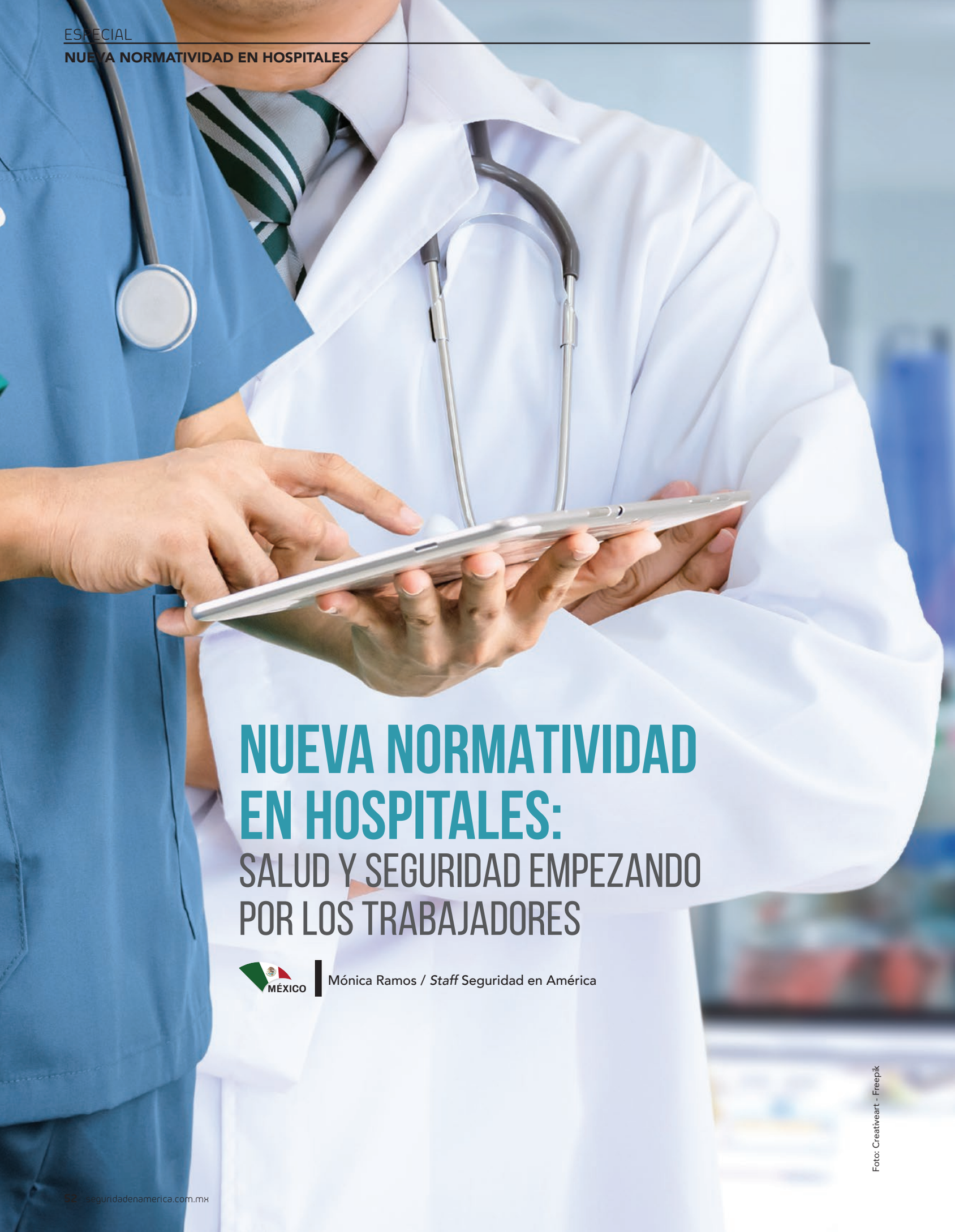
Y es la convergencia de la tecnología con el factor humano, con sistemas de videovigilancia, controles de acceso, sistemas de nómina, Recursos Humanos, lo que viene para el futuro donde todas las áreas tengan comunicación entre sí, sumando y eficientando los procesos productivos y la seguridad integral.

"Las crisis que nos habla del futuro, se encuentran ya con nosotros, tenemos que estar preparados en la continuidad del negocio, el manejo de las crisis, con las nuevas tecnologías, la crisis de COVID-19 ha dejado muchas enseñanzas, es un parteaguas para saber cómo enfrentarse y resolver diferentes situaciones", finalizó Darío Preza. ■

Foto: Creativeart - Freepik

REFERENCIAS

[1] *https://es.statista.com/estadisticas/1114051/vehiculo-produccion-america-latina-por-tipo/*
[2] *https://www.sige.org.mx/nom-035-stps-2018-factores-de-riesgo-psicosocial-en-el-trabajo-identificacion-analisis-y-prevencion/*



NUEVA NORMATIVIDAD EN HOSPITALES:

SALUD Y SEGURIDAD EMPEZANDO POR LOS TRABAJADORES

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Foto: Creativeart - Freepik

Hasta octubre del presente año, se habían registrado 233,7 millones de casos de coronavirus (SARS-CoV-2) en todo el mundo, siendo Estados Unidos, India y Brasil los países con más personas contagiadas; las políticas de seguridad sanitaria modificaron sus protocolos y prioridades con base en los riesgos y vulnerabilidades que la pandemia amerita, empezando por la protección del personal hospitalario, ya sean trabajadores de la salud, administrativos y personal de seguridad

Los protocolos de seguridad y la normatividad en hospitales cambian constantemente adaptándose a los nuevos riesgos que surgen dentro de este sector, uno de los más delicados, y que implica diferentes retos para los trabajadores de la salud, el personal administrativo y de seguridad. La pandemia ocasionada por el virus COVID-19 provocó incertidumbre en todo el mundo, la economía y principalmente la vida de las personas quedaron expuestas a ésta, uno de los actores esenciales para sobrellevar y actualmente salir adelante ante esta crisis de salud, ha sido el personal hospitalario.

El número de casos confirmados de coronavirus en el mundo hasta octubre del presente año, fue de 233.7 millones, encabezando la lista Estados Unidos (44.3 millones de positivos confirmados), continuando con la India (33 mil 766 millones), y Brasil en tercer lugar (21 mil 427 millones), mientras que México ocupó el lugar 15 con 3 mil 664 millones de positivos confirmados en el mismo periodo[1].

Conforme pasaron los meses y los expertos en materia de salud, ciencia, tecnología y seguridad fueron analizando, estudiando y comprendiendo las mutaciones que el SARS-CoV-2 tuvo, se implementaron nuevos protocolos de bioseguridad a nivel mundial, en el trabajo, en casa, en la calle, espacios públicos, etcétera.

En el caso de los hospitales y ante la emergencia a la que se enfrentaron, las políticas de salud modificaron sus requerimientos y al día de hoy continúan adaptándose, visualizando un año 2022, y gracias a la llegada de más vacunas

contra el COVID-19, probablemente con más control de la situación y disminución de los contagios, no obstante las medidas de bioseguridad actuales llegaron para quedarse.

RIESGOS EN HOSPITALES

Cada país enfrentó, y continúa haciéndolo, la pandemia con los recursos que tenía y se alimentaron de la experiencia, conocimientos y ejemplo de otros países. Sin embargo, la desigualdad social ya existente marcó el avance o estancamiento frente al virus.

De acuerdo con la Organización Mundial de la Salud (OMS), "la enfermedad y la muerte causadas por la COVID-19 han afectado en mayor medida a los grupos que sufren discriminación, pobreza y exclusión social, y han de hacer frente a diario a unas condiciones de vida y de trabajo sumamente adversas, en particular, en las crisis humanitarias. Se estima que el año pasado (2020) entre 119 y 124 millones de personas más se vieron arrastradas a la pobreza extrema a causa de la pandemia"[2].

"Entendemos como riesgos, aquellas situaciones o condiciones que pueden poner en peligro tanto la organización como a las personas que la integran. Los riesgos más comunes a los que nos enfrentamos en los hospitales son los psicosociales", **Diego Zorzoli**

Múltiples estudios han sido publicados referentes a la pandemia, uno de los temas que se analizan es la gestión del personal hospitalario, los retos a los que se ha enfrentado, las medidas que ha tomado, siempre considerando la nueva normatividad y la seguridad jugando un papel fundamental para su cumplimiento.

La OMS enumeró siete clases de riesgos inherentes al sector hospitalario, que son:

1. **Biológicos.** Tienen vinculación directa con los virus, enfermedades patógenas (hepatitis, la tuberculosis, el síndrome de inmunodeficiencia adquirida, COVID-19).
2. **Químicos.** Con productos como ácidos, contacto con glutaraldehído y óxido de etileno.
3. **Físicos.** Como el ruido y las radiaciones.
4. **Ergonómicos.** Derivados de las malas prácticas en relación al cuerpo (levantamiento de objetos pesados, malas posiciones).
5. **Psicosociales.** Por ejemplo estrés y violencia.
6. **Relacionados con el fuego, explosiones.** Referente a la estructura hospitalaria.

"Entendemos como riesgos y muy sintéticamente, aquellas situaciones o condiciones que pueden poner en peligro tanto la organización como a las personas que la integran. Existen los riesgos inherentes a la propia actividad dentro del hospital. Los riesgos más comunes a los que nos enfrentamos son los psicosociales. Aquellas situaciones de violencia que pueden presentar familiares de pacientes que están alterados, sobre todo en las guardias y lógicamente a los riesgos biológicos, lo cual quedó expuesto de manera brutal con la aparición de la pandemia por COVID-19", comentó en entrevista para **Seguridad en América** (**SEA**), Diego Zorzoli, licenciado en Tecnologías Aplicadas a La Seguridad y supervisor de Prevención y Seguridad del Hospital Nacional "Profesor Alejandro Posadas" en Buenos Aires, Argentina.

Ante estos riesgos, son tres las principales herramientas de seguridad que se requieren para los hospitales:

1. **Seguridad Física.** Compuesta por el recurso humano.
2. **Seguridad electrónica.** Todos aquellos elementos inherentes a la parte de *hardware* y *software* complementario a la seguridad física, por ejemplo videovigilancia, control de accesos. Y con la aparición del COVID-19, implementación de cámaras con sensor de temperatura, los termómetros digitales, aplicaciones integradas a las cámaras como control de afore, control de sectores críticos, etc.
3. **Prevención de riesgos.** Es el primer paso a realizar previo al desarrollo de las actividades del área de Seguridad. ¿A qué se enfrenta? ¿Cómo lo va a enfrentar? ¿Qué herramientas o estrategias se van a usar? ¿Cuál será el costo o la inversión para prevenir el riesgo?

"Los hospitales públicos de Argentina son asistidos por elementos de prevención y seguridad en algunos con empresas privadas y otros por ejemplo donde estoy yo, conformado por el personal propio del hospital, lo cual es una gran ventaja porque al ser personal propio éste conoce de manera íntima la idiosincrasia del funcionamiento, las características del hospital y además esto genera cierto sentido de pertenencia, de trabajar en el hospital y no sufre lo que las empresas de seguridad privada que es la rotación constante de personal", comentó Zorzoli, quien lleva 17 años laborando en esa institución.

NUEVA NORMATIVIDAD

La actividad en los hospitales en el año 2020 empezó a duplicar y triplicar su aforo dado el incremento de los contagios en cada país, esto obligó a las autoridades de cada uno, a adaptar los protocolos de seguridad, las normas que ya tenían y readaptarlos a esta nueva situación.

"En nuestro caso, el Ministerio de Salud empezó a generar nuevos protocolos en cuanto al tratamiento de la persona en la etapa de posible

SISSA
DIGITAL

SOLUCIÓN DE automatización y control de SISSA

Vector SCADA System
(VSS Release R1.0)

Vector SCADA System, permite el monitoreo, automatización y control de los tres grandes rubros tecnológicos que comprende una planta automotriz:

SISTEMAS ELECTRÓNICOS
de seguridad

SISTEMAS DE TECNOLOGÍAS
de la información

SISTEMAS DE SOPORTE
a la operación

Conoce más de NOSOTROS

@sissamx

www.sissamx.com.mx

55.1954.2832

contagio, de contagio consumado, pos contagio, para tratar tanto al trabajador como a su grupo familiar en la situación completa. A partir de ahí se adaptaron diferentes protocolos tomando la experiencia de otros países y lo que mejor se adaptó al nuestro", explicó Zorzoli.

Estos protocolos fueron desarrollados pensando tanto en la seguridad y salud de los trabajadores hospitalarios como en los pacientes. Un ejemplo que menciona el experto, es que las guardias se dividieron, por un lado para el tratamiento de patologías que no tenían que ver con el COVID-19 y otras específicamente para tratar el virus o detectarlo con enfermedades respiratorias relacionadas. Situación similar en los hospitales en México.

En el artículo "Gestión hospitalaria de la pandemia en la Ciudad de México. Un análisis desde el enfoque de burocracia a nivel de calle", Oliver Meza y Elizabeth Pérez Chiqués, profesores investigadores titulares de la División de Administración Pública, junto a Sergio Campos González y Samanta Varela, egresado y estudiante del Doctorado en Políticas Públicas (DPP) del CIDE (Centro de Investigación y Docencia Económicas), respectivamente, analizaron la situación del personal médico en México, realizando entrevistas directas con los trabajadores de salud.

"Uno de los principales hallazgos que tuvo la investigación fue el cambio de jerarquías. Normalmente, en los hospitales, el personal médico cumple con determinados roles de acuerdo con su conocimiento y experiencia, permitiendo organizar la vida y la toma de decisiones; sin embargo, esto cambió con la pandemia; los roles dentro del hospital dejaron de tener sentido debido a que el COVID-19 era una enfermedad poco estudiada y los médicos no conocían mucho sobre ella. Por otro lado, doctores de otras especialidades tuvieron que atender la demanda de enfermos que llegaba a los hospitales", señaló una nota del CIDE[3].

La capacitación para enfrentar esta crisis sanitaria fue aplicada tanto al área de enfermería, médicos, médicos especialistas, administrativos y al personal de seguridad. Puesto que la pandemia continúa, las medidas de seguridad respecto al virus seguirán presentes, y la normatividad se irá adaptando conforme la pandemia y las necesidades de seguridad que se requieran.

Por su parte, Francisco Daniel Zea Jiménez, evaluador de Hospital Seguro de los Servicios de Salud del estado de Puebla, comentó que estas normativas en su región incluyeron establecer protocolos epidemiológicos a través de códigos hospitalarios y cercos sanitarios en el acceso-recepción y manejo de pacientes e usuarios internos y externos.

Foto: Creativeart - Freepik

INVERSIÓN PARA BIOSEGURIDAD

En un comunicado emitido en abril de este año[4], la OMS exhortó a los países a continuar invirtiendo en salud para así evitar que crezca la desigualdad social y aumente la pobreza en el mundo. "Al menos la mitad de la población mundial sigue sin tener acceso a servicios de salud esenciales; más de 800 millones de personas emplean al menos el 10% de sus ingresos familiares en atención sanitaria, y los gastos por cuenta propia hunden en la pobreza a casi 100 millones de personas cada año.

A medida que los países vayan superando la crisis de la COVID-19, será fundamental evitar todo recorte en el gasto público destinado a la salud y a otros servicios sociales. Esos recortes podrían aumentar las dificultades a que se enfrentan los grupos desfavorecidos, socavar el buen funcionamiento del sistema sanitario, acrecentar los riesgos para la salud, agravar la presión fiscal en el futuro y poner en peligro los logros alcanzados en materia de desarrollo", indicó conmemorando el Día Mundial de la Salud (7 de abril de 2021).

Hizo la recomendación de destinar un 1% adicional del PIB (Producto Interno Bruto) a la atención primaria de salud. Así como "reducir el déficit mundial de profesionales sanitarios necesarios para alcanzar la cobertura sanitaria universal antes de 2030, que asciende a 18 millones de trabajadores. Ello implica crear al menos 10 millones de puestos de trabajo adicionales a jornada completa en todo el mundo y redoblar los esfuerzos en materia de igualdad de género".

Los hospitales siempre han tenido riesgos constantes a los que se enfrenta todo el personal, sin embargo el COVID-19 implicó además del tratamiento hospitalario a los contagiados, la implementación de medidas como la instalación de control de accesos, cámaras con sensores térmicos, termómetros digitales, abastecimiento de elementos de protección personal (cubrebocas, guantes, gel antibacterial, sanitizante, etc.).

Todo ese equipamiento requirió de inversión, al igual que la ciberseguridad. "De acuerdo a diferentes estudios que revisé, creció la actividad de robo de datos con respecto a las historias clínicas electrónicas, es decir cuando las tazas de contagio empezaron a aumentar, aquellas personas que se internaban en

los hospitales y desarrollaban historias clínicas electrónicas brindaban datos, mismos que eran buscados por ciberdelincuentes, entonces se tuvieron que implementar medidas de prevención para luchar contra el ciberdelito, esto se agregó a los gastos emitidos durante la pandemia", indicó el entrevistado.

Diego Zorzoli resaltó la importancia de estos gastos que en realidad son inversiones necesarias para la protección de datos del trabajador, del paciente y la imagen del hospital, información muy sensible que requiere atención y cuidado.

De acuerdo con los conocimientos de Francisco Zea, estos son algunos de los requerimientos para un hospital sea considerado "seguro", y que requiere de inversión:

- Procesos diseñados a las necesidades de la unidad hospitalaria.
- Capacitación permanente al usuario interno y externo.
- Simulacros de eventos y evaluación de los mismos para una mejora continua.

"Lo que nos planteamos quienes estamos a cargo de la seguridad en hospitales, es que debemos trabajar para que sean instituciones resilientes, incluyentes y amigables con el medio ambiente", **Francisco Zea**

También se debe considerar que si el empleado presenta síntomas relacionados al COVID-19, los protocolos a seguir implican, de ser positivo, enviarlo a casa para su recuperación. "Si el trabajador presenta algunos de los síntomas del virus, inmediatamente se le sugiere aislamiento y se asiste a través de los canales de comunicación del hospital o de instituciones dedicadas al tema. De igual manera si había tenido contacto con alguna persona contagiada. En el hospital también trabajamos el control de aforo, tomar distancia, teniendo aislado el caso, y de ser positivo, se le daba la atención diaria hasta su recuperación para que regrese a sus actividades", explicó Zorzoli.

TECNOLOGÍA DE LA MANO DE LA SEGURIDAD

Los expertos coinciden que el uso de tecnología complementa y facilita el cumplimiento de las nuevas normativas en hospitales, así como en otros sectores. A raíz de la pandemia, los proveedores de estas soluciones optaron por adaptar las funciones de su tecnología para el bien de la población mundial. Marcas como Axis Communications ya ofrecían herramientas tecnológicas para este sector, lo que hicieron fue encontrar el buen funcionamiento para esta crisis sanitaria.

"Integrar soluciones de video en red va más allá de la implementación de cámaras, incluye también el audio IP (Internet Protocol) para mandar mensajes de alerta o indicaciones al personal o familiares de pacientes. El análisis inteligente ofrece la posibilidad de identificar potenciales síntomas como la tos, el uso de cubrebocas, así como hacer un informe sobre las personas que ingresan a un hospital logrando localizar zonas con gran afluencia u horarios de alta demanda. Los videoporteros, por ejemplo, permiten la comunicación bidireccional con cada uno de los pacientes para proteger su salud y la posibilidad de mantenerlo monitoreado sin necesidad de contacto físico", comentó en un comunicado de prensa Ignacio Cabañas, *Business Development manager* para Latinoamérica en Axis Communications.

La situación sanitaria actual, ha exigido nuevas estrategias para la protección de las personas. Por ejemplo, la Administración de Alimentos y Medicamentos de Estados Unidos (The U.S. Food and Drug Administration) sugiere utilizar sistemas de video IP para aumentar el control en el cuidado de los pacientes[5].

"Según el Centro Estadounidense para el Control y Prevención de Enfermedades, el costo promedio en un hospital de una lesión por caída es de aproximadamente 35 mil dólares, por lo que las soluciones de video son ideales para prevenir estos inconvenientes. La tecnología funciona mediante imágenes que detectan las acciones de los pacientes situados ante las cámaras en combinación con analíticas inteligentes, el dispositivo puede activar alertas en respuesta a movimientos bruscos o posibles riesgos de accidentes en pacientes o personal del recinto, de manera que el equipo médico pueda emprender acciones de inmediato para atender la situación"[6].

Foto: Creativeart - Freepik

Algunas de las soluciones que promueve Axis para enfrentar los nuevos retos por la pandemia y las exigencias de las políticas sanitarias son:

1. **Prevención de riesgos a través del análisis de video para la detección de accidentes.** En ocasiones resulta necesario el monitoreo de pacientes las 24 horas del día, por ese motivo prevenir que sufran accidentes es una de las principales tendencias de seguridad, lo cual ha orillado a desarrollar soluciones específicas para detectar y alertar cuando una persona sufre algún accidente y permanece en el suelo durante un tiempo determinado.

2. **Protección efectiva de la privacidad, a través de soluciones que ayudan a verificar lo que sucede sin recopilar datos personales.** Esto permite tener mayor confianza de parte de los pacientes y de las demás personas que acceden al lugar, además trae muchos beneficios de rentabilidad para los hospitales.

3. **Aumento de la seguridad mediante la detección facial.** Uso de un *software* de análisis de video que captura la imagen de la cara de las personas, inmediatamente comienza una búsqueda de coincidencia con la base de datos de quienes sí pueden acceder a ciertos lugares y como resultado, la solución genera alarmas a los centros de monitoreo para avisar que una persona quiere acceder a una zona prohibida o bien permite el acceso.

4. **Análisis para detectar movimientos e intrusión.** La seguridad física de los hospitales es una prioridad, por lo que asegurar las áreas críticas para detectar amenazas y alertar al personal es sumamente necesario, sobre todo en las inmediaciones.

"El análisis inteligente ofrece la posibilidad de identificar potenciales síntomas como la tos, el uso de cubrebocas, así como hacer un informe sobre las personas que ingresan a un hospital logrando localizar zonas con gran afluencia u horarios de alta demanda", **Ignacio Cabañas**

Foto: Creativeart - Freepik

PANORAMA DE LA SEGURIDAD HOSPITALARIA PARA EL AÑO 2022

Pfizer/BioNTech, AstraZeneca/Oxford, Janssen, Moderna y Sinopharm, son las vacunas aprobadas hasta octubre del presente año por la OMS, en México además se aplicaron Sputnik V y CanSino (ambas no aprobadas por la OMS), la aparición de las vacunas en tan poco tiempo, brinda una esperanza para el control de la pandemia, al menos en la disminución de decesos. Sin embargo las medidas preventivas continuarán por varios años más.

"Lo que estamos trabajando es en desarrollar, desde la capacitación, la generación de herramientas protocolares de protección y prevención, buscando como principal foco de atención, la protección del trabajador, para una vez garantizada esa parte, desarrollar todos aquellos programas que permitan interactuar con el paciente. Si yo no me siento seguro, no puedo brindar mi trabajo de manera plena", puntualizó Zorzoli.

La pandemia por COVID-19 trajo nuevos retos, problemas sociales y económicos, pero también nuevos aprendizajes para desarrollar mejores estrategias de seguridad que permitan seguir adelante a la humanidad. "Lo que nos planteamos quienes estamos a cargo de la seguridad en hospitales, es que debemos trabajar para que sean instituciones resilientes, incluyentes y amigables con el medio ambiente", finalizó Francisco Zea. ■

REFERENCIAS

[1] *"Número de casos confirmados de coronavirus en el mundo a fecha de 24 de septiembre de 2021, por país", Statista https://es.statista.com/estadisticas/1091192/paises-afectados-por-el-coronavirus-de-wuhan-segun-los-casos-confirmados/*

[2 y 4] *"La OMS insta a los países a construir un mundo más justo y saludable tras la pandemia de COVID-19". Organización Mundial de la Salud (OMS) 06/04/2021 https://www.who.int/es/news/item/06-04-2021-who-urges-countries-to-build-a-fairer-healthier-world-post-covid-19*

[3] *"Analizan gestión del personal hospitalario durante la pandemia por COVID-19". Centro de Investigación y Docencia Económicas, A.C. Viernes, Jun. 04, 2021 https://www.cide.edu/saladeprensa/analizan-gestion-del-personal-hospitalario-durante-la-pandemia-por-covid-19/*

[5 y 6] *"Cuatro tendencias globales de seguridad para la asistencia sanitaria". Por Mauricio Swain, gerente de Desarrollo de Negocios para Latinoamérica en Axis Communications/ Comunicado de Prensa 19/12/2020*

COLEMAN

Jetlife

EL PODER DE VOLAR

RENTA DE AVIONES PRIVADOS Y HELICÓPTEROS

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

Powered by:
SEGURIDAD EN AMÉRICA

IS-BAO

REGISTERED OPERATOR
verify with wyvern

AEROPUERTO INTERNACIONAL DE TOLUCA

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

Tel.: 55.7672.4992

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

Socio Director, Altair Security Consulting &Training.

Más sobre el autor:

EL LIDERAZGO EN SEGURIDAD

Foto: Creativeart - Freepik

LATINOAMÉRICA

Confieso que desde que estudiaba la universidad he sido un adicto a los temas de liderazgo, negociación y estrategia. Me ha encantado involucrarme desde entonces con diversas visiones y sueños. ¿Por qué? Tal vez porque he admirado y me han inspirado grandes líderes de la historia que han movido mentes y transformado naciones completas echando mano de estas herramientas, ellos me han tocado fibras sensibles.

El liderazgo *per se* es un eje toral para los puestos ejecutivos y es imprescindible para los buenos resultados del área y de la organización. En el sector de seguridad no es la opción.

Sin entrar en discusión de si el líder nace o se hace, estoy convencido que una persona puede aprender a ejercer un liderazgo que ayude a que se den los resultados esperados. El ser líder no te lo da un puesto, sino tu forma de ejercer, te lo da la gente, la sociedad, tu equipo.

El liderazgo es necesario para que te ayude a reunir a un equipo sólido en los niveles táctico y operativo, que tenga torque propio y esté convencido para que contribuyan de manera activa en los objetivos. El liderazgo te permite darles eficiente guía y tutoría para que cada uno de ellos desarrolle con calidad su trabajo o se conviertan en otros líderes. El liderazgo transparente y con espíritu de equipo, que la gente lo note y se suba al barco. Con coherencia, transparencia y humildad.

Hablando del liderazgo transformacional, ahora muy en boga éste ha existido durante siglos y ha estado a merced de nosotros, habiendo decenas de casos que transforman mentes. Aprender de ello es indispensable si se desea trascender.

El liderazgo te permite darles eficiente guía y tutoría para que cada uno de ellos desarrolle con calidad su trabajo o se conviertan en otros líderes

DESARROLLO DE ALTO NIVEL

En el medio de la seguridad hay pocos programas académicos para ejecutivos que incluyen el liderazgo dentro de la academia, cosa que lamento. No obstante, les sugiero dos que he vivido muy de cerca y que además de incluir los temas técnico-estratégicos, considera el liderazgo dentro de su plan de estudios:

1) 'Effective Management for Security Professionals' del Instituto de Empresa de España: a mediados de este año tuve la valiosa oportunidad junto con una decena de colegas de tres continentes, de atender este programa desarrollado en idioma inglés, en esta universidad que se ostenta entre las mejores del mundo de los negocios y liderazgo.

Este programa lo recomiendo ampliamente y es llevado a cabo por expertos enfocado en cuatro grandes pilares para el desarrollo de los profesionales de seguridad de nivel ejecutivo: Finanzas, Estrategia, Negociación y Liderazgo. Pilares esenciales para hacer frente con eficiencia a los retos actuales y futuros en un mundo tan global e incierto como el actual. Permite calibrar estos temas y adaptarlos con el fin de que la visión de seguridad sea como una ventaja competitiva y parte estratégica para el cumplimiento de los objetivos generales de las instituciones. Conoce el programa en: *https://www.ie.edu/exponential-learning/programs/effective-management-security-professionals/*

> El ser líder no te lo da un puesto, sino tu forma de ejercer, te lo da la gente, la sociedad, tu equipo

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

2) Diplomado en Dirección de Seguridad Corporativa: en este 2021 en México surgió un muy buen programa desarrollado por GEMARC (Grupo de Ejecutivos en Manejo de Riesgos Corporativos), la asociación más prominente de ejecutivos de seguridad y se ha posicionando como una gran opción de desarrollo de los líderes de seguridad corporativos de habla hispana.

Es un programa impartido por especialistas prácticos de alta dirección de seguridad que les permitirá incorporar a su experiencia altos estándares para las tareas estratégicas de seguridad. Conoce este programa en: *https://gemarc.org*

En fin, un par de programas de excelencia y liderazgo que están al alcance nuestro para afilar la sierra como líderes de seguridad y aspirar al C-Suite dentro de las organizaciones. ■

Columna
EL TIGRE TIENE RAYAS

presidencia.gremioseguridad@gmail.com

Más sobre el autor:

Omar A. Ballesteros, presidente del Gremio del Bajío de Seguridad Privada, A.C.

EL LÍDER DE SEGURIDAD

Foto: Creativeart - Freepik

MÉXICO

Saludos amigos, es un gusto compartirles mi nueva columna sobre el tema de liderazgo que llamo "EL TIGRE TIENE RAYAS", la nombré así porque el tigre siempre tiene rayas, no importa si le cambias el color de pelo, o le pones botas, o tratas de adiestrarlo, el tigre es un tigre y siempre tiene rayas, esto quiere decir que su personalidad está siempre ahí, aunque traten de domarlo siempre tendrá su temperamento y carácter, así como lo tienes tú, no copies modelos de liderazgo, usa tu personalidad para lograr tus metas de equipo. Como presidente del Gremio de Seguridad, me enfrento con esto para lograr la integración de mi equipo de trabajo.

El Instituto Médico de Investigación Francés descubrió hace algunos años las "neuronas espejo", que son las causantes de que las personas puedan socializar copiando comportamientos y de igual manera puedan asimilar modelos de liderazgo. ¿Te has preguntado por qué hay personas que nos asombran o llaman nuestra atención?

Hay quienes son más llamativas que otras y es precisamente su personalidad la que nos obliga a voltear a verlas, cuando estamos frente a un grupo de personas muchas veces sentimos miedo y no sabemos cómo expresarnos, usamos muletillas como "este", "umm", "aaa", entre otras. Usamos inadecuadamente las manos o la expresión del cuerpo es pobre, no logramos convencer a nuestro equipo de trabajo y terminamos mencionando: "No sé, es lo que me dijo el director…". No tienes la culpa del todo, nadie te enseñó cómo expresarte y usar tu personalidad para lograr que tu equipo de trabajo, motivadamente, logre las metas marcadas.

Puedes leer muchos libros de liderazgo como los de John C. Maxwell, Bill Gates, Carlos Slim, entre otros libros que hay en el mercado actual, y tratar de asimilarlos, terminas de leerlo y motivado buscas aplicarlo, pero te topas con la realidad de que tus compañeros de trabajo, subordinados, empleados, etc., tienen una apatía terrible que por más que luchas para cambiarles la mentalidad y se sientan integrados, parte de la empresa, no lo logras, te frustras, te molestas y puede

En tu trabajo debes ver las personalidades de esa gente que necesitas convencer para lograr los objetivos planteados.
Un error que muchas empresas extranjeras tienen al llegar a México es que no saben cómo piensa y actúa el mexicano, no conocen nuestra cultura

que la gran mayoría de las veces, se te baja la batería para seguir; pero lo que no has logrado entender es que el primero al que tienes que convencer ¡es a ti mismo! Si no te logras convencer, ¿cómo pretendes que los demás te sigan o te hagan caso?

El liderazgo empieza contigo, ve al espejo y reconoce al líder que tienes dentro, si no lo ves, búscalo nuevamente, porque mientras no lo encuentres seguirás buscando modelos y tratarás de copiarlos, y en muchos casos serás sólo una mala copia de ellos, o te compararán, porque te comportas de la misma manera. ¿Eso quieres? ¿Que te comparen y ser una copia de alguien más? ¿No será mejor que ellos se admiren de ti? ¿Sabes qué es la envidia? Es la admiración por alguien más —lo repito— es la admiración por la personalidad de alguien más, no es el deseo de tener lo que los demás tienen, porque tú no lo tienes, todo comienza con la personalidad.

¿CÓMO SER UN LÍDER?

Para comenzar con tu formación de líder, primero debes encontrar eso que te hace diferente y único, eso que te distingue de otros, buscamos personas en común pensando que si piensan lo mismo que nosotros nos sentiremos más cómodos, pero en realidad nos atraen las personas originales, aquellas que no son iguales, nos enamoran las personas con pensamientos originales, con ideas propias, ¿lo has notado? Lo mismo pasa con el líder, su principal cualidad es ser original, ¿ya descubriste qué te hace único? El orador griego de la época antigua llamado Demóstenes, ¡era tartamudo! Y fue un excelente orador, ¿cómo fue posible eso? Usó su tartamudez como su principal herramienta para lograr su liderazgo.

Como presidente del gremio de seguridad privada en el Bajío, me encuentro con un sinfín de opiniones dentro de las reuniones de Consejo, todos tienen una opinión que dar y quieren ser tomados en cuenta. Conforme a mi formación de liderazgo he logrado mantener una unión entre los miembros, siendo que tenemos una enorme variedad de personalidades… Después te digo cómo lo estoy logrando.

Me han tratado de cambiar el carácter (no saben lo que me piden en realidad), ya que una de mis cualidades es que soy impulsivo, enérgico y fuerte, y "al tigre no le puedes quitar las rayas", eres como eres y no puedes ser igual a nadie, eres único y los demás lo notan si lo resaltas.

Albert Einstein era un líder de su época, no era político, no era impulsivo, era tranquilo generalmente, y sin embargo los científicos de su época lo buscaban, porque necesitaban de su sabiduría y opinión, y él no lo buscaba.

¿He logrado obtener tu interés hasta ahora? En tu trabajo debes ver las personalidades de esa gente que necesitas convencer para lograr los objetivos planteados. Un error que muchas empresas extranjeras tienen al llegar a México —y lo he visto—, es que no saben cómo piensa y actúa el mexicano, no conocen nuestra cultura.

Los japoneses quieren llegar trayendo filosofías de ejercicios tempranos antes de ingresar a la línea de operación, notas en la cara de los mexicanos que no es agradable hacer los ejercicios, en la mayoría de los casos, y lo comento sobre las personas de producción, ellos prefieren la dieta de la "T" (tacos, tortas, tamales), los ejecutivos de oficinas son diferentes de los Operativos, como lo es el personal de Ventas, de Publicidad, y lo mismo pasa con el guardia de seguridad, es tan diferente como el área de Ventas.

Reconocer quién es quién te permitirá conocer sus necesidades emocionales, tienes que darte cuenta que la personalidad de tus compañeros es 100% emocional, igual que la tuya. ¿Sabes distinguir cuando alguien llega enojado, molesto, triste o feliz? ¿Sabes cómo sacas a una persona de su apatía?

Foto: Creativeart - Freepik

Como líderes tenemos que influir en las personas mediante el subconsciente, ya que si te diriges al consciente y dependiendo de su estado emocional, no te harán caso, pero si te diriges al subconsciente es seguro que la persona te note, logres su interés y te haga caso

Paul Ekman reconoció los estados emocionales de las personas expresados por el lenguaje corporal en alegría, coraje, repudio, asco y tristeza. ¿Sabes distinguirlos? Si no lo sabes y ese día alguno de tus colaboradores tiene coraje, es decir, llegó molesto de casa y tiene la cabeza pensando en sus problemas maritales, por más que trates de instruirlo, no te pondrá atención ni mucho menos estará motivado, porque está enojado o corajudo. Sigamos entonces.

¿QUÉ ES EL TEMPERAMENTO?

Es lo que te define como un ser único y diferente del resto, es con lo que naces y no se puede cambiar: tus corajes, alegrías, motivaciones, ascos, en fin, todo lo que eres tú, entonces ¿qué es el carácter? Es la tolerancia a la frustración y es aprendida por el ambiente y las experiencias, es el control ante las situaciones y condiciones que se enfrentan y que evitan reaccionar impulsivamente, ante el peligro debes tener control de tus emociones, ya que la gran mayoría sale corriendo lastimando a otros y a ellos mismos, o ante un insulto.

De aquí una vez que reconoces esto, tienes que pasar a los estados psíquicos establecidos por Sigmund Freud: consciente, inconsciente y subconsciente (existe también el pre-consciente, pero ese no lo tocaré por ahora), y además tienes que identificar el Ello, el Yo y el Superyó, todos estos elementos son necesarios para lo que te voy a explicar.

- **El consciente** es el hoy, reconoces que existes y quién eres y dónde estás. Ejemplo: soy Omar.

- **El inconsciente** es la parte del cerebro que no reacciona hasta que el subconsciente se lo indica, es la reacción del subconsciente. Ejemplo: gritas en una película de terror sin pensarlo.

- **El subconsciente** es la parte de nuestro comportamiento que se va reservando conforme vamos tomando consciencia de nuestra vida. Ejemplo: cuando éramos bebés no nos importaba la crítica, fue hasta que tomamos consciencia nos interesó.

