SEGURIDAD®
EN AMÉRICA

25th ANIVERSARIO
SEGURIDAD® EN AMÉRICA

Fuente de conocimiento y actualización

Especiales:
Seguridad en bancos
Nuevo perfil de guardias y protección ejecutiva

Reportaje: Seguridad en plantas automotrices

Año 25 / No.146
Septiembre - Octubre

www.seguridadenamerica.com.mx

COBERTURA NACIONAL

A QUIEN VALOR MERECE

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

@MultiprosegOficial @MULTIPROSEGOFICIAL MULTIPROSEG OFICIAL

ALGUNOS DE NUESTROS CLIENTES

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

AMESP

CDMX
CIUDAD DE MÉXICO

CNS

ASIS INTERNATIONAL

redconocer

ISO

BAC

ema
entidad mexicana de acreditación, a.c.

ANERPV

COPARMEX

REPSE

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

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

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

+ 52 (55) 79599598

INFO@MULTIPROSEG.COM.MX

SEGURIDAD EN AMÉRICA

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

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

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

Coordinación de Diseño
José Arturo Bobadilla Mulia

Administración
Oswaldo Roldán
oroldan@seguridadenamerica.com.mx

Reportera
Mónica Ramos
redaccion1@seguridadenamerica.com.mx

Medios Digitales
Estefania Hernández
mdigital@seguridadenamerica.com.mx

Circulación
Alberto Camacho
acamacho@seguridadenamerica.com.mx

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

María Esther Gálvez Serrato
egalvez@seguridadenamerica.com.mx

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

Luz María González Medina
luz@seguridadenamerica.com.mx

Carlos Román Martínez Sánchez
César Ortiz Anderson
Chesus M. Gay
Dante García Martínez
David Chong Chong
Enrique Tapia Padilla
Gabriel Esteban Escobar González
Hermelindo Rodríguez Sánchez
Jaime A. Moncada
Javier Nery Rojas Benjumea
Jeimy Cano
Johan Paulsson
Jorge Gabriel Vitti
Jorge Rayas
José Luis Sánchez Gutiérrez
Manuel Sánchez Gómez-Merelo
Omar Ballesteros
Rafael E. Vera
Ricardo Nava Rueda
Valente Del Angel Santos

Año 25 / No. 146 / Septiembre | Octubre / 2024

Portada:
Seguridad en América

Síguenos por

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

COMPARTE ESTA REVISTA
COMPARTIR ES RECICLAR

Conmutador: 5572.6005
www.seguridadenamerica.com.mx

Seguridad en América es una publicación editada bimestralmente por Editorial Seguridad en América S.A. de C.V., marca protegida por el Ins-tituto de Derechos de Autor como consta en la Reserva de Derechos al Uso exclusivo del título número: 04-2005-040516315700- 102, así como en el Certificado de Licitud de Contenido número: 7833 y en el Certificado de Licitud de Título número: 11212 de la Secretaría de Gobernación. Editor responsable: Samuel Ortiz Coleman. Esta revista considera sus fuentes como confiables y verifica los datos que aparecen en su contenido en la medida de lo posible; sin embargo, puede haber errores o variantes en la exactitud de los mismos, por lo que los lectores utilizan esta información bajo su propia responsabilidad. Los colaboradores son responsables de sus ideas y opiniones expresadas, las cuales no reflejan necesariamente la posición oficial de esta casa editorial. Los espacios publicitarios constantes en esta revista son responsabilidad única y exclusiva de los anunciantes que oferten sus servicios o productos, razón por la cual, los editores, casa editorial, empleados, colaboradores o asesores de esta publicación periódica no asumen responsabilidad alguna al respecto. Porte pagado y autorizado por SEPOMEX con número de registro No. PP 15-5043 como publicación periódica. La presentación y disposición de **Seguridad en América** son propiedad autoral de Samuel Ortiz Coleman. De esta edición fueron impresos 12,000 ejemplares. European Article Number EAN-13: 9771665658004. Hecho en México. Se imprimió en los talleres de Esténtor Impresos, Calle Virgen de Chiquinquira 706, Col. La Virgen, Ixtapaluca, Estado de México, C.P. 56530.