Ahora qué es:

- **El Yo:** es quien soy.

- **El Ello:** el placer, y no le importa qué, el cerebro siempre quiere placer.

- **El Superyó:** los valores y la moral, y está contenido en el lóbulo frontal de la cabeza.

Una persona con poca preparación educativa e intelectual (no digo que no vaya a la escuela, hay de todo, tanto universitarios sin intelecto como gente culta con grado primaria) tiende a comportarse mediante el placer más que por los valores, y su influencia al subconsciente es más notoria.

¿Para qué nos interesa lo anterior? La personalidad de cada sujeto con los que tenemos que trabajar tiene eso, y el simple hecho de saberlo nos permite tomar ventaja para descubrir sus motivaciones.

Como líderes tenemos que influir en las personas mediante el subconsciente, ya que si te diriges al consciente y dependiendo de su estado emocional, no te harán caso, pero si te diriges al subconsciente es seguro que la persona o personas te noten, logres su interés y te hagan caso.

Mientras una persona lee menos, es más propensa a la influencia de los demás, a nivel operativo la televisión los controla más que un libro, no te digo que los hagas leer, no lo harán, pero si les platicas de un libro que estás leyendo (y si no lo estás haciendo, es tiempo que lo hagas) y le pones emoción a tus palabras, entonces lograrás meterles la curiosidad en el tema, es decir, que llamarás su atención. Mientras más entusiasmo le pones a tu discurso, más logras su admiración, porque les estarás dando algo que ellos no tienen, recuerda hay que ser originales.

Estoy sumamente emocionado de compartirles mis experiencias en liderazgo como presidente del gremio en las próximas publicaciones, y con este artículo comienzo "El tigre tiene rayas". Finalizo con una frase: "O te tienen miedo o te tienen respeto…¿Cuál quieres?". ■

Foto: Creativeart - Freepik

El liderazgo empieza contigo, ve al espejo y reconoce al líder que tienes dentro, si no lo ves, búscalo nuevamente, porque mientras no lo encuentres seguirás buscando modelos y tratarás de copiarlos

Todas las plataformas de seguridad son iguales, como los coches, 4 ruedas y un motor

M360

Para quienes aspiran a un deportivo alemán

Powered by

SEPSISA

RANGER SWAT MÉXICO

GUARDIAS INTRAMUROS: SERVICIO ESPECIALIZADO ANTE LA STPS

La Secretaría de Trabajo y Previsión Social a través del Registro de Prestadores de Servicios Especializados u Obras Especializadas, busca regular y fiscalizar a las personas físicas o morales que presten servicios especializados, entre ellos la Seguridad Privada, considerando la subcontratación como un delito

Foto: Creativeart - Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Con la entrada en vigor de la reforma (fiscal) al *outsourcing* en México (1° de septiembre del 2021), que prohíbe la subcontratación de personal, a excepción de aquellos servicios y obras especializadas que no formen parte del objeto de la empresa, y que busca eliminar las malas prácticas que dañan los derechos laborales y así evitar entre otras situaciones, la defraudación fiscal, distintos sectores de la economía tuvieron que registrarse en la plataforma del Registro de Prestadores de Servicios Especializados u Obras Especializadas (REPSE), entre ellas las empresas de seguridad privada.

El REPSE es regulado por la Secretaría de Trabajo y Previsión Social (STPS) y su objetivo es "registrar, regular y fiscalizar a las personas físicas o morales que presten servicios especializados o ejecuten obras especializadas a través de un Padrón Público de Servicios Especializados u Obras Especializadas"[1]. Una de las intenciones es además de la legalidad laboral, que generen opiniones positivas de tres instancias gubernamentales: Instituto Mexicano del Seguro Social (IMSS), Servicio de Administración Tributaria (SAT), y el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (Infonavit).

Aquellas que no cumplan con el REPSE serán sancionadas con multas que van de los 179 mil pesos (8 mil 900 dólares) a los 4 millones 480 mil pesos (223 mil dólares). La seguridad privada está dentro del catálogo de servicios especializados, estar dentro del REPSE le da un valor agregado para sus clientes, además de encontrarse dentro de la legalidad, la regulación y las buenas prácticas.

Este sector considerado "esencial" a partir de la pandemia ocasionada por el COVID-19 y ahora especializado con el REPSE, ha dejado más a la vista lo indispensable que es, puesto que los ín-

dices de inseguridad no han disminuido y por el contrario en algunos sectores ha incrementado.

De acuerdo con los resultados de la Encuesta Nacional de Seguridad Pública Urbana, emitida por el Instituto Nacional de Estadística y Geografía (INEGI), la percepción de inseguridad de los mexicanos aumentó del 66.4% en marzo al 66.6% en junio del presente año[2], es decir se tuvo un alza de 0.2 puntos porcentuales frente al resultado del trimestre anterior y falta que se publique el cierre del año.

Respecto a los espacios físicos, la encuesta evidenció que el 77.6% de la población comentó sentirse insegura en los cajeros automáticos localizados en la vía pública, el 71.4% en el transporte público, 63% en el banco y 59.6% en las calles que habitualmente usa. Datos que influyen en el seguir contratando empresas de seguridad privada con guardias intramuros capacitados y cumpliendo con la reforma al ser un servicio tercerizado, pero especializado y necesario dados los índices de inseguridad y el incremento de actividades en el país.

Es por ello que **Seguridad en América** (SEA), realizó una serie de entrevistas con expertos en guardias intramuros para conocer la situación actual de este sector y las estrategias que aplican en la nueva normalidad y normatividad.

RODRIGO GUTIÉRREZ GUILLÉN, RESPONSABLE DE SEGURIDAD Y PREVENCIÓN DE PÉRDIDAS COPPEL

SEA: ¿Cuál es la importancia de contar con guardias intramuros en su sector?

Rodrigo Gutiérrez **(RG):** tocar temas tan sensibles sobre la seguridad suelen ser un poco difíciles, ya que se suelen encadenar muchas controversias, tanto positivas como negativas y más cuando se habla de costo-beneficio, las empresas realizan un análisis tanto externo como interno para definir estrategias y utilizar este recurso en su máxima expresión.

Cuando escuchamos o incluso vemos guardias en algún lugar no les tomamos la importancia adecuada, no entendemos que la seguridad privada realmente esta para cuidarnos ayudarnos e incluso arriesgar su vida por la de los demás y tal vez no te pueda defender como la seguridad pública lo hace, pero sí puede hacer algo para evitar que te asalten o que roben ya que tienen la capacidad de analizar e identificar situaciones que pueden representar un riesgo.

Los guardias de seguridad son los puntos clave para proteger el patrimonio de los lugares donde les toca dar su servicio sobre la protección de las personas que están a su alrededor, el porqué de la importancia de la seguridad privada es por el constante aprendizaje y la capacitación que se les otorga, ya que para desarrollar sus habilidades no es en cuestión de uno o dos días, sino que tiene que pasar por un determinado tiempo para que puedan desarrollar las habilidades que necesita tener.

SEA: En su experiencia, ¿cuáles son las deficiencias del servicio de guardias intramuros?

RG: la rotación de personal. Por muchos años he observado que una de las principales deficiencias que las empresas de seguridad privada tienen en su proceso de reclutamiento y selección es no dejar claro al guardia para que se le está contratando, explicar a detalle las funciones, actividades y responsabilidades que tendrá al ser parte de la empresa que está solicitando este servicio.

El constante aprendizaje y la capacitación que se les brinda a los elementos, al no cumplir este requisito, es ahí precisamente donde yo veo otra deficiencia de las empresas de seguridad, al no considerar una inversión en temas de reclutamiento de acuerdo a los perfiles solicitados y, sin esta capacitación, herramientas y conocimientos necesarios difícilmente se obtendrá el objetivo esperado por la empresa contratante.

SEA: ¿En lo particular, ¿considera que la reforma del *outsourcing* afectará al costo de guardias intramuros? Sí, no, ¿por qué?

RG: en lo particular no considero que vaya a existir una afectación con relación al costo de guardias para las empresas contratantes, lo que sí es cierto es que habrá una depuración de las empresas que proveen guardias de seguridad, debido a que la mitad de ellas están en la informalidad.

Esta reforma de *outsourcing* beneficiará a las empresas formales, porque existe una competencia desleal con aquellas que contratan al personal de forma irregular y que no tenían prestaciones o estaban incompletas, de tal forma que sólo podrán obtener un registro aquellas que demuestren tener una operación formal y que respeten los derechos laborales de los empleados.

Rodrigo Gutiérrez Guillén

Formación: cursó la carrera de Ingeniería Industrial en la Universidad Central de México, en Puebla (México), tiene conocimiento sobre diferentes herramientas de la seguridad: sistemas de alarmas y CCTV (Circuito Cerrado de Televisión). Cuenta con cursos y participación en conferencias de centros de monitoreo a Nivel Banca.

Cursos: Técnicas de Entrevistas e Interrogatorio; Cadena de Custodia y Sistema de Justicia Penal en el Instituto Nacional de Ciencias Penales (INACIPE).

Camino a la seguridad: durante el inicio de sus estudios universitarios (año 2000), fue invitado por su hermano para trabajar en una empresa de seguridad privada que prestaba sus servicios para el hoy extinto Banco Serfin, derivado de su buen desempeño, fue considerado para trabajar en el centro de monitoreo, con la absorción de Banco Serfin por Santander, todos los centros de monitoreos se unificaron, realizando una migración a la Ciudad de México, donde se tendría todo el control a nivel nacional.

En el año 2005 se integró al centro de monitoreo de Santander y por más de 15 años se desempeñó en distintas actividades de esa área, su último puesto fue de coordinador operativo (del año 2011 a 2020).

Actualmente colabora en la empresa Coppel con nuevos retos y adquiriendo conocimientos en temas de Seguridad y Prevención de Pérdidas.

JORGE LUIS ACATITLA ANGUIANO, DIRECTOR CORPORATIVO DE SEGURIDAD INTEGRAL DE GRUPO XCARET

SEA: ¿Cuáles considera que son las estrategias de seguridad que se deben implementar con los guardias intramuros?

Jorge Luis Acatitla (JLA): hoy en día las actividades que realiza un guardia intramuros son muy variadas, anteriormente estaba más enfocado al control de acceso sobre todo de personas, actualmente además de esa función, debe estar registrando el ingreso y salida de materiales, de equipos, realizar rondines para identificar áreas vulnerables o incluso hacer recomendaciones de mejora, identificación de vulnerabilidades y hasta observaciones sobre si una normativa está siendo suficiente para cubrir alguna actividad y de esta manera minimizar los riesgos.

Además, con la presencia de la pandemia por COVID-19 ha asumido mayores responsabilidades, como tomar la temperatura, el proporcionar los insumos, como gel, a la gente que llega a las instalaciones, verificar que pase por los tapetes de sanidad, es decir que cumpla con las recomendaciones de bioseguridad.

Entonces las estrategias de seguridad son muy amplias y depende también del sector donde se desarrolle y lo que específicamente se requiera del elemento y la posición que cubra.

SEA: de acuerdo a su experiencia, ¿cuáles son los beneficios y desventajas de contratar una empresa de seguridad privada o contar con elementos propios?

JLA: puedo dar una opinión bastante objetiva al respecto, ya que he trabajado tanto en empresas que contratan el servicio de guardias intramuros para su seguridad, en empresas que cuentan con un grupo propio de seguridad y en una empresa de seguridad privada que proporciona el servicio de seguridad a terceros, es decir las tres opciones de servicio que considero pueden existir. En mi opinión, el tener guardias propios tiene muchas ventajas, la principal es que puedes crear sentido de pertenencia, también, tienes la oportunidad de seleccionar a tus elementos de seguridad bajo un perfil muy específico, proporcionarles la capacitación acorde al tipo de negocio al que te dedicas.

También el equipo que le proporcionas para desempeñarse adecuadamente sus funciones, conocimiento de actividades muy particulares, crearles un plan de vida y carrera donde pueden escalar en las diferentes posiciones de la empresa, lo que se resume a una satisfacción integral por parte del personal. La única desventaja que veo es el costo, al final de cuentas es asumir todos los gastos de contratación que una empresa de seguridad privada te ahorra.

Ahora bien, contratar una empresa de guardias puede funcionar muy bien cuando el gerente de Seguridad participa activamente en la capacitación, selección, supervisión, en el pago justo de los elementos, que les brinden todas las prestaciones de la ley.

SEA: ¿Cómo es el proceso de selección y capacitación de los guardias intramuros a su cargo?

JLA: el proceso es extenso, empezamos proporcionándole un perfil del puesto al área de Recursos Humanos, con datos muy específicos sobre edad, peso, estatura, formación académica; y una vez que cumple con estas características hay una entrevista con el candidato, para pasar posteriormente a la realización de exámenes psicométricos, toxicológicos, psicológicos, estudio socioeconómico en su domicilio para la validación de información, exámenes de control de confianza.

Ya cuando pasa todos estos procesos, sigue la capacitación con un curso general de inducción, otro específico de los temas de seguridad en su área y la organización. La capacitación periódica es muy importante para nosotros.

Foto: © Jarp3 | Dreamstime

Jorge Luis Acatitla Anguiano

Formación: Licenciado en Administración de Empresas, cuenta con el Diplomado en Habilidades Gerenciales impartido por el Tecnológico de Monterrey; Diplomado de Desarrollo de Habilidades para el Directivo de la Seguridad Integral (DSI), actualmente promovido por la Asociación Mexicana de Especialistas en Seguridad Integral A.C. (AMEXSI); Dirección de Seguridad en Empresas (DSE), dictado por la Universidad Pontificia Comillas, entre otros.

Así como una maestría en Administración de la Seguridad, con especialidad en ciberseguridad impartido por la UDLAP JENKINS. Certificación en Protección Profesional (CPP) por ASIS Internacional.

De camino a la seguridad: inició en Servicio Panamericano de Protección (30 años), durante seis meses colaboró con una empresa de guardias intramuros. Perteneció al área de Seguridad de Televisa por ocho años, y actualmente es, director corporativo de Seguridad Integral de Grupo Xcaret.

ARTURO GUIDO, RESPONSABLE DE SEGURIDAD CORPORATIVA PARA MÉXICO Y LATAM EN ZURICH ASEGURADORA MEXICANA

SEA: mencione 5 características que requiere de un guardia intramuros para su sector.

Arturo Guido **(AG)**: en mi opinión, las características de los guardias deben definirse de acuerdo a las necesidades de cada cliente, locación y actividad específica a realizar. Por ejemplo, no es lo mismo el perfil de un guardia para una caseta de acceso en una planta industrial, que el perfil de un guardia en una recepción de un edificio corporativo. Sin embargo las cinco características que considero más importantes son:

1. La definición de un perfil específico por posición a cubrir (escolaridad, conocimientos, experiencia, etc.).

2. Confiabilidad. Asegurar que la compañía de seguridad lleve a cabo procesos detallados de reclutamiento y selección, saber quién es, de dónde viene.

3. Conocimientos mínimos de seguridad. Aquí es importante saber cuál es la capacitación básica que provee la empresa de seguridad, y muy importante definir la capacitación necesaria y específica para el desempeño en su puesto de seguridad, así como un programa de entrenamiento continuo.

4. La personalidad del oficial debe ser de estricto apego a reglas y procedimientos, así como proactivo en sus labores, disciplinado.

5. Que tenga valores (integridad, responsabilidad) para el desempeño diario de sus funciones, de ahí la importancia de la evaluación del personal en los procesos de selección).

SEA: en su experiencia, ¿cuáles son los errores más comunes que cometen los guardias intramuros?

AG: 1. Administrativos (llenado correcto de reportes), 2. Comunicación (omisión) y 3. No estar alertas, caer en el exceso de confianza.

SEA: ¿Cómo considera que afectará o beneficiará el REPSE al servicio de guardias intramuros?

AG: considero que en lo que respecta a los servicios de seguridad privada, las empresas internacionales y nacionales serias, ya cumplían con los marcos legales antes de la promulgación del REPSE. Creo que REPSE no debió ser para el sector de la seguridad privada, ya que en estricta teoría nunca se han considerado *outsourcing*, siempre ha sido un servicio especializado el cual estaba regulado por los municipios, estados y federación, además de que es el único servicio especializado con ley.

Foto: © Mbolina | Dreamstime

Arturo Guido

Formación: Licenciado en Comercio Internacional con Maestría en Administración por la UNIVA (Universidad del Valle de Atemajac) en Guadalajara, Jalisco. Cuenta con un Diplomado en Gestión Humana Organizacional por el ITESO (Instituto Tecnológico y de Estudios Superiores de Occidente-Guadalajara, Jalisco), así como un curso Gerencial del ICAMI (Centro de Formación y Perfeccionamiento Directivo), adicional a varios cursos especializados en materia de seguridad.

Fue presidente de BASC Capítulo Occidente. Actualmente es *Co-Chair* del Capítulo de OSAC en Occidente. Y miembro activo de ASIS y GEMARC (Grupo de Ejecutivos en Manejo de Riesgos Corporativos).

De camino a la seguridad: debido a su experiencia en el área de Comercio Internacional en una compañía electrónica, el gerente de Seguridad de la planta de IBM en aquel tiempo (1998), lo invitó a ser parte de su equipo para apoyarlo en el área de Seguridad en la distribución de los productos, que en aquel tiempo se fabricaban en la planta del Salto Jalisco (PC, *laptops*, discos duros y servidores) y que eran distribuidos prácticamente en todo el continente, así como Asia Pacifico.

Y es así como fue su primer contacto con la Seguridad y de la cual se enamoró, desde esa fecha hasta hoy se ha venido desempeñando en diversas posiciones de liderazgo en empresas líderes de los ramos: manufactura, alimenticio, servicios de seguridad, logística y al día de hoy como responsable de Seguridad Corporativa para México y LATAM en Zurich Aseguradora Mexicana, teniendo bajo su responsabilidad países como Brasil, Argentina, Ecuador, Chile, Colombia y, por supuesto, México.

ARTURO MARTÍNEZ AVALOS, DIRECTOR GENERAL ADJUNTO EN MSPV SEGURIDAD PRIVADA

SEA: ¿Cuáles son los principales beneficios de contratar guardias intramuros?

Arturo Martínez (**AM**)**:** el tener guardias intramuros, como lo dicen los estándares internacionales, proporciona grandes beneficios por ejemplo, tener la capacidad de crear, crecer, disminuir o eliminar una plantilla en el momento que se necesite, porque esto lo brinda un tercero, solamente le dices a tu proveedor y esto no genera impacto económico dentro de tu empresa.

Específicamente hablando de México, tener seguridad privada es una necesidad. Contar con este servicio, brinda un valor agregado a nuestros clientes y sus procesos. Anteriormente era considerada como un 'mal necesario', pero al día de hoy, es un ingrediente indispensable que si no está, puede repercutir con alto impacto al *core* de nuestro cliente: puede dejar de producirse, bajar la calidad o el ritmo de producción, de tal manera que hoy la seguridad privada brinda un valor agregado a la cadena productiva de nuestros clientes.

Por lo tanto, nos estamos volviendo un proveedor crítico. En MSPV lo tomamos con toda seriedad, contamos con certificaciones como ISO 9001 (International Organization for Standardization) versión 2015, BASC (Business Alliance for Secure Commerce), cumpliendo en los estándares y exigencias de nuestros clientes. Hoy la seguridad privada es un aliado y un proveedor crítico dentro de la cadena productiva.

SEA: ¿Cuáles son los servicios que ofrece MSPV Seguridad Privada y cómo los adaptaron a la nueva normalidad?

AM: el sector de la seguridad privada tuvo una demanda importante el año pasado (2020). La pandemia nos reafirmó como un servicio esencial para apoyar a nuestros clientes. En MSPV Seguridad Privada, contamos con guardias intramuros y recientemente, guardias intramuros armados a través del Cuerpo de Seguridad Auxiliar del Estado de México (CUSAEM), que nos fue asignado en estos últimos meses.

Foto: Creativeart - Freepik

También ofrecemos el servicio de custodias a bordo, con el acompañamiento de un vehículo o a través de motocicletas, así como consultoría en seguridad patrimonial y servicios de *cybersecurity*.

SEA: ¿Qué sectores implican mayores retos para los guardias intramuros? ¿Por qué?

AM:

- **Automotriz.** Este es un segmento que nos encanta y en el que tenemos varios clientes en el país. Sus procesos son tan pulcros que nos deja completamente claro qué es lo que tenemos que hacer, en dónde y cuándo tenemos que participar.

- **Procesos alimenticios.** En este sector, el elemento de seguridad debe estar capacitado en temas de seguridad muy específicos, por ejemplo, los requisitos para entrar a áreas inocuas, o respetar y hacer respetar los procesos de esas zonas en donde los alimentos están colocados. Todo ello implica un reto mayor tanto para nosotros. Estos sectores nos exigen tanto que provoca la generación de mejorías en nuestros procesos, lo que valoramos mucho.

- **Almacenes (centros comerciales, tiendas departamentales).** Aquí hay muchos retos por los *modus operandi* de estos sitios. El guardia es un eslabón clave en el plan integral de seguridad del gerente o director patrimonial de ese negocio: el elemento de seguridad ayudado por las cámaras de seguridad, tiene que identificar robo hormiga, tiene que prevenirlo, disuadirlo y evitarlo si es posible. Éste ha sido un mercado muy complicado, en el que hemos aprendido mucho por lo que hoy tenemos muy buenas prácticas, incluso algunos de nuestros clientes nos han dado una calificación *gold*, dentro de la cadena de clientes y proveedores que tienen.

- **Establecimientos de comida rápida.** Su complejidad radica en que ahora está muy presente la modalidad del robo de artículos personales de los comensales. Hemos implementado la modalidad de guardia *hoster* dentro de estas instalaciones, para tener una imagen preventiva y disuasiva que contribuye a que los ladrones se alejen del lugar. Hemos tenido que aprender al paso de lo que les va sucediendo día con día, para adaptar los procesos de seguridad.

Arturo Martínez Avalos

Formación: Ingeniero en Sistemas Computacionales, Técnico en Electrónica. Certificación en Protección Profesional (CPP), certificación como Investigador Profesional (PCI), emitidas por ASIS Internacional. Presidente de la Asociación Mexicana de Especialistas en Seguridad Integral A.C. (AMEXSI), durante el periodo 2019-2020.

De camino a la seguridad: inició en el área de Ingeniería en Northern Computers (hoy Honeywell), al paso de los años, el Banco Nacional de México (Banamex) lo invitó a formar parte de la Seguridad Corporativa, administrando más de 4 mil 800 cajeros y responsable de toda la estrategia de seguridad de los cajeros automáticos de todo el país.

Colaboró en distintas áreas del banco, hasta ser el administrador del proyecto de implementación de estrategias de seguridad y crear junto con el la Asociación Mexicana de Bancos, el *Manual de Seguridad y Protección Bancaria,* con base en las 10 medidas de seguridad bancarias emitidas en 2002 por el gobierno.

Después de casi 20 años de trabajar en Banamex como subdirector de Proyectos de Seguridad, se independizó como consultor en gestión de cambio organizacional y gestión de riesgos empresariales. Durante una reunión de trabajo con el Ing. Jorge Septién Esnaurrizar, presidente de MSPV Seguridad Privada; y Frank González Sojo, director general de la misma firma, Arturo presentó un proyecto de cambio organizacional con el que a la fecha continúa laborando en la empresa. MSPV Seguridad Privada, misma que recientemente (6 de septiembre) cumplió 27 años en el mercado.

- **Condominios (clientes que administran unidades habitacionales).** Este sector es muy complejo, ya que existen 'n' cantidad de departamentos, por lo que el guardia de seguridad va a tener 'n' cantidad de jefes, lo que implica un reto operativo muy demandante.

SEA: ¿Considera que la reforma al outsourcing en México y el registro en el REPSE, afectará o beneficiará al sector de la seguridad privada?

AM: puede afectar como beneficiar. Por el lado del colaborador, podrá gozar de todos sus derechos como lo solicita la ley. De este lado, de la persona moral, lo que estamos teniendo como como resultado, es que nuestro gasto interno operativo está incrementándose. Unas cosas por otras… puedo vislumbrar que esto se va a traducir, a largo plazo, en muchos beneficios que el cliente va a tener como un mejor servicio, mayor calidad y personal más satisfecho por el cumplimiento de todos sus derechos.

Foto: Creativeart - Freepik

PRINCIPALES DIFERENCIADORES DE MSPV SEGURIDAD PRIVADA

1. Calidad del servicio.
2. Infraestructura técnica y humana.
3. Personal operativo y directivo capacitado y profesional.
4. Comunicación efectiva y clara.
5. Gestión con los clientes.

5 ASPECTOS A CONSIDERAR AL CONTRATAR EL SERVICIO DE GUARDIAS INTRAMUROS

De acuerdo con Arturo Martínez Avalos, director general adjunto en MSPV Seguridad Privada, son:

1. Calidad del servicio.
2. Cobertura (puesto cubierto en todo momento por el guardia).
3. Supervisión constante del guardia.
4. Gestión directiva y gerencial a nivel del administrador de riesgos o director de Seguridad, empatía con el cliente a nivel ejecutivo y gerencial, que genera una buena comunicación.
5. Precio. ■

REFERENCIAS

1 Gobierno de México, Secretaría de Trabajo y Previsión Social-REPSE https://repse.stps.gob.mx/

2 "Percepción de inseguridad en México sube a 66.6% en junio: Inegi", Forbes-EFE, 19/07/2021 https://www.forbes.com.mx/percepcion-de-inseguridad-en-mexico-sube-a-66-6-en-junio/

SOS (SECURITY OUTSOURCING SOLUTION)

¿En qué consiste la nueva reforma sobre el outsourcing?

MÉXICO | Jaime Domínguez Martínez

Las entidades jurídicas que tienen empleados contratados a través de servicios de *outsourcing* (subcontratación) se encuentran en una disyuntiva para tratar de cumplir con las nuevas disposiciones en materia laboral.

Este año comenzaron las obligaciones para que los patrones pongan en marcha las nuevas disposiciones en materia de *outsourcing* que se establecieron con las reformas a la Ley Federal del Trabajo, la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, la Ley del Seguro Social, la Ley del Impuesto Sobre la Renta, el Código Fiscal de la Federación, la Ley del Impuesto al Valor Agregado, entre otros más.

Debido a todo esto, el proceso de adaptación y cumplimiento no ha sido ni será sencillo para las empresas, principalmente para las micro, pequeñas y medianas que seguramente tendrán que recurrir a especialistas para que las asesoren y así evitar caer en incumplimiento, lo que originaría cargos innecesarios. Estas obligaciones legales conllevan a los empresarios a generar erogaciones no consideradas.

En México, donde en promedio el 90 por ciento de las empresas son micro, pequeñas y medianas empresas y en la mayoría de los casos no tienen la posibilidad de tener al alcance el conocimiento para hacer frente personalmente a estos hechos y tampoco tener la posibilidad económica para contratar servicios

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

de asesoría especializada, la carga financiera será otro tema a considerar para ellas.

Las reformas legales aprobadas en este año establecen que está prohibido el *outsourcing*, pero sí se permite en servicios especializados que no formen parte del objeto social ni preponderancia de la beneficiaria de estos servicios y que el prestador del servicio esté registrado en el padrón público que la Secretaría de Trabajo y Previsión Social (STPS) tendrá a su cargo.

Las empresas que no cumplan con estas disposiciones legales de *outsourcing* podrán ser acreedoras a multas que llegan hasta 50 mil UMAs (Unidad de Medida Actualizada que en México es de 89.62 pesos —4.37 dólares—), equivalentes a 4 millones 481 mil pesos (218 mil 650 dólares). Que incluso puede ser por cada trabajador.

El 24 de mayo de 2021 se dieron a conocer en el Diario Oficial de la Federación (DOF) los detalles para que las personas jurídicas que presten servicios especializados se registren en el Padrón Público ante la STPS (Secretaría del Trabajo y Previsión Social), con el propósito de controlar e identificar a las personas jurídicas que presten estos servicios.

SOBREREGULACIÓN

Consideramos importante que la STPS, dirigida por la secretaria Luisa María Alcalde, otorgue asesoría a las personas jurídicas que así lo requieran para el buen cumplimiento del proceso.

Pese a este dilema administrativo y financiero las disposiciones laborales en materia de *outsourcing* se pueden llevar a cabo sin mayor contratiempo, pero son los requisitos de seguridad social y regulaciones fiscales lo que preocupan más a los empresarios.

Estas medidas de sobreregulación de *outsourcing* pueden provocar que las personas jurídicas caigan en errores involuntarios y por ende la posibilidad de multas y tomen la decisión de dejar de prestar este tipo de servicio lo que afectaría el crecimiento económico y la fuente de empleo lícito.

Estas medidas de sobreregulación de *outsourcing* pueden provocar que las personas jurídicas caigan en errores involuntarios y por ende la posibilidad de multas

La sobreregulación podría originar cosas adversas para lo que fueron creadas las reformas legales sobre el *outsourcing*, que los empresarios implementen o integren a los trabajadores subcontratados como personas físicas por honorarios o la figura de asimilados a salarios o en el peor de los escenarios prescindir de ellos.

La Asociación Mexicana de Empresas de Capital Humano (AMECH) en una encuesta publicada en la primera quincena de marzo de 2021, señala la probabilidad de que los empresarios no integren a sus trabajadores a la nómina.

Por último, recordemos que la pandemia afectó a poco más del 85% de las empresas mexicanas con la disminución de sus ingresos (sin considerar a las que tuvieron que cerrar sus puertas definitivamente por falta de ventas), la poca demanda y el poco flujo de servicios y productos, además casi el 6% reporta haber recibido algún apoyo por parte del gobierno, de acuerdo con la Encuesta sobre el Impacto Económico Generado por las Empresas (ECOVID-IE 2020), elaborada por el INEGI (Instituto Nacional de Estadística y Geografía). ■

Jaime Domínguez Martínez, DSI, PDM, DES,
representante de Security Outsourcing Solution.

Más sobre el autor:

CYBER BLACK, SEGURIDAD DE CUARTA GENERACIÓN

Bajo el lema "inteligencia que protege", Luis Miguel Dena lidera una de las empresas de seguridad corporativa que ha ido evolucionando y que ofrece su experiencia y habilidades dentro y fuera de México, siendo la ciberinteligencia su principal aliado

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Uno de los retos más desafiantes en el mundo empresarial durante la pandemia por COVID-19, fue el de la continuidad de negocios, y quienes lograron identificar los riesgos a los que estaban expuestos ante este suceso, de forma interna y externa, fueron los que hoy en día continúan laborando. Sin embargo, la gestión de riesgos, y hablando específicamente de seguridad, es un tema de suma importancia para el buen desarrollo de las actividades de una empresa, cual sea su rubro. Es por eso que entrevistamos a Luis Miguel Dena, CEO y fundador de Cyber Black y su marca BlackIND, empresa dedicada a la ciberinteligencia.

Seguridad en América (SEA): *¿Cómo se formó Cyber Black?*
Luis Miguel Dena (LMD): Cyber Black nace el 14 de febrero de 2018, pero es una empresa que tiene un linaje muy antiguo, porque a partir de 1990 se materializa como una empresa de seguridad privada, que con la experiencia de mi papá, Sebastián Dena Bustos, quien estuvo como director de seguridad del Metro con la Policía Bancaria Industrial, y perteneciente a esa generación de militares y policías bancarios que salieron al empresariado mexicano a fomentar un modelo de negocio de seguridad de segunda generación, hasta llegar a lo que ahora tenemos: una empresa de cuarta generación.

SEA: *¿Cuáles son los servicios que ofrece CB?*
LMD: nosotros hacemos que la inteligencia tanto estratégica como operativa, con una vinculación tecnológica permita gestar una seguridad corporativa que está presente en cada uno de los tramos de responsabilidad de las diferentes áreas de una empresa.

Cyber Black, dentro de su eslogan que es "inteligencia que protege", define un sistema de gestión de riesgos que involucra prevención (manuales, protocolos, procesos, auditorías), y otra parte que es protección (seguridad física, lógica). Entonces cuando hablamos de este componente que va tomando la experiencia de todas estas generaciones en un nuevo modelo de negocio estamos hablando de Cyber Black, S.A. de C.V., una empresa de seguridad de cuarta generación.

SEA: ¿Cuál es la importancia *de la gestión de riesgos en una empresa?*
LMD: la gestión de riesgos es un proceso para definir las fuentes de peligro, establecer el factor de exposición del cliente al que vamos a hacerle este trabajo, para comprender qué tan expuesto está a esa fuente de peligro y así poder establecer con una matricidad la frecuencia de la amenaza a la que puede estar expuesto y advertir la capacidad de daño que esa fuente de peligro tiene para vulnerarlo con capacidad de daño, o con capacidad de pérdida. Los riesgos pueden ser naturales, tecnológicos o sociales, y hoy en día de salud.

SEA: *¿Cuál es la importancia de pertenecer a AMESP?*
LMD: la Asociación Mexicana de Empresas de Seguridad Privada tiene un espacio para la evolución de todas nuestras empresas con una bandera que es la más importante: profesionalización. Nos permiten aportar, participar hacer certificaciones a través de la red CONOCER. Es un espacio de participación donde hay respeto, convivencia y en la cual soy presidente de la Comisión de Tecnología, trabajando bajo un solo principio: unidos por un México seguro. ■

Fotos: Cyber Black

Para ver la entrevista completa, escanea:

PROTEGE.MX

GRUPO CORPORATIVO DE PREVENCIÓN

XV años

17 años en el mercado
ahora bajo el mando de
Grupo Corporativo de Prevención, S.A.

Armados para el traslado de valores
Armados Intramuros.

- Contamos con la experiencia y la infraestructura necesaria para brindar servicios de calidad.
- Nuestros elementos armados, son monitoreados de forma constante desde nuestro centro de monitoreo las 24 hrs.
- Cumplimos con las leyes y reglamentos que norman a las empresas de seguridad con licencias de portación de armas.

Somos una **empresa especializada** para brindar servicios de personal de seguridad con **portación de armas**

manuelgm@grupogcp.mx / www.grupogcp.mx

55 79316739

Calle Leona Vicario #6 Col. Santa María Tianguistengo,
Cuautitlán Izcalli, Estado de México, C.P. 54710.

LA SEGURIDAD PRIVADA COMO SERVICIO ESPECIALIZADO: REPSE

MÉXICO | Mónica Ramos / Staff Seguridad en América

A partir del 1° de septiembre del presente año, entró en vigor la reforma al outsourcing en México, pasando a ser delito la subcontratación de personal, a excepción de aquellas empresas que presten servicios especializados y cumplan con el registro en el REPSE, por ejemplo, la seguridad privada

La reforma al *outsourcing* en México entró en vigor a partir del 1° de septiembre del presente año, con ella se modificaron ocho leyes más: Ley Federal del Trabajo, Ley del Seguro Social, Ley del Infonavit, el Código Fiscal de la Federación, la Ley del ISR (Impuesto Sobre la Renta), la Ley del IVA (Impuesto sobre el Valor Añadido), la Ley Federal de los Trabajadores al Servicio del Estado, así como la Ley Reglamentaria, con el objetivo de prohibir la subcontratación del personal, a excepción de los servicios especializados como la seguridad privada.

Para ello se creó el Registro de Prestadoras de Servicios Especializados u Obras Especializadas (REPSE), operado por la Secretaría de Trabajo y Previsión Social (STPS), la cual podrá sancionar a aquellas empresas que no cumplan con este requisito u operen en la ilegalidad con multas que van de los 179 mil pesos (8 mil 900 dólares) hasta los 4 millones 480 mil pesos (223 mil dólares), es decir de 2 mil a 50 mil veces la Unidad de Medida y Actualización (UMA).

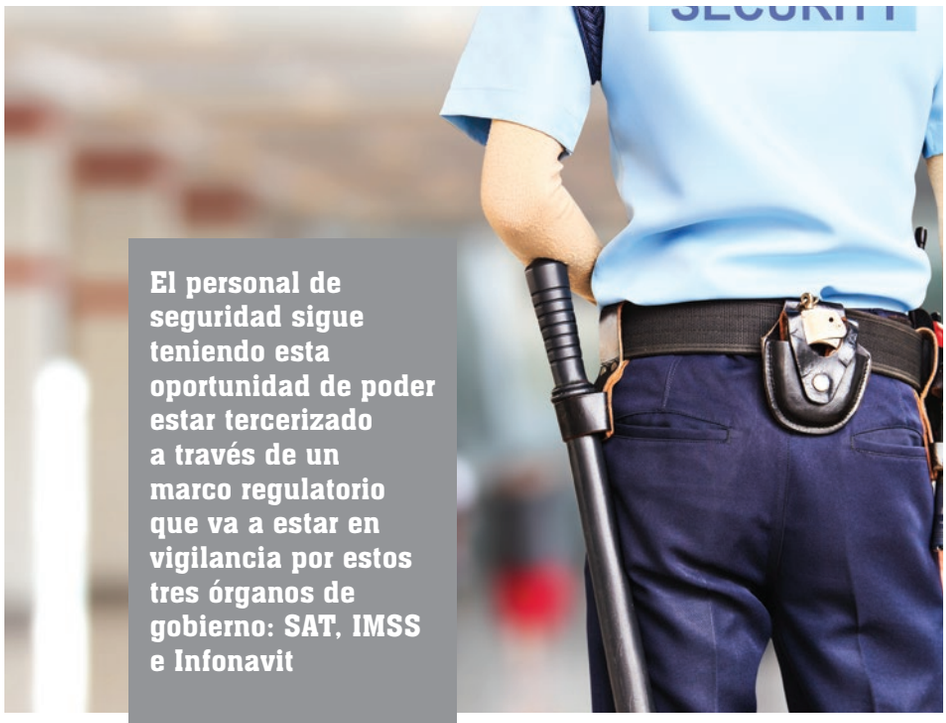
Comedores industriales, empresas de limpieza, de reparación, mantenimiento, jardinería, vigilancia o seguridad, de Salud ocupacional, agencias de diseño, *marketing* y/o productoras de videos, entre otras, entran en la categoría de servicios especializados, pero a su vez deberán estar en orden y con opinión positiva de las tres instancias gubernamentales involucradas en la nueva reforma y respecto a su propio personal: SAT (Servicio de Administración Tributaria), IMSS (Instituto Mexicano del Seguro Social) e INFONAVIT (Instituto del Fondo Nacional de la Vivienda para los Trabajadores).

"En esencia, el *outsourcing* es un esquema de solución para reducir costos de una empresa de manera estratégica o para ser más competente, sin embargo en México y otros países del mundo, se utilizó como una figura para llevar a cabo malas prácticas: evasión de impuestos, informalidad laboral, incumplimiento de los patrones con las obligaciones con el trabajador como seguridad social, salario competitivo y condiciones dignas de trabajo; así como disminución de sueldos, pagos divididos, una parte del salario en un esquema y otro en uno diferente. Es por ello que el gobierno está reestructurando a través del REPSE toda la figura de control que tenían con el *outsourcing*", explicó Mónica Sandoval Arvizu, contadora pública.

SAT
Servicio de Administración Tributaria
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

IMSS

INFONAVIT



El personal de seguridad sigue teniendo esta oportunidad de poder estar tercerizado a través de un marco regulatorio que va a estar en vigilancia por estos tres órganos de gobierno: SAT, IMSS e Infonavit

Foto: Creativeart - Freepik

MODIFICACIONES AL ARTÍCULO 15 DE LA LFT

En esencia, el REPSE es una plataforma que se hace valida a través de la Secretaría de Trabajo y Previsión Social (STPS), para el registro de prestadores de servicios especializados u obras especializadas, y éste nace a raíz del artículo 15 y del artículo 15 A de la Ley Federal del Trabajo:

Artículo 15°	Artículo 15°A
• Las personas físicas o morales que proporcionen los servicios de subcontratación, deberán contar con registro ante la Secretaría del Trabajo y Previsión Social. Para obtener el registro deberán acreditar estar al corriente de sus obligaciones fiscales y de seguridad social.	• El trabajo en régimen de subcontratación es aquel por el cual un patrón denominado contratista ejecuta obras o presta servicios con sus trabajadores bajo su dependencia, a favor de un contratante, persona física o moral, la cual fija las tareas del contratista y lo supervisa en el desarrollo de los servicios o la ejecución de las obras contratadas. a) No podrá abarcar la totalidad de las actividades, iguales o similares en su totalidad, que se desarrollen en el centro de trabajo. b) Deberá justificarse por su carácter especializado. c) No podrá comprender tareas iguales o similares a las que realizan el resto de los trabajadores al servicio del contratante. De no cumplirse con todas las condiciones, el contratante se considerará patrón para todos los efectos de esta ley, incluyendo las obligaciones en materia de seguridad.
• El registro a que hace mención este artículo deberá ser renovado cada tres años.	
• La Secretaría del Trabajo y Previsión Social deberá pronunciarse respecto de la solicitud de registro dentro de los veinte días posteriores a la recepción de la misma, de no hacerlo, los solicitantes podrán requerirla para que dicte la resolución correspondiente, dentro de los tres días siguientes a la presentación del requerimiento. Transcurrido dicho plazo sin que se notifique la resolución, se tendrá por efectuado el registro para los efectos legales a que dé lugar.	
• La Secretaría del Trabajo y Previsión Social negará o cancelará en cualquier tiempo el registro de aquellas personas físicas o morales que no cumplan con los requisitos previstos por esta ley.	
• Las personas físicas o morales que obtengan el registro a que se refiere este artículo quedarán inscritas en un padrón, que deberá ser público y estar disponible en un portal de Internet.	
• La Secretaría del Trabajo y Previsión Social expedirá las disposiciones de carácter general que determinen los procedimientos relativos al registro a que se refiere este artículo.	

Fuente: Ley Federal del Trabajo (https://www.gob.mx/cms/uploads/attachment/file/156203/1044_Ley_Federal_del_Trabajo.pdf)

OBJETIVOS DEL *OUTSOURCING* (EN EL "DEBER SER"):

- Agilizar actividades de una organización.
- Contar con un socio de negocios que tuviera los conocimientos, recursos, tecnología, y los procesos para ejecutar una tarea de la que adolecía la empresa que lo contratara.
- Asumir tareas de gestión.

Mónica Sandoval Arvizu,
contadora pública

"El artículo 15°A es más preciso respecto a la subcontratación. Sí y sólo sí, el personal podrá ser subcontratado si no es parte del objeto por el cual se constituyó esa empresa. Por ejemplo, si yo tengo una empresa que produce botes de leche, yo no voy a poder utilizar para realizar ese bote de leche personal subcontratado, pero sí voy a poder utilizar para vigilar el turno de la noche un personal subcontratado. Entonces el personal de seguridad sigue teniendo esta oportunidad de poder estar tercerizado a través de un marco regulatorio que va a estar en vigilancia por estos tres órganos de gobierno: SAT, IMSS e Infonavit", indicó la contadora.

A través de la plataforma del REPSE se va hacer un registro ante el SAT, el IMSS a través de su plataforma llamada ICSOE y a través de la plataforma del Infonavit, SISUB, ambas de manera cuatrimestral, para cumplir con todo esto se necesita estar en opiniones positivas con las tres instancias, de caso contrario vendrán las sanciones.

El REPSE se ha convertido en un valor agregado necesario y ya algunas empresas de seguridad privada lo agregan a su portal digital como un plus de sus servicios, beneficio directo para los clientes que desean opiniones positivas de las instancias gubernamentales y así evitar caer en la ilegalidad.

"La seguridad tiene la plusvalía de que siempre ha sido un objeto tercerizado, perteneciente a un *outsourcing* táctico, no han estado dentro del objeto de negocio de las empresas, sin embargo sus clientes sí van a tener que estar al margen de la ley si desean tercerizar esa mano de obra y si quieren seguir teniendo ese objeto de negocio, porque quienes lo ignoren tendrán repercusiones, tanto el subcontratante como el contratista. Nadie va a querer tirar su dinero a la basura, por una deducción que no va a ser válida", señaló.

En el caso de las empresas de seguridad privada que tengan a sus empleados en *outsourcing* van a tener que agregar "mayor normatividad a su desarrollo administrativo", es decir los que estén en malas prácticas y quieran seguir vendiendo su negocio, tendrían que regularizar su situación y una vez regularizada con el número de registro, van a poder seguir vendiendo sus servicios, porque si no, además de caer en un delito, los clientes no podrán deducir esa inversión porque no cumplen con las características requeridas.

BENEFICIOS DEL REPSE

Algunos de los beneficios del REPSE son:

- Regulación de las empresas con el SAT, IMSS, Infonavit.
- Eliminación de la subcontratación (pertenecientes al objeto de la empresa).
- Valor agregado como empresa al estar en regla con la ley.
- Regularización de las prestaciones a los empleados (IMSS, Infonavit).

Foto: Creativeart - Freepik

Si la empresa se encuentra en orden con las tres instancias mencionadas, el REPSE sólo será un trámite administrativo. Pese a que los trabajadores pasan al esquema de seguridad social propio, no influye en la igualdad de sueldos o la dignificación de los trabajadores.

"El REPSE, está más enfocado —tristemente— a un tema de fiscalización del SAT, porque no hay forma de igualar si está directamente contratado o no, entonces no viene a subsanar esa dignificación de salario por habilidades iguales, viene solamente a sumar a la fiscalización y que eso de manera cualitativa no se refleja en la remuneración al trabajador, lo único que van a lograr si quieren seguir vendiendo su servicio es que los trabajadores vayan al corriente con IMSS e Infonavit", finalizó Mónica Sandoval.

El gobierno incrementó de mil a mil 500 inspectores para vigilar que estas medidas se cumplan. ■

El *outsourcing* es un esquema de solución para reducir costos de una empresa de manera estratégica o para ser más competente, sin embargo en México y otros países del mundo, se utilizó como una figura para llevar a cabo malas prácticas

REFERENCIAS

- *Secretaría de Trabajo y Previsión Social (REPSE) https://repse.stps.gob.mx/*
"Reforma sobre Ioutsourcingl: 7 puntos para entenderla. El Financiero, 30/08/2021 https://www.elfinanciero.com.mx/economia/2021/08/30/reforma-sobre-outsourcing-7-puntos-para-entenderla/
"¿Qué empresas deben registrarse en REPSE? Alcon, 28/07/2121 https://www.alconmx.com/que-empresas-deben-registrarse-en-repse/

Para ver la entrevista completa, escanea:

GRUPO EMPRESARIAL CASA

SEGURIDAD PRIVADA

PROFESIONALES DE LA SEGURIDAD A SU SERVICIO

CUSTODIA

INTRAMUROS

CONSULTORÍA

SEGURIDAD PRIVADA | INTRAMUROS

www.gecsa.com.mx

info@gecsa.com.mx

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

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

www.twitter.com/gecsa

www.facebook.com/gecsa

www.youtube.com/gecsa

LAS NUEVAS TENDENCIAS EN HORAS LABORALES PARA OFICIALES INTRAMUROS

Las empresas de seguridad privada deben cuidar a sus oficiales, es importante poner atención a las jornadas laborales extenuantes a los que se exponen y mejorar sus condiciones de trabajo

MÉXICO | Adhaf Raúl Hatem López

Tradicionalmente el gremio de la seguridad privada intramuros (armados y no armados) ha tenido una tendencia donde los horarios laborales son extraordinarios y difíciles de cubrir con la efectividad laboral que se requiere, en México y con tendencia en la mayor parte de Latinoamérica es muy común encontrar que los proveedores de seguridad ofrezcan y los usuarios les pidan oficiales en turnos de 24 x 24, esto quiere decir que un oficial labora 24 horas y descansa las siguientes 24 horas —trabaja la mitad del tiempo— o en turnos de 12 x 12 con un día de descanso a la semana (sin considerar los tiempos de traslado hogar – puesto de trabajo) prácticamente también trabaja la mitad del tiempo.
Estas condiciones laborales tienen diversas dificultades y sobre todo riesgos, en las que destacan el factor salud del personal que labora estas jornadas, el factor salarial y horas de trabajo marcadas en la Ley Federal de Trabajo (siendo permitidos por contratos de horarios extraordinarios), adicionando un bajo rendimiento y gran riesgo que provocan estas jornadas.

CONDICIONES DE SALUD

La falta de sueño y el no acostumbrar a que nuestro cuerpo tome por lo menos ocho horas de descanso diario puede provocar estrés, ansiedad y factores irreversibles como padecimientos cardiacos y endocrinológicos, provoca enfermedades como Alzheimer y demencia senil, el índice de masa corporal es un 3.6% superior a la media, según estudio de un equipo de investigación de la Universidad de Stanford (Estados Unidos). Esto sumado a que disminuye la capacidad cognitiva del cerebro y afecta la capacidad de atención, la memoria y su retención, sin duda alguna contraproducente y de alto riesgo de salud para la labor y actividades que se les encomienda.

EN LAS CONDICIONES DE LEGALIDAD

Dando paso a los cálculos salariales, son muy pocas las empresas que generan una nómina con salario y paguen tiempo extra en horas dobles y triples, aunque hay una vía legal ante estas jornadas (contratos colectivos de horas extraordinarias), lo cual permite que se puedan laborar con un excedente de horas.

Pero en la ley fuera de estos contratos extraordinarios, sí estipula el cómo debe pagarse, la Ley Federal del Trabajo indica que la jornada diurna es de ocho horas diarias (48 horas a la semana), la nocturna de siete horas diarias (42 horas a la semana) y si es mixta 7.5 horas diarias (45 horas a la semana), después de este máximo de horas las siguientes se deben pagar como horas dobles (las siguientes tres horas diarias por un máximo de tres días a la semana, nueve horas a la semana extra), pasando este máximo de horas, las siguientes que se laboren deberán pagarse por tres (triples).

Foto: Creativeart - Freepik

Para este año 2021, el salario mínimo se estipuló en 141.70 pesos (6.90 dólares), haciendo un pequeño ejercicio con esa base, un oficial que trabaja en turnos de 24 x 24, una semana puede estar en turno efectivo hasta 96 horas y la siguiente semana labora 72 horas, con estos datos, podemos calcular lo siguiente: como la labor es mixta (jornadas diurnas y nocturnas, 7.5 horas) podríamos ajustar las siguientes cantidades con base en el salario mínimo:

- Salario mínimo 141.70 pesos (6.90 dólares) por ocho horas.
- Hora de trabajo (mixto de 7.5 horas al día) por 18.89 pesos (0.92 dólares).
- Hora doble de trabajo por 37.78 pesos (1.84 dólares).
- Hora triple de trabajo por 56.67 pesos (2.76 dólares).

Una jornada de 24 horas continuas está formada por:

- Salario diario por ocho horas 141.70 pesos (6.90 dólares).
- 3 horas extra (pagadas al doble) de 1 día 113.34 pesos (5.52 dólares).
- 13 horas extra (pagadas al triple) de 1 día 736.71 pesos (35.88 dólares).
- Total de 991.75 pesos (48.30 dólares) por una jornada de 24 horas.

La semana que labora un 4° día todas las horas extras serán pagadas al triple, ya que excedimos de los primeros tres días tres horas extra, por lo que incrementa a 1,048.42 pesos (51.04 dólares) por una jornada de 24 horas con un 4° día laborado. Teniendo en cuenta que en turnos de 24 x 24 un oficial labora una semana tres días y otros cuatro días:

- Semana que labora tres días 24 horas debería pagársele 2,975.25 pesos (144.88 dólares) a la semana.
- Semana que labora cuatro días de 24 horas debería pagársele 4,023.67 pesos (195.95 dólares) a la semana.

Considerando un promedio anual de 52 semanas entre 12 meses nos resultan 4.33 semanas promedio al mes, bajo esta ecuación: pago promedio a cada oficial son 3,499.46 pesos (170.42 dólares) a la semana y 15,152.66 pesos (737.89 dólares) al mes y esta cantidad es calculada sin considerar otros pagos como días de descanso obligatorio (7° día) prima dominical, los gastos de impuestos (ISN – Impuesto Sobre Nómina, SAT - Servicio de Administración Tributaria, IMSS - Instituto Mexicano del Seguro Social, INFONAVIT - Instituto del Fondo Nacional de la Vivienda para los Trabajadores, AFORE - Administradora de Fondos para el Retiro, etc.), bonos, subsidios, uniformes, proporcionales de aguinaldo, vacaciones, incapacidades, gestión operativa y administrativa de la organización correspondiente, prorrateo de permisos y autorizaciones locales, federales de diversas entidades de gobierno, registros, entre otros gastos. En este ejemplo sólo se considera el pago de horas trabajadas de forma efectiva.
Este mismo ejercicio, pero dando un máximo de 60 horas diarias en turnos de 12 x 24 o 12 horas de labor por cinco días y dos días de descanso, así como se generan nueve horas dobles y sólo tres horas triples a la semana.

En un uso correcto de las horas establecida en la LFT (Ley Federal del Trabajo), donde nos indica una jornada de ocho horas, con un día de descanso, bien podríamos decir que lo correcto sería contratar a 3.5 oficiales para cubrir las 24 horas del día en tres turnos de ocho horas diarias (con un día de descanso) y las 48 horas a la semana sin horas extra, y esto nos daría con "salario mínimo" un pago semanal de 987.00 pesos (48.10 dólares) y mensual de 4,273.71 pesos (208.24 dólares) sin considerar todo lo observado en el párrafo anterior.

La falta de sueño y el no acostumbrar a que nuestro cuerpo tome por lo menos ocho horas de descanso diario puede provocar estrés, ansiedad y factores irreversibles como padecimientos cardiacos y endocrinológicos, enfermedades como Alzheimer y demencia senil, el indíce de masa corporal es un 3.6% superior a la media

Foto: Creativeart - Freepik

CONDICIONES DE RENDIMIENTO Y RIESGOS

También es una luz de alerta que nos puede provocar riesgos y pérdida considerable o irreversible, imaginemos que un oficial esté encargado de revisar un acceso y hacer rondines cada hora de un área donde existe equipo de alto valor, desde el inicio de su jornada hasta la hora 10 lo hace sin afectación, atraso o imposibilidad alguna, pero en las horas subsecuentes va mermando su capacidad de atención, de concentración y reacción, quedándose dormido a la hora 20 de jornada continua y esto provoca que no dé su rondín, teniendo una intrusión y robando el equipo de alto valor, sube el nivel de riesgo, cuando llega su relevo a la hora 24 detecta que no ha revisado ni dado rondines en las últimas cuatro horas, y lamentablemente el robo ya se consumó, esto provocará una afectación económica a la organización del cliente.

En un caso extremo esta falta de concentración y atención puede provocar que un conato de incendio no se atienda a tiempo provocando el riesgo más grande que existe, la eliminación por incendio del inmueble y el de mayor valor, la vida del oficial. ¡Los riesgos de estas jornadas son muchos y los beneficios no existen!

La nueva tendencia es generar esta conciencia en los usuarios y compradores de servicios de seguridad privada intramuros para que éstos de forma justificada soliciten o autoricen el gasto acorde a lo necesario, y de lado de los proveedores no abaratar a costa de realizar malas prácticas y en prejuicio de los empleados, adicional a esto proponer soluciones integrales como: integrar por lo menos una posición más para una cobertura 24/7 y acomodar al personal solamente en turnos de 12 horas, puede ser turnos de 12 x 24 o de 12 horas con dos días de descanso a la semana, compartiendo horas mixtas y bajando el costo de horas triples, adicionando un mejor y mayor descanso para los oficiales, mejorando calidad de vida personal y familiar, en este esquema se genera un máximo de días laborados de cinco y de 60 horas a la semana. Realizar un estudio de posiciones necesarias y certificar actividades de acciones remotas, en las cuales una persona podría controlar dos o más posiciones, teniendo apoyo de cámaras para identificación de personal, aperturas remotas, bocinas de información e instrucción, sensores de movimiento, con ellos eliminamos el riesgo de contacto físico y elevamos el control tecnológico, documental y la administración de riesgo, teniendo la posibilidad de estar al pendiente de más de un punto fijo vía remota.

La falta de sueño y el no acostumbrar a que nuestro cuerpo tome por lo menos ocho horas de descanso diario puede provocar estrés, ansiedad y factores irreversibles como padecimientos cardiacos y endocrinológicos, enfermedades como Alzheimer y demencia senil, el índice de masa corporal es un 3.6% superior a la media

Foto: Creativeart - Freepik

EN CONCLUSIÓN

Un esquema donde se trabaje un máximo de 60 horas (12 x 24 o 12 x 12, cinco de siete días a la semana) o mejor aún, un máximo de 48 horas (tres turnos diarios de ocho horas con un día de descanso a la semana) a diferencia de uno donde se trabaje un máximo de 96 horas (24 x 24) no debería ni siquiera tener un incremento de costos considerable, ya que las horas triples bajarían de forma semanal hasta en un 73% y prácticamente de estas horas extra sale un salario para la tercera o cuarta posición propuesta.

Además de que las condiciones de salud mejoran de forma física y mental, los tiempos de esparcimiento, recreación y vida familiar provocan un mejor rendimiento laboral, esto se verá reflejado de forma inmediata en la mejora de concentración y aplicación de actividades a realizar, controlando el riesgo de omisión de consignas, actividades y observación, obteniendo oficiales con retención y atención de sus labores tradicionales.

Sólo hagamos conciencia de la base de la pirámide de todo un sistema de seguridad, los oficiales. Las organizaciones y usuarios debemos cuidarlos, capacitarlos y desarrollar las mejores prácticas, para tener personal con buenas condiciones laborales repercutiendo en una mejora continua en todos los aspectos. ■

Adhaf Raúl Hatem López,
CEO de MEXSEPRO.

Más sobre el autor:

Promoción 50% de descuento

Renta de Suburban blindada con chofer $8,500 pesos por día.

*Costo más IVA. Sólo aplica para servicios en CDMX y área metropolitana. No incluye gasolina.
El servicio por día es por 10 horas máximo. Promoción válida hasta el 31 de diciembre de 2021

Renta de blindados

Nivel III

20 Aniversario COLEMAN

www.rentadeblindados.com.mx

Tel. 55 5572 6005 Cel. 55 7672 4992

krauda@seguridadenamerica.com.mx

RENTA DE BLINDADOS

COLEMAN

SEGURIDAD EN LA INDUSTRIA HOTELERA

Foto: Creativeart - Freepik

El sector de hotelería y turismo incluye empresas como hoteles, agencias de viajes, operadores turísticos y diversos tipos de empresas relacionadas con el ocio, como campos de golf, entre otros. Lo que todas estas empresas tienen en común es que operan amplios espacios con numerosos visitantes en movimiento. El servicio es una prioridad, y la base de un buen servicio comienza con una buena seguridad[1]

MÉXICO

Erick Martínez / *Staff* Seguridad en América

Cuando una persona o un grupo de personas (ya sean familias) deciden alojarse en un hotel por cualquiera que sea el motivo, muchos dan por hecho que la institución ha realizado todas las acciones necesarias para mantener seguro a sus huéspedes, pues en teoría cuando se busca un alojamiento por motivo turístico o de negocio la seguridad será un factor para decidir alojarse ahí. "Sin seguridad no puede haber comodidad", así lo estima Vicente Ignacio López de Miguel, presidente de AESET (asociación dedicada a la consultoría de seguridad especializada en establecimientos hoteleros), que explica que hasta hay empresas, principalmente en Estados Unidos, que antes de alojar a sus empleados en un determinado hotel se informan de las medidas de seguridad con que cuenta éste.[2]

La seguridad en la industria hotelera tiene muchas vertientes y formas de gestionarla, es un abanico de actividades cuyo fin último es la integridad, primero de las personas y luego de las instalaciones. Al diseñar un proyecto de seguridad integral en un hotel, es imprescindible llegar a un compromiso entre las dos facetas materiales y personales.

Un sistema de seguridad ha de cumplir cinco puntos considerados básicos: prevención o disuasión, detección y alarma, reconocimiento e identificación, retardo y reacción.

Héctor Gerardo Ramírez Reyes, gerente de Prevención y Control de Riesgos de Grupo Presidente, abrió una reflexión sobre los cambios en el comportamiento y exigencias en los clientes en tiempos de COVID-19 en la industria hotelera, y cómo afectan en la percepción del riesgo de la seguridad.

La continuidad de negocio sólo es y será posible para quienes tuvieron un buen plan de manejo de crisis, sin él era "imposible" poder sostener las operaciones, y más en zonas como la Ciudad de México, que comprende a los viajeros de negocios, al contrario de hoteles de playa que son en su mayoría viajes de placer. "Hoy en día es mucho más alta la oferta, y muy poca la demanda", afirmó Héctor Ramírez.

"El *travel manager* debe saber qué hacer si hay una crisis donde viajan los colaboradores, si alguno de ellos está potencialmente afectado, conocer el hotel donde se hospeda y la ciudad. Esta información está sincronizada con los datos que identifican o a los viajeros afectados", **Adolfo Márquez**

LA PERCEPCIÓN DE LA SEGURIDAD EN LOS HOTELES

Derivado de la pandemia, las recomendaciones y regulaciones sanitarias de la Secretaría de Salud en México, se adaptaron para poder otorgar servicios en hoteles, salones y restaurantes, por lo que resultó en el rediseño de los procesos, elaboración de planes diferentes, nuevos esquemas de capacitación, nuevos métodos para la retención del cliente.

Entre 2019 y 2020 todos se enfocaron en la seguridad de los clientes, empleados, instalaciones, finanzas, información, planes estratégicos, aplicación de estándares y cumplimiento legal. Mientras que el cliente busca nuevas experiencias auténticas desde una perspectiva local, con una mejor relación precio calidad, poder promover sus políticas de sustentabilidad y responsabilidad social.

Aunado a ello también se suma que los nuevos clientes buscan la seguridad sanitaria que ofrece el destino, las enfermedades locales que existen en el lugar, la coordinación que existe entre el lugar en donde se hospedarán y la capacidad de atención médica de la zona, y también alternativas de viaje por menos dinero sin sacrificar calidad.

"Hoy en día, dentro de nuestra matriz de riesgo debe encontrarse la confianza del cliente", enfatizó Héctor Ramírez. Hay temas que se deben tener en la mira con anticipación, no sólo por algún robo, extravío de bienes, sino por la experiencia que tiene que ver con la seguridad, y un especial cuidado en la responsabilidad de control para mantener dentro la confianza del cliente.

IMPLEMENTACIÓN TECNOLÓGICA

Tras la implementación de tecnología para mejorar la experiencia del cliente, los lineamientos y filtros de seguridad sanitaria, los cuales representan un gasto "no contemplado", no debe haber preocupación por dónde va a salir ese dinero, pues es donde se reconoce a una empresa por una buena gestión de crisis, la que pudo resolver en el momento que fue necesario. Por ello es que surgen nuevos lineamientos de organizaciones nacionales e internacionales, las cuales desarrollan protocolos y certificaciones para garantizar que los espacios de turismo sean seguros.

La innovación tecnológica dependerá de tres actores: fabricante, usuario final e integrador, y por consiguiente una buena relación entre los tres. Las herramientas digitales no son universales, cada una es para un sector en específico con sus necesidades particulares, no innovar tecnológicamente, hará que dejen de ser competitivos y por consiguiente se perderán oportunidades.

La tecnología, si bien resultó ser un gran aliado para mejorar la seguridad de los hoteles, también surge el cuestionamiento sobre si no se está ahora más vulnerable por ciberdelincuentes, pues así como la tecnología avanza, la delincuencia se actualiza, e invierte en herramientas tecnológicas para seguir penetrando en la seguridad.

Previo a decidir sobre la tecnología que se requiere debe de quedar claro que antes de hacerlo, cada hotel tiene particularidades, dependen de las zonas, las necesidades, el clima, los

"Son 50 llamadas de extorsión que se reciben a la semana y para ello se debe capacitar a la gente y al personal en cuanto a protocolos y seguimiento de actuación ante este importante tema", **Adolfo Márquez**

Foto: Creativeart - Freepik

"Una planificación adecuada hace la diferencia entre la recuperación y la desaparición de una empresa", **Héctor Ramírez**

clientes, y cada uno satisface ciertas necesidades. Por ello se debe trabajar con base en una matriz de riesgos, análisis de riesgos, plan de gestión de riesgos, plan de gestión de crisis, de continuidad del negocio y Plan de Recuperación ante Desastres (DRP) para los servicios de Tecnología de la Información. Si no lo hace apoyado en lo anterior la administración de la gestión no puede ser muy buena, y también habrá que considerar si los cambios son necesarios, si es rentable, el costo, el riesgo y qué tanto se puede depender de esa tecnología.

¿QUÉ APRENDIMOS DE LA PANDEMIA?

Todos nos enfrentamos a factores internos y externos que pusieron en duda el cumplimiento de las metas y objetivos de las compañías. "Hoy después de más de un año iniciada la pandemia, podemos asegurar que la participación entre la alta dirección y la parte gerencial, equilibra la manera en que se gestiona una crisis, organizando todos los niveles de la compañía", aseguró Héctor Gerardo Ramírez Reyes.

Además, mencionó que se tendrá que seguir estudiando los contextos externos e internos, incluido el comportamiento humano y los factores culturales, más ahora con los cambios en el comportamiento social que nos deja la pandemia.

El sector hotelero presenta particularidades y retos estratégicos que requieren un análisis de carácter muy específico, por lo que trabajar sobre los análisis de riesgos, y balancear adecuadamente los recursos humanos, tecnológicos estructurales y administrativos, permite anticiparnos, nuestras estrategias deben sumar valor al trabajo de los responsables del área de Seguridad. "Una planificación adecuada, hace la diferencia entre la recuperación y la desaparición de una empresa", mencionó Héctor Gerardo.

DUTY OF CARE

La estabilidad social, económica y política en un marco globalizado hace que los viajeros se enfrenten a diferentes amenazas en sus desplazamientos como el contagio de COVID-19, la delincuencia, extorsiones, etc., y esto lo enfrenta la Seguridad.

Adolfo Márquez Peñalva, director de Seguridad Corporativa para México y Latinoamérica de City Express Hoteles, define el *duty of care* como "la obligación moral y legal de la empresa de tomar medidas para garantizar la seguridad de los viajes de negocios de sus empleados, mientras que la gestión de riesgo se refiere a la aplicación concreta de estas medidas".

Existen múltiples lugares de alto riesgo que deben ser evitados y en el caso de no ser posible existen recomendaciones y consejos para evitar ser víctimas de algún delito:

- No llevar logo de empresa visible, aunque puede ser una estrategia de *marketing* también puede poner en riesgo al agente de viajes.
- No dar información personal, viajar al sitio destino únicamente, informar sólo a la familia detalles del viaje y a pocos compañeros de trabajo sobre los detalles de éste.
- Evitar entrar y salir de hotel a las mismas horas y ser aleatorio en las entradas.
- Vestir un atuendo adecuado y adaptado entorno del país destino.

"El *travel manager* debe saber qué hacer si hay una crisis donde viajan los colaboradores, si alguno de ellos está

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

potencialmente afectado, conocer el hotel donde se hospeda y la ciudad. Esta información está sincronizada con los datos que identifican o a los viajeros afectados", mencionó Adolfo Márquez. Una de las mayores preocupaciones del viajero es la seguridad y la salud, durante la pandemia las centrales de turismo implementaron medidas para operar de manera segura, tanto para viajeros por motivos de trabajo y de placer.

AMENAZAS

En 2017, según cifras del Secretariado Ejecutivo, los secuestros virtuales en la Ciudad de México son agentes foráneos con reservación previa, los extorsionadores realizan llamadas al teléfono fijo para confirmar que es la posible víctima. Durante la pandemia continuaron las extorsiones, aunque en principio algunos hoteles sólo otorgaron servicio para alojar personal médico, e incluso ellos fueron víctimas. "Son 50 llamadas de extorsión que se reciben a la semana y para ello se debe capacitar a la gente y al personal en cuanto a protocolos y seguimiento de actuación ante este importante tema", comentó Adolfo Márquez.

Otro de ellos son los secuestros virtuales, entendido como una modalidad de extorsión telefónica, la cual se ha convertido en un delito que aumenta su comisión en fines de semana y temporada vacacional. Para su ejecución, los delincuentes logran que la víctima que eligieron al azar salga de su domicilio o del hotel donde se encuentra hospedada a través de engaños, vía telefónica. Si no se sabe dónde está el CEO (*Chief Executive Officer*), puede haber extorsiones de negocio al detectar horarios donde no están los responsables.

Cuando sale de viaje el CEO es importante conocer los *modus operandi* existentes y en tendencia. Para tener el control de la situación, le solicitan trasladarse a algún sitio específico (hoteles o lugares públicos) y le exigen apagar su celular para limitar la comunicación con sus seres queridos o con las autoridades.

Durante el tiempo en el que la víctima se encuentra incomunicada, los extorsionadores realizan llamadas a los familiares argumentando un supuesto "secuestro" con el objetivo de conseguir lo más pronto posible el pago del "rescate", el cual obtienen mediante depósitos bancarios o en tiendas de conveniencia.

GESTIONAR LA SEGURIDAD DEL VIAJERO

El responsable de los viajeros de negocio debe dar seguimiento desde el punto de destino al punto final, donde indique el hotel, restaurante que estuvo, todo el itinerario del colaborador, asociado o principal. Asistencia 24/7, localización y aplicación móvil para el viajero de negocios, que sepa trasladarse y conocer los riesgos de la localidad.

Disponer de un *call center* de la misma empresa o a través de la agencia organizadora del viaje, para resolver cualquier problema del empleado en el momento que lo requiera. Este tipo de asistencia debe disponer de toda la información acerca del miso: situación, estancia, vuelo, etc. Contar con un sistema de seguimiento del viajero, mediante sistemas de localización, que ayuden a saber dónde está el empleado a cualquier hora del día y en cualquier lugar, apoyado de uso de aplicaciones especializadas en gestión de viajes.

LA PERCEPCIÓN DE VIAJERO DE NEGOCIOS

La Asociación Global de Viajes de Negocio (GBTA, por sus siglas en inglés) realizó una encuesta a viajeros de Estados Unidos y Reino Unido; estos fueron los resultados:

- 80% piensa que su empresa tiene la obligación legal de garantizar su seguridad mientras viaja al extranjero por negocios.
- 54% no tiene un número de teléfono de contacto específico para usar en una crisis en el extranjero.
- 52% considera emprender acciones legales si no recibieran el apoyo adecuado.
- 46% trabaja para empresas sin políticas claras de seguridad en viajes.
- 36% tiene poca confianza en que su empresa proporcione información correcta durante emergencias en el extranjero.

Para Adolfo Márquez los puntos a considerar en un programa de gestión de riesgos para viajeros de negocios y placer: políticas y procedimientos como lo más importante, que se cuente con una buena política de gestión del riesgo en viajes y procedimientos claros en los desplazamientos. Evaluación de riesgos, información de riesgo, mitigación de riesgo, seguimiento de riesgo, respuesta, notificación, gestión de la información y comunicación. ■

REFERENCIAS

[1] *https://www.securitas.com.mx/Soluciones-de-Seguridad/segmentos-de-mercado/hoteleria-y-turismo/*
[2] *https://www.hosteltur.com/129490_seguridad-hoteles-aproximacion.html*

CAMINO DE LA C-SUITE

Educación ejecutiva para directores de Seguridad

Foto: Creativeart - Freepik

ESPAÑA | Juan Muñoz

Conceptos como el valor añadido o la ventaja competitiva no son habituales entre los responsables de seguridad corporativa. Pero en realidad son críticos para la plena integración de estos departamentos en la vida de las organizaciones constituyendo un pilar de sus estrategias e incluso para participar en el diseño de éstas. Es aquí donde la educación ejecutiva resulta una herramienta imprescindible para conseguirlo. En la era pos-COVID-19 esta va a ser una condición *sine qua non*.

4 ASPECTOS A CONSIDERAR

Leyendo un antiguo artículo de McKinsey titulado "Repensando el papel del estratega"[1], me vino a la cabeza llevar a cabo este mismo ejercicio aplicado en el caso de los responsables de seguridad corporativa, los denominados CSO's (*Chief Security Officer* o directores de Seguridad), cuyo acronismo en inglés es igual al de los *Chief Strategist Officers* o directores de Estrategia. Muy interesante por cierto la clasificación de estos últimos en cinco arquetipos compatibles y perfectamente extrapolables a los primeros: el arquitecto o constructor de ideas, el motivador o gestor de proyectos, el visionario o innovador, el superviviente y el gestor de fondos y recursos.

Para ello he tomado en consideración cuatro aspectos que considero de interés. **El primero,** es el crecimiento del alcance de la seguridad corporativa derivado del aumento de las responsabilidades directas y/o compartidas y de la forma de actuación, lo que ha conllevado un cambio en los perfiles, los conocimientos y las habilidades requeridas para los profesionales que la desempeñan. No es atrevido afirmar que esta función es una de las que más ha cambiado en los últimos 10 años, empezando por adquirir un enfoque más holístico, y que hoy en día la gestión de riesgos de todo tipo (antiguos, nuevos y previsibles de acuerdo con la rápida evolución del escenario) se ha convertido en una variable determinante en las operaciones de las empresas.

Junto con la seguridad corporativa tradicional, y no me refiero al obsoleto modelo 3G (*guards, gates and guns* o vigilantes, accesos y armas), hablamos ahora también de la gestión de riesgos (muy vinculada a los seguros), de la gestión de crisis, de la inteligencia empresarial y de la continuidad de negocios, como las principales, pero donde podría añadirse partes de cumplimiento normativo, por ejemplo. Como consecuencia de este proceso la seguridad pública y la seguridad privada se han ido alejando con dos enfoques cada día más diferentes. El paso de la primera a la segunda requiere ahora más que nunca un claro proceso de transición, formación y adaptación para adquirir los nuevos conocimientos requeridos, lo que todavía muchos no están dispuestos a aceptar. Además, no todos valen, como en el pasado.

El segundo componente está relacionado con el primero y se trata de la familiarización con las tecnologías de la información y en general con el ámbito STEM (Science, Technology, Engineering and Mathematics), vital para todos los ejecutivos actuales incluyendo por supuesto los de seguridad corporativa. Este interés ya fue identificado en el informe de la Universidad de Phoenix y la ASIS Foundation publicado en 2015 con el titulo de "Los riesgos de seguridad en las empresas: competencias de sus profesionales"[2].