Apoyando a:

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

TRUSTGROUP MR

En Seguridad, "Nadie Conoce México Como Nosotros".

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

www.trustgroup.com.mx

Veinte años brindando servicios profesionales de seguridad

ASIS

CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

EDITORIAL

En las elecciones presidenciales de México, llevadas a cabo el 2 de junio de 2024, Claudia Sheinbaum, candidata de la coalición "Sigamos Haciendo Historia", se convirtió en la virtual ganadora y primera presidenta del país, quien tomará posesión como mandataria el próximo 1 de octubre de 2024.

En tema de seguridad, detalló en conferencia de prensa, que su estrategia se ajustará a las necesidades que haya en cada región del país y que sí tomará en cuenta a las policías municipales, siempre y cuando éstas funcionen.

"Ya se verá en cada caso, en cada estado. Estamos trabajando en una estrategia que atienda las causas, fortalecimiento de la Guardia Nacional, inteligencia e investigación. Vamos a enviar una iniciativa de ley para crear el Sistema Nacional de Inteligencia e Investigación para la Seguridad Pública y el gabinete diario de seguridad", indicó.

Claudia Sheinbaum también recordó que parte de su estrategia de seguridad será la coordinación entre poderes e instituciones, así como la atención a las causas. Reiteró su intención de enviar una iniciativa al Congreso para crear el Sistema Nacional de Inteligencia e Investigación para la Seguridad Pública, mismo que estará a cargo de Omar García Harfuch, como titular de la Secretaría de Seguridad y Protección Ciudadana de México (SSPC).

¿QUIÉN ES OMAR GARCÍA HARFUCH?

De acuerdo con CNN Español, Omar Hamid García Harfuch nació el 25 de febrero de 1982 en Morelos. Es licenciado en Derecho por la Universidad Continental y en Seguridad Pública por la Universidad del Valle de México.

Inició su carrera en los cuerpos de seguridad en 2008, cuando ingresó a la Policía Federal (PF) como jefe de departamento en la Coordinación de Inteligencia, según su perfil en LinkedIn. La División de Seguridad Regional lo designó en 2012 como coordinador estatal de Guerrero.

En 2015 fue titular de la División de Investigación de la Policía Federal. Un año después fue designado titular de la Agencia de Investigación Criminal de la Procuraduría General de la República.

Al comienzo de la administración de Sheinbaum en la Ciudad de México, García Harfuch se desempeñaba como jefe de la Policía de Investigación y coordinador de Inteligencia de Seguridad Ciudadana.

Entre 2019 y 2023 fue secretario de Seguridad Ciudadana de la capital. Y en septiembre de 2023, García Harfuch dejó la SSC, para incorporarse al equipo de precampaña de Sheinbaum.

El pasado 2 de junio, García Harfuch ganó la elección para senador por la Ciudad de México. El 11 de junio, estuvo presente también en la reunión entre la asesora de Seguridad Nacional del presidente Biden, Elizabeth Sherwood-Randall, y Claudia Sheinbaum.

Estimado lector, ¿cuál cree usted que son los principales retos en seguridad que el gobierno de México deberá enfrentar en este nuevo sexenio? ■

Envíe sus comentarios y/o sugerencias a *prensa@seguridadenamerica.com.mx*


SISSA
Monitoring Integral
Más seguridad, más confianza
Seguridad Electrónica | Fábrica de Software | Infraestructura de TI
www.sissamx.com.mx

RECONOCIMIENTO

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

En la presente edición, el director general de esta casa editorial, Samuel Ortiz Coleman, entregó los reconocimientos a Ricardo Nava Rueda, "*Lost Boy*", director de Difusión y Relaciones Públicas de la Asociación Mexicana de Niños Robados y Desaparecidos, A.C. y líder del proyecto Encuéntrame de Seguridad por México (Iniciativa Chapultepec, A.C.); y a Manuel Sánchez Gómez-Merelo, consultor internacional de Seguridad, quienes en generosas ocasiones han presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

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

Si desea conocer más acerca de Ricardo Nava Rueda, consulte su currículo:

Si desea conocer más acerca de Manuel Sánchez Gómez-Merelo, consulte su currículo:

ENTREVISTA EXPRÉS CON

Adrián G. Charansonnet,

colaborador del área de Análisis de Riesgos en Dilme

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

El fenómeno económico de relocalizacion efectivamente es una gran oportunidad de desarrollo de negocio para la seguridad privada, especialmente en aspectos más selectos como el diseño de estrategias logísticas de prevención del delito en traslado de mercancía y materias primas, así como el análisis de condiciones de desarrollo y riesgos en las ubicaciones y entornos de operación de estos puntos de maquila, producción y almacenaje de productos terminados e insumos. Es imperante priorizar las estrategias de diseño de prevención y no olvidar el factor de protección civil, que pueden ser la diferencia entre un punto atractivo laboral o una crisis de rotación de personal por infraestructura, riesgos laborales y transporte. ■

Uncover The Unseen™

GARRETT

¡Paragon establece el estándar para el futuro!

Ambiscan

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

ESCANEAR PARA MÁS INFORMACIÓN

MADE IN THE USA

ÍNDICE

Septiembre | Octubre

GRUPO IPS

GARANTÍA EN SEGURIDAD

La nueva era de la seguridad.

Protección inteligente para tu empresa.

- Telemetría
- Registro de incidentes
- Sistemas de acceso
- Biométricos

Contacta a un asesor

30 AÑOS DESDE 1995

55-5525-3242

grupoipsmexico.com

EL DESAFÍO DE LA BANCA: SIMPLIFICAR LA OPERATIVA DIARIA CON INTELIGENCIA

Modernizar los sistemas de seguridad en las entidades financieras es una inversión esencial que debe abordarse de manera integral

ESPAÑA

Chesus M. Gay

Modernizar el sistema de seguridad de las entidades financieras involucra a múltiples departamentos por lo que provoca que este proceso sea complejo y costoso.

En el sector bancario donde la cantidad y la complejidad de los procesos es elevada, es clave encontrar herramientas que permitan integrar y coordinar las aplicaciones existentes con las nuevas soluciones de seguridad electrónica y que sea capaz de evolucionar.

Estas herramientas deben ofrecer algo más que la mera protección de personas, activos y datos; hasta el punto de convertirse en una herramienta transversal que simplifique la operativa diaria y sea eficiente.

La transformación digital, el cambio en el hábito de los clientes, el crecimiento de dispositivos, IoT, etc., presentan nuevos desafíos para la seguridad bancaria que apuestan cada vez más, por plataformas que permitan una gestión centralizada y la integración con otros sistemas, la incorporación de la Inteligencia Artificial y su explotación a través de herramientas de *Big Data*; y siempre, contando con los máximos niveles de ciberseguridad.

GESTIÓN CENTRALIZADA DEL SISTEMA

Para que los operadores puedan visualizar múltiples cámaras de distintos sitios o sucursales desde una central de monitoreo es necesario una infraestructura que permita transportar imágenes de miles de equipos con anchos de banda limitados, sin preocuparse por el almacenamiento y la transmisión de video.

El uso de herramientas *software* para la administración remota y centralizada del sistema de videovigilancia es crucial para mejorar la coordinación entre equipos, facilitar la obtención de pruebas forenses y reducir los costos operativos asociados al área de seguridad.