> Con un análisis superficial de la composición de una C-Suite estándar está claro que no pueden formar parte de ella varios directores relacionados con la gestión de riesgos, aunque sea ésta ahora una variable determinante, y que tarde o temprano uno de ellos va a responsabilizarse de representar el modelo es ese órgano de dirección

Foto: IE Business School

Esta importancia no viene sólo derivada de la convergencia entre la seguridad física y la seguridad lógica, sino también por el impacto de la tecnología en otros muchos aspectos de la seguridad corporativa. Junto con el conocimiento STEM, el informe destaca el ERM (Enterprise Risk Management), ahora ESRM (Enterprise Security Risk Management), el liderazgo y las habilidades de comunicación, el pensamiento estratégico y anticipatorio, y la educación ejecutiva con un acento especial en la vertiente financiera.

Estas cinco forman las competencias fundamentales necesarias para los responsables de seguridad. Lo cierto es que la convergencia entre la llamada seguridad física y la seguridad lógica es un proceso imparable y aquellos que no puedan adaptarse, en especial los procedentes de la primera, tienen pocas capacidades de liderar el modelo integrado e incluso de sobrevivir en el futuro cercano.

El tercer componente también esta relacionado con el primero. Es una ambición muy razonable de los responsables de Seguridad la de formar parte del C-Suite (comité de Dirección) de sus organizaciones, lo que es no es fácil, o al menos estar muy cerca de él reportando directamente a algún director que sí forme parte de este grupo selecto.

Formar parte o estar próximo para conocer en profundidad la estrategia de sus organizaciones y en un escenario perfecto participar activamente en su diseño e implementación. Lo que muchas veces se denomina alinear la estrategia de seguridad con la estrategia de la organización. Y otra vez aparece aquí la educación ejecutiva como una herramienta clave para conocer y comunicarse en la misma frecuencia y tener la misma visión con este pequeño grupo de directores bajo cuya responsabilidad está el presente y el futuro de una organización.

> La pandemia SARS-CoV-2 constituye una oportunidad única para el futuro de la función de seguridad corporativa con una dimensión y un enfoque más holístico y también más estratégico

Pero esto no es nuevo. Ya en 1995 la revista *Security Management* publicó un artículo de Ira Sommerson, CPP, titulado "La nueva generación"[3], donde este escribía "los profesionales de seguridad deben expandir sus conocimientos en educación ejecutiva y gestión para cumplir sus responsabilidades e incluso para asumir otras nuevas". Por cierto que este artículo puede considerarse como una referencia y de una visión estratégica poco habitual en nuestra profesión.

Diez años más tarde, en 2005, la consultora británica Demos publicaba el informe "El negocio de la resiliencia: la seguridad corporativa en el siglo XXI"[4], donde el resumen ejecutivo incluía, entre otros, una conclusión de gran interés. Decía que "los departamentos de Seguridad Corporativa debían abandonar la antigua asumpción sobre de donde procedía su legitimidad y poder. Su posición no se apoyaría en adelante en lo que les hacía diferentes con base en sus conocimientos específicos, lo que se denomina la experiencia en seguridad (las llamadas *hard skills*), sino en los conocimientos ejecutivos y las habilidades con la gente (las llamadas *soft skills*), y sobre en todo en su capacidad de comunicación". Para Joseph Ranucci, CPP, "el éxito en la seguridad corporativa va mucho allá de quién eres y se se basa ahora en lo qué sabes"[5].

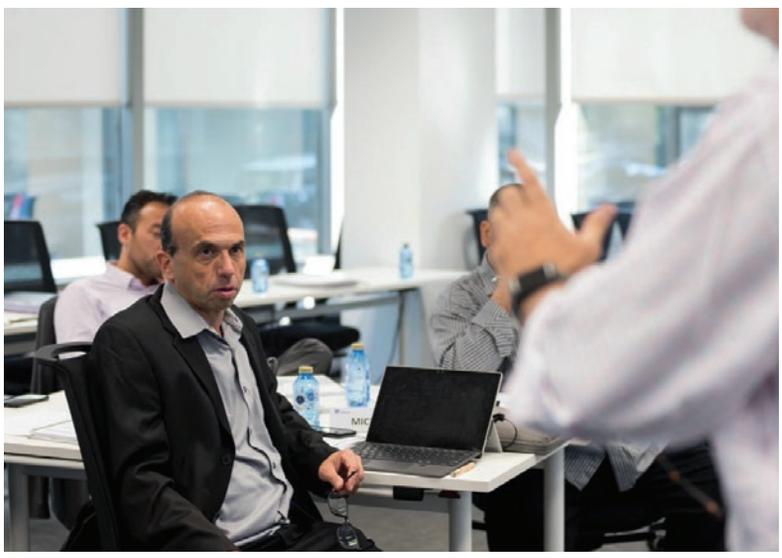


Foto: IE Business School

El cuarto y último componente tiene que ver con el factor humano. La seguridad pública, las fuerzas armadas y los servicios de inteligencia han sido, son y continuarán siendo una valiosa fuente de profesionales de la seguridad corporativa, aunque no son las únicas y además existen diferencias importantes entre los

diferentes países e incluso entre las distintas culturas. Sin embargo, esta situación podría estar evolucionando.

Estas diferencias se repiten en mayor o menor medida para llevar a cabo los procesos de transición necesarios para pasar del lado público al privado, donde el confort y otros criterios juegan un papel fundamental. Todavía hoy muchas empresas no conocen el valor añadido que puede proporcionar una función de seguridad corporativa moderna e integral con un enfoque estratégico, operacional y táctico. Esta situación se repite en el caso de las empresas de selección de ejecutivos, supuestamente en la vanguardia del *know-how* y las tendencias, que siguen centradas en los paradigmas tradicionales.

El deseo o la ambición de los responsables de Seguridad de formar parte o estar lo más cerca posible de la C-Suite ha salido a la luz y todas y cada una de las conferencias de seguridad internacionales en las que he participado en las dos últimas décadas. Cuando hablamos de educación ejecutiva lo hacemos de áreas como las finanzas operativas, la estrategia, la negociación y el liderazgo, pero también de otras añadidas más recientemente como la gestión del cambio, la gestión de proyectos y el modelo Agile, por mencionar algunas.

LOS *CHIEF*

Precisamente este parece el momento ideal para profundizar algo en la C-Suite, que se refiere al pequeño grupo de ejecutivos del máximo nivel que forman parte del comité de dirección de una organización y que se conocen habitualmente por una denominación que comienza por *Chief*. Los más conocidos son el director ejecutivo (CEO), el director financiero (CFO), el director de Operaciones (COO), el director de Recursos Humanos (CHRO), el director de los Sistemas de Información (CIO), el director de Riesgos (CRO) o el director legal (CLO). Además, están el director de Seguridad de los Sistemas de Información (CISO) y el director de Seguridad (CSO), aparte de otros posibles como el director de Estrategia (también CSO). Es conveniente aclarar que no todos los gerentes e incluso los directores de Seguridad pueden ser considerados CSO's.

Con un análisis superficial de la composición de una C-Suite estándar está claro que no pueden formar parte de ella varios directores relacionados con la gestión de riesgos, aunque sea ésta ahora una variable determinante, y que tarde o temprano uno de ellos van a responsabilizarse de representar el modelo es ese órgano de dirección. El consenso parece estar evolucionando hacia aquel de disponga de tres elementos muy importantes y complementarios. Primero, que sea un especialista en alguna de las áreas. Segundo, que disponga de una capacidad de liderazgo adecuada para representar y gestionar a todos los demás. Tercero, y no por ello menos importante, que posea la mejor y más amplia formación y experiencia ejecutiva.

La publicación por parte de ASIS International del estándar del CSO en 2008, y en 2013 de su versión mejorada (CSO.1-2013), constituyó un paso crítico en la revalorización de la seguridad

> La convergencia entre la llamada seguridad física y la seguridad lógica es un proceso imparable y aquellos que no puedan adaptarse, en especial los procedentes de la primera, tienen pocas capacidades de liderar el modelo integrado e incluso de sobrevivir en el futuro cercano

Foto: Creativeart - Freepik

Foto: IE Business School

Basta con analizar las nuevas competencias y habilidades que requieren estos nuevos directores de Seguridad de acuerdo con este estándar para identificar un área de oportunidad inmediata, que es la de la educación ejecutiva

corporativa y su enfoque estratégico dentro de las organizaciones. Basta con analizar las nuevas competencias y habilidades que requieren estos nuevos directores de Seguridad de acuerdo con este estándar para identificar un área de oportunidad inmediata, que es la de la educación ejecutiva. Así lo interpreto ASIS International y fue el origen de la creación de los programas de la Universidad de Warthon en Estados Unidos y de la IE Business School en Madrid (EMSP - *Effective Management for Security Professionals*), el cual tengo el honor de dirigir desde 2015.

Es precisamente el cuadro resumen con las áreas de responsabilidad, las competencias y las habilidades del CSO.1-2013 el que sirvió en su momento para el diseño del programa EMSP, que cada año es revisado y actualizado. Competencias y habilidades que se han articulado sobre cuatro áreas de conocimiento que constituyen el pilar del programa.

Primero la estrategia, para conocer los conceptos básicos y las diferentes herramientas necesarias para desarrollar una mentalidad estratégica y un pensamiento crítico que permita identificar el valor añadido y convertirlo en ventajas competitivas. Después, las finanzas operativas, no sólo para trabajar en conceptos como el ROI (*Return on Investment*) para la construcción de oportunidades de negocio o inversión, sino también para la creación de valor financiero intangible, que lo hay y mucho, bajo el eterno dilema coste o inversión.

En tercer lugar, la negociación como un componente fundamental para alcanzar los objetivos de la organización, pero también en su doble capacidad de influenciar dentro y fuera de ésta. Algunos hablan ya del CIO (*Chief Influential Officer*) como la nueva generación de CSO's. Y en cuarto y último lugar, el liderazgo transformacional que actuá además como enlace transversal entre las cuatro áreas y que se convierte en una tarea compleja cuando se ejecuta bajo el elevado grado de incertidumbre actual y el impacto de los cambios constantes. Un nuevo modelo organizativo cada vez menos jerárquico y tranversal. En resumen, un programa diseñado para convertir a los responsables de Seguridad en líderes más efectivos y mejores para la toma de decisiones.

En mi opinión, la pandemia SARS-CoV-2 constituye una oportunidad única para el futuro de la función de seguridad corporativa con una dimensión y un enfoque más holístico y también más estratégico. Pero no está siendo ni va a ser un proceso sencillo. La realidad de la extrema situación derivada de la COVID-19 ha puesto al descubierto la necesidad vital de la organizaciones de disponer de una estrategia de gestión de riesgos, de resiliencia organizacional, que las permita enfrentarse y sobrevivir a las numerosas incertidumbres del futuro.

Responsables que, con mentalidad estratégica en el contexto empresarial, sepan convertir un modelo de seguridad corporativa en una ventaja competitiva identificando las fases de la cadena de valor donde pueden ser eficaces o imprescindibles y puedan comunicarla en el mismo lenguaje. Que además sepan (conocimientos y habilidades) y puedan (con el apoyo y la concienciación de sus organizaciones) moverse a esos niveles de decisión dentro de las complejas estructuras corporativas tan influenciadas por las cuentas de resultados y los balances de situación.

Es precisamente dentro de este contexto de gestión donde la educación ejecutiva para los profesionales de seguridad, como complemento de sus conocimientos técnicos, constituye el hecho diferencial y un elemento fundamental de la formula para alcanzar el objetivo de sus organizaciones, de sus departamentos y de ellos mismos. Estamos hablando de arquitectos, de motivadores y de visionarios. ■

REFERENCIAS

1. *Rethinging the role of the strategist – Birsham, Gibbs y Strovink – McKinsey – Nov2014.*
2. *Enterprise Security Risks: Workforce Competencies – Phoenix University & ASIS Foundation – 2015.*
3. *The Next Generation – Ira Sommerson – Security Management – 1995.*
4. *The Busines of Resilience: Corporate Security for the 21st Century – Demos – 2005.*
5. *Knowledge check – Joseph Ranucci CPP – Security Management – Oct2020.*

Juan Muñoz,
CPP, CSMP, CSyP F.ISRM, MBA, CEO y Founder en Associated Projects International.

Más sobre el autor:

Para poder prevenir la violencia en el trabajo debemos prestar atención al sistema de creencias de la organización que es la que permite por un lado justificar la violencia y por otro obliga a los miembros a reaccionar de una determinada manera

LA MEDICIÓN DEL CLIMA ORGANIZACIONAL PARA **PREVENIR LA VIOLENCIA EN EL TRABAJO**


Foto: Creativeart - Freepik

ARGENTINA | Juan Manuel Iglesias

En artículos anteriores vimos cómo el clima organizacional hostil era un obstáculo que impedía a los directores y colaboradores extraer los elementos necesarios para satisfacer sus necesidades vitales.

A su vez los valores de masculinidad que impone la sociedad patriarcal influyen muy fuertemente en los directores con "Síndrome de Cronos" determinando muchas veces climas organizacionales desfavorables en donde se emplea la amenaza ante el miedo de despido, las relaciones clientelares y paternalistas, el terrorismo laboral, el acoso y sobre todo el *mobbing*.

Para poder prevenir esta violencia institucional es necesario que los corporativos de seguridad puedan tener una mirada compleja de la situación. Para ello necesitamos recuperar la concepción de la violencia como una totalidad que abarca todas las formas humanas de violencia.

MODELO ECOLÓGICO DE BRONFENBRENNER

La violencia es una Gestalt, es decir parafraseando a Perls, una totalidad, una forma particular en la que se organizan las partes individuales que la constituyen. La violencia en la empresa es entonces una parte de la violencia humana.

Entonces tenemos que observar todos los elementos que componen la totalidad, que como dice Barudy, "todas estas violencias, la organizada, la social, la familiar emergen de sistemas humanos donde no solo existen interacciones y comportamientos violentos y abusivos, sino también un sistema de creencias que permiten al abusador, justificarse o mistificar el abuso de poder y la violencia".

Como veremos ese sistema de creencias se infiltrará en la empresa y formará parte de la "cultura y clima organizacional".

¿Cómo entender esta dinámica? Para ello recurriremos al modelo ecológico de Bronfenbrenner: este modelo concibe al ambiente ecológico como un conjunto de estructuras seriadas y estructuradas en diferentes niveles, en donde cada uno de esos niveles contiene al otro. Del más particular al más general.

- **Microsistema:** es la más cercana a la persona. Tal como describimos en los últimos tres artículos: las experiencias tempranas de maltrato y apego de los gerentes "Cronos", así como los aprendizajes de estrategias de afrontamiento y de contacto con el ambiente, el rol de la familia y la escuela forman parte de este sistema.

- **Mesosistema:** a su vez el individuo pertenece a una familia que está influenciada y en interacción con un sistema más amplio conformado por las relaciones laborales, sociales, recreativas, espirituales de los miembros de la familia con la sociedad. Aquí aparece la empresa como una institución que influye sobre la familia y la familia sobre la empresa.

- **Exosistema:** a su vez la familia y la empresa se encuentran abarcados por un sistema más amplio que incluyen ciertos rituales sociales como por ejemplo la organización del trabajo, la forma de hacer las cosas, de organizar el aprendizaje, etc. Esto influye en la conformación de los elementos de la cultura corporativa y en la percepción del clima organizacional.

- **Macrosistema:** aquí encontramos el sistema de creencias que van a incidir en la cultura corporativa y en la violencia. Por ejemplo, la familia y la empresa absorben los valores patriarcales a partir del proceso de retroalimentación y a su vez aportan elementos que permiten perpetuar esos valores en forma de justificación de la violencia y construcción de representaciones en donde el abuso de poder y el maltrato están legitimados.

IMPOSICIONES PATRIARCALES

Es por ello que para poder prevenir la violencia en el trabajo, además de considerar los factores individuales antes vistos, debemos prestar atención al sistema de creencias de la organización que es la que permite por un lado justificar la violencia y por otro obliga a los miembros a reaccionar de una determinada manera.

A las experiencias de maltrato se suman las imposiciones de la moralidad patriarcal que establece imperativos como:

- El éxito económico es sinónimo de masculinidad.
- El varón debe demostrar fortaleza en todo momento y siempre ganar, lo cual implica que el otro pierda.
- La negociación ganar-ganar es vista como un signo de debilidad.
- Están prohibidos el reconocimiento de necesidades afectivas, así como también la expresión de ciertas emociones como el miedo y la tristeza.
- Todo lo que se considera femenino se debe rechazar porque se lo considera débil e inseguro, sin embargo se busca lo femenino como objeto de conquista, como trofeo.
- Está prohibido pedir y reconocer la ayuda porque es signo de una masculinidad débil.
- Está prohibido expresar el dolor en palabras y llorar.
- No existe un lenguaje adecuado para los sentimientos y emociones, porque se los considera poco importantes.

El modelo ecológico de Bronfenbrenner concibe al ambiente ecológico como un conjunto de estructuras seriadas y estructuradas en diferentes niveles, en donde cada uno de esos niveles contiene al otro

Foto: Creativeart - Freepik

Es por ello que proponemos un modelo de medición de clima organizacional que pueda hacer un relevamiento sobre la existencia o no de estos elementos dentro de la cultura corporativa:

- El estudio consiste básicamente en una (o varias) encuesta(s), que son distribuidas entre los empleados de la empresa o departamento que se desea consultar.
- Puede ser aplicada de forma tradicional o en línea.
- Debe ser confidencial y voluntaria.

¿QUÉ SE MIDE? (ALGUNOS MODELOS DE PREGUNTAS A MODO DE MUESTRA)

1. **Aspectos generales:** ¿Considera usted que la organización es un buen lugar para trabajar?

2. **Objetivos**:
   - Conozco y entiendo la visión y misión de la organización.
   - Estoy satisfecho y comprometido con las directrices estratégicas de mi organización.

3. **Comunicación:** generalmente soy alentado a compartir mi conocimiento/experiencias con los demás.

4. **Equipo de trabajo:**
   - En mi equipo trabajamos juntos para resolver los problemas de la organización.
   - En mi equipo los miembros restantes aprecian mis contribuciones.
   - En mi equipo puedo expresar mi punto de vista, aún cuando contradiga al de los demás miembros.

5. **Oportunidades de carrera:**
   - La organización prepara adecuadamente a sus empleados para que sean promovidos.
   - Mi supervisor(a) me alienta a participar en programas de adiestramiento.

6. **Competencia supervisora:** recibo *feedback* adecuado por parte de mi supervisor(a) sobre la calidad de trabajo que realizo.

7. **Reconocimiento:** los empleados de la organización que tienen un desempeño sobresaliente son reconocidos, etc.

Si como resultado las personas están "muy de acuerdo" o "de acuerdo" en la mayoría de estas afirmaciones, estaremos ante la percepción de un buen clima laboral sin riesgo de creencias y elementos que permitan justificar la violencia. ■

Juan Manuel Iglesias,
magíster en Counseling Educativo, Diplomado en Recursos Humanos y Riesgos Laborales y gerenciador de Seguridad Corporativa.

Más sobre el autor:

LA BUENA COMUNICACIÓN: EL ÉXITO DE UN BUEN PLAN DE GESTIÓN DE RIESGOS

Foto: Creativeart - Freepik

En el ambiente de administración de riesgos la comunicación es fundamental desde el inicio cuando se toma contacto con toda la organización con el fin de identificar todos los procesos, personas, insumos, recursos en general y mediar el grado de involucramiento de la organización en la gestión

PERÚ | Herbert Calderón

La comunicación (del latín *communicatio, -ōnis.*[1]) es la acción consciente de intercambiar información entre dos o más participantes con el fin de transmitir o recibir información u opiniones distintas. Los pasos básicos de la comunicación son la formación de una intención de comunicar, la composición del mensaje, la codificación del mensaje, la transmisión de la señal, la recepción de la señal, la decodificación del mensaje y finalmente, la interpretación del mensaje por parte de un receptor.

La comunicación en general toma lugar entre tres categorías de sujetos principales: los seres humanos (lenguaje), los organismos vivos (biosemiótica) y los dispositivos de comunicación habilitados (cibernética). En un sentido general, la comunicación es la interacción verbal, el contacto con otros seres, y se puede definir como el proceso mediante el cual se transmite una información de un punto a otro (Wikipedia).

Su propósito u objetivo se puede denominar bajo la acción de informar, generar acciones, crear un entendimiento o transmitir cierta idea. Los comunicadores tienen como función entregar información verídica y confirmada por más de tres fuentes. La comunicación es el arte de transmitir pensamientos y es un arte porque une lo invisible con lo visible, lo abstracto con lo concreto.

La única finalidad de la comunicación es recordarle a la mente lo que ha olvidado y lo que ha olvidado es lo único que existe. La comunicación es, por lo tanto, una herramienta que, puesta al servicio de tu profesión, se convierte en el puente hacia la realidad, no sobre las ideas o pensamientos que tenías sobre algo que aparentemente funcionaba bien.

La comunicación asertiva se basa en la honestidad, el respeto, la empatía y la claridad: por lo tanto, consiste en comunicar nuestro punto de vista sobre cualquier asunto de forma clara y totalmente honesta, y defenderlo con firmeza de manera calmada y educada, respetando las creencias y las ideas de los demás. Esto también implica elegir bien el momento de transmitir nuestras ideas. Por lo tanto, para poder comunicarnos de forma asertiva es tan importante lo que queremos decir, la forma en cómo lo decimos y cuándo lo decimos.

Lo cierto es que la comunicación es la trasmisión y recepción de información, indispensable para una gestión de cualquier orden en una organización. En el caso de la conducción de riesgos y la continuidad del negocio, es sumamente importante desde lo más sencillo hasta lo estratégico o más complicado.

En el proceso de identificación de riesgos externos e internos, dependemos mucho de la información ofrecida por los proveedores, clientes, visitas, delincuentes, entorno, organismos públicos y privados, etc.

GESTIÓN E IDENTIFICACIÓN DE RIESGOS

En el ambiente de gestión de riesgos la comunicación es fundamental desde el inicio cuando se toma contacto con toda la organización con el fin de identificar todos los procesos, personas, insumos, recursos en general y mediar el grado de involucramiento de la organización en la gestión.

También en el proceso de identificación de riesgos externos e internos, dependemos mucho de la información ofrecida por los proveedores, clientes, visitas, delincuentes, entorno, organismos públicos y privados, etc. Con respecto a las amenazas a las que puedan estar expuestas las organizaciones como: fraude, sabotaje, accidentes, hurto, cibercrimen, incumplimiento de políticas, desastres naturales, clima laboral, etc.

Luego en la etapa del diseño de sistema de protección, necesitamos involucrar también a toda la organización, con el principio que el sistema protege todos sus recursos de operación, el éxito, la retroalimentación, de las personas involucradas en toda la operación, depende grandemente de nuestro estilo.

Finalmente y lo más importante de todo, el grado de involucramiento o conciencia de todas las personas con nuestro plan estratégico u operativo dependerá de cómo hayamos influido en ellas, y esto nos lleva al tema central, de cómo hemos transmitido nuestras ideas, políticas, planes, objetivos, entrenamiento, alistamiento, resultados y esto es el estilo de comunicación asertiva que utilizamos, la cual si no se da en buenos términos puede producir un fracaso, si se da bien asertivamente produce excelentes resultados, y esto se observa muy rápidamente, se crea una cultura, los empleados se involucran, se crea una conciencia, se logran los objetivos, los recursos son protegidos, los informes llegan de todos los lados.

Muchas organizaciones fracasan por no utilizar un buen estilo de comunicación asertiva, la cual es transmitida y monitoreada desde los más altos niveles y a toda la organización, el éxito consiste en que esa comunicación también se revierte de los bajos niveles a los más altos niveles organizacionales. ■

Foto: Creativeart - Freepik

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

Más sobre el autor:

AUDITORÍA DE SEGURIDAD Y PREVENCIÓN DE RIESGOS

Foto: Creativeart - Freepik

GUATEMALA | Enrique Jiménez Soza

Es un instrumento de gestión que pretende reproducir la imagen fiel del sistema de prevención de riesgos laborales de la empresa con una triple finalidad: valorar su eficacia, detectar las posibles deficiencias que puedan derivar en incumplimientos de la normativa de prevención y adoptar las decisiones precisas para el perfeccionamiento y mejora del sistema

¿EN QUÉ CONSISTE?

La auditoría de seguridad consiste en realizar un diagnóstico de seguridad de la situación actual de seguridad preventiva, operativa y reactiva de un residencial, condominio o complejo industrial. Por medio de este diagnóstico (FODA), se logra determinar las fortalezas, debilidades, amenazas y riesgos del lugar.

Al concluir la evaluación se presenta un informe escrito al contratante; en este informe se incluyen los hallazgos de la evaluación y las recomendaciones a implementar a corto, mediano y largo plazo.

A) OBJETIVOS DE LA AUDITORÍA DE SEGURIDAD

1. **Detectar amenazas internas y externas en las instalaciones.**

2. **Detectar riesgos, actuales y futuros, dentro del sitio.**

3. **Proponer recomendaciones orientadas a:**
   - Proteger la integridad de las personas permanentes y visitantes.
   - Evitar daños a la propiedad inmueble y vehículos locales.
   - Garantizar la normal continuidad de las actividades del lugar.
   - Fortalecer los procedimientos existentes y subsanar las deficiencias detectadas por la auditoría.

4. **Servir de base para desarrollar los planes de seguridad, enfocados en:**
   - Prevención de siniestros y accidentes vehiculares y peatonales.
   - Evacuación de las instalaciones habitacionales y recreativas.
   - Qué hacer en caso de siniestros, desastres naturales y eventualidades amenazantes como robo, asalto, daño, ataque armado y amenazas externas/internas.

B) ÁREAS QUE CUBRE LA AUDITORÍA DE SEGURIDAD

1. **Análisis de la situación actual del área donde se encuentra ubicado el objetivo. El análisis se basa en los siguientes temas:**
   - Delincuencia común y organizada.

- Evaluación de servicios básicos (agua, desagües, alumbrado público, telecomunicaciones, etc.).
- Vecinos, población, proveedores y negocios contiguos.
- Servicios de apoyo e instituciones de rescate y asistencia médica.
- Vías de acceso y rutas de evacuación del área.

C) EVALUACIÓN DE LOS SISTEMAS Y PROCEDIMIENTOS DE SEGURIDAD DEL RESIDENCIAL

1. **Personal de seguridad:**
   - Grupo de seguridad propio o contratado.
   - Organización grupal y supervisión.
   - Actividades de seguridad y vigilancia.
   - Turnos, rondas internas.
   - Equipamiento autorizado, letal y no letal. Uso de radios de comunicación.
   - Cámaras y alarmas de seguridad preventiva.

2. **Seguridad perimetral e interna:**
- **Seguridad perimetral de la lotificación.**
   - Garitas de control ingreso/salidas.
   - Control de visitas y proveedores.
   - Control de acceso del personal de servicio.
   - Sistema de identificación de personal.
   - Puertas peatonales.
   - Control de acceso de vehículos.
   - Sistema de alarma (botón de pánico): robo, asalto, siniestros.
   - Sistema de CCTV (funcionamiento e ubicación en puntos estratégicos).
   - Comunicaciones internas/externas.
   - Alumbrado público.

3. **Seguridad industrial y vehicular:**
- **Señalización adecuada (normas requeridas).**
   - Control de velocidad vehicular.
   - Prevención de accidentes y minimización de riesgos.
   - Medidas de seguridad en áreas de recreación.
   - Utilización de Equipo de Seguridad Industrial.
   - Qué hacer en caso de desastres naturales y siniestros.
   - Primeros auxilios, botiquín y acceso a hospitales cercanos.

4. **Otros riegos por situaciones emergentes:**
   - Desastres naturales: terremoto, incendios, inundaciones.
   - Pánico causado por amenazas telefónicas, extorsiones y otras situaciones.
   - Ciberataques electrónicos.
   - Vecinos, visitantes y residentes “indeseables”.
   - Otros específicos. ■

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Enrique Jiménez Soza,
director general de
I.D.E.A. Seguridad Táctica,
Guatemala, Centroamérica.

Más sobre el autor:

TWCI Y LA SEGURIDAD CORPORATIVA

Two Worlds Collaborative Intelligence (TWCI) ha desarrollado un modelo de colaboración novedoso y adaptado a las necesidades de los clientes, orientado tanto a las grandes como a las medianas y pequeñas empresas, siendo estas últimas las que tienen mayores dificultades para contar con sus propios equipos de inteligencia

ESPAÑA | Jesús De Miguel Sebastián

1) INTRODUCCIÓN

Podría comenzar haciendo un panegírico de la seguridad, en la medida que ésta ha sido y sigue siendo un factor fundamental a considerar, ya sea en su tradicional visión estatocéntrica, ya en su relación con las organizaciones, sean públicas o privadas, pero hoy en día en un entorno nacional e internacional tremendamente complejo e incierto las empresas necesitan más que nunca incorporar la seguridad y la inteligencia a sus procesos, pasando a ser una función transversal que afecta a los diferentes departamentos y/o actividades de la empresa.

Otra cuestión que conviene resaltar en esta introducción es que cuando hablamos de la empresa, en esta palabra incluimos a todo tipo de organizaciones empresariales y evidentemente existen notables diferencias cuando abordamos la seguridad desde una gran corporación que cuando lo hacemos desde una compañía familiar, o más precisamente una pequeña empresa. Esto no quiere decir que las pymes no deban prestar atención a la seguridad, al contrario, éstas se ven afectadas de una manera directa y en ocasiones dramática por los riesgos, incluso en ocasiones de manera más significativa que las grandes corporaciones, las cuales cuentan con más y mejores recursos para moverse en la incertidumbre.

Desarrollar todo lo que significa el concepto de la seguridad excede con mucho de lo que pretendo en este breve artículo, el cual se focaliza en la seguridad

Foto: Creativeart - Freepik

La seguridad es algo que no se improvisa, es un área de conocimiento de muy amplio espectro que precisa una gran preparación. Al igual que a nivel nacional, la seguridad es una de las principales políticas de cualquier organización, en una empresa la seguridad debe estar directamente vinculada a la alta dirección

Foto: Creativeart - Freepik

corporativa u organizacional, y en particular cómo, mediante la aplicación una adecuada herramienta de inteligencia, permite la detección temprana de riesgos de toda índole y, en consecuencia, la anticipación y respuesta temprana a los diferentes desafíos que enfrentan las empresas, especialmente cuando éstas tienen que desarrollar su actividad en mercados internacionales y con ello con un mayor grado de incertidumbre, consiguiendo la anticipación, condición *sine qua non* de un adecuado sistema de seguridad.

2) HABLANDO DE LA SEGURIDAD EN EL MUNDO EMPRESARIAL

Para abordar la seguridad en el mundo empresarial conviene hacer un rápido repaso sobre algunos conceptos básicos sobre ella. En primer lugar, debemos recordar que la supervivencia del objeto a proteger es el fin último de la seguridad.

Pero, ¿qué es lo que define la supervivencia de una empresa? No se trata de establecer las prioridades entre su personal, sus activos, sus resultados económicos, etc., que todos son importantes, mas lo que determina la supervivencia de una organización empresarial es su continuidad de negocio, el cual se refiere a preservar el normal desarrollo de los procedimientos y medidas para garantizar la permanencia de las funciones esenciales de la organización.

Para determinar el alcance de la seguridad deberíamos ser capaces de dar respuestas al menos a estas tres preguntas clave: ¿Qué es lo que tengo que proteger? —el objetivo—; ¿de qué/quién lo tengo que proteger? —los riesgos y las amenazas—; y ¿cómo lo tengo que proteger? —estrategias y medios—.

Objeto a proteger. El fin último de la seguridad empresarial —supervivencia— es garantizar la continuidad de negocio y para ello se tienen que atender muchos aspectos. Uno de ellos, hoy en día de vital importancia como consecuencia de la interconectividad de las sociedades, es la reputación, entendida ésta como el impacto y percepción de nuestra actividad en los diferentes *stakeholders*. Otro aspecto al que se debe prestar una atención especial es sobre los procesos que conforman la operación empresarial, entendiendo que éstos pueden ser afectados tanto de una manera física, como virtual, mediante un uso perverso el ciberespacio; a lo anterior debemos añadir la protección de activos; así como, y no por citarla la última menos importante, las personas, en el convencimiento que desde la dirección corporativa de una empresa existe la obligación de proteger a sus empleados. Lo anterior pone de manifiesto que también en el ámbito empresarial debemos analizar la seguridad desde un enfoque multidimensional.

Determinar aquello que nos puede afectar. Los desafíos a los que se enfrenta una empresa (amenazas y riesgos) pueden tener una dimensión física como es un daño a sus trabajadores, ya se trate de acciones delictivas (secuestro, extorsión, etc.) como las que están relacionadas con la seguridad en el trabajo (riesgos laborales); las que se dirigen contra bienes inmuebles y muebles, como en el caso anterior, independientemente de su origen (intrusión, incendios, afectaciones por catástrofes naturales, etc.); contra sus activos ya sean económicos o financieros, debiendo protegerlos de actividades delictivas como el robo, fraude, etc., ya sea dentro o fuera de la empresa.

Y hoy en día han tomado una importancia creciente la protección contra todo tipo de agresiones desde el ciberespacio; así como el control de las redes sociales desde la que se puede ver afectada de manera notable la reputación y por ello, la comunicación debe estar íntimamente relacionada con la seguridad.

Definir las políticas y estrategias de seguridad y disponer de la organización y los medios adecuados. Se trata con ello de integrar la seguridad como una de las políticas transversales de las empresas que, dirigidas por la alta dirección, infieren en la actividad de los diferentes departamentos de la organización. En este apartado se tendrán en cuenta el diseño de la estrategia de seguridad de la empresa, el plan de continuidad de negocio, los planes de contingencia, incluyendo los que se refiere a la gestión de emergencias y crisis.

También se deberán determinar los medios necesarios para proporcionar una seguridad efectiva y eficiente en los diferentes campos de la actividad empresarial.

Una vez que se ha dado respuesta a las tres preguntas mencionadas, se

puede decir que tenemos definido el armazón de la seguridad de nuestra organización, el cual determinará el grado de seguridad que se puede alcanzar, puesto que la seguridad plena es imposible, y con base en él se estará en condiciones de determinar la vulnerabilidad que se puede asumir y en consecuencia habrá quedado definido el "nivel aceptable de inseguridad". Esto es precisamente uno de los motivos por los que la seguridad es un problema complejo, incluso "perverso", pues tiene lugar en al marco de la inseguridad, sin disponer normalmente de todas las capacidades necesarias, y en ocasiones ni de las competencias, para solucionarlos.

Una vez analizado cómo se adaptan los conceptos básicos de la seguridad a las organizaciones empresariales nos adentraremos en la descripción del modelo de seguridad corporativa. Aunque no existe una definición precisa para ella, ésta se entiende como el conjunto de políticas, procedimientos y recursos humanos, organizativos y técnicos destinados a la protección de las personas, de los activos tangibles e intangibles y de la reputación de una organización.

Más allá del valor de esta definición, quizás sea más oportuno considerarla como una función, la cual tiene por objeto la identificación, gestión y mitigación, en una fase temprana, de cualquier situación que pueda amenazar la resiliencia y la capacidad de supervivencia de una organización. Desde esta doble perspectiva, se nos permite comprender su objeto, es decir la continuidad de negocio y en consecuencia la supervivencia de la empresa, así como su carácter integral al incluir a todos los elementos —tangibles e intangibles— de la organización.

La seguridad corporativa va más allá de la seguridad física de sus activos, aspecto que, por otra parte, la vincula con la seguridad privada, incluyendo el análisis y evaluación de los diferentes procesos directivos. Estamos ante una función transversal relacionada con diferentes departamentos y áreas de negocio lo cual justifica que se encuentre directamente subordinada a la alta dirección.

La Dirección de Seguridad Corporativa asumirá normalmente los siguientes cometidos generales:

- **Relacionados con la gestión.** Será el primer responsable de los siguientes asuntos:
  - **Cumplimiento.** Más conocido por su equivalente en inglés de '*compliance*', se refiere a la gestión orientada al cumplimiento normativo de las empresas. Con ello se trata de vigilar y supervisar la observancia normativa para asegurar el desempeño de las organizaciones dentro de la legalidad y que permitan adoptar las acciones necesarias para evitar o al menos mitigar los riesgos.
  - **Área de riesgos.** La gestión de riesgos, para que sea eficaz, debe tener un carácter preventivo, lo que significa contar con una Inteligencia que permita su identificación, análisis y evaluación; es necesario diseñar una organización para la gestión de riesgos que permita la continuidad de negocio; y disponer de unos planes y procedimientos que deberán ser implementados de manera escalonada y progresiva.
  - **La protección** de todos los activos de la organización, incluida la reputación.
  - **La seguridad de la información,** lo que aconseja designar un responsable bajo su directa supervisión de la seguridad de la información y la protección frente a agresiones en el ciberespacio.
- Además de lo anterior deberá **coordinar y en su caso asesorar** en los siguientes campos:
  - En la actividad de las diferentes unidades de negocio con el objeto de analizar potenciales riesgos y amenazas, e identificar posibles áreas de oportunidad en relación con sus competidores, aliados y asociados, mediante procesos de '*due dillegence*'.
  - En los diferentes procesos de personal, en particular en los procesos de selección y el ya referido de cumplimiento. En este ámbito de actividad cobra especial importancia la vigilancia del fraude interno.
  - La administración y las finanzas son funciones de gran importancia para la continuidad de negocio y en consecuencia se deberán establecer unos mecanismos de control para asegurar su integridad.