PLATAFORMA DE INTEGRACIÓN DE SISTEMAS

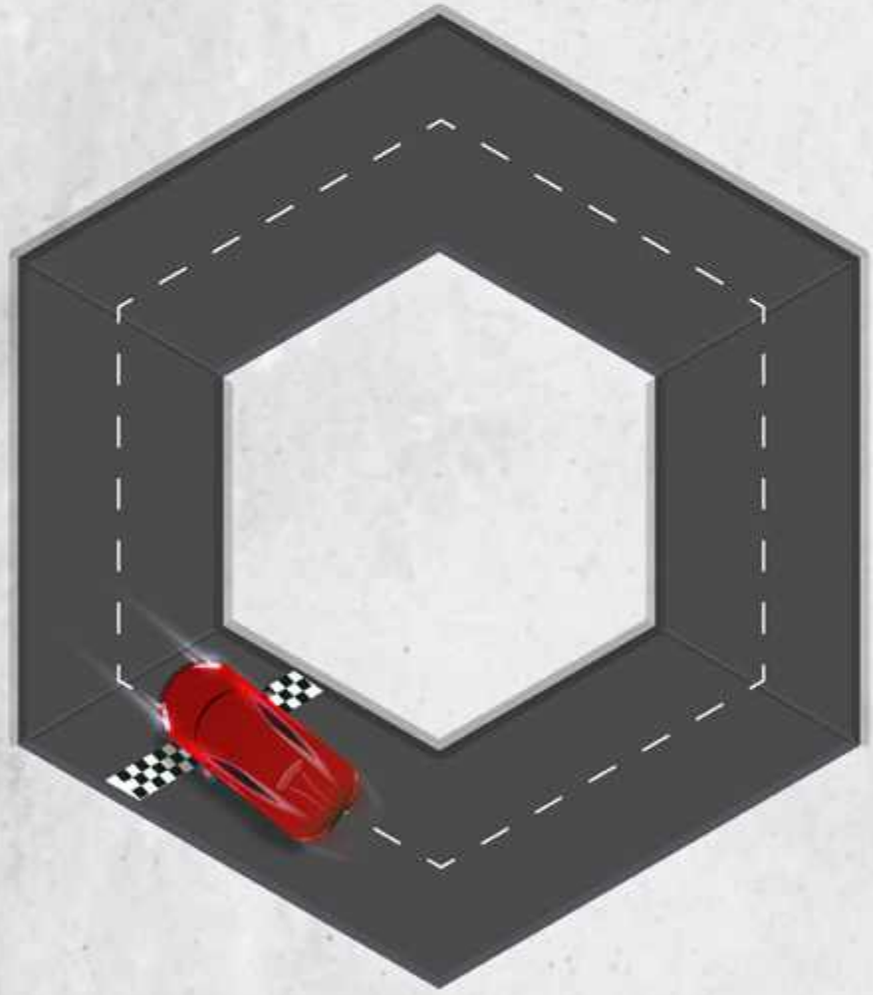
Para los usuarios finales, una plataforma de integración se vuelve esencial cuando se enfrentan a la necesidad de gestionar múltiples sistemas de seguridad de manera integrada y efectiva: sistemas de videovigilancia, control de accesos, incendios, alarmas y otros relacionados con la automatización y control de edificios inteligentes.

Esta plataforma deber ser flexible, escalable y facilitar la interoperabilidad entre los sistemas. También debe tener capacidad para rastrear y auditar todas las actividades y eventos para una posterior investigación de incidentes y para fines de responsabilidad y ofrecer la posibilidad de crear procedimientos específicos de respuesta ante eventos que se produzcan en sus instalaciones: como la activación de alarmas o el bloqueo de áreas, para una acción inmediata. De esta forma se aumenta la eficiencia del sistema gracias a una acción coordinada de todos sus elementos.

SISSA
Monitoring Integral

LA META ES LA SEGURIDAD:

El futuro se mueve con nosotros



Seguridad Electrónica | Fábrica de Software | Infraestructura de TI

www.sissamx.com.mx

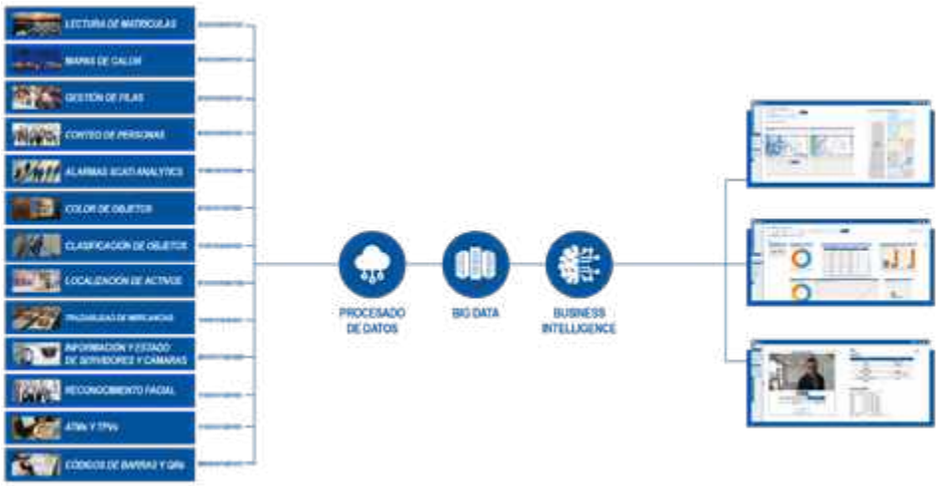
DE LA IMAGEN AL RENDIMIENTO: ¿CÓMO LA ANALÍTICA DE VIDEO IMPULSA LA GESTIÓN DEL NEGOCIO?

Con la creciente demanda de soluciones inteligentes, la integración de tecnologías con base en desarrollos que incorporan Inteligencia Artificial se presenta como un pilar fundamental de seguridad para 2024.

Gracias al uso de sistemas con IA se obtiene información sobre los usuarios y sus comportamientos para mejorar el negocio a través de mapas de calor, gestión de filas, conteo de personas, reconocimiento facial, etc.

Los datos, mediciones e informaciones procedentes de los sistemas de seguridad pueden ser aprovechadas por otras áreas de la empresa para optimizar procedimientos, mejorar el conocimiento de los clientes, aumentar el volumen de negocio, mejorar la eficiencia operativa, detectar áreas de mejora y optimizar el funcionamiento de cada sucursal.

Cada vez son más los bancos que comprueban la necesidad de invertir en soluciones de analítica de datos por una sencilla razón: la información es poder y los sistemas de videovigilancia con Inteligencia Artificial no sólo protegen los activos, sino que además se convierten en una herramienta transversal para todos los departamentos.



PRIORIDAD N°1: SISTEMAS CIBERSEGUROS

En la era digital actual, el Internet de las Cosas (IoT) ha transformado la forma en que vivimos y trabajamos. Sin embargo, a medida que aumentan los beneficios de la conectividad, también lo hacen las vulnerabilidades y amenazas cibernéticas.

El fortalecimiento de la seguridad en dispositivos físicos conectados a la red va en aumento y el objetivo es que tanto *hardware* como *software* sean seguros desde su fabricación y cuenten con todos los estándares de ciberseguridad actuales; cifrado de la información transmitida, encriptación de la información almacenada, autenticación de usuario de alto performance, seguridad en puertos de red, certificados de seguridad, *firmware* firmados y protegidos, etc.

Dado el aumento del número de ciberataques, así como de los incidentes en el mundo real, es necesaria la convergencia de la ciberseguridad y la seguridad física y para SCATI, al hablar de tendencias o innovaciones, creen que el objetivo es conformar un sistema de seguridad integral que no deje resquicios a los delincuentes, prevenga que se comentan ilícitos y ofrezca grandes capacidades de analítica forense para investigar lo sucedido.

Evaluar los riesgos de seguridad de una forma continua y disponer de un sistema de seguridad física infalible que pueda complementar las medidas de ciberseguridad implementadas por el área de TI, y proporcionar así una seguridad 360° a la entidad.

UN SOCIO TECNOLÓGICO

Los cambios tecnológicos suceden cada vez en menos tiempo, por lo que es imprescindible contar con un socio tecnológico capaz de evolucionar ante cualquier reto o cambio.

Este socio debe tener una clara orientación al cliente para comprender cuáles son los problemas que tiene cada institución financiera y poder adaptar sus soluciones. Para conseguir adaptarse, es necesario contar con tecnología propia y ofrecer una solución completa que además pueda ser gestionada bajo un único interfaz que simplifique la operativa diaria en las instalaciones.