Para determinar el alcance de la seguridad deberíamos ser capaces de dar respuestas al menos a estas tres preguntas clave: ¿Qué es lo que tengo que proteger? —el objetivo—; ¿de qué/quién lo tengo que proteger? —los riesgos y las amenazas—; y ¿cómo lo tengo que proteger? —estrategias y medios—

Foto: Creativeart - Freepik

- En lo que se refiere a los sistemas de información, estableciendo medidas de control (clasificación, difusión, custodia, etc.), tanto en lo que se refiere a la documentación física como a la información en red. Otra actividad esencial es la supervisión de la seguridad de las diferentes plataformas tecnológicas y sistemas de información. Las medidas de ciberseguridad es algo que tiene una importancia creciente, dada su especialización y complejidad, en muchas será preciso externalizar esta función.

3) ¿QUÉ PUEDEN APORTAR LAS SOLUCIONES DE INTELIGENCIA A LA SEGURIDAD CORPORATIVA EN UNA PYME?

De acuerdo con lo expuesto en el punto anterior la seguridad debe observarse con cuatro diferentes lentes: la del estado o condición a alcanzar y mantener, con esta lente nos centramos en el objeto referente de la seguridad —continuidad de negocio—; la lente de la situación que debe de ser manejada, centrándose en los desafíos que afectan o pueden afectar a los valores e intereses , es decir, deberemos identificar, analizar y evaluar los riesgos y las amenazas a la seguridad; la de la acción, o mejor conjunto de acciones a desarrollar, o lo que es lo mismo la definición de estrategias y planes, y la aplicación de medios; y la que se corresponde con la función que define la responsabilidad de los actores, entendiendo de este modo a la seguridad como un conjunto de relaciones.

Entendida esta visión ampliada de la seguridad estaremos en mejores condiciones de comprender cómo puede contribuir a ella la inteligencia. Para ello utilizaremos las dos primeras lentes: la que tiene que ver con el objetivo o referente a proteger, y la que atañe a la seguridad como situación para detectar, identificar, analizar y valorar los riesgos y amenazas que pueden afectarla.

Por otra parte, la Inteligencia no se limita al ámbito de la seguridad, sino que se trata de una actividad o función básica en los procesos de toma de decisiones que orientan la actividad y en su caso el cambio de toda organización empresarial, como es el caso de la inteligencia competitiva. Todo cambio está normalmente forzado, y siempre condicionado, por el contexto en el que se mueve la organización. Quiere decir, que además de conocer nuestras propias fortalezas y debilidades, se precisa conocer las oportunidades y amenazas que conforman el contexto en el que desarrollamos nuestra actividad, ya nos refiramos al Estado o a una organización empresarial.

La Inteligencia es la herramienta capital que nos va a facilitar la información precisa sobre los procesos internos, así como del contexto externo, permitiendo con ello alcanzar una posición de ventaja en la toma de decisiones.

Centrándonos en la relación de la inteligencia con la seguridad, cabe concluir, a la vista de lo hasta aquí expuesto que no es tarea fácil, sin duda, dar certeza, o al menos reducir la incertidumbre, en entornos tan complejos como los sistemas abiertos, como es el caso de la seguridad en nuestros días, y por ello la Inteligencia también ha tenido y tiene que adaptarse permanentemente a este nuevo y complejo contexto.

La primera consideración en la obtención de la inteligencia —primera lente— es que ésta debe orientarse a su finalidad fundamental, la supervivencia del objeto a proteger: la continuidad de negocio en el caso de las empresas. Se podría afirmar que éste ha sido uno de los principios inmutables en la obtención de inteligencia: el objetivo como foco de la actividad de la inteligencia.

Lo que ha cambiado no es tanto el concepto de la "inteligencia centrada en el objetivo", como acertadamente nos propone Robert M. Clark[1], sino la naturaleza del propio objetivo, el que tradicionalmente ha sido un sistema cerrado en el que las interacciones exteriores eran relativamente limitadas, para pasar hoy en día a constituir un sistema abierto, con unos niveles de relaciones mucho más extensos, con organización no lineal, sin responder a un orden jerárquico, y caracterizados por mayor dinamismo. Un sistema en sí mismo complejo.

Desde la lente de la situación para entender la seguridad, ésta se centra sobre los riesgos y las amenazas, lo que requiere a su vez un exhaustivo análisis del contexto.

Los riesgos, de naturaleza y origen muy variables, son también muy numerosos, máxime en el contexto de complejidad e incertidumbre ya descrito, por ello resulta materialmente imposible atender de manera permanente a todos ellos y en consecuencia se trata de priorizar los esfuerzos con base en su impacto sobre el objeto a proteger y la probabilidad de que se materialice. De manera que sobre los más probables y peligrosos será necesario establecer unas medidas permanentes de prevención y respuesta, sobre aquellos que aún siendo de menor probabilidad su impacto sea considerable (umbral de riesgo) se formulan planes y o medidas de contingencia, y para el resto se deberán establecer los correspondientes sistemas de alerta (temprana).

Desde la perspectiva del análisis, éste ha tenido que centrarse de una manera más eficiente atendiendo a esta mayor complejidad del objetivo, esto, entre otras consecuencias, ha motivado la necesidad de reconfigurar el tradicional y rígido ciclo de inteligencia, para conformar uno más abierto y dinámico. Pero, además, atendiendo al carácter multidimensional de la seguridad ha motivado a que la inteligencia se haya

Ilustración 1. Las Cuatro Lentes de la Seguridad

visto obligada a ampliar sus campos de actuación, lo que ha motivado abrir nuevos conceptos como es el de la Inteligencia Colaborativa, la cual supone compartir el conocimiento apoyándose en las nuevas tecnologías, de manera que se podría decir que la Inteligencia ha pasado de "la información es poder" a "el conocimiento es compartir". Consecuencia directa de estas dos orientaciones, y posiblemente causa de ellas ha sido el desarrollo exponencial de las nuevas tecnologías, lo que, entre otras cosas, ha alterado la relación entre las diferentes fuentes de Inteligencia, cobrando una importancia creciente las fuentes abiertas (OSINT - Open Source Intelligence).

Para ser competitivo en la economía global de nuestros tiempos, debemos aprender a pensar de manera colaborativa e innovadora. Son muchas las organizaciones que desde hace unos años apuestan por el reclutamiento y la retención de talento corporativo, con lo que partimos de la base de que contamos con empresas repletas de talento y de ideas innovadoras que encuentran un terreno propicio en los entornos que favorecen la colaboración, y que por supuesto cuentan con los recursos tecnológicos y la financiación para poder llevar a cabo proyectos ambiciosos.

"The fact that we are different doesn't mean that one of us is wrong. It just means that there's a different kind of right", Faith Jegede

Conscientes de esta necesidad del mundo empresarial, TWCI2 ha desarrollado un modelo de colaboración novedoso y adaptado a las necesidades de los clientes, orientado tanto a las grandes como a las medianas y pequeñas empresas, siendo estas últimas las que tienen mayores dificultades para contar con sus propios equipos de inteligencia. Para ello ha construido una red de colaboradores en diferentes áreas de conocimiento y en distintas regiones del mundo que permite la integración de productos de inteligencia eficientes y competitivos.

Uno de estos productos es el denominado "Sistema de Vigilancia e Inteligencia", como una de las herramientas más importantes para el desarrollo de nuevos negocios, para con ella acelerar y respaldar la toma de decisiones en proyectos con alta incertidumbre.

Aunque se traten de dos conceptos diferenciados son, a su vez, complementarios. Mientras la vigilancia centra su actividad en la identificación de necesidades y monitorización sistemática, organizada y permanente de información relevante para su empresa, la inteligencia se encarga de analizar dicha información para transformarla en conocimiento útil para su organización.

La convergencia de ambas materias conforma el Sistema de Vigilancia e Inteligencia (SVI), el cual consiste en un procedimiento ético y sistemático de recolección, análisis, difusión y comunicación de información estratégica empresarial que tiene como fin último mejorar la toma de decisiones.

Independientemente de qué tipo de dimensión de actuación quiera darse, la vigilancia y la inteligencia como herramienta integrada supondrá varios beneficios para la actividad de la empresa en la medida que contribuye a disminuir la incertidumbre; a acelerar los proyectos de innovación, identificando socios tecnológicos o comerciales e incentivando actividades cooperativas y colaborativas; a definir las estrategias de innovación y desarrollo; a reducir la subjetividad e influencia de sesgos cognitivos; reforzar la prevención mediante un sistema de alertas tempranas sobre cambios en el entorno y en cualquier ámbito de interés para la empresa; así como detectar riesgos, entendiendo éstos como amenaza y como oportunidad, así como identificar las debilidades y las fortalezas de la organización.

Ilustración 2. Sistema de Vigilancia e Inteligencia by TWCI

Se trata de un producto de amplio espectro, cuyas principales áreas de actividad son:

- Ámbito competitivo o corporativo.
- Ámbito tecnológico.
- Ámbito reputacional.
- Ámbito de seguridad.

El SVI es aplicable a cualquier tipo de empresa gracias a la capacidad de TWCI de adaptarse a las necesidades concretas de su organización independientemente de su tamaño, sector o zona geográfica.

Incluso si aún posee procesos muy tradicionales, el SVI le ayudará a entender cuáles son las innovaciones más idóneas para ciertas áreas de su empresa, sin tener que pasar por un proceso de "ensayo y error" poco informado. El SVI dará soluciones más viables, acertadas y concretas.

Se trata de un producto que genera valor mediante la realización actividades encaminadas a:

- Vigilancia digital en fuentes abiertas. Escucha social y monitorización en fuentes abiertas de las temáticas de interés definidas en el alcance del servicio.

- Detección de oportunidades. A partir de la monitorización de temáticas destacadas y sub-temáticas, actores de interés y comunidades destacadas.

- Sistema de alertas. Alertas automáticas y generadas por los analistas para identificar impulsores y disparadores de riesgo. Visualizados mediante indicadores.

- Modelo de entregable. Posibilidad de ajustar la modalidad de los entregables de acuerdo con las necesidades del cliente.

- Presentación de la información. Presencia de indicadores gráficos que reúna los puntos claves en una presentación ejecutiva.

El SVI es aplicable a cualquier tipo de empresa gracias a la capacidad de TWCI de adaptarse a las necesidades concretas de su organización independientemente de su tamaño, sector o zona geográfica

Ilustración 3. El SVI como valor añadido

4) CONCLUSIONES

A la hora de diseñar las políticas y estrategias de seguridad es importante tener presente dos patrones de conducta irrenunciables. El primero, es que la seguridad es proactiva y en consecuencia se precisa disponer de las herramientas necesarias para anticiparnos a las situaciones adversas, siendo la principal de ellas la Inteligencia la que ayudará a mantener la ventaja competitiva. Pero asumiendo la necesidad de anticipación a los acontecimientos, también, y no menos importante, se debe fomentar la "cultura de crisis", es decir la capacidad de tomar decisiones ante acontecimientos no previstos, sin temor al error.

Al contrario, el error es una extraordinaria fuente de aprendizaje, mientras que la inacción, característica de la "cultura del miedo", supone el camino al fracaso. El segundo patrón de conducta es comprender que los procesos de toma de decisiones estratégicas se fundamentan en "hacer lo correcto", es decir determinar de manera clara el fin y los medios a emplear, mientras que en los niveles más bajos de decisión se trata de "hacer las cosas bien", pues el camino ya está trazado. En ambos niveles de decisión se requiere contar con la inteligencia adaptada a la situación y acorde con las necesidades de la organización.

La seguridad es algo que no se improvisa, es un área de conocimiento de muy amplio espectro que precisa una gran preparación. Esta es una función básica para cualquier organización, en consecuencia, al igual que a nivel nacional la seguridad es una de las principales políticas de cualquier organización, en una empresa la seguridad debe estar directamente vinculada a la alta dirección.

La inteligencia es una herramienta irrenunciable para los tomadores de decisiones y hoy en día, atendiendo a la amplitud de campos que abarca y a la propia complejidad del entorno en el que las empresas desarrollan sus actividades la inteligencia colaborativa está cobrando una importancia creciente.

De un modo sintético se podría afirmar que ésta es más propia de grupos de trabajo que de grandes masas de personas; que se ve facilitada cuando el objetivo a conseguir o reto a superar se encuentra bien identificado y definido; que requiere una precisa selección de los participantes en el proyecto, con base en sus competencias y habilidades; y debe contar con las herramientas digitales adecuadas para su desarrollo.

El Sistema de Vigilancia e Inteligencia desarrollado por TWCI, y customizado a cualquier empresa, supone un proyecto de gran valor para proteger tanto los elementos tangibles como los intangibles de una organización; para identificar las oportunidades de desarrollo de negocio; y para detectar las señales de alarma que prevengan situaciones no deseadas. ■

REFERENCIAS

[1] *Clark, Robert M. 2017 "Intelligence Analysis. A Target Centric Approach. SAGE. London, UK.*

[2] *Empresa española de consultoría en seguridad e inteligencia estratégica, en particular sobre los procesos complejos de la internacionalización, los cuales requieren contar con el más amplio conocimiento posible del contexto exterior para identificar las oportunidades y amenazas, así como disponer de la información oportuna y precisa de los requisitos normativos del país de destino, y todo ello sin olvidar la necesidad de conocer y entender los diferentes modelos culturales.*

Jesús De Miguel Sebastián,
Coronel del Ejército de Tierra de España en Retiro y Socio Fundador Two Worlds Collaborative Intelligence.

Más sobre el autor:

¿POR QUÉ INVERTIMOS EN CONTINUIDAD DEL NEGOCIO **EN BRASIL?**

Foto: Creativeart - Freepik

Tenemos la oportunidad de ayudar a cambiar la cultura de seguridad de dicho país y llevar innovación a quienes ya tienen experiencia

BRASIL | Pupo Neto

"¡Ocurrió algo inesperado!", escuchamos a menudo. De hecho, los imprevistos ocurren cualquier día, a cualquier hora; pero en un país con reputación de dejarlo todo para el último minuto, esto puede parecer normal. Pero no es cierto para quienes trabajan en *Business Continuity*.

Cualquiera fuera de este mercado puede pensar que las empresas no están preparadas para enfrentar incidentes o crisis; pero la realidad es diferente, en la mayoría de las grandes empresas de Brasil. Numerosos equipos de ejecutivos de diversas áreas —análisis de riesgos, seguridad, prevención de pérdidas, gestión de crisis, etc.— tienen conocimientos, planes y herramientas en procesos muy complejos, bien mapeados y monitoreados.

La mayoría de los ejecutivos de seguridad con los que he tenido contacto en los últimos dos años estaban muy bien fundamentados en sus procesos, pero no estaban familiarizados con las tecnologías que pueden mejorar sus procesos. La mayoría de estas empresas mostraron dificultad en la actualización y capacitación; y la integración con las nuevas tecnologías es una oportunidad de mejora que dará el salto en la relevancia de los temas relacionados con la gestión de crisis.

Entonces, ¿por qué invertimos en traer una plataforma de seguridad y continuidad del negocio en Brasil? El tamaño de este país, diferencias geográficas, sociales y culturales. La diversidad hace de Brasil una oportunidad única y así introdujimos a CoSafe en este segmento, ya muy consolidado en Europa. Incluso considerando la experiencia y la estructura ya presentes aquí, identificamos una gran brecha en el mercado en relación a la tecnología.

Estos profesionales de las grandes empresas, están acostumbrados a las rutinas de análisis de riesgos y cómo prepararse para ellas. Lo que les ofre-

Las empresas que ya utilizan nuestra plataforma para equipos especializados han aumentado el número de usuarios del producto, por ejemplo, en la necesidad de hacerse cargo del trabajo remoto y presencial de quienes no pueden parar

cemos es tecnología para actuar con mayor rapidez y precisión ante cualquier incidente, evitando crisis; o ayudar a superar las crisis de la forma más segura posible. Si bien las grandes empresas de Brasil ya cuentan con planes de continuidad comercial, pocas utilizan herramientas digitales; una gran brecha que encontramos. Trazamos mucho el mercado y tuve la oportunidad de hablar con grandes líderes del mercado de seguridad y crisis hasta que lanzamos oficialmente CoSafe en Brasil, justo antes de que la pandemia llegara al país.

Foto: Creativeart - Freepik

ACELERADOR DIGITAL

2020 y 2021 fueron un importante acelerador digital para todos. Estimularon mucho la búsqueda de la innovación, y participamos en algunos programas donde grupos de grandes empresas multinacionales buscaban soluciones innovadoras para integrarse a esta nueva realidad, que llegó tan abruptamente. Sin embargo, innovar no era una opción, era obligatorio.

Para nuestros clientes, la pandemia ha aumentado el alcance de uso de la plataforma. Esto sucedió muy rápido en varios mercados con los que trabajamos —grandes cadenas minoristas, bancos, oficinas, aeropuertos, fábricas, etc.—. Las empresas que ya utilizan nuestra plataforma para equipos especializados han aumentado el número de usuarios del producto, por ejemplo, en la necesidad de hacerse cargo del trabajo remoto y presencial de quienes no pueden parar.

Si bien las grandes empresas de Brasil ya cuentan con planes de continuidad comercial, pocas utilizan herramientas digitales; una gran brecha que encontramos

Para tener una idea del potencial del mercado en Brasil, sólo en 2019, el mercado de seguridad electrónica movió 7,17 mil millones de reales (un millón 301 mil dólares) en el país, según la Asociación Brasileña de Empresas de Sistemas de Seguridad Electrónica (ABESE). Para este año, incluso con la crisis, el movimiento debería ser aún mayor.

Y también tuvimos que adaptarnos, crear nuevas funciones, ajustar otras. Para nosotros, este año fue el momento de demostrar que quienes trabajan con la continuidad del negocio también necesitan que sus planes sean revisados y rápidamente. Invertir en un mercado sin explotar podría ser bueno, pero invertir en un mercado existente, aportando ahorros y mejoras en el proceso, ha demostrado ser un mar de oportunidades. Y por eso estamos aquí. Lo que tenemos a la mano es la oportunidad de ayudar a cambiar la cultura de seguridad del país y llevar innovación a quienes ya tienen experiencia. Como en toda *startup*, en muchos momentos parecía una locura, o algo imposible, ¡pero lo logramos! ■

Foto: Creativeart - Freepik

Pupo Neto,
CEO de CoSafe en Brasil.

Más sobre el autor:

LOS EVENTOS MÁS IMPORTANTES QUE MARCARON EL AÑO 2021

En 2021 se puso a prueba todo lo aprendido durante la crisis sanitaria, donde también fue momento de crear nuevas condiciones, nuevos enfoques y superar todos los pronósticos que para la mayor parte del mundo no eran alentadores

MÉXICO

Erick Martínez / *Staff* Seguridad en América

El año 2020 sin duda alguna cambió al mundo. La pandemia provocada por el COVID-19, puso a prueba a la humanidad, la incertidumbre se hizo presente tanto a nivel económico, político y sobre todo social, la salud de las personas, su vida y la rutina que llevaban hasta ese momento, se vio afectada de forma súbita. Indudablemente 2020 fue un año de nuevos aprendizajes y grandes pérdidas. Con la llegada de las vacunas, la esperanza surgió y todo lo aprendido ese año, se pondría a prueba en 2021, sin embargo los retos sobre todo en materia de seguridad continuaron cambiantes y desafiantes, no sólo por la pandemia, sino también por la propia naturaleza y los conflictos politícos ideológicos entre diversos países.

A continuación se presentan algunos de los eventos más importantes de 2021 hasta el cierre de esta edición, que impactaron y conmocionaron al mundo de diferentes maneras.

Foto: Creativeart - Freepik

6 DE ENERO

Asalto al Capitolio de los Estados Unidos. Fue un acontecimiento que se produjo el 6 de enero de 2021 cuando partidarios del entonces presidente saliente de los Estados Unidos, Donald Trump, irrumpieron en la sede del Congreso violando la seguridad y ocupando partes del edificio durante varias horas. El evento ocurrió después de numerosos intentos anteriores de Trump de anular los resultados de las elecciones tras un supuesto fraude electoral.

12 DE ENERO

Mutación del SARS-CoV-2. A finales de 2020 e inicios de 2021 se encontró que el virus que provoca el COVID-19 estaba mutando en algunas partes de Europa, principalmente en Reino Unido, el cual ponía en mayor riesgo a la población del mundo, provocando un mayor impacto a la salud, además de su ampliación en fácil propagación. Sin embargo, múltiples institutos epidemiológicos comentaron que era algo que se tenía previsto que podía suceder, esa y nuevas variantes del mismo virus en diferentes partes del mundo y que afectaron de diferentes maneras al cuerpo humano. Una pregunta clave es: ¿Las mutaciones pueden tener implicaciones para la efectividad de las vacunas? Es algo que muchos expertos consideran improbable, al menos a corto plazo.

20 DE ENERO

Joe Biden toma posesión como presidente de los Estados Unidos de Norteamérica. El nuevo presidente enfrenta grandes retos ante su mandato: acabar con la triple crisis que atraviesa Estados Unidos: sanitaria, económica y social. La vicepresidenta electa, Kamala Harris, juró el cargo junto a Biden, siendo la primera mujer en ocupar este importante puesto en el gobierno. Trump es el cuarto presidente en la historia del país en no ser reelecto.

21 DE ENERO

Estados Unidos se une a COVAX, la iniciativa de la Organización Mundial de la Salud (OMS) para la distribución equitativa de las vacunas contra la COVID-19 en todo el mundo. El objetivo de COVAX es acelerar el desarrollo y la fabricación de vacunas contra el COVID-19 y garantizar su acceso justo y equitativo a todos los países del mundo. Más de 170 naciones, incluidas Inglaterra, Canadá y la Unión Europa pertenecen a la iniciativa que procura dosis para las poblaciones más vulnerables[1].

7 DE FEBRERO

Elecciones presidenciales de Ecuador. Dando como resultado ganador a Guillermo Lasso, ex banquero conservador de 66 años, quien obtuvo 52.36% de los votos ante Andrés Arauz, de izquierda, con el 47.64%. A la par se llevaron a cabo las elecciones legislativas, primera vuelta.

15 DE FEBRERO

Empieza la jornada de vacunación en México, comenzando con los adultos mayores, después de haber vacunado al personal médico de primera línea de control COVID-19. Con un total de 87 mil vacunados en todo el territorio mexicano. Personal de salud y de las Fuerzas Armadas fueron los encargados de distribuir las primeras dosis del biológico producido por AstraZeneca que llegaron al país. Ante esta ardua labor se sumaron múltiples empresas de logística, transporte y seguridad privada, quienes apoyaron en la distribución las vacunas en las siguientes etapas.

28 DE FEBRERO

Tragedia carcelaria en Guayaquil, Ecuador. Producto de amotinamientos en varios centros penitenciarios del país, dejaron como resultado 79 muertos. Una serie de eventos simultáneos que comenzó en el Centro de Privación de Libertad Masculino Guayaquil no.1, se extendió al Centro de Privación de Libertad Regional Guayas no. 4; luego se reportaron amotinamientos en el Centro de Privación de Libertad Azuay no. 1, y en el Centro de Privación de Libertad Regional Latacunga, en la ciudad de Latacunga, Cotopaxi.

27 DE FEBRERO

Se superan las
185 mil 715 muertes
a causa de COVID-19, tras un año del primer contagio de esta enfermedad en México, así lo publicó la Secretaría de Salud del Estado mexicano.


Foto: Creativeart - Freepik

8 DE MARZO

Día Internacional de la Mujer. "El 8 de marzo es un día que desde años anteriores destaca en el calendario internacional al recordar que la desigualdad de género aún es una realidad en todo el mundo y que si bien han sido muchos los logros alcanzados quedan muchas injusticias por superar". El 8M no es un día donde se "felicite" a la mujer, sino un día para analizar y evidenciar la desigualdad en la que viven las mujeres en las diferentes esferas públicas y privadas, y así poner fin a las brechas salariales, oportunidades laborales, distribución equitativa de educación a los niños, y también para exigir un alto a los feminicidios, violaciones, desapariciones. En México cada día mueren y desaparecen 10 mujeres. A pesar de los esfuerzos y protestas, marzo es el mes más violento y letal para las mujeres desde que se tiene registro en 2015. Por ello cada año salen a marchar miles de mujeres en diferentes partes del mundo[2].

16 DE ABRIL

Se publica la Reforma a la Ley Federal de Telecomunicaciones y Radiodifusión, mediante la cual se crea el Padrón Nacional de Usuarios de Telefonía Móvil (PANUT), donde se pedirán a los usuarios de telefonía móvil, ya sean personas físicas o morales, datos biométricos (huellas dactilares, escaneo de iris, escaneo de rostro, etc.), del usuario en caso de persona física o del representante legal de la persona moral. Este evento causó gran controversia para los millones de usuarios alegando la violación de derechos a la protección de datos personales, principio de retroactividad, proporcionalidad y el principio de legalidad.

28 DE ABRIL

Tras la reactivación económica, se vio la necesidad de crear el Día Mundial de la Salud y Seguridad en el Trabajo. Evento realizado para analizar la seguridad y salud en los lugares de trabajo, el cual forma parte de una actividad a nivel mundial desarrollada por la OIT (Organización Internacional del Trabajo) en América Latina y el Caribe. Se centra en las estrategias para fortalecer los sistemas nacionales de seguridad y salud en el trabajo (SST) con el fin de desarrollar resiliencia para hacer frente a las crisis[3].

1° DE MAYO

Comienza la retirada de las tropas estadounidenses de Afganistán ya anunciada en abril. Las fuerzas estadounidenses, Reino Unido y países miembros de la OTAN (Organización del Tratado del Atlántico Norte) **invadieron el país en 2001** después de los ataques terroristas del **11 de septiembre de 2001,** y la guerra resultante se convirtió en el compromiso militar más largo de Estados Unidos. El secretario de Estado, Antony Blinken, dijo que la decisión se tomó para concentrar los recursos en China y la pandemia de COVID-19.

5 DE MAYO

Miles de manifestantes toman las calles de Colombia tras la reforma de la Ley Tributaria que anunció el presidente del país, Iván Duque. Las protestas se extendieron por semanas más adelante, hasta la tercera jornada de paro nacional convocado por centrales obreras y sindicatos, luego de no llegar a acuerdos en su primera reunión con el Gobierno colombiano. Se estiman más de 40 muertes por represión policiaca y abuso de autoridad.


Foto: Creativeart - Freepik


Foto: Creativeart - Freepik

29 DE MAYO

Socavón en Puebla. Un gigantesco agujero en el estado de Puebla, México, que inicialmente era de cinco metros de diámetro, superó los 120 metros de diámetro y 56 en la parte de mayor profundidad. El evento, según especialistas, posiblemente se debe a las fuertes lluvias registradas en la zona y el reblandecimiento de la tierra hasta que incluso se "tragó" una casa, otra de las posibles causas es la explotación de mantos acuíferos del subsuelo.

6 DE JUNIO

Se celebra la segunda vuelta de elecciones presidenciales en Perú, donde semanas después se declaró ganador, por el Jurado Nacional de Elecciones, el candidato de izquierda de Perú Libre, Pedro Castillo. Esto tras la primera vuelta electoral en abril del presente año para elegir al presidente de la república, dos vicepresidentes de la misma, 130 congresistas y cinco parlamentarios andinos para el periodo gubernamental 2021-2026.

6 DE JUNIO

Las elecciones más grandes de la historia de México, fue el nombre que se le denominó a las elecciones del 6 de junio, no sólo por el crecimiento del número electoral, sino también por el número de cargos que se elegirían, pues las 32 entidades del país tendrían elecciones locales concurrentes con la federal. Cabe destacar que también fueron las elecciones más violentas, con 90 políticos asesinados en las campañas, homicidios, secuestros y amenazas, fueron algunas de las 782 agresiones registradas contra políticos y candidatos en el proceso electoral. De acuerdo con el Quinto Informe de Violencia Política con México, realizado por la consultora Etellek, desde el 7 de septiembre de 2020 y hasta el pasado 31 de mayo, se registraron 782 agresiones dirigidas a 737 víctimas.

9 DE JUNIO

El Salvador es el primer país en reconocer el *bitcoin* como moneda legal de intercambio. La Ley *Bitcoin* regula el curso legal de la criptomoneda, que podrá utilizarse en cualquier transacción y a cualquier título que las personas naturales o jurídicas públicas o privadas quieran realizar.

Foto: Creativeart - Freepik

29 DE JUNIO

El máximo tribunal de la justicia mexicana falla a favor de la Declaratoria General de Inconstitucionalidad (DGI) que invalida varios artículos de la Ley General de Salud y despenaliza el autoconsumo lúdico de cannabis en el país. El documento fue aprobado por ocho de los 11 magistrados y especifica que no es legal su comercialización. Igualmente, la magistrada Norma Lucía Piña declaró que el consumo será avalado únicamente para mayores de edad y no se podrá hacer en espacios públicos. A raíz del fallo de la Corte, los mexicanos podrán pedir permisos a la Comisión Federal para la Protección contra Riesgos Sanitarios (Cofepris), para consumir, cultivar y portar marihuana con propósitos recreativos

Foto: Creativeart - Freepik

7 DE JULIO

Es asesinado el presidente de Haití, Jovenel Moise, por un grupo de hombres armados que asaltaron su domicilio en Puerto Príncipe, mientras su esposa, Martine Moise, resultó herida de bala. Días después se descubrió que un escuadrón de mercenarios extranjeros, entre ellos ex militares colombianos y estadounidenses, habían efectuado el asesinato.

22 DE JULIO

Argentina añade en su DNI (Documento Nacional de Identidad) la opción para personas de sexo no binario, el primer país en América Latina en dar este paso. El DNI tendrá una casilla con una X que incluirá a todas aquellas personas que no se identifiquen con las opciones binarias. Argentina se une así a otros países del mundo como Canadá, Australia y Nueva Zelanda que ofrecen esta opción.

23 DE JULIO

Dan inicio los Juegos Olímpicos de Tokio 2020, a un año de que fueran interrumpidos por la pandemia del SARS-CoV-2, manteniendo su nombre oficial de Tokio 2020. Estas olimpiadas fueron muy especiales para todo el mundo, el haber sido pospuestas un año y además, el poder adaptar todos los recintos y destinos turísticos para poder ofrecer seguridad sanitaria a los visitantes y atletas, por ello se tuvieron que implementar todas las medidas de protección anti-COVID-19, lo que representó una inversión y esfuerzo aún mayor de lo ya previsto. No obstante, hubo atletas que en plenos Juegos Olímpicos dieron positivo a este virus, truncando así su carrera a las preseas olímpicas.

14 DE AGOSTO

Un terremoto con magnitud de

7.2 MW

golpea fuertemente Haití. Cuando todavía no se recuperaba del terremoto de 2010. Al menos

136 mil 800

edificios resultaron dañados o destruidos, las muertes se estimaron en

2 mil 207

al 22 de agosto de 2021. La UNICEF calculó que más de medio millón de niños se vieron afectados.

Foto: Creativeart - Freepik

30 DE AGOSTO

El ejército estadounidense finaliza su retirada de Afganistán, después de una misión que duró casi 20 años de invasión y guerra en el país asiático. Más de 79 mil civiles del Aeropuerto Internacional Hamid Karzai, incluyendo a 6 mil estadounidenses y más de 73 mil ciudadanos de terceros países y afganos. Poco después de la partida estadounidense, los talibanes se apoderaron del aeropuerto de Kabul y celebraron la recuperación completa del país con disparos y cánticos durante toda la noche. Este histórico hecho también marcó un camino hostil hacia los derechos humanos y civiles, sobre todo para las mujeres afganas al reestablecerse el orden talibán, lo cual aterró a cientos de ciudadanos, que en un intento desesperado por huir del país perdieron la vida tratando de colgarse de los aviones a como diera lugar, y al menos siete personas murieron.

Foto: Creativeart - Freepik

1° DE SEPTIEMBRE

Entra en vigor la Reforma sobre *outsourcing* en México, después de mucho tiempo de análisis. Este esquema funcionaba de manera que "si trabajas para una empresa, pero tu contrato no lo firma dicha compañía, sino otra." La minuta aprobada en abril reforma ocho leyes: Ley Federal del Trabajo, Ley del Seguro Social, Ley del Infonavit (Instituto del Fondo Nacional de la Vivienda para los Trabajadores), el Código Fiscal de la Federación, la Ley del ISR (Impuesto Sobre la Renta), la Ley del IVA (Impuesto sobre el Valor Añadido), la Ley Federal de los Trabajadores al Servicio del Estado, así como la Ley Reglamentaria. Se permitirá la subcontratación de servicios especializados u obras especializadas que no forman parte del objeto social, ni de la actividad económica preponderante de la beneficiaria de los mismos, siempre que las empresas contratistas estén registradas en el padrón público que estará a cargo de la Secretaría del Trabajo y Previsión Social (STPS)[5].

7 DE SEPTIEMBRE

Venezuela recibe el primer lote de la vacuna de Sinovac Biotech contra el nuevo coronavirus, esto a través del mecanismo COVAX de la Organización Mundial de la Salud (OMS). Las vacunas fueron adquiridas a través del Fondo Rotatorio de la Organización Panamericana de la Salud (OPS), agente de adquisición reconocido ante COVAX para los países de la región de las Américas y constituyen el primer lote del total de 12 millones 68 mil dosis de vacunas que recibiría Venezuela por medio de este mecanismo global[5].

18 DE SEPTIEMBRE

Se celebra la VI Cumbre de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC) en la Ciudad de México, donde se dieron cita 17 presidentes de la región. El anfitrión mexicano, el presidente Andrés Manuel López Obrador, había pedido sustituir la política de bloqueos

y de malos tratos por "la opción de respetarnos, caminar juntos y asociarnos por el bien de América sin vulnerar nuestras soberanías". Estas palabras reflejan la disposición de tratar de restablecer la acción unitaria en la región a pesar de las diferencias ideológicas, lo cual resulta difícil ante la ausencia de Brasil, debido a que su presidente, Jair Bolsonaro, había retirado su país de este organismo internacional, entre otros países, como Argentina y Colombia —cuyos presidentes no participaron en la reunión—.

30 DE SEPTIEMBRE

Alrededor de

4.8 millones

de personas han fallecido a nivel mundial a consecuencia del COVID-19. Mientras que, en Asia, continente en el que se originó el brote, la cifra de muertes asciende a alrededor de un millón de personas, los decesos en Europa superan en más de 265 mil personas dicha cifra. En concreto, se han registrado aproximadamente

1.3 millones de muertes

por el coronavirus en el viejo continente. Sin embargo, ya no es el continente con mayor número de fallecidos por COVID-19, la cifra contabilizada en América supera ya los dos millones de decesos.

Foto: Creativeart - Freepik

3 DE OCTUBRE

Pandora Papers. Los nombres de empresarios, políticos, líderes mundiales, deportistas y celebridades aparecieron en los '*Pandora Papers*', una investigación que revela tratos de sociedades *offshore* de cientos de las personas más ricas y poderosas a nivel mundial. Los *Pandora Papers* son una filtración de casi 12 millones de documentos que revelan riqueza oculta, evasión de impuestos y, en algunos casos, lavado de dinero por parte de algunas de las personas más ricas y poderosas del mundo. En la mayoría de los países, estos hechos no son enjuiciables.

4 DE OCTUBRE

200 años de la Armada de México. En explanada del Astillero de Marina, en la Tercera Zona Naval en Coatzacoalcos, Veracruz, se llevó a cabo la ceremonia de conmemoración de los 200 años de la fundación de la Armada de México, Es la rama marítima de las Fuerzas Armadas de México y depende de la Secretaría de Marina. Se encarga de la vigilancia y salvaguardia de las costas, el mar territorial, la zona económica exclusiva y el espacio aéreo marítimo de México, también tiene a su cargo la inspección de las aguas interiores, vías fluviales y lacustres navegables.

4 AL 8 DE OCTUBRE

Semana de la Ciberseguridad. La Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México, a través de la Unidad de Policía Cibernética, realizó la Séptima Semana Nacional de Ciberseguridad del 4 al 8 de octubre de 2021. Durante las actividades se informó sobre el uso adecuado de las herramientas tecnológicas que se encuentran al alcance de la ciudadanía, los peligros que existen en Internet; además se emitieron recomendaciones a los cibernautas para prevenir delitos en la red, promoviendo una cultura del autocuidado y civismo digital.