Modernizar los sistemas de seguridad en las entidades financieras es una inversión esencial que debe abordarse de manera integral. La colaboración entre departamentos, el uso de tecnología avanzada y la asociación con socios tecnológicos confiables son los pilares para asegurar que las entidades financieras no sólo protejan sus activos, sino que también optimicen sus operaciones y fortalezcan su posición en el mercado. La clave está en una visión a largo plazo que combine innovación, eficiencia y una ciberseguridad robusta, garantizando así un entorno seguro y eficiente. ■

Fotos: SCATI

Chesus M. Gay, *Key Account Manager* de SCATI. *Más sobre el autor:*

TIMUR
Latinoamérica

GALEAM

NUESTRO VALOR, SU SEGURIDAD

CONSULTORÍA

GUARDIAS INTRAMUROS

PROTECCIÓN EJECUTIVA

info@galeam.mx
info@timurlatinoamerica.com

56 3048 9610 / 55 6840 1036

www.galeam.mx
www. timurlatinoamerica.com

LAS 5 TENDENCIAS TECNOLÓGICAS QUE AFECTARÁN AL SECTOR DE LA SEGURIDAD EN 2025

Los proveedores tienen que desarrollar sus propias tecnologías y operar sus propios negocios de manera que apoyen los requisitos de cumplimiento de sus clientes

Foto—Freepik

SUECIA | **Johan Paulsson**

Incluso para quienes llevamos décadas trabajando en el sector tecnológico, el ritmo de cambio de los últimos 12 meses ha sido extraordinario.

Una vez más, no nos cabe duda de que las innovaciones tecnológicas nos brindan enormes oportunidades y nos plantean retos más complejos que nunca, y no muestran signos de desaceleración. Seguir el ritmo de los cambios y sus implicaciones —para proveedores, clientes y reguladores— exige concentración, energía y diligencia.

Las principales tendencias tecnológicas que creemos que afectarán al sector de la seguridad en 2025 reflejan este entorno en rápida evolución. Como siempre, son una mezcla de oportunidades positivas que hay que aprovechar, junto con los retos que hay que abordar.

1.- EL POTENCIAL DE LA IA GENERATIVA EN EL SECTOR DE LA SEGURIDAD

En anteriores entradas sobre tendencias tecnológicas se ha destacado el potencial de la IA y el aprendizaje profundo en el sector de la seguridad, con especial atención al análisis avanzado en el borde de la red, en las propias cámaras.

Esta proliferación del aprendizaje profundo en los bordes se está acelerando. Prácticamente cualquier cámara de red nueva que se lance incorpora capacidades de aprendizaje profundo, que mejoran enormemente la precisión de los análisis. Estas capacidades son la base para construir soluciones escalables en la Nube, ya que eliminan los requisitos de ancho de banda tan pesados, reducen el procesamiento en la Nube y hacen que el sistema sea más fiable.

Sin embargo, en términos de IA, 2023 ha sido el año en el que los grandes modelos de lenguaje (LLM) como base de la IA generativa se han abierto paso en la conciencia pública. Esta forma de IA permite la creación de nuevos contenidos —palabras, imágenes e incluso videos— a partir de preguntas e indicaciones en lenguaje natural de los usuarios.

Todas las empresas están estudiando los posibles casos de uso de la IA generativa, y el sector de la seguridad no es diferente. En 2025, veremos aparecer aplicaciones centradas en la seguridad basadas en el uso de LLM e IA generativa. Entre ellas se incluirán probablemente asistentes para operadores, que les ayudarán a interpretar con mayor precisión y eficacia lo que ocurre en una escena, y como atención interactiva al cliente, que proporcionará respuestas más útiles y procesables a las consultas de los clientes. Además, la IA generativa

ya ha demostrado su valor en el desarrollo de *software*, y este será un beneficio que se verá en todo el sector de la seguridad.