10 DE OCTUBRE

Elecciones municipales en Paraguay. Por la actual pandemia de COVID-19, estas votaciones se suspendieron en 2020, lo que permitió que las autoridades extendieran su mandato por un año. Se eligieron a los futuros intendentes para ser jefes comunales y concejales que integrarán las Juntas Municipales. Fueron electos 261 intendentes municipales para igual número de ciudades y 2 mil 781 miembros de Juntas Municipales titulares y la misma cantidad de suplentes.

PRÓXIMAS ELECCIONES DE 2021 EN LATINOAMÉRICA:

- **Nicaragua:** elecciones presidenciales y legislativas, 7 de noviembre.
- **Argentina:** elecciones legislativas, 14 de noviembre.
- **Chile:** elecciones presidenciales y legislativas, 21 noviembre.
- **Honduras:** elecciones generales, 28 de noviembre. ■

REFERENCIAS

1 *https://news.un.org/es/story/2021/01/1486902*
2 *http://www.famp.es/es/actualidad/noticias/MANIFIESTO-8-de-MARZO-DE-2021-DIA-INTERNACIONAL-DE-LA-MUJER-MAS-MUJERES-AL-FRENTE-DE-LA-ACCION-LOCAL/*
3 *https://www.ilo.org/americas/eventos-y-reuniones/WCMS_778611/lang--es/index.htm*
4 *http://dof.gob.mx/nota_detalle.php?codigo=5619148&fecha=24/05/2021*
5 *https://apnews.com/article/noticias-8eb7053932a89f60523eb79fc73e13a2*

PANORAMA DE LA SEGURIDAD EN **PLANTAS AUTOMOTRICES**

Las organizaciones de esta industria pueden tener monitores y controles preventivos que minimicen algunos de los riesgos que se pudieran presentar

MÉXICO | José Luis Sánchez Gutiérrez

Lo primero que debemos considerar en la seguridad de la plantas automotrices es lograr el objetivo de proteger la salud de todos, prevenir accidentes y promover el cuidado del material de los laboratorios. Todo esto por medio del seguimiento impecable de los procesos y el conjunto de las normas básicas de seguridad.

Estas normas básicas son la clave que previene accidentes y realmente promueven prácticas seguras en el sector automotriz dentro de las plantas de producción.

El uso adecuado de todos los elementos de protección física a las personas salva día a día la vida de los empleados dentro de las instalaciones en la planta automotriz. Hablamos específicamente de la protección auricular, de ojos, respiratoria con elementos de caucho y fieltro, protección de manos, de pies, ropa protectora y no olvidar la protección de cabeza con casco o sombrero con concha de plástico de alto impacto.

Recordemos que en el exterior de las plantas algo muy recurrente en México, es el asalto a los trabajadores de plantas automotrices que va en aumento.

INSEGURIDAD EN EL PAÍS

La industria automotriz en México posee un peso más que significativo en términos económicos y sociales. Representa el 18% del PIB (Producto Interno Bruto) manufacturero, genera casi 200 mil empleos y más de 18 mil millones de dólares en exportaciones, lo que se traduce a cerca de 350 mil millones de pesos. Su importancia es muy destacada.

Sabemos que una serie de problemas afectan la estabilidad de la industria automotriz en el país. Ya hemos observado cómo diferentes factores externos impactan en las ventas e inciden en el crecimiento, pero también existen factores internos que afectan directamente a las empresas automotrices. Uno de los más importantes es la inseguridad.

La inseguridad que se vive en México: donde el obrero, el que se dedica, justamente, a la construcción de los autos que conducimos, o que se venden al extranjero.

En las entidades y localidades que cuentan con plantas automotrices, los trabajadores se encuentran a merced de los delincuentes; se ha registrado un aumento al asalto a los empleados cuando ingresan o salen de sus labores.

La inseguridad afecta de manera directa a la industria automotriz, sobre todo en el sector patrimonial; por ejemplo, una persona que trabaja en una planta automotriz, esperando el transporte es asaltado, esa persona ahí no va a trabajar más, por lo tanto hay rotación, y si se cuantifica es un número que está afectando a la competitividad de las empresas.

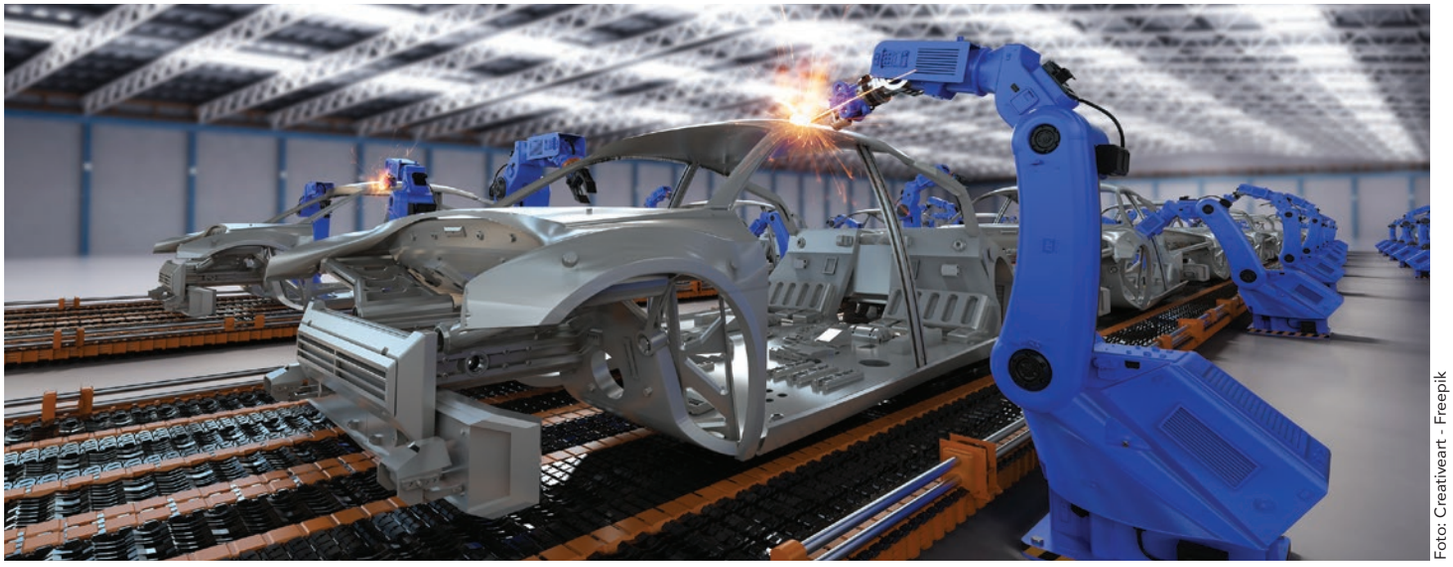


Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Si bien las empresas no pueden eliminar los riesgos en su totalidad, sí pueden tener planes de contingencia y estar preparadas para reaccionar de la mejor forma y con las menores pérdidas posibles

Además del asalto a los trabajadores, también se registra aumento del robo de materias primas a través del asalto a los camiones que las transportan. Esto es importante, si las materias primas con las que deben trabajar no llegan a las líneas de producción, deben pararse, lo que termina siendo costoso, tanto para empresa como para trabajadores.

La industria automotriz tiene que trabajar de la mano con el gobierno federal y con los diversos gobiernos estatales, para que la seguridad tanto de sus trabajadores como de sus líneas de suministro, sean protegidas; de otra manera, se corre el riesgo de perder una gran cantidad de empleos.

En el ambiente de negocio automotriz, el término "riesgo" ciertamente se ha convertido en una palabra que puede tener cientos de implicaciones negativas. Especialmente en la industria automotriz, los riesgos en la cadena de suministros pueden llevar a pérdidas que llegan al 5% de los ingresos anuales. El costo por detener la línea de producción llega a los 500 dólares por minuto. El costo de ciberataques llega a los 100 mil dólares por hora de producción detenida.

Es un hecho que las empresas que no le pongan la debida atención a la gestión de riesgos están en peligro sufrir enormes pérdidas e incluso de quedar fuera del negocio.

De acuerdo a las encuestas que la empresa QAD hace con ejecutivos de la industria automotriz en México, tanto armadoras como proveedores de autopartes priorizan los riesgos como sigue:

- Interrupciones en la cadena de suministro: 72%.
- Fallas en equipos operativos: 72%.
- Desastres naturales: 42%.
- Incendios: 24%.
- Huelgas: 20%.

CADENA DE SUMINISTRO

Detener la cadena suministro conlleva fuertes penalizaciones en la industria automotriz, por lo que estar en control de los motivos que pudiesen detenerla es un tema clave para las empresas.

Conociendo los factores que pueden detener la cadena de suministro: los empresarios mencionan varios riesgos a considerar (ausentismo, ciberataques,

Foto: Creativeart - Freepik

falta de capacitación, rotación de personal, alteraciones en las vías de comunicación, entre muchos otros riesgos que llevan a la interrupción de la operación).

Si bien las empresas no pueden eliminar los riesgos en su totalidad, sí pueden tener planes de contingencia y estar preparadas para reaccionar de la mejor forma y con las menores pérdidas posibles. Desastres naturales ocasionados por el cambio climático, como los que todos hemos atestiguado a últimas fechas; factores geopolíticos como la revisión del TLC (Tratado de Libre Comercio) que sin duda afecta fuertemente a la industria automotriz en Latinoamérica y ciberataques como el *ransomware* que literalmente secuestran los servidores a las empresas son tan sólo algunos de los muchos riesgos que llevan a la industria automotriz y a muchas otras a tomar medidas para conservar su eficiencia y competitividad en los mercados.

Adicionalmente, las cadenas de suministro en la industria automotriz, cada vez más largas y complejas requieren de una mayor gestión a cada paso de los procesos. Las empresas deben, sin duda, tener planes de contingencia actualizados con una directriz concisa entre las plantas y los corporativos que deje bien clara la situación y rol de cada uno de ellos durante una emergencia ya sea de tipo ambiental, política, socioeconómica, o por falla en alguno de los muchos procesos de la misma cadena de suministro.

El estricto cumplimiento de estándares es uno de los pasos fundamentales que las empresas automotrices siguen, y que incluyen planes de contingencia es el cumplimiento de estándares y regulaciones como

Foto: Creativeart - Freepik

La industria automotriz en México posee un peso más que significativo en términos económicos y sociales. Representa el 18% del PIB manufacturero, genera casi 200 mil empleos y más de 18 mil millones de dólares en exportaciones

Foto: Creativeart - Freepik

son el ISO / 9001 estándar internacional para calidad de administración de los sistemas; el IATF 16949, que es la especificación para la gestión de los sistemas de calidad en la industria automotriz; finalmente la MMOG / LE para el desarrollo de un sistema de gestión de la cadena de suministro que contenga mejoras continuas.

Dentro de las soluciones; una de las preguntas más frecuentes es ¿cómo lograr una mentalidad de prevención de riesgo?

La respuesta es relativamente simple y no difiere mucho de empresa a empresa. Adoptar una mentalidad de prevención, de acuerdo a los lineamientos ISO/9001:2015 requiere de comunicación, trabajo en equipo, y disciplina entre las áreas de la organización:

- Primero, determine los factores que pudieran alejar los procesos y el sistema de gestión de calidad de los resultados esperados.
- Segundo, ponga en marcha controles preventivos para minimizar los efectos.
- Tercero, aprovechar al máximo las oportunidades de mejora.

Para llegar a este estado de consciencia, es fundamental que las organizaciones sigan pasos específicos:

1. Definir los riesgos.
2. Priorizar.
3. Tener planes de acción actualizados y disponibles.
4. Hacer simulacros, entrenamientos, pruebas y sesiones de validación de las soluciones y forma de prevenir y/o enfrentar los riesgos.
5. Tener monitores continuos y enfoque en la prevención.

Sabemos que es imposible estar totalmente blindados ante la multitud de riesgos que pudieran afectar a las empresas; sin embargo, las organizaciones ciertamente pueden tener monitores y controles preventivos que minimicen algunos de los riesgos que se pudieran presentar.

Recordemos que la seguridad y la prevención y gestión de riesgos la hacemos todos. El compromiso debe existir en todas las áreas de la empresa, desde la dirección hasta los obreros en las plantas deben tener acceso a los planes de contingencia y deben cubrirse todos los posibles requerimientos incluidos en los pasos para mitigar los efectos de los riesgos.

Finalmente, lo que mantiene a las compañías fuertes en su posición ante sus clientes y proveedores es la calidad de sus productos y sus procesos. La satisfacción del cliente es el resultado de la totalidad de los procesos ejecutados adecuadamente y que hace a las empresas eficientes.

Todo esto lo logramos desde el área de Prevención y Protección al cumplir la razón de ser del área que se enfoca en dar la oportuna continuidad de operaciones y servicio además de sumar en concretar de manera permanente la rentabilidad del negocio. ■

José Luis Sánchez Gutiérrez,
gerente nacional de Protección Laboral y Patrimonial en Cadena de Suministro OXXO y Nuevas Avenidas de Negocio.

Más sobre el autor:

SEGURIDAD EN AMÉRICA

2021

Roadshows & Eventos ONLINE

Seguridad en Casas de Empeño y Servicios Prendarios
13 de enero

Videovigilancia en Zonas Urbanas
27 de enero

Gestión de Seguridad en Aeropuertos
10 de febrero

Seguridad en Pruebas de Confianza
24 de febrero

Seguridad en la Industria Manufacturera
10 de marzo

Administración de Flotillas
24 de marzo

Seguridad en Plataformas Marítimas
7 de abril

Centrales de Monitoreo
28 de abril

Seguridad en Parques Industriales
12 de mayo

Seguridad en Centros Educativos
26 de mayo

Seguridad en la Industria Farmacéutica
9 de junio

Seguridad en Bancos
22, 23 y 24 de junio

Cumbre Latinoamericana de Seguridad
14 y 15 de julio

Seguridad en Plantas Automotrices
11 y 12 de agosto

Seguridad en la Industria Hotelera
25 y 26 de agosto

Seguridad en la Industria Alimentaria
8 de septiembre

Seguridad en Aduanas y Recintos Fiscales
29 de septiembre

Blindaje Automotriz
13 de octubre

Soluciones de Seguridad en *Data Centers*
27 de octubre

Seguridad en Hospitales
10 de noviembre

Seguridad para Supermercados y Tiendas de Conveniencia
24 de noviembre

Seguridad en Casinos y Centros de Entretenimiento
1 de diciembre

Seguridad en Maquiladoras
15 de diciembre

100 Más Influyentes de la Seguridad Privada (Presencial)
29 de enero 2022

Reunimos a los tomadores de decisiones de la seguridad en distintos sectores para que usted ofrezca sus productos y/o servicios por medio de conferencias dinámicas.

Beneficios:

- Usted podrá impartir su conferencia a más de 500 profesionales de la seguridad.
- Interactuar directamente con tomadores de decisiones.
- Promocionar sus productos y servicios.

El patrocinio incluye:

- Base de datos de los asistentes.
- Reporte analítico de la estrategia de publicidad.
- Presentación de 30 minutos.

telemarketing@seguridadenamerica.com.mx
www.seguridadenamerica.com.mx
(55) 5572 6005

El análisis de los conceptos de calidad en la educación resulta una condición necesaria para promover la práctica reflexiva y continua

PANORAMA DE LA ACREDITACIÓN EN CALIDAD EN INSTITUCIONES DE EDUCACIÓN SUPERIOR DE **CRIMINOLOGÍA EN MÉXICO**

Foto: Creativeart - Freepik

MÉXICO

Wael Sarwat Hikal Carreón

INTRODUCCIÓN

El cambio educativo se convierte en un objeto de estudio cuando de éste se determina averiguar qué ocurre, los cambios y tendencias a los cuales se quiere dirigir para mejorar (Cantú, 2015). Así en el presente estudio se abordan los sistemas de calidad educativa como herramienta para el autoconocimiento, proceso de reflexión y mejora en los centros de educación superior en materia de criminología.

La metodología y método empleado es mediante la revisión documental de diversas fuentes, primero para conocer cómo se define calidad educativa, también el marco legal de esta desde la normatividad mexicana, que a su vez, da origen a organismos evaluadores. Se revisa la cantidad de escuelas que existen, y de estas, se investiga cuáles están en estándares de calidad nacional, lo cual, mediante metodologías de normalización, fueron evaluadas en aspectos de instalaciones, contenidos académicos, personal administrativo, docente e investigador, para arrojar resultados para el cambio, permanencia y/o continuación de la calidad.

De tal modo, como resultado, se presentan los centros escolares que han trabajado en ello. No se agota el tema aquí, la conclusión es una proposición a que otras escuelas se sumen a la autoevaluación y búsqueda de mejorar sus procesos, con repercusiones tangibles en su prestigio, economía, y responsabilidad social universitaria (Iñigo-Bajos y Sosa-Castillo, 2015).

La calidad es un término presente en diversos aspectos de la vida, esta es un marco referencial para direccionar la producción y prestación de servicios, siendo la calidad educativa el área que aquí se aborda. Miguel (1995) menciona la necesidad de construir indicadores de calidad objetivables, precisos y seguros porque la evaluación interna es el único instrumento que permite detectar trayectorias erróneas y corregirlas en la dirección marcada" (p. 3.). También "con base en el diseño de perfiles, parámetros e indicadores" (Acuña-Gamboa y Pons-Bonals, 2016, p. 167). Esto es

puesto que vivimos en un ambiente de la calidad o cultura de calidad.

Señala Rodríguez-Arocho (2010) que "la calidad educativa es entendida de forma multidimensional y contextual. Más allá de los índices de matrícula, retención y aprovechamiento académico" (p. 18). Parte de los procesos de la calidad, son: inspeccionar, asegurar la calidad, mantener el nivel, con esto se tiene una "calidad total", el primero entendido como la evaluación de la producción o los procesos de producción, el segundo, como, una vez identificados, descritos y controlados los procesos, se puede trabajar en el perpetuar las actividades inherentes, finalmente, con el ciclo continuo, se tiende a mantener tal nivel. En calidad total, se asumiría como la satisfacción de deseos y expectativas de los clientes. Esto, si se aplica al centro escolar, procura atender a los intereses particulares de la población (Rodríguez-Arocho, 2010).

La calidad también es vista "como lo propio de algo que lo hace diferente" (Vásquez-Tasayco, 2013, p. 49), pone en relieve la funcionalidad en relación a los elementos que conducen a la eficacia en los sistemas, y poner atención en el producto, en el que se vierte el resultado de la funcionalidad y se mide con la satisfacción o el nivel de complacencia (Bonifacio-Barba, 2018).

Se desmenuza que en el proceso de calidad, se parte en elementos que dan lugar a tal, y de lo formado por la relación de sus compuestos de manera lógica, muestran lo diferente y específico de ese total, lo que también se entiende como el desarrollo de la construcción de una unidad, en este caso, calidad educativa.

Los elementos de la calidad desde un enfoque de sistema serían (Vásquez-Tasayco, 2013): insumos (infraestructura, equipamiento, docentes, personal administrativo, libros, espacios adecuados, laboratorios, bibliotecas), procesos (auditorías), productos (programas educativos, alumnos), dinámica (relaciones que permiten adquirir compromisos, planeación docente), redes de calidad interna (quienes ayudan a lograr objetivos) y externa (organismos de normalización) (Acuña-Gamboa y Pons-Bonals, 2016).

En México, la calidad educativa se asentó en las normas federales que rigen el funcionamiento de las instituciones públicas y privadas que imparten educación. La principal norma es la Constitución Política de los Estados Unidos Mexicanos (Cámara de Diputados, 2019-a), presentando la plataforma del sistema educativo nacional y su operación, posteriormente la legislación especial de la materia, Ley General de Educación (Cámara de Diputados, 2019-b) que amplía los procesos de la educación en México, y los estándares de calidad.

La Constitución Política de los Estados Unidos Mexicanos (Cámara de Diputados, 2019-a) establece en su artículo 3, que los estados deben proveer la educación superior. De los elementos estructurales para la calidad educativa, se desprende el primero de ellos referente a los formadores del conocimiento, señala: "Las maestras y los maestros son agentes fundamentales del proceso educativo y, por tanto, se reconoce su contribución a la trasformación social" (Cámara de Diputados, 2019-a, p. 5).

La relación de dependencia para el desarrollo de la calidad es: la institución de educación superior es reconocida en sus programas educativos de buena calidad de pregrado o posgrado

Otro aspecto primordial son las instituciones: "Los planteles educativos constituyen un espacio fundamental para el proceso de enseñanza aprendizaje" (Cámara de Diputados, 2019-a, p. 6), y como tercer elemento, los contenidos de la formación: "Los planes y programas de estudio tendrán perspectiva de género y una orientación integral, por lo que se incluirá el conocimiento de las ciencias y humanidades" (Cámara de Diputados, 2019-a, p. 6).

La máxima educativa, rectora del proceso de enseñanza en todos sus niveles es: "El criterio que orientará a esa educación se basará en los resultados del progreso científico, luchará contra la ignorancia y sus efectos, las servidumbres, los fanatismos y los prejuicios" (Cámara de Diputados, 2019-a, p. 6).

Retomando Ley General de Educación (Cámara de Diputados, 2019-b), está encuentra su aplicación a través de la Secretaría de Educación Pública (SEP) que respecto la calidad educativa, aborda la evaluación de los planteles y da creación también a los organismos privados acreditadores, establece que dentro de sus facultades están: "Ejercer la supervisión y vigilancia que proceda en los planteles que impartan educación" (Cámara de Diputados, 2020, p. 42).

La primicia se asienta en el artículo 72: "Recibir una educación de excelencia" (Cámara de Diputados, 2019-b, p. 25). Es útil para principiar y mantener los estándares iniciales de calidad en la

Foto: Creativeart - Freepik

estructura y funcionamiento, focalizado a la mejora educativa. La SEP autoriza al Consejo para la Acreditación de la Educación Superior (COPAES) y Comités Interinstitucionales para la Evaluación de la Educación Superior (CIEES) para la evaluación y acreditación.

COPAES "es una asociación civil sin fines de lucro que confiere el reconocimiento formal y supervisa a organizaciones cuyo fin sea acreditar programas académicos del tipo superior que se imparten en México, en cualquiera de sus modalidades" (Consejo para la Acreditación de la Educación Superior, 2019). Mientras que los CIEES "son el organismo que le dio nacimiento en 1991 al proceso de aseguramiento de la calidad de la educación superior mexicana" (Secretaría de Educación Pública, 2018).

Por último, se abordan también aspectos de progreso más allá de la formación básica superior, señala que: "[…] El Estado apoyará la investigación e innovación científica, humanística y tecnológica, y garantizará el acceso abierto a la información que derive de ella, para lo cual deberá proveer recursos y estímulos suficientes [...]" (Cámara de Diputados, 2019-a, p.7).

Esto enlaza con una norma especial creada para el fomento a la ciencia, Ley Orgánica del Consejo Nacional de Ciencia y Tecnología (Cámara de Diputados, 2014). Tal norma da lugar al nacimiento del Consejo Nacional de Ciencia y Tecnología, el cual evalúa la calidad y funciones de instituciones públicas y privadas, centros de investigación, publicaciones en revistas, evalúa publicaciones, las certifica, genera estímulos para apoyo a la labor del desarrollo científico mediante programa de jóvenes investigadores, investigadores nacionales, sistema de becarios, entre otros programas y estrategias (Consejo Nacional de Ciencia y Tecnología, 2020).

METODOLOGÍA

El método empleado es el documental, primero se revisan conceptos de calidad en la educación tomados de diferentes autores (Bonifacio-Barba, 2018; Acuña-Gamboa y Pons-Bonals, 2016; Vásquez-Tasayco, 2013; Rodríguez-Arocho, 2010; Miguel, 1995) para establecer las bases sobre qué aspectos se consideran en referencia durante los procesos de evaluación.

Posteriormente, se buscan las bases legales de la educación de calidad en las normatividades federales en México, por lo que se consulta la Constitución Política de los Estados Unidos Mexicanos (Cámara de Diputados, 2019-a), Ley General de Educación (Cámara de Diputados, 2019b) y la Ley Orgánica del Consejo Nacional de Ciencia y Tecnología (Cámara de Diputados, 2014) que dan las directrices para la calidad en los centros escolares de manera estructural, así como en sus programas de estudio de pre y posgrado, además de facultar a órganos privados y descentralizados para evaluar y acreditar.

Se consulta el "Censo de centros escolares y programas educativos en criminología, criminalística, victimología y carreras afines en México" (Hikal-Carreón, 2020) para conocer el universo de instituciones que imparten los estudios en criminología y áreas afines, y en qué niveles (pre y posgrado).

Finalmente, se realiza una consulta mesográfica en los padrones de programas educativos de los portales electrónicos de las instituciones facultadas (Secretaría de Educación Pública y Consejo Nacional de Ciencia y Tecnología) por las leyes antes señaladas, para identificar qué centros, qué programas de estudio, qué organismos las acreditaron (Comités Interinstitucionales para la Evaluación de la Educación Superior y Consejo para la Acreditación de la Educación Superior) y en el caso de posgrados, en qué nivel están acreditados en calidad (reciente creación, en desarrollo, consolidado o competencia internacional).

> La relación de dependencia para el desarrollo de la calidad es: la institución de educación superior es reconocida en sus programas educativos de buena calidad de pregrado o posgrado

Foto: Creativeart - Freepik

RESULTADOS Y DISCUSIÓN

Consultado el "Censo de centros escolares y programas educativos en criminología, criminalística, victimología y carreras afines en México" (Hikal-Carreón, 2020), se obtuvo que el universo de centros escolares es de 401 instituciones que imparten los niveles de bachillerato técnico, licenciatura, en línea, especialidad, maestría y doctorado, de los cuales, son 527 programas educativos.

La SEP cuenta con el Padrón Nacional de Programas Educativos de Calidad (PNPEC) (Secretaría de Educación Pública, 2018), el cual se forma de los programas educativos y centros escolares que fueron evaluados y acreditados por los organismos autorizados

(COPAES y CIEES) (Comités Interinstitucionales para la Evaluación de la Educación Superior, 2020) por la SEP para tales fines. En su fuente de datos, indican que existen de manera global de todos los programas educativos en todas las áreas del conocimiento, 4 mil 811 están en el PNPEC, de las cuales, para el área que interesa en este estudio, el resultado se muestra en la siguiente tabla:

PROGRAMAS LICENCIATURA		
Programa	Institución educativa	Certificación
Licenciatura en Criminalística	Centro de Estudios Universitarios Xochimilco (plantel Rampa Yujimalinda)	COPAES
Licenciatura en Criminalística	Centro de Estudios Universitarios Xochimilco (plantel calle Novena)	COPAES
Licenciatura en Criminología	Universidad Autónoma de Nuevo León, Facultad de Derecho y Criminología	COPAES CIEES
Licenciatura en Criminología	Universidad Autónoma de Querétaro, Facultad de Derecho	CIEES
Licenciatura en Criminología	Universidad Autónoma de Tamaulipas, Unidad Académica Multidisciplinaria Reynosa-Aztlán	CIEES
Licenciatura en Criminología	Universidad Ixtlahuaca	CIEES
Licenciatura en Criminología, Criminalística y Técnicas Periciales	Colegio Libre de Estudios Universitarios (plantel Puebla)	CIEES
Licenciatura en Seguridad Pública	Universidad Abierta y a Distancia México	CIEES

Por: Wael Sarwat Hikal Carreón.

Por otra parte, en el Padrón Nacional de Posgrados de Calidad (PNPC) del CONACYT, de 2 mil 394 programas acreditados en todos los campos del saber, los siguientes posgrados en materia criminal están reconocidos (Consejo Nacional de Ciencia y Tecnología, 2019). Los niveles mostrados se fundamentan en la clasificación que establece el CONACYT, estos se refieren a: 1) Reciente creación (estándares básicos), 2) En desarrollo (metas de mejora), 3) Consolidados (pertinencia e impacto en la formación y producción), y 4) Competencia internacional (redes, movilidad, producción) (Consejo Nacional de Ciencia y Tecnología, 2019).

PROGRAMAS POSGRADO		
Programa	Institución educativa	Nivel
Doctorado en Criminología	Universidad Autónoma de Nuevo León, Facultad de Derecho y Criminología	En desarrollo
Doctorado en Psicología con Énfasis en Salud y Violencia	Universidad Autónoma de Ciudad Juárez, Instituto de Ciencias Sociales y Administración	En desarrollo
Maestría en Criminología y Ciencias Forenses	Universidad Autónoma de Tamaulipas, Unidad Académica Multidisciplinaria Reynosa-Aztlán	Consolidada
Maestría en Medicina Forense	Universidad Veracruzana, Instituto de Medicina Forense	Consolidada
Maestría en Valuación	Universidad Autónoma de Nuevo León, Facultad de Arquitectura	En desarrollo
Especialidad en Familias y Prevención de la Violencia	Universidad Autónoma de Querétaro, Facultad de Ciencias Políticas y Sociales	En desarrollo
Especialidad en Género, Violencia y Políticas Públicas	Universidad Autónoma del Estado de México, Facultad de Ciencias Políticas y Sociales	En desarrollo

Por: Wael Sarwat Hikal Carreón.

La Licenciatura en Criminología de la FACDYC de la UANL es la única escuela en el país que cuenta con doble acreditación. Asimismo, es la única con un programa de doctorado acreditado en CONACYT

De lo observado en las tablas, resalta la atención la Licenciatura en Criminología de la Facultad de Derecho y Criminología (FACDYC) de la Universidad Autónoma de Nuevo León (UANL), que es la única escuela en el país que cuenta con doble acreditación (COPAES y CIEES). Asimismo, es la única con un programa de doctorado acreditado en CONACYT.

Los programas de calidad son el resultado de dictámenes técnicos llevados por organismos acreditadores especializados, autorizados por la SEP y que no sean gubernamentales, que se realiza a petición de la institución educativa, y como resultado tiene observaciones y sugerencias, que de ser atendidas, y nuevamente evaluadas, la institución recibe el "testimonio público de calidad" (Secretaría de Educación Pública, 2018). Es útil para principiar y mantener los estándares iniciales de calidad en la estructura y funcionamiento, focalizado a la mejora educativa.

De modo general, el proceso consiste en un autodiagnóstico de la institución para detectar qué condiciones están y qué podrían mejorar, seguido de solicitar la asistencia de evaluadores externos, se realizan auditorías de calidad, evaluación de calidad, revisando los procesos, prácticas, programas y servicios, entre otros, puede ser de manera voluntaria, a diferencia de que para poner en función una institución de educación, es obligada la vigilancia. La acreditación de la calidad, permite controlar la misma, cumplimiento de estándares, rendición de cuentas, transparentar procesos, mejorar, favorece el prestigio de la institución, impulsa la economía, permite la vinculación institucional, entre otros objetivos y beneficios.

El PNPEC sirve para dar a conocer al público interesado "los programas de calidad reconocidos por organismos evaluadores y acreditadores" (Unidad de Educación Media Superior Tecnológica Industrial y de Servicios, 2018). Por su parte, estar en el PNPC, es: "El reconocimiento a la calidad de la formación de los programas de posgrado que ofrecen las instituciones de educación superior y los centros de investigación se lleva a cabo mediante rigurosos procesos de evaluación por pares académicos" (Consejo Nacional de Ciencia y Tecnología, 2019).

Para que una institución educativa postule sus posgrados, deben atender a las convocatorias que el CONACYT publica en sus medios de difusión, de los beneficios que se obtienen, de manera general, por parte de la SEP y el CONACYT es el reconocimiento de estas dos instituciones hacia sus programas académicos de formación de recursos humanos de alta calidad y competitividad, son las máximas acreditaciones que a nivel nacional se pueden obtener, el beneficio para el alumnado es formarse en un posgrado de máxima calidad nacional, obtener manutención económica durante el tiempo de estudios, estancias educativas y de investigación, servicio de salud pública, así como la posibilidad de continuar al posdoctorado, y oportunidades laborales.

Foto: Creativeart - Freepik

En síntesis, la relación de dependencia para el desarrollo de la calidad es: la institución de educación superior es reconocida en sus programas educativos de buena calidad de pregrado o posgrado, en efecto, ofertan buena calidad educativa, que implica su alta capacidad académica, competitividad e innovación, que le antecede la gestión universitaria adecuada (Gaete, 2015), por ende la distinción de certificación de sus procesos académicos (Cantú-Medonza, 2015).

Esto no demerita la calidad y esfuerzos del resto de los posgrados que no lo están, pero es una invitación a que se sumen y mejoren los contenidos de los programas, estructura de sus edificios, distribución de áreas, planta docente, y áreas de investigación (cuerpos, inclusión de alumnos, generación de líneas), entre otros esfuerzos que impactan positivamente en la sociedad (Barfusón, 2018).

> Miguel (1995) menciona la necesidad de construir indicadores de calidad objetivables, precisos y seguros, porque la evaluación interna es el único instrumento que permite detectar trayectorias erróneas y corregirlas en la dirección marcada

CONCLUSIONES

El análisis de los conceptos de calidad en la educación resulta una condición necesaria para promover la práctica reflexiva y continua, comprender de qué se trata a nivel diagnóstico de las condiciones que guarda el centro educativo, y las líneas de cambio a trabajar con base en las características, fines y objetivos de los estándares de calidad en la educación.

COPAES “es una asociación civil sin fines de lucro que confiere el reconocimiento formal y supervisa a organizaciones cuyo fin sea acreditar programas académicos del tipo superior que se imparten en México, en cualquiera de sus modalidades”

No se especula sobre los procedimientos de mejora educativa con bases en la introducción de la calidad, sino que tiene una secuenciación lógica de actividades las cuales se ven establecidas por organismos evaluadores y acreditadores; es decir, agentes externos a la institución educativa, que mediante parámetros específicos, auditan, sugieren y evalúan, en México, según el grado a evaluar, el programa educativo, entre otros, es la institución que le evaluara.

La acreditación es una garantía de calidad, a los fines de esta investigación, el aplicar sistemas de gestión de calidad resulta útil para iniciar con un régimen de evaluaciones internar (autodiagnósticos) y externa (por agentes ajenos) que permita identificar aspectos a trabajar para mejorar como institución con diversos resultados: mejora interna en la institución, mejores prácticas y procesos, personal idóneo y comprometido, apto para sus funciones administrativas, como cuando corresponda, en la formación de los educandos.

Y que éstos sean capacitados con calidad, abundancia de recursos, en el conocimiento, práctica, humanismo, ética, compromiso social, y de esto se espera una correspondencia de satisfacción personal con la profesión en el ámbito emocional, familiar, económico, social, que a su vez resulte en responsabilidad social; es decir, atender las funciones para las cuales fue creada una profesión, o los problemas sociales en su caso.

Se espera que este artículo sirva de guía para otras escuelas que deseen aproximarse a los estándares de calidad educacional, de manera general y puntual se presentaron las bases legales, ideales de la educación, instituciones evaluadoras, procesos, y beneficios.

El presente artículo fue publicado en la revista “Atenas. Revista Científico Pedagógica”, núm. 55, julio-septiembre, 2021. ■

Foto: Creativeart - Freepik

REFERENCIAS

- *Acuña-Gamboa, L.A. y Pons-Bonals, L. (2016). Calidad educativa en México. De las disposiciones internacionales a los remiendos del proyecto nacional. Revista Internacional de Investigación en Ciencias Sociales, 12(2), 155-174. http://scielo.iics.una.py/pdf/riics/v12n2/2226-4000-riics-12-02-00155.pdf*
- *Bonifacio-Barba, J. (2018). La calidad de la educación. Los términos de su ecuación. Revista Mexicana de Investigación Educativa. 23(78), 963-979. https://www.comie.org.mx/revista/v2018/rmie/index.php/nrmie/article/view/1184/1167*
- *Cámara de Diputados (2020). Ley Orgánica de la Administración Pública Federal. http://www.diputados.gob.mx/LeyesBiblio/pdf/153_110121.pdf*
- *Cámara de Diputados (2019-a). Constitución Política de los Estados Unidos Mexicanos. http://www.diputados.gob.mx/LeyesBiblio/pdf/1_201219.pdf*
- *Cámara de Diputados (2019-b). Ley General de Educación. http://www.diputados.gob.mx/LeyesBiblio/pdf/LGE_300919.pdf*
- *Cámara de Diputados (2014). Ley Orgánica del Consejo Nacional de Ciencia y Tecnología. http://www.diputados.gob.mx/LeyesBiblio/pdf/243.pdf*
- *Cantú-Mendoza, R. (2015). Nuevos retos a la gestión de la educación superior en México. En R. Cantú-Mendoza (Editor). La Responsabilidad Social de las Universidades Contemporáneas (pp. 13-38). Universidad Autónoma de Nuevo León y Editorial Itaca.*
- *Comités Interinstitucionales para la Evaluación de la Educación Superior (2020). Padrón Nacional de Programas Educativos de Calidad de la SEP. https://www.ciees.edu.mx/version1/padrones-de-buena-calidad/padron-nacional-de-programas-educativos-de-buena-calidad-de-la-sep/*
- *Consejo Nacional de Ciencia y Tecnología (2020). Inicio. https://www.conacyt.gob.mx/*
- *Consejo Nacional de Ciencia y Tecnología (2019). Programa Nacional de Posgrados de Calidad. https://www.conacyt.gob.mx/index.php/becas-y-posgrados/programa-nacional-de-posgrados-de-calidad*
- *Consejo para la Acreditación de la Educación Superior (2019). Origen de COPAES. https://www.copaes.org/copaes.html#mision*
- *Gaete-Quezada, R. (2015). El gobierno y la gestión universitaria como ámbito de aplicación de la responsabilidad social. En R. Cantú-Mendoza (coord). La Responsabilidad Social de las Universidades Contemporáneas (pp. 143-156). Universidad Autónoma de Nuevo León y Editorial Itaca.*
- *Hikal-Carreón, W.S. (2020). Censo de centros escolares y programas educativos en criminología, criminalística, victimología y carreras afines en México. Archivos de Criminología, Seguridad Privada y Criminalística, 8(15), 154-182. http://doi.org/10.5281/zenodo.3840708*
- *Iñigo-Bajos, E. y Sosa-Castillo, A.M. (2015). Mitos y objetivos de la responsabilidad social universitaria. En R. Cantú-Mendoza (coord). La Responsabilidad Social de las Universidades Contemporáneas (pp. 157-174). Universidad Autónoma de Nuevo León y Editorial Itaca.*
- *Miguel, De, F.M. (1995). La calidad de la educación y las variables de proceso y de producto. Ikastaria: Cuadernos de Educación, 8, 29-52. http://www.euskomedia.org/PDFAnlt/ikas/08/08029051.pdf*
- *Rodríguez-Arocho, W. (2010). El concepto de calidad educativa: Una mirada crítica desde el enfoque históricocultural. Revista Electrónica “Actualidades Investigativas en Educación”, 10(1), 1-28. https://www.redalyc.org/articulo.oa?id=44713068015*
- *Secretaría de Educación Pública (2018). Padrón Nacional de Programas Educativos de Calidad. https://www.pnpec.sep.gob.mx/*
- *Unidad de Educación Media Superior Tecnológica Industrial y de Servicios (2018). Padrón Nacional de Programas Educativos de Calidad. https://uemstis.sep.gob.mx/index.php/la-dgeti-hoy/296-padron-nacional-de-programas-educativos-de-calidad-pnpec*
- *Vásquez-Tasayco, A. (2013). Calidad y calidad educativa. Investigación Educativa. 17(2), 49-71. https://revistasinvestigacion.unmsm.edu.pe/index.php/educa/article/view/8206/7157*

Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León, México.

Más sobre el autor:

SEGURIDAD EN CONJUNTOS HABITACIONALES

Entre vecinos te verás

Foto: Creativeart - Freepik

MÉXICO | David Chong Chong

Los conjuntos habitacionales constituyen un microcosmos de la sociedad, con un perfil de diversidad, complejidad y heterogeneidad de personalidades, costumbres e intereses compartiendo y conviviendo en un mismo espacio, con un potencial inevitable e ineludible de conflictos que alteran el orden y tranquilidad de la comunidad, y por ende involucra la intervención del personal de seguridad, lo cual requiere de habilidades muy particulares, en especial de interacción personal.

Un conjunto habitacional consiste en un espacio delimitado, o al menos acotado con alguna forma de barrera o señalización, en el que se ubican varias residencias (casas o departamentos), bajo ciertas reglas o normas de convivencia. Estos espacios pueden ubicarse en estructuras cerradas (edificios) o dispersas (casas), y comprenden espacios particulares, que corresponden a las residencias, y áreas comunes, como las vialidades y áreas de esparcimiento.

La población presente puede ser de residentes (propietarios o inquilinos), habituales (personal de servicio doméstico, servicios técnicos o servicios públicos como recolección de basura, correo), o esporádicos (visitantes y autoridades). Asimismo, la dinámica dentro del conjunto detenta un perfil predominantemente rutinario, con permanencia dentro de las residencias en ciertos horarios, así como en las áreas comunes y deambulación en las vialidades.

La normatividad de un conjunto habitacional se orienta a regular las condiciones de convivencia entre los residentes, el uso de las áreas y servicios comunes, así como de vialidades, y en ciertos casos el control de acceso al mismo. En este contexto, la Seguridad del conjunto habitacional está enfocada en mantener el clima de orden y tranquilidad, con dos objetivos básicos:

- Control de acceso, es decir, gestionar las entradas y salidas de personas y bienes a la instalación.
- Continuidad de la dinámica comunitaria, es decir que las actividades, tanto rutinarias como esporádicas, se desarrollen sin interrupciones ni interferencias, asegurando la observancia y cumplimiento de las normativas, y enfrentando, cuando sea necesario, las amenazas contra las personas y sus propiedades dentro de la instalación.

Para estos efectos, el personal de seguridad en estas instalaciones debe contemplar dos vertientes de atención, una genérica que se refiere a las amenazas o riesgos comunes que suelen provenir de agentes externos o internos (intrusos, agresores, etc.), y una particular, que se refiere al potencial de conflictos derivados de la propia dinámica dentro de la instalación.

FUENTE DE RIESGOS

El potencial de conflictos suele surgir, más que del quebrantamiento de estas normas, de los efectos de su incumpli-

miento tanto sobre la comunidad como en algún segmento de la población dentro del mismo, derivado, entre otras, de las siguientes situaciones:

- Comunidad vs. privacidad. La fuente más frecuente de conflictos es el choque de los intereses comunitarios con la privacidad de los residentes, o bien de residentes entre sí. Esas discrepancias se derivan de la diversidad de personalidades, hábitos y costumbres, proyectados como efectos "ambientales" (sonidos, olores, acciones, objetos, etc.), los cuales, de alguna manera "invaden" áreas comunes o espacios de privacidad de otros residentes. Entre las causas más comunes de esta situación destacan aspectos subjetivos de interpretación de las normas (por lo regular en favor del interés particular de un residente), empatía interpersonal, visión de vida, etc. Asimismo, la misma población, en especial los residentes, bajo esta óptica de interpretación de la normatividad, abre espacios de oportunidad para agentes externos al facilitarles el acceso a la instalación, dando "la ocasión que hace al ladrón".

- Persistencia por la convivencia. Los conflictos dentro del conjunto, en especial entre residentes, suelen generar una secuela de resentimientos que no desaparecen con el tiempo, sino se amplían y distorsionan por la diaria convivencia entre las partes en conflicto, de tal suerte que pueden reactivarse por otras causas que, sin el conflicto previo, no generarían un mayor problema, pero que con los antecedentes, provocan una nueva confrontación.

- Contaminación vecinal. Las secuelas de un conflicto dentro del conjunto no se limitan a las partes involucradas directamente, sino que se extienden a los círculos sociales de cada parte (amigos, conocidos, familiares o simpatizantes), que tienden a solidarizarse con su perspectiva parcial del evento, de tal manera que se crean visiones de animadversión entre segmentos de la población (el síndrome "Montescos contra Capuletos"). Y paradójicamente, con el tiempo se llega a olvidar la causa inicial de tales antagonismos.

De tal suerte que se puede proyectar como la fuente más probable de conflictos, y por ende de riesgos, dentro de un conjunto habitacional, a la propia población en todas sus modalidades. En este contexto, es más probable que el personal de seguridad enfrente situaciones de conflicto interno que amenazas externas, de tal manera que, para un desempeño efectivo de sus responsabilidades, debe tener un conocimiento y preparación, además de aspectos genéricos como el conocimiento del terreno y de la normatividad, otros más especializados para este tipo de instalaciones, que comprenden, entre otros, reconocimiento visual de los residentes, y si es posible de los

Foto: Creativeart - Freepik

El personal de seguridad en estas instalaciones debe contemplar dos vertientes de atención, una genérica que se refiere a las amenazas o riesgos comunes; y una particular, que se refiere al potencial de conflictos derivados de la propia dinámica dentro de la instalación

habituales, la dinámica comunitaria, y la identificación y ubicación de puntos y partes en conflicto entre la población.

Asimismo, la efectividad del personal de seguridad puede comprometerse por el trato frecuente con la población, que propicia relaciones de cercanía y empatía personal, que derivan en tratos preferenciales ajenos a sus funciones nominales (encargos, favores), o en intervenciones en conflictos, lo que se puede intensificar si las condiciones laborales del personal no son satisfactorias, así como por prácticas de extorsión por parte de la población, ejercidas bajo la premisa de "el que paga manda", sobre todo de residentes, y más aún si detentan alguna forma de autoridad dentro de la comunidad.

Por ello, para procurar la efectividad del servicio de seguridad, es recomendable que el personal en estas instalaciones esté capacitado en el manejo de interacciones personales y mediación de conflictos, además de reducir la insatisfacción laboral y los espacios de oportunidad para las prácticas de extorsión de la población, por medio de acuerdos de responsabilidades y facultades de actuación, bajo la consigna general de "que no le pase nada" a las personas y bienes dentro de la instalación, aún en ausencia de sus propietarios. ■

Foto: Creativeart - Freepik

David Chong Chong,
secretario general para México de la Corporación Euro Americana de Seguridad (CEAS) México.

Más sobre el autor:

Foto: Creativeart - Freepik

SEGURIDAD PREVENTIVA INTEGRAL: LA REALIDAD NO VOLVERÁ A SER IGUAL A LO QUE ERA ANTES DE LA PANDEMIA

El ciudadano debe tomar conciencia de que su seguridad depende exclusivamente de sí mismo y no de alguien que lo esté vigilando o controlando

PERÚ | César Ortiz Anderson

En este artículo desarrollaremos la perspectiva de Aprosec (Asociación Pro Seguridad Ciudadana del Perú) respecto a la importancia que tiene adoptar una nueva cultura de Seguridad Preventiva Integral para poder acceder a la "nueva normalidad" en pandemia y en pospandemia, no sin antes advertir que Aprosec estudia y analiza la problemática de la inseguridad ciudadana teniendo en cuenta las particularidades de la idiosincrasia de nuestro pueblo.

Antes que nada debemos resaltar que: no es posible vivir en una "nueva normalidad" en pandemia si es que no se adopta una nueva cultura de Seguridad Preventiva.

La pandemia ha alterado el orden social en el mundo entero y la realidad no volverá a ser igual a lo que era antes de la pandemia. No se sabe exactamente la magnitud del impacto sociocultural de la pandemia ni hasta dónde ni cuánto va a cambiar el mundo. La única certeza posible es la "nueva normalidad" que nos permite seguir más o menos con un orden social estable aplicando protocolos de seguridad establecidos evitando los contagios y la propagación del virus que causa la pandemia.

INCREMENTO DE LA CRIMINALIDAD

Como uno de los países con más pobreza en la región, el Perú es uno de los países más golpeados por la pandemia en el mundo, con una mayor cantidad de víctimas mortales por millón de habitantes. Al mismo tiempo gran parte de la "nueva clase media peruana", producto del "milagro económico peruano" ha caído nuevamente en la pobreza por la crisis económica y desempleo. En consecuencia, la violencia y la inseguridad se incrementan, por lo que la prevención de la criminalidad y del delito ya sea de parte de las autoridades o de de los mismos ciudadanos, dependen hoy más que nunca de la Seguridad Preventiva Integral.

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

A pesar de los procesos de vacunación masiva que han alcanzado a millones de personas todavía nos encontramos en plena incertidumbre, porque la ciencia médica no sabe con certeza en qué momento de la pandemia nos encontramos

En el contexto de pandemia o pospandemia encontramos crisis social y económica, desempleo, aumento de la violencia y la criminalidad, una deficiente salud física y mental de la población, inestabilidad política, entre otros problemas que ponen en riesgo el orden social y la gobernabilidad de los países. Es por eso que en el contexto pospandemia la gobernabilidad sólo será posible a través de una nueva cultura de la Seguridad Preventiva Integral.

A pesar de los procesos de vacunación masiva que han alcanzado a millones de personas todavía nos encontramos en plena incertidumbre, porque la ciencia médica no sabe con certeza en qué momento de la pandemia nos encontramos. Debemos recordar la experiencia de la Gripe Española, la pandemia que azotó el mundo hace 100 años, cuando la segunda y la tercera ola fueron más letales porque la población descuidó los protocolos de seguridad al final de la primera ola.

RESILIENCIA

Otro factor en juego es la resiliencia y las consecuencias de diferente impacto que en la sociedad dejan la pérdida de los seres queridos, el quiebre y bancarrota de empresas, negocios y ahorros, con el respectivo golpe moral y el deterioro en la salud mental que esto significa. Acá es necesario indicar que debemos cambiar nuestras normas de vida, afrontar la realidad con una actitud diferente que es la prevención integral.

Con la pandemia el mundo cambió y nada volverá a ser igual que antes. La nueva cultura de Seguridad Preventiva Integral implica adoptar:

a) **Una nueva rutina:** un nuevo orden y una nueva disciplina alrededor de la cual organizamos nuestros días y nuestras vidas.

b) **Nuevos hábitos, prácticas, costumbres y tradiciones.** Por ejemplo, nuevos hábitos de consumo, abandonar ciertas costumbres, dar prioridad a unas cosas sobre otras como prestarle más atención al cuidado de la salud o a la seguridad personal que a la diversión o al esparcimiento.

c) **Nueva economía, nuevos negocios, formas de trabajar, de estudiar etc.**

Resulta imperioso que cada uno personalmente y, la sociedad en su conjunto, adopten una nueva cultura de Seguridad Preventiva Integral, porque nunca hemos sido capaces de convivir en una cultura preventiva del delito. El ciudadano no siente que pueda ser partícipe de una cultura preventiva del delito y percibe que es una responsabilidad que corresponde exclusivamente de las autoridades. Este concepto de la seguridad debe cambiar por otro en donde el ciudadano es protagonista de la seguridad preventiva adoptando nuevas costumbres, nuevos hábitos, nuevas rutinas que prevengan la vulnerabilidad y la victimización del ciudadano ante el delito.

Asimismo, en nuestro país (Perú) la gente sólo cumple las normas para evitar la sanción pero no por conciencia, por modo propio o por su propia seguridad. Esta mentalidad debe cambiar. El ciudadano debe tomar conciencia de que su seguridad depende exclusivamente de sí mismo y no de alguien que lo esté vigilando o controlando.

En conclusión, la nueva normalidad de la sociedad depende totalmente de la nueva cultura de la prevención. No seguir una cultura de Seguridad Preventiva Integral hoy nos puede costar la vida, por la pandemia o por la delincuencia.

Finalmente, como reflexión, observamos que a pesar de todo el impacto negativo que la pandemia produce en la humanidad, ésta no ha cambiado en su proceder en cuanto al egoísmo y avaricia de intereses particulares que en medio de la pandemia continúan corrompiendo países, empresas, y gobiernos. Creemos en el progreso moral de la humanidad, el cual tiene que ir por delante de todo avance en la economía o en la ciencia. ■

César Ortiz Anderson,
presidente de Aprosec (Asociación Pro Seguridad Ciudadana del Perú).

Más sobre el autor:

"La única medicina contra el sufrimiento, la delincuencia, y todos los demás males de la humanidad, es la sabiduría", Thomas H. Huxley (Biólogo británico – 1825-1895)

LA EVOLUCIÓN DE LA MODALIDAD DELICTIVA *"MOTOCHORROS"*

ARGENTINA | Jorge Gabriel Vitti

En la edición 115, me había referido a una modalidad delictiva en aumento en las áreas urbanas: los "motochorros". Este particular *modus operandi* se materializa con el robo a mano armada (normalmente arma de fuego), por parte de delincuentes que se desplazan en motocicletas por parejas, en uno o más vehículos. Una vez seleccionada la víctima (normalmente en arterias poco transitadas y contra personas solitarias), el acompañante desciende y ejecuta el ilícito, y se vuelve a subir a la moto para darse a la fuga.

Asimismo, es muy preocupante el empleo efectivo de armas de fuego por parte de los agresores, aun cuando la situación no lo amerita, e incluso en oportunidad de darse a la fuga. La maniobrabilidad y velocidad de los desplazamientos de los vehículos utilizados permiten un escape impune. Ahora bien, al no ser una situación nueva, debemos tomar debida nota de la evolución:

LA OPORTUNIDAD CRIMINAL

Siempre juega un papel preponderante la oportunidad criminal. En términos de prevención, se han tornado peligrosos los alrededores inmediatos de los establecimientos educativos. Numerosos hechos con esta modalidad delictiva se han producido en dichos lugares, particularmente dirigido al robo de celulares aprovechando la distracción de los padres que esperan a los niños, como así también contra aquellos menores que se desplazan en soledad. En tal sentido, la pandemia y el cese de la presencialidad dejaron de lado medidas de prevención comunitarias como los corredores escolares, por ejemplo. Es menester retomar estos procedimientos de probada eficacia, con el retorno de la asistencia escolar.

EL OBJETIVO CONCRETO *VS.* EL OBJETIVO TRASCENDENTE

También la economía criminal ha cambiado. Lo que antes representaba el celular robado como elemento de lucro concreto y único, ahora se ha diversificado. No es sólo la venta del aparato en sí, sino que se ha ampliado por el auge de los delitos informáticos. Resulta notable la habilidad adquirida para las estafas, fraudes y suplantación de identidad llevadas a cabo desde los dispositivos robados. De hecho, constituyen el objetivo predominante o trascendente del robo.

Es así como, por ejemplo, el 24 de julio en una pizzería de la ciudad de Córdoba, Argentina, un delincuente aprovechó un descuido de los empleados y se robó el celular del comercio, dándose a la fuga en la moto que lo estaba aguardando. En forma inmediata y utilizando el móvil, los delincuentes se transfirieron unos 25 mil 390 pesos argentinos (257 dólares) a una cuenta bancaria, y solicitaron un crédito de 100 mil pesos argentinos (1,014 dólares) y también se lo transfirieron. Si bien el comerciante logró la cobertura por parte de los seguros, los delincuentes lograron su objetivo. Por suerte, luego fueron capturados.

Es sólo una muestra entre infinidad de denuncias del mismo tipo. Como recomendación principal, es menester seguir una estricta política de seguridad de la información, no utilizando las opciones de autocompletado ni de recordar contraseñas. También es recomendable consultar frecuentemente las cuentas para detectar movimientos extraños y, de esa forma, hacer una rápida denuncia para acceder a la cobertura de los seguros. Y, obviamente, utilizar sólo lo indispensable el celular en vía pública y, en lo posible, de espaldas a una pared con visión periférica para disuadir.

LA ORGANIZACIÓN CRIMINAL

Si bien hay proliferación de delincuentes aislados, la tendencia es a aumentar la complejidad de las bandas, en su dirección, organización y distribución de tareas. Así es como en junio de 2021, y luego de un paciente y complejo trabajo de investigación, la Policía de la Ciudad de Buenos Aires, Argentina, detuvo a los 10 integrantes de una banda, conocida como la "Banda de Cachete". Esta organización operaba desde un estacionamiento donde, oculto en un vehículo, el jefe de la banda daba las directivas para el seguimiento de las personas que concurrían a entidades financieras o bancarias. Estos delincuentes se desplazaban en bicicletas o motos, disfrazados de personal de *delivery* (llamados "rompedores"), y eran quienes atacaban a las víctimas "marcadas" por el jefe. Después de hacer trizas las ventanillas, y bajo amenazas, robaban

Foto: Diario La Nación

Desde otro ángulo, y en el mismo momento, se puede apreciar una moto de apoyo a los "rompedores"

Foto: Diario La Nación

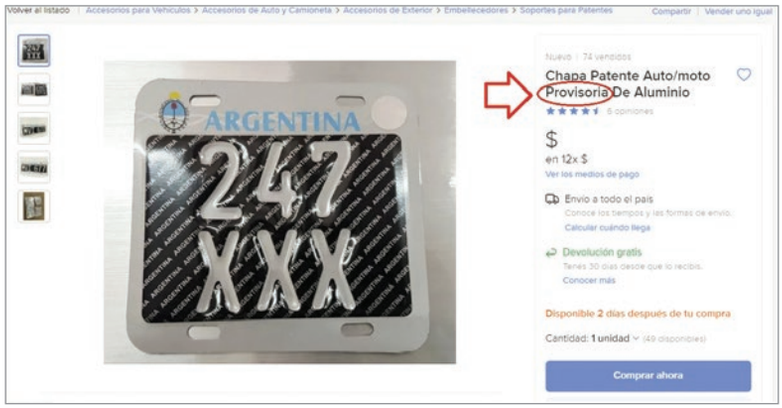
La "banda de Cachete", en acción. Momento en el cual los "rompedores" (flecha roja), atacan el vehículo "marcado" recién estacionado, con el conductor aún en su interior. Con flechas amarillas, las motos de apoyo de los delincuentes

bolsos, mochilas y carteras —allí donde estuviese guardado el dinero— para escapar en moto.

La citada banda tiene comprobada su acción criminal en nueve ataques a clientes de entidades bancarias y financieras del microcentro porteño desde el 5 de febrero pasado (“salideras”). No es la única banda en su tipo, habiéndose detectado “flotas de motochorros”.

LA LOGÍSTICA CRIMINAL Y NUEVOS DELITOS QUE GENERA

El Anillo Digital, un sistema de control de última generación de la Policía de la Ciudad de Buenos Aires permite identificar, a través de sus patentes, a los vehículos que tengan impedimentos para circular y que utilizan las 74 entradas y salidas del distrito. Dispone de dos centros de monitoreo, con un total de 498 lectoras de patente y 120 cámaras de video. Allí comparten jurisdicción la Policía de la Ciudad y la Policía de la Provincia de Buenos Aires, para prevenir el delito en ambas jurisdicciones.



Las ofertas en el portal (se eliminaron los valores)

Su funcionamiento representó una dificultad a salvar por los delincuentes ya que, en casi todos los casos, los vehículos utilizados para delinquir son robados. Esta necesidad de logística criminal generó nuevos delitos: los robos y la falsificación de patentes. Así es como los robos de patentes vehiculares sufrieron un gran aumento en los últimos años, ya que eran necesarias para eludir los controles.

En un portal de Internet algunos usuarios ofrecían patentes para motos, autos y tráileres. Por medio de un trabajo en conjunto con el portal y empresas de telefonía e Internet, fue localizado el origen de las publicaciones. En un local de venta de repuestos y accesorios de motos, se vendían patentes falsas y las hacían en el momento, según la indicación del cliente. En total, se incautaron 50 chapas patentes apócrifas, 4 CPU, 10 cajas con calcos de letras y números. Los responsables fueron detenidos y puestos a disposición de la justicia.

Actualmente, el Anillo Digital ya tiene la capacidad de chequear consistencias entre la patente denunciada y el modelo y tipo de vehículo al que corresponde. Asimismo, las chapas patentes son documentos oficiales, sólo legítimos cuando son emitidos por el Registro de Propiedad Automotor, y protegidos por numerosas medidas de seguridad que no permiten su copia fiel al original. Su costo de reposición no es elevado, por lo que no justifica una copia ilegal más barata. Debe denunciarse el robo de patente en forma inmediata, y solicitar su reposición en el Registro Automotor donde el vehículo se encuentra registrado. ■

Foto: Diario La Nación

Pórtico del Anillo Digital

Foto: Diario Perfil, gentileza MJS CABA

Los materiales para falsificar patentes incautados

Jorge Gabriel Vitti,
magíster en Inteligencia Estratégica por la Universidad Nacional de La Plata y Licenciado en Seguridad.

Más sobre el autor:

CRISIS Y CRIMINALIDAD EN EL SISTEMA PENITENCIARIO DEL ECUADOR

"Los problemas estructurales aún vigentes en el sistema penitenciario ecuatoriano hacen que la rehabilitación de los detenidos y su reinserción en la sociedad se conviertan en una utopía"

ECUADOR

Óscar Fredy Paredes Muñoz

En la década de los 80 el Estado ecuatoriano reconoció que el sistema penitenciario adolecía de graves problemas: la ausencia de una política penitenciaria, el fracaso de la labor rehabilitadora de las cárceles, la precariedad de las instalaciones, el hacinamiento, el fracaso de los sistemas de clasificación y la limitada preparación del personal penitenciario. Décadas más tarde esos mismos problemas estructurales persisten, pero la diferencia es que hoy el sistema penitenciario atraviesa por la peor y más violenta crisis que ha rebasado la capacidad de las autoridades responsables del mismo.

El problema de fondo en el sistema carcelario es que éste no llega realmente a ofrecer una rehabilitación social para las personas privadas de la libertad, complicando más su futura reinserción en la sociedad. Precisamente, en una entrevista a un canal de televisión el nuevo director del Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y Adolescentes Infractores (SNAI), Fausto Cobo, reconoció que "la rehabilitación no existe por el momento y tampoco es posible […] ¿qué rehabilitación puede haber en un camal humano?".

Fuente: www.dw.com

VIOLENCIA EN LAS CÁRCELES

La mayor y más violenta masacre ocurrida en el país se presentó el 23 de febrero de 2021. Ese día en tres cárceles (Latacunga, Guayaquil y Cuenca) ocurrieron motines simultáneos que dejaron como resultado un total de 79 personas fallecieron. Los videos que circularon en las redes sociales mostraron la crueldad y violencia con la que fueron asesinadas.

Entre el 1° de enero de 2010 hasta el 25 de febrero de 2021 se presentaron 248 muertes violentas en las cárceles y centros de detención preventiva. La última masacre con un saldo de 21 detenidos muertos sucedió simultáneamente el 21 de julio de 2021 en dos cárceles (Latacunga y Guayaquil). Este tipo de violencia incide en la falta de garantías a la integridad personal de las personas privadas de libertad.

Fuente: Wambra. Periodismo comunitario

SOBREPOBLACIÓN CARCELARIA

Los Centros de Privación de Libertad tienen una capacidad de guarecer a 28 mil 554 personas, sin embargo, en 2020 albergó en promedio a 38 mil 618 personas privadas de la libertad. El hacinamiento promedio en ese mismo año fue del 29.83%. Entre 2017 y 2020 el promedio del hacinamiento fue del 33.05%.

Fuente: Wambra. Periodismo comunitario

INFRAESTRUCTURA Y PERSONAL

Según el Informe de Rendición de Cuentas del año 2020 del SNAI, el sistema penitenciario cuenta con 54 Centros de Privación de Libertad (CPL) y 11 Centros de Adolescentes Infractores (CAI) insuficientes en capacidad, habitabilidad y recursos ante las reales necesidades.

Respecto al Cuerpo de Seguridad y Vigilancia Penitenciaria (CSVP) el número de agentes penitenciarios es insuficiente, mal pagado y propenso a la corrupción por la precariedad de su trabajo. Hasta el 30 de junio de 2021 el SNAI tenía en nómina a 2 mil 785 funcionarios. Entre ellos, 1,609 agentes penitenciarios de seguridad. Según el SNAI existe un déficit de 2 mil 261 agentes.

Hace falta la profesionalización de los agentes de vigilancia y seguridad penitenciaria y que las personas designadas para dirigir el SNAI y los responsables de los Centros de Privación de Libertad cuenten con la formación y especialización necesarias para su adecuada administración.

RESPUESTA DEL ESTADO

Luego de los motines que se presentaron el 21 de julio de 2021, el nuevo presidente del Ecuador, Guillermo Lasso, anunció algunas medidas urgentes para tratar de resolver la situación de las cárceles: decretó el estado de emergencia en el sistema carcelario a fin de movilizar todos los recursos humanos y económicos para reestablecer el orden; se estableció un control militar en el acceso del filtro 1 y un control policial en el filtro 2 y 3 de todos los centros carcelarios; y, se nombró a un nuevo director del SNAI. Asimismo, anunció que una de las medidas para combatir la crisis carcelaria será reducir el hacinamiento y otorgar derechos de prelibertad a 5 mil personas que no hayan cometido delitos graves.

PRONUNCIAMIENTO DE LAS ORGANIZACIONES DE DERECHOS HUMANOS Y DE LA SOCIEDAD CIVIL

La Fundación Regional de Asesoría en Derechos Humanos (INREDH) y la Alianza Contra las Prisiones, conformada por ocho organizaciones sociales y de derechos humanos, exhortaron al Estado ecuatoriano para que establezca un modelo de gestión penitenciario y una política pública integral que evite el incremento desmesurado de la población penitenciaria observada en la última década.

Exigen que la Función Legislativa no agrave la problemática del sistema penitenciario a través de la producción de normas hiperpunitivas, criminalizadoras y regresivas a los derechos humanos y que los eventos de violencia en las cárceles no deben abordarse como una cuestión de reincidencia criminal por parte de las personas privadas de la libertad, sino que el enfoque debe ser proyectado hacia la reincidencia omisiva por parte de las entidades estatales que no logran resolver la crisis en cárceles. Finalmente, señalan que el atribuir la problemática únicamente al comportamiento de las personas privadas de la libertad obstaculiza la planeación y ejecución de políticas públicas que urgen para remediar este sector.

Si bien para el nuevo Gobierno la situación del sistema penitenciario es un problema heredado, lo cierto es que tiene al frente un gran reto: recuperar el control de las cárceles, garantizar la integridad y vida de los internos, disminuir el hacinamiento, fortalecer la infraestructura carcelaria, contar con un cuerpo de seguridad y vigilancia penitenciaría profesional, directivos idóneos y la promulgación de políticas públicas integrales. Estas medidas contribuirán a que la rehabilitación social y la reinserción en la sociedad de las personas privadas de la libertad, no sea una utopía sino una realidad. ■

REFERENCIAS

- *Informe de Rendición de Cuentas del año 2020 del Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y Adolescentes Infractores (SNAI).*
- *https://www.primicias.ec/noticias/politica/cambios-burocraticos-no-resuelven-problemas-carceles/*
- *https://www.primicias.ec/noticias/sociedad/sistema-carcelario-todo-mal-informe/*
- *https://www.vistazo.com/politica/fausto-cobo-que-rehabilitacion-puede-haber-en-un-camal-humano-GE574989*
- *https://inredh.org/ante-los-hechos-de-violencia-en-los-centros-penitenciarios-de-latacunga-y-guayaquil-del-21-de-julio-de-2021/*
- *https://www.lahora.com.ec/guillermo-lasso-busca-resolver-la-situacion-carcelaria-repitiendo-las-mismas-medidas/*

Óscar Fredy Paredes Muñoz,
magíster en Seguridad y Defensa, consultor en Seguridad Corporativa y Gestión de Riesgos.

Más sobre el autor:

LA IMPORTANCIA DE LOS PRIMEROS AUXILIOS PSICOLÓGICOS (PAP) EN LA FORMACIÓN DE LOS ELEMENTOS DE SEGURIDAD

Es responsabilidad de las empresas de seguridad capacitar a sus elementos en los protocolos de intervención que comprenden los PAP con la finalidad de brindar apoyo emocional y práctico

MÉXICO | Ulises Figueroa Hernández

Dado que el fin principal de la Seguridad Pública es salvaguardar la integridad y derechos de las personas y que ésta debe regirse por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos. Es verdaderamente indispensable y absolutamente necesario incluir en los procesos de formación de las personas que se dedican a la seguridad un conjunto de conocimientos, habilidades y destrezas que dentro de un marco humanista con el enfoque de seguridad humana contribuyan a la profesionalización de los mismos.

Y que además constituyan una herramienta que permita a los cuerpos de seguridad de todos los ámbitos (federales, estatales, municipales, públicos o privados) atender a la comunidad de manera profesional, sobre todo a aquellos que han sido víctimas o testigos presenciales de un evento traumático, fatal e inesperado como un desastre natural, accidente de tránsito, violencia urbana o intrafamiliar, extorsión, hurto, secuestro, violación, abuso de menores, intento de suicidio, incendios o experiencia traumática que se presente en la comunidad y ante la cual el elemento de seguridad debe reaccionar de manera asertiva, dentro de un marco de respeto a la dignidad y los derechos humanos de las personas afectadas brindando apoyo a quienes lo necesiten.

Foto: Creativeart - Freepik

EVENTOS TRAUMÁTICOS

La gran mayoría de las personas puede experimentar alguna situación traumática al menos una vez en su vida y más aún debido al clima de inseguridad y violencia actual, lo que produce un malestar emocional intenso donde la persona afectada se siente fuertemente perturbada psicológicamente; ante este tipo de vivencias las personas experimentan un gran cúmulo de emociones y sensaciones que desbordan su capacidad de afrontamiento y que deben ser atendidas lo más pronto posible con la finalidad de disminuir el riesgo de un daño emocional permanente, además de contribuir al restablecimiento del orden público en caso de desastres masivos.

El caso es que al ocurrir un evento traumático, como los ya descritos, dentro de todo el caos que estas situaciones producen en las que puede haber estallidos de violencia, llanto, desesperación, ataques de pánico, etc. Las personas afectadas necesitan ayuda emocional eficiente y el hecho es que

Cuando las personas se ven envueltas en situaciones extremas de inseguridad es deber y responsabilidad de los cuerpos de seguridad proporcionar los medios para reestablecer la sensación de seguridad

Aunque los elementos de seguridad centran sus funciones en labores de prevención del delito, la mayor parte del tiempo lo emplean en actividades de restablecimiento del orden público, muchas de las cuales implican intervenciones en crisis

Foto: Creativeart - Freepik

siempre que suceden este tipo de casos en todo momento estará presente o acudirá un policía o un elemento de seguridad pública o privada quien será el responsable de proporcionar ese apoyo temporal e inmediato en tanto llegan los servicios de emergencia.

Es aquí donde entran en escena los Primeros Auxilios Psicológicos (PAP) que son una primera medida de intervención brindada por personal de atención primaria, es decir quienes acudan primero al lugar o ya estén presentes que desde luego siempre serán los uniformados o elementos de seguridad a quienes además el público afectado o testigos acuden siempre en busca de ayuda.

Lo interesante es que los PAP son una medida de intervención que puede ser brindada por personal no especializado en salud mental, es decir no es necesario ser psicólogo aunque si se requiere que el elemento de seguridad esté capacitado en la técnicas que se aplican en la intervención; los objetivos principales de los PAP son proporcionar alivio emocional inmediato que contribuya a que la persona afectada eche a andar sus capacidades naturales de resiliencia, prevenir el desarrollo de secuelas a largo plazo y de manera más práctica conectar a las personas con sus redes de apoyo ya sean familiares o especializadas, existe evidencia científica derivada de los estudios realizados por diversas instituciones que señalan que los PAP logran los objetivos mencionados.

Está comprobado que aunque teóricamente los elementos de seguridad centran sus funciones en labores de prevención del delito, la mayor parte del tiempo lo emplean en actividades de restablecimiento del orden público, muchas de las cuales implican intervenciones en crisis y no necesariamente relacionadas con la actividad delincuencial, teniendo en cuenta que los policías y elementos de seguridad son personas de primera línea que por la naturaleza de sus funciones en cualquier momento deberán intervenir en situaciones traumáticas o eventos perturbadores.

CONCLUSIONES

Por todo lo anterior se puede concluir que es responsabilidad de las instituciones y empresas de seguridad capacitar a sus integrantes en los protocolos de intervención que comprenden los PAP teniendo presente en todo momento que los PAP son intervenciones no invasivas inmediatas y de corta duración dirigidas a aquellas personas que están pasando por una crisis con la finalidad de brindar apoyo emocional y práctico, además de contribuir a mejorar el servicio de atención ciudadana con un enfoque de seguridad humana en la actuación policial.

En este tenor pudiera darse la idea de que las intervenciones en crisis no son asuntos de atención primordial de los policías o elementos de seguridad, pero no hay nada más lejos de la realidad; la seguridad en sí misma es la sensación de estar alejado de las amenazas o peligros, pero cuando las personas se ven envueltas en situaciones extremas de inseguridad es deber y responsabilidad de los cuerpos de seguridad proporcionar los medios para reestablecer la sensación de seguridad en las personas a través de diversas técnicas y no sólo por medio de la reacción armada o el uso de la fuerza, sino atendiendo también sus necesidades emocionales.

Las intervenciones de PAP están orientadas no sólo a proporcionar apoyo a las personas afectadas, sino también contribuyen a reducir las contingencias policiales que pudieran presentarse y que muchas veces son detonantes de la perturbación del orden público dentro de un contexto de por sí ya vulnerado que pudiera ser propicio para que se lleve a cabo algún delito si es que la situación se desborda.

Es por ello que el tema de los PAP deben ser materia indispensable en los programas de capacitación y adiestramiento de las instituciones de seguridad, a fin de conformar un esquema integral de atención ciudadana, buscando en todo momento cumplir la misión tan noble de cada elemento de seguridad que es proteger y servir a la comunidad. ■

Ulises Figueroa Hernández,
Licenciado en Seguridad Pública del Servicio de Protección Federal.

Más sobre el autor:

ACONTECIMIENTOS DE LA INDUSTRIA DE **LA SEGURIDAD PRIVADA**

Fecha:
28 de julio de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 60 invitados.

ALAS Comité México realiza reunión sobre suplantación de identidad

La Asociación Latinoamericana de Seguridad (ALAS) Comité Nacional México llevó a cabo la Mesa de Café "¡Te juro que yo no fui! Identidad Suplantada", a cargo de Alan Contreras, *hacker* ético. El *webinar* fue presentado y moderado por Manuel Zamudio, presidente de la asociación.

Alan explicó acerca de cómo actúan los ciberdelincuentes y cómo a través de los datos compartidos en redes sociales es como se nutren de información para elegir a sus víctimas, además de las vulnerabilidades que pueden producir las cuentas de WhatsApp, ya que hay una cantidad muy importante de información que maneja cada usuario, así como en la computadora, las aplicaciones que se descargan en los dispositivos, el correo electrónico, etc. Mediante una demostración en vivo, Alan explicó cómo es posible poder suplantar una cuenta de WhatsApp a través de códigos QR. ■

Alan Contreras,
hacker ético

Fecha:
9 de agosto de 2021.

Lugar:
Puebla, México.

Asistentes:
más de 170 concurrentes.

ASIS Capítulo Puebla-Sureste realiza reunión sobre análisis de espionaje y hackeos corporativos

ASIS Capítulo Puebla-Sureste llevó a cabo su reunión mensual con la participación de Gustavo Cruz, vicepresidente de dicho Capítulo, quien además de leer el código de ética, presentó al ponente del día: Fernando Thompson de la Rosa, mentor de estudiantes, emprendedores y Endevor.

Con la ponencia titulada "Análisis de espionaje y hackeos corporativos", Thompson explicó cómo a raíz de la crisis sanitaria y la llegada de la nueva normalidad ha cambiado la ciberseguridad en las empresas, las cuales no están preparadas para este nuevo esquema y destacó que en México no se tiene una estrategia de ciberseguridad. También señaló que uno de los principales vectores de ataque en nuestro país para las Mipymes es el *ransomware*, un tipo de *malware* donde compromete tu equipo y secuestra la información y exige un pago de rescate. ■

Fernando Thompson de la Rosa,
mentor de estudiantes, emprendedores y Endevor

Fecha:
11 y 12 de agosto de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 350 participantes.

Seguridad en América realiza *Roadshow* "Seguridad en plantas automotrices"

Seguridad en América (SEA) a través de Seguridad en América Academy, llevó a cabo el *Roadshow* "Seguridad en plantas automotrices", donde participaron múltiples expertos en materia y compartieron algunas de las mejores prácticas, consejos, y soluciones innovadoras para la industria. El evento fue presentado por Samuel Ortiz Coleman, director general de SEA, junto con Alex Parker, *Sales Manager* de la misma empresa.

JORNADA 1

Darío Preza, *National Security Officer* en México de Daimer Trucks North America, participó con su ponencia "Manejo de crisis y continuidad de negocio en la industria automotriz", en la que habló de cómo los riesgos son también una oportunidad de crecimiento a partir de cómo se gestionan, partiendo de la capacitación y especialización, así como la posibilidad de reemplazo del trabajo humano en algunas áreas, poder identificar los riesgos asociados al futuro, como son: la Inteligencia Artificial (IA), el *Big Data*, inclusive los *bitcoins* y con ello las vulnerabilidades que pueden tener los ciberataques y delitos.

Jesús Juárez, gerente de Operaciones en SISSA, dictó la conferencia "Convergencia de tecnologías de la información: tendencia clave en la reestructuración automotriz"; para continuar con Jorge Uribe Maza, director comercial de IPS, con su participación "Control de personal en la industria automotriz".

Martín Yánez, *Sales manager* para Latinoamérica de la empresa NEDAP, con su ponencia "Control vehicular y RFID en plantas automotrices", y para finalizar el primer día del evento, Alejandro Espinosa, *PACS Director of Sales LAM North* de HID Global, quien platicó acerca de la evolución de la credencialización a través de su funcionalidad y la seguridad que proveen.

Darío Preza,
National Security Officer en México de Daimer Trucks North America

JORNADA 2

Erik Navarro, director de Seguridad y Prevención de Incendios de Stellantis México, dictó la conferencia "La seguridad como elemento de valor de las operaciones en la industria automotriz", en la que habló acerca de la relevancia de la industria automotriz en México, la cual es uno de los grandes pilares, representando el 3.8% de Producto Interno Bruto (PIB) nacional y 20.5% del PIB en el sector manufactura, por ende, son muchas las familias mexicanas que dependen de este sector, México se posiciona como el 4to exportador a nivel mundial.

Arturo Martínez Avalos, director general adjunto de MSPV Seguridad Privada, con su ponencia "MSPV Un aliado en el proceso productivo". Más adelante tuvo lugar la empresa Hikvision, donde participó Arturo Martínez Oliveros, *Entreprise Business Development Manager* de la marca, con la charla "Soluciones de seguridad avanzadas de Hikvision para la Industria".

Jesús Cerón, presidente y director general de CyMEZ, habló sobre la "Previsibilidad de los riesgos del crimen organizado en parques industriales y su impacto en partes interesadas". Y para finalizar, Daniel Ballanto, director de Tecnología en Prosegur, presentó la conferencia "Integración de plataformas de seguridad con sistemas de gestión de recursos humanos". ■

Erik Navarro,
director de Seguridad y Prevención de Incendios de Stellantis México

Fecha:
19 de agosto de 2021.

Lugar:
León, Guanajuato, México.

Asistentes:
más de 60 personas.

Primer Simposio Internacional de Seguridad Privada **León 2021**

Se llevó a cabo el Primer Simposio Internacional de Seguridad Privada, en el que el gobierno de Guanajuato y el municipio de León, suman iniciativas que fortalecen a la seguridad pública. Lo anterior lo dijo el gobernador, Diego Sinhue Rodríguez Vallejo, durante su participación en dicho evento; en donde reiteró que, de acuerdo a la Ley de Seguridad Privada del Estado, este personal es auxiliar en la función de la seguridad pública, e incluso pueden coadyuvar en situaciones de urgencia o desastre.

"La paz y la tranquilidad social, son demandas de primer orden; por eso, todos los esfuerzos que sumen al logro de esos objetivos, son bienvenidos y la seguridad privada tiene mucho que aportar en estos esfuerzos", indicó. Además, se realizó el panel de "Capacitación como Plan de Mejoramiento Continuo en el Proceso de Profesionalización de la Seguridad Privada", iniciando con la bienvenida de Mario Bravo Arrona, secretario de Seguridad Pública de Guanajuato. ■

ASIS INTERNATIONAL™
CAPÍTULO MÉXICO 217

#ASISLoConstruimosTOD@S

MEMBRESÍA

ÚNETE A LA RED DE PROFESIONALES DE SEGURIDAD MÁS GRANDE DEL MUNDO

PAGA 12
Y RECIBE
3 MESES +
GRATIS

Tu membresía anual te brinda:

- Oportunidades de networking inigualables en eventos locales, regionales y globales, como GSX de ASIS Internacional.
- Acceso a "ASIS Connects", nuestra exclusiva comunidad en línea para establecer contactos, colaborar y encontrar soluciones comerciales.
- Recibe noticias galardonadas, tendencias y artículos destacados de Security Management, la revista mensual de ASIS.
- Obtén grandes ahorros en educación dirigida por expertos, incluidos seminarios web, conferencias globales, desarrollo ejecutivo y más.
- Conoce nuestras certificaciones profesionales reconocidas a nivel mundial que validan tu competencia en la industria de la gestión de la seguridad.
- Acceso digital gratuito a todos los estándares y pautas de ASIS.

No esperes más, escríbenos a socios@asis.org.mx o visítanos en nuestra webpage o redes sociales para encontrar los pasos para afiliarte.

PRÓXIMAS REUNIONES MENSUALES

19 OCTUBRE
DILME servicios de personal

9 NOVIEMBRE
TRUSTGROUP

14 DICIEMBRE
Multiproseg

ESCANEA ESTE QR PARA FORMAR PARTE DE NUESTROS SPONSORS

Fecha:
25 y 26 de agosto de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 300 concurrentes.

Seguridad en América efectúa el *Roadshow* **"Seguridad en la industria hotelera"**

Seguridad en América (SEA) llevó a cabo el evento *Roadshow* "Seguridad en la Industria Hotelera", con la participación de expertos en la materia. El evento fue presentado y conducido por Samuel Ortiz Coleman, director de SEA; junto con Alex Parker, *Sales Manager* de la misma empresa. Miguel Ángel Champo, presidente de ASIS Capítulo México, tuvo la primera participación al invitar a los ponentes a ser parte de la comunidad más grande de seguridad en América Latina.

DÍA 1

Adolfo Márquez, director de Seguridad Corporativa Mex-Latam de City Express Hoteles, habló acerca de todas las medidas de seguridad y prevención que un ejecutivo CEO de la compañía, debe tomar en cuenta en un viaje de negocios, además del papel fundamental de la empresa para darle soporte y seguimiento en cualquier situación que se pueda presentar.

Cesar Santillán García, *Presales Manager* de SISSA, participó con la ponencia "Soluciones de seguridad e infraestructura crítica para la industria hotelera". Más adelante participó Alberto Pérez, *Sales Director Latam* de SCATI, con la charla "Cómo convertir huéspedes en fans de tu hotel con un sistema de CCTV".

Para finalizar el día, Miguel Arrañaga, director de Pre-venta en Hikvision México, mencionó los principales problemas de la seguridad en los hoteles: robos, los perímetros, disturbios y cómo poder crear un entorno seguro en cuanto a seguridad física, electrónica y sanitaria.

DÍA 2

La conferencia magistral estuvo a cargo de Héctor Gerardo Ramírez Reyes, gerente de Prevención y Control de Riesgos titulada "¿Qué nos deja el COVID en temas de seguridad hotelera?", en la que abrió una reflexión sobre los cambios en el comportamiento y exigencias en los clientes en tiempos de COVID-19 y cómo afectan en la percepción de los riesgos de la seguridad.

La primera conferencia comercial estuvo a cargo de Andrés Efrén Álvarez Garduño, ingeniero de Soporte de Producto de la empresa Onity, con la ponencia "Soluciones de seguridad e infraestructura crítica para la industria hotelera".

Por su parte, David Sánchez Ramos, gerente de Ventas de Milestone México Norte, habló sobre "El poder de la plataforma abierta en hotelería". La última conferencia, fue dictada por el Cap. Manuel Herbeles Rascón, presidente de Guardian Global Security Group, la cual tituló "Seguridad hotelera, oportunidad y desafío" ■

Adolfo Márquez,
director de Seguridad Corporativa Mex-Latam de City Express Hoteles

David Sánchez Ramos, gerente de Ventas de Milestone México Norte; **Alex Parker,** *Sales Manager* de SEA; y **Samuel Ortiz Coleman,** director general de SEA

EXPO BLINDAJE

BLINDANDO LA SEGURIDAD EN MÉXICO

1ER CONGRESO INTERNACIONAL DE SEGURIDAD Y JUSTICIA

Te esperamos del

15 al 17 de Junio de 2022

en Expo Guadalajara

Organizado por:

BUSINESS MARKET CONNECTION

Revista oficial

SEGURIDAD EN AMÉRICA

Ventas nacionales: contacto@bmcm.mx
+52 (55) 7259 1114 +52 (55) 1702 0317

Ventas internacionales:
rmarroquin@bmcm.mx +52 (81) 1527 5228

Fecha:
8 de septiembre de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 250 participantes.

Seguridad en América organiza el *Roadshow* **"Seguridad en la industria alimentaria"**

Seguridad en América (SEA) llevó a cabo el *Roadshow* "Seguridad en la industria alimentaria", en el que el director general de esta casa editorial, Samuel Ortiz Coleman; junto con Alex Parker, *Sales Manager* de la misma empresa, aperturaron el evento dando paso a los primeros invitados de las asociaciones hermanas.

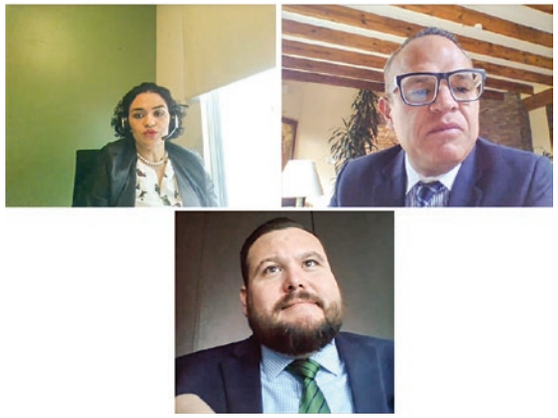
Miguel Ángel Champo, presidente de ASIS Capítulo México, invitó a todos los integrantes a ser parte de la comunidad más grande de seguridad. Por su parte, Manuel Zamudio, presidente de ALAS Comité Nacional México, también invitó a los asistentes a conocer toda la gama de oferta que ALAS ofrece a sus asociados y los espacios de colaboración.

CONFERENCIAS

La charla magistral titulada "Aprendizajes en la identificación de riesgos y planes de mitigación en la protección de activos en la industria alimentaria", estuvo a cargo de Dora Elena Cortés, directora de Seguridad de Cargill, en la que habló acerca del esquema de cadena alimentaria, el cual consta de todo el proceso para que un producto final pueda llegar a la mesa de las familias: producción, elaboración, distribución y consumo. Señaló que el top 5 riesgos basados en la experiencia son:

1. Robo de carga en tránsito (camión y tren).
2. Extorsión y ciberdelitos a empleados.
3. De país productor a consumidor de drogas ilícitas.
4. Violencia y delitos colaterales.
5. Activismo social.

Luis Saavedra, *Regional Sales Manager* de Tyco by Johnson Controls, habló acerca de cómo en dicha compañía invierte en tecnologías que permiten lograr una diferenciación estratégica, a través de Inteligencia Artificial (IA) y Aprendizaje Profundo, y Ciberseguridad.



Dora Elena Cortés, *directora de Seguridad de Cargill;* **Samuel Ortiz Coleman,** director general de SEA; y **Alex Parker,** *Sales Manager* de SEA

Los productos que ofrece al mercado cada uno opera de forma autónoma e independiente, pero también de forma integrada como una solución en la Nube, integran sistemas de terceros para utilizar la infraestructura existente y poder utilizar la misma inversión, los servidores son en sitio o servidores 100% en la Nube, con acceso de manera remota.

Más adelante, Diana López Agis, gerente de Ventas Internas de HID Global México, habló acerca de las investigaciones de HID sobre control de acceso, y credenciales donde las tarjetas de proximidad de baja frecuencia de 125 kHz son las más utilizadas. Los principales obstáculos para actualizar una solución innovadora es el costo, seguido por la integración de sistemas preexistentes, capacitación sobre aprendizajes de un nuevo sistema, entre otros, buscando mejorar siempre la motivación para actualizar las soluciones, tal es el caso de mejorar la comodidad de los usuarios y el flujo de personas en entradas de control de acceso y ahora las herramientas que evitan el contacto por la situación de la pandemia. ■

Diana López Agis, gerente de Ventas Internas de HID Global México; **Alex Parker,** *Sales Manager* de SEA; y **Samuel Ortiz Coleman,** director general de SEA

GRACIAS POR PARTICIPAR Y HABER FORMADO PARTE DE ESTE RETO DE 21 DÍAS

SEGURIDAD POR MÉXICO

CERTEZA • CONFIANZA • BIENESTAR SOCIAL

/SeguridadPorMexico

@segpormexico

/in/seguridad-por-méxico-

#JuntosHacemosSeguridad

Algunos de nuestros aprendizajes fueron:

Solidaridad

Tolerancia

Respeto

Unidad

Amor

Trabajo en equipo

Legalidad

y muchos más

Te invitamos a seguir siendo parte de nuestros eventos mensuales

Fecha:
7, 8 y 9 de septiembre de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de mil espectadores.

AMRACI presenta **"Fire Protection Virtual Congress 2021"**

Se llevó a cabo el "Fire Protection Virtual Congress 2021", organizado por AMRACI (Asociación Mexicana de Rociadores Automáticos Contra Incendios). En el último día se presentó un panel especial a nivel internacional, liderado por Juan José Camacho, presidente de AMRACI.

Camacho estuvo acompañado por los panelistas: Jaime Gutiérrez Casas, director internacional para Latinoamérica NFPA (National Fire Protection Association); Alejandro Ramírez, presidente de la Asociación Nacional de Protección Contra Incendios de Chile; José Luis Torero, profesor y director del Departamento de Ingeniería Civil Ambiental y Geomático de la University College London; Alonso Panizo Otero, presidente Engineering Service SAC, Perú; y Marcelo Lima, director general del Instituto Sprinker Brasil, con el tema: ¿Por qué Latinoamérica no ha podido lograr una regulación adecuada en la protección contra incendios? ■

Fecha:
8 de septiembre de 2021.

Lugar:
Costa Rica y México.

22 años de profesionalizar la seguridad en América Latina: **Samuel Ortiz Coleman**

Durante la emisión del programa "Hablemos de Seguridad con ACES" en "Radio Costa Rica" se llevó a cabo una entrevista con el director general de **Seguridad en América (SEA)**, Samuel Ortiz Coleman. La entrevista fue presidida por Huanelge Gutiérrez respecto a los diferentes temas de seguridad que se comentan en la revista. Samuel Ortiz relató los inicios de Seguridad en América justo hace 22 años, informando a la comunidad de seguridad, inicialmente empezó en la ciudad de México y gracias a Internet y las redes sociales, ha logrado llegar a más de 15 países en toda Latinoamérica. La intención de Samuel Ortiz es sentirse honrado, porque su objetivo principal y misión es profesionalizar al sector.

Para concluir la entrevista, hizo una invitación a directores de empresas que contratan servicios de seguridad a que busquen asesoría de profesionales que estén respaldados por asociaciones las cuales demuestran la seriedad de las empresas. ■

Huanelge Gutiérrez, presentador de Radio Costa Rica; y **Samuel Ortiz Coleman,** director general de SEA

Fecha:
15 de septiembre de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 140 participantes.

Desayuno ALAS
Comité Nacional México

Se llevó a cabo el Desayuno ALAS (Asociación Latinoamericana de Seguridad) Comité Nacional México junto con la marca Anixter con el tema principal "*Retail* un desafío para la IA, un paso más allá de la seguridad". El evento fue presentado por René Cuenca, secretario de ALAS Comité Nacional México; y Manuel Zamudio, presidente de la misma asociación. Posteriormente Erwin Villa, *Business Development Manager* en Anixter, habló de manera introductoria de las necesidades para el *retail* de hoy: la prevención de pérdidas, los robos que cuestan miles de millones a la industria minorista y la integración con sistemas EAS (Electronic Article Surveillance).

También participaron Iván Octavio Flores Coronado, responsable de Tecnología y Soluciones de Seguridad en las tiendas OXXO; e Iván Gustavo Islas Castillo, subdirector de Prevención de Pérdidas para Logística y Transportes Liverpool. ■

Fecha:
22 de septiembre de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 50 invitados.

Airbus México organiza *webinar* sobre Transformación Digital de las Comunicaciones Móviles

Airbus SLC México organizó el *webinar* "Transformación Digital de las Comunicaciones Móviles Seguras", en el que participaron los expertos Luis Núñez, desarrollador de Estrategias de MXWIDE para México, Erik Cárdenas, gerente de Pre-venta para MXWIDE; e Isidro Martínez Torres, gerente de Canales SMVNO de Airbus SLC.

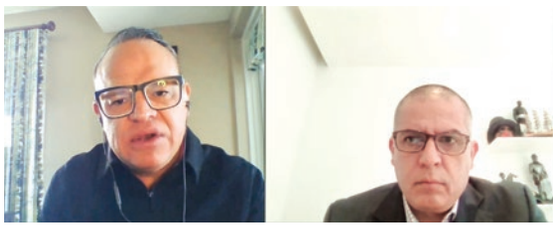
Luis Núñez comentó lo que es Airbus, el cual es pionero internacional en la industria aeroespacial, que han construido más de 200 satélites casi la mayoría en órbita, destacó la experiencia de Airbus donde cuentan con dos millones de usuarios en más de 180 países, donde además tienen 19 redes nacionales para fuerzas de seguridad pública y más de 30 en fuerzas de la defensa, con la presencia en más de 20 aeropuertos coordinando la logística y más de 100 líneas del metro equipadas con soluciones de comunicación crítica. ■

Fecha:
29 de septiembre de 2021.

Lugar:
Ciudad de México.

Asistentes:
150 personas.

Seguridad en América organiza *Roadshow* **"Seguridad en aduanas y recintos fiscales"**



Samuel Ortiz Coleman, director general de SEA; y **José Aguilar Méndez,** *Security & Customs Compliance Senior Director* de DHL

Seguridad en América (SEA) llevó a cabo el *Roadshow* "Seguridad en aduanas y recintos fiscalizados", conducido por Samuel Ortiz Coleman, director general de SEA; junto con Alex Parker, *Sales Manager* de la misma casa editorial.

Previo a las conferencias, Miguel Ángel Champo, presidente de ASIS Capítulo México, dio un mensaje a los asistentes acerca de lo que ASIS representa para el gremio de la seguridad privada, los beneficios que tiene ser socio en una de las asociaciones más importantes. También Manuel Zamudio, presidente de ALAS Comité México, mencionó que ser parte de esta la asociación tiene consigo importantes aportes para sus agremiados, como en capacitación y especialización.

CHARLAS MAGISTRALES

José Luis Saavedra Hernández, gerente de Seguridad Patrimonial de Scorpion, dictó la conferencia titulada "Estructura de seguridad para un recinto fiscalizado dentro de una aduana", en la que explicó cómo está compuesto un recinto fiscalizado, dividido en: áreas públicas, controladas, restringidas y centros de monitoreo.

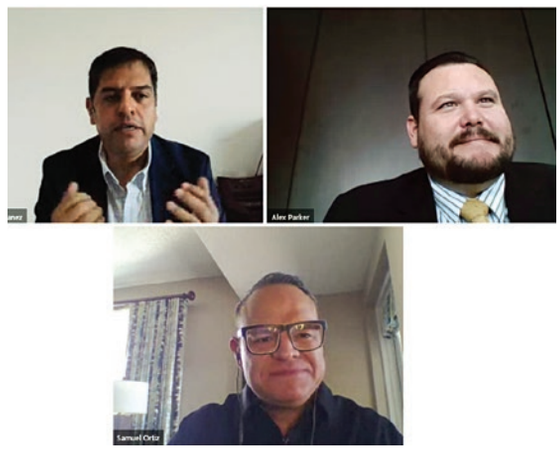
La estructura operativa de seguridad debe contar con una Jefatura Patrimonial directa del titular de la concesión, seguridad en piso, centro de monitoreo CCTV (en éste sí puede ser un tercero), inspección de carga. Las políticas deben ser muy claras, contar con un manual de seguridad, el cual va se va a seguir tal cual los protocolos marquen. "En un recinto fiscal no se puede improvisar", mencionó.

La siguiente conferencia magistral titulada "Seguridad logística en los recintos fiscalizados", fue por parte de José Aguilar Méndez, *Security & Customs Compliance Senior Director* de DHL, quien dijo que los recintos fiscalizados en México deben dar cumplimiento a las obligaciones establecidas en la ley aduanera y a los estrictos controles de vigilancia, seguridad y seguridad digital, que permitan garantizar el control de las operaciones de mercancías de comercio exterior de importación y exportación.

CONFERENCIA COMERCIAL

La conferencia "Control vehicular a larga distancia en aduanas y recintos fiscalizados", estuvo a cargo de Martín Yánez, L*atin America Sales Manager* de Nedap, quien comentó que los vehículos que entran en un recinto fiscalizado o en una aduana son muchos tipos y para ello se requieren de diferentes puntos de control internos y externos que requieren ser controlados. Un ejemplo de ello son los montacargas, vehículos internos para moverse dentro de los recintos, como en puertos, donde mueven contenedores y vagones.

Martín presentó a Nedap Identification Systems, un ecosistema de gestión de seguridad. También habló de Transit, lectoras con tecnología 2.45 GHZ, en las que se puede controlar al conductor y vehículo con una tarjeta de proximidad para acceso peatonal, ofrece lectura exacta en vehículos blindados y polarizados, con eficacia en la lectura en condiciones extremas. ■



Martín Yánez, *Latin America Sales Manager* de Nedap; **Alex Parker,** *Sales Manager* de SEA; y **Samuel Ortiz Coleman,** director general de SEA

NUESTROS SERVICIOS

Manned Security: Nuestro personal altamente capacitado brinda seguridad y ayuda en la mitigación de riesgos. Contamos con servicios de:

- Oficiales de Seguridad
- Custodia de mercancías
- Protección ejecutiva
- Monitoristas

Technology: Las soluciones de tecnología comprenden servicios básicos de monitoreo hasta complejos desarrollos de automatización:

- CCTV
- Control de Accesos
- Detección de incendios
- Alarmas

Risk: Brindamos servicios de:

- Consultoría de gestión de riesgos de seguridad
- Planeación y asesoría en manejo de crisis
- Investigaciones y verificación de información
- Pláticas de seguridad
- Evaluación de C-TPAT
- Inspecciones y análisis de seguridad
- Análisis de riesgo
- Entrenamiento de manejo evasivo/defensivo

SÚPER EMPRESAS EXPANSIÓN 2021 TOP companies

ventas@mx.g4s.com | (+52) 55 5337 0400 | www.g4s.mx

Hanwha Techwin fortalece sus procesos de ciberseguridad con el SOC Wisenet7

La compañía surcoreana Hanwha Techwin entiende la importancia de la seguridad cibernética, por lo que ha incorporado en su nuevo *chipset*, Wisenet7, con protocolos mejorados de protección, encriptación y bloqueo de puertas traseras, lo que le permite mantener vigentes los permisos y aprobaciones del gobierno estadounidense a sus productos de videovigilancia. Los dispositivos con Wisenet7 utilizan el sistema propietario de emisión de certificados que incorpora certificados únicos en cada producto durante el proceso de fabricación. Dentro de las políticas de ciberseguridad de Hanwha Techwin se incluyen arranque seguro, sistema operativo seguro, almacenamiento seguro y su plataforma abierta segura, que garantizan la ciberseguridad de los productos en cada paso del camino. ■

Milestone Systems saluda la llegada de la nueva directora de *Marketing* al equipo de Liderazgo Ejecutivo

Milestone Systems anunció el nombramiento de Christina Molt Wengel como nueva directora de *Marketing*. "Para continuar el viaje estratégico y cumplir con la ambición de crecimiento masivo de Milestone, me complace dar la bienvenida a Christina al Equipo de Liderazgo Ejecutivo. Christina llega con una vasta experiencia en liderazgo *senior* y *marketing* y tiene un profundo conocimiento de cómo construir una marca y comprender las necesidades del cliente", afirmó Thomas Jensen, director ejecutivo de Milestone. "En el viaje para fortalecer aún más la marca como una empresa basada en datos que opera en un mundo basado en datos, estoy seguro de que Christina será un gran activo para Milestone y fortalecerá y llevará al equipo de marketing al siguiente nivel", agregó Jensen. "Soy una transformadora empresarial de corazón, comprometida con hacer que las empresas avancen y asciendan", agregó Christina. ■

Axis Communications celebra 25 años de la creación de la primera cámara IP del mundo

En 1996, Axis Communications decidió hacer uso de sus habilidades en redes y lanzó la primera cámara IP (Internet Protocol) del mundo, la AXIS Neteye 200, capaz de transformar para siempre el sector de la vigilancia. "Hoy quiero felicitar a Axis por sus primeros 25 años de la primera cámara IP del mundo, pero también por cumplir 25 años de transformar los sectores. Quiero extender esta felicitación a todos aquellos que forman parte del gran ecosistema de Axis: a nuestros usuarios finales, nuestros integradores y a nuestra red de distribuidores, porque sin ellos, esto tampoco hubiera sido posible. Sobre todo, felicito a todo nuestro equipo de trabajo extendido en el mundo y particularmente en Latinoamérica que son pieza clave en el liderazgo de la compañía", comentó Leopoldo Ruiz, director regional para Latinoamérica en Axis Communications. ■

Hikvision México dona soluciones de seguridad al CECyT #1 del IPN

Hikvision realizó una donación de 80 productos de videoseguridad, equivalente a 23 mil 805 dólares, al Centro de Estudios Científicos y Tecnológicos N° 1 "Gonzalo Vázquez Vela" del Instituto Politécnico Nacional (IPN), unidad académica con una superficie de 15 mil 361.20m^2, y que cuenta, al día de hoy, con 4 mil 577 alumnos inscritos y una plantilla de personal de 351 personas. En un acto realizado en las instalaciones del CECyT 1 —que contó con la participación de Dr. Dimitri Cab, director de CECyT 1 del IPN; Camilo Muñoz, *Channel Director* de Hikvision México, así como de destacados profesores del plantel y ejecutivos de Hikvision—, fueron entregadas diversas cámaras de seguridad, sensores de alarmas, infrarrojos, controles de acceso, videoporteros, cierres magnéticos, lectores de tarjeta, entre otros equipos. ■

SCATI moderniza el sistema de videovigilancia de **DSM Nutritional Products**

SCATI dio a conocer que la planta de Jaguáre en São Paulo (Brasil) de DSM Nutritional Products, empresa dedicada a la fabricación y venta de vitaminas, carotenoides, enzimas y otros productos para la industria de nutrición animal, estaba protegida por un sistema de videovigilancia compuesto por 15 cámaras analógicas cuya gestión, almacenamiento y control se realizaba de forma local. Por lo que decidió actualizar el sistema de videovigilancia migrándolo a tecnología IP (Internet Protocol) y se ha ampliado hasta tener más de 50 cámaras que se gestionan a través de servidor, grabador y *software* de SCATI, fabricante de soluciones de video inteligente. La gestión integral de las cámaras IP se realiza a través de una plataforma de grabación de la Gama PRO de SCATI FENIX, capaz de gestionar hasta 64 cámaras IP megapixel simultáneamente. ■

Genetec lanza su nueva página en español para América Latina y España

Genetec Inc. anunció el lanzamiento de su nueva página web en español, que ofrece una experiencia de usuario totalmente mejorada, nuevo contenido local de Latinoamérica y España, videos y muchos otros recursos. Los nuevos colores, el modo oscuro y el dinamismo del nuevo sitio web reflejan el concepto de la marca. Según Sandra Morales, gerente de *Marketing* para Latinoamérica de Genetec: "Desde que nuestros clientes actuales y potenciales interactúen con nuestra página web, hasta que utilicen nuestro *software*, tendrán la misma experiencia de usuario y marca que sólo Genetec brinda", señaló. Así mismo, encontrarán información detallada de diferentes industrias como energía, aeropuertos, *retail*, gobierno, entre otras. ■

HID Global mejora la emisión de boletos móviles para el transporte público

HID Global anunció que es el primer proveedor de soluciones de emisión de boletos del mundo en ofrecer un kit de desarrollo de *software* (SDK) que cumple plenamente con los estándares del sistema HCE (Emulación de tarjeta del sistema) de Calypso para la emisión segura y cómoda de boletos móviles en teléfonos inteligentes. La certificación especifica cómo proteger los datos de los boletos almacenados en la billetera del dispositivo móvil, lo que ayuda a las empresas de transporte a combatir de forma eficaz el fraude, al impedir la duplicación, transferencia o alteración de los boletos. Empleado por redes de transporte público y ciudades de todo el mundo, Calypso es un estándar abierto para aplicaciones de emisión de boletos sin contacto en las que se utilizan tarjetas Calypso y teléfonos móviles con tecnología NFC. ■

TRENDnet presenta Hive, un administrador avanzado para la gestión centralizada y remota de la red

TRENDnet® presentó TRENDnet Hive™, un avanzado administrador de red en la Nube diseñado para ahorrar costos y tiempo a los usuarios al simplificar y centralizar la gestión y la supervisión de la red. "El trabajo a distancia se ha convertido en una necesidad esencial hoy en día. Los administradores e integradores de redes se enfrentan a estos nuevos obstáculos, pero el mantenimiento de las redes a distancia seguirá siendo siempre una función esencial a medida que construimos un nuevo futuro de dispositivos gestionados", dijo Evan Davis, director general de Ingeniería de Soluciones en TRENDnet. "La solución Hive de TRENDnet permite a los usuarios llevar su red con ellos cuando están de viaje, sin importar dónde estén. La gestión remota de la red con TRENDnet Hive permitirá a los usuarios el acceso inmediato a todos los datos que necesitan", indicó. ■

SEGURIDAD EN EL TRÁFICO VEHICULAR

El robo al transporte de carga fue uno de los problemas de inseguridad que continuó agravándose durante el año 2021, así como el robo de vehículos particulares con uso de violencia sobre todo al aumentar las actividades diarias de la población. Es por ello que **Seguridad en América** (**SEA**), comparte los siguientes consejos de seguridad extraídos del Blog de David Lee, autor del *Manual de Seguridad para la Prevención de Delitos*.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1. **Guarde sus cosas.** No deje a la vista objetos, principalmente bolsos, computadoras, celulares, portafolios. Resguárdelos debajo del asiento o, idealmente, en la cajuela del vehículo, así disminuirá las posibilidades del famoso "cristalazo".

2. **Manténgase alerta.** Observe y permanezca alerta de su entorno, evite distraerse manipulando su teléfono celular o el radio, no lo lleve a todo volumen. Sea amable, paciente y tolerante al conducir. Desconfíe de personas que le indiquen que su vehículo presenta una avería señalándolo, de ser necesario comuníquese con las autoridades en un lugar seguro.

3. **Manos libres.** Utilice el "manos libres" para recibir llamadas de teléfono. No envíe textos ni manipule su teléfono, conecte el equipo vía *Bluetooth*.

4. **Dispositivo musical o de GPS.** Si escucha música o utiliza con frecuencia los servicios de geo localización (Maps, Waze, etc.), considere hacerlo en un dispositivo distinto a su teléfono inteligente: utilice un teléfono inactivo o un dispositivo que le permita conectarlo a través de *Bluetooth* a su teléfono y compartirle datos de Internet.

5. **No sea ostentoso.** Recuerde que debe mantener un perfil bajo en todo momento, incluso al conducir. Evite exhibir joyas, relojes o teléfono inteligente, evite mostrarlos al colocar su brazo en el descansabrazos. Extienda estas medidas a sus acompañantes. ■

Foto: Creativeart - Freepik

FOMENTE LA CULTURA DE LA SEGURIDAD
Consulte la revista digital en
www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

SEGURIDAD EN AMÉRICA

ÍNDICE DE ANUNCIANTES

EN NUESTRO TRABAJO ESTÁ
SU SEGURIDAD

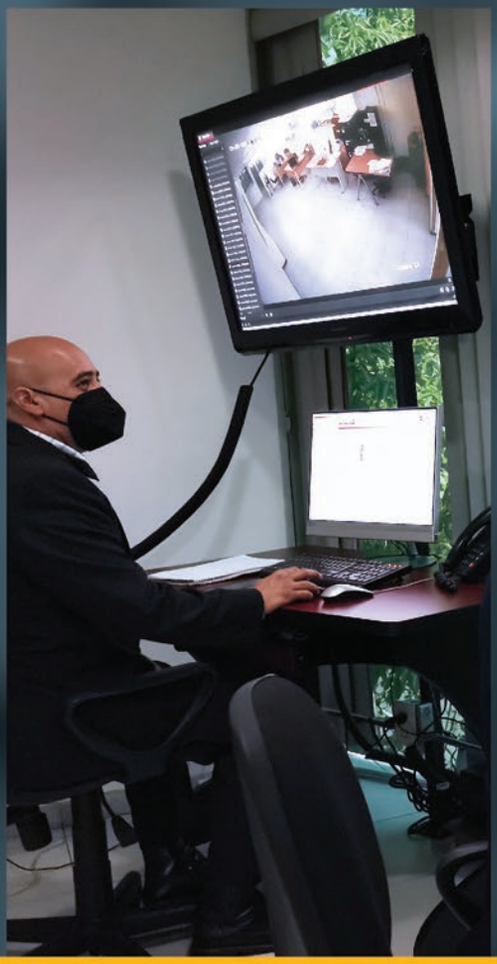
TECNOLOGÍA Y SEGURIDAD, UNIDOS
PARA BRINDARLE EL MEJOR SERVICIO

GSI
GRUPO SEGURIDAD INTEGRAL

impactoTOTAL

NUESTROS SERVICIOS

- Patrullaje y reacción con motocicleta
- Rastreo y localización
- Vigilancia Aeroportuaria
- Custodia de mercancía y bienes
- Oficiales intramuros y patrullas
- Videovigilancia y controles de acceso



ESR EMPRESA SOCIALMENTE RESPONSABLE

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

ASIS INTERNATIONAL

DNV·GL

COPARMEX

Atención a clientes 01 800 461 0457 www.impactototal.mx

"SEPSISA se ha transformado en SER grande"

Facility Services

Grupo

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.

- Guardias
- Comercializadora
- Limpieza
- Consultoría
- Custodia
- Seguridad Electrónica
- GPS / Monitoreo

17 YEARS ANNIVERSARY

EMPRESA SOCIALMENTE RESPONSABLE

ISO 9001:2015 COMPANY

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

ASIS

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

BASC

COPARMEX®

CDMX, Estado de México, Monterrey, Guadalajara, San Luis Potosí, Aguascalientes, Hermosillo, Querétaro, Guanajuato, Pachuca, Puebla, Cuernavaca, Acapulco, Veracruz, Villahermosa, Mérida, Cancún, Mexicali, Chihuahua, Tijuana, Ensenada.

www.sepsisa.com.mx ventas@sepsisa.com.mx 5662 6039