Por supuesto, debemos ser conscientes de los riesgos y las posibles trampas de la IA generativa. Habrá debates sobre qué modelos emplear y cómo, y en particular sobre el uso de modelos de código abierto frente a modelos propietarios, pero el mayor riesgo será ignorarlo.

2.- EFICIENCIA EN LA GESTIÓN DE SOLUCIONES QUE IMPULSA LA ARQUITECTURA HÍBRIDA

Las arquitecturas de soluciones híbridas —aquellas que emplean las ventajas de las tecnologías *in situ*, en la Nube y en el perímetro— se han establecido como el nuevo estándar en muchas soluciones de seguridad. Las funcionalidades se despliegan donde es más eficiente, utilizando lo mejor de cada instancia en un sistema, añadiendo un mayor nivel de flexibilidad. En última instancia, las arquitecturas de los sistemas deben estar al servicio de las necesidades del cliente, no de la estructura preferida del proveedor.

En gran medida, es una cuestión de accesibilidad. Cuanto más de una solución exista en entornos fácilmente accesibles, tanto para los vendedores como para los clientes, más capacidad tendrán los vendedores de gestionar elementos del sistema, asumiendo una mayor responsabilidad y reduciendo la carga de los clientes.

Las arquitecturas híbridas también son compatibles con los próximos casos de uso para la asistencia de IA y la automatización en la gestión y el funcionamiento de soluciones; una mayor accesibilidad al sistema es valiosa tanto para la asistencia humana como para la de IA, aprovechando los puntos fuertes de cada instancia diferente.

3.- SEGURIDAD SIEMPRE, PERO TAMBIÉN PROTECCIÓN

La seguridad y la protección se han relacionado a menudo como un único tema. Cada vez se reconocen más como casos de uso separados: la seguridad está relacionada con la prevención de actos intencionados —robos, vandalismo, agresiones a personas, etc.— y la protección está relacionada con los peligros e incidentes no intencionados que pueden causar daños a las personas, los bienes y el medio ambiente. Por una serie de razones, el uso de la videovigilancia y la analítica en casos de uso de seguridad está creciendo rápidamente y seguirá haciéndolo.

Una de las razones, por desgracia, es el cambio climático. Con unas condiciones meteorológicas extremas que provocan inundaciones, incendios forestales, corrimientos de tierras, avalanchas, etc., la videovigilancia, los sensores medioambientales y la analítica serán cada vez más utilizados por las autoridades para alertar, con antelación, posibles catástrofes y apoyar la respuesta más rápida y eficaz.

La gestión de riesgos, el cumplimiento de las directivas de salud y seguridad, y los requisitos normativos son otra razón clave para el continuo crecimiento de los casos de uso relacionados con la seguridad. La videovigilancia se utilizará ampliamente en las organizaciones para garantizar el cumplimiento de las políticas de salud y seguridad y las prácticas de trabajo seguras, como el uso de los equipos de protección individual (EPI) necesarios. Cuando se produzcan incidentes, la videovigilancia será una herramienta cada vez más útil e importante en las investigaciones.

La seguridad como caso de uso de la vigilancia está bien establecida. La seguridad seguirá evolucionando.

4.— LA REGULACIÓN Y EL CUMPLIMIENTO IMPULSAN LA TECNOLOGÍA

Hablando de conformidad, el entorno normativo mundial tiene cada vez más repercusiones en el desarrollo de la tecnología, su aplicación y su uso. El cumplimiento de estas normativas es algo de lo que proveedores y usuarios finales deben ser conscientes y para lo que deben trabajar en estrecha colaboración.

La inteligencia artificial, la ciberseguridad, la sostenibilidad,

Foto:-Freepik

Las arquitecturas de soluciones híbridas —aquellas que emplean las ventajas de las tecnologías in situ, en la Nube y en el perímetro— se han establecido como el nuevo estándar en muchas soluciones de seguridad

Cuanto más de una solución exista en entornos fácilmente accesibles tanto para los vendedores como para los clientes, más capacidad tendrán los vendedores de gestionar elementos del sistema, asumiendo una mayor responsabilidad y reduciendo la carga de los clientes


Foto:–Freepik

el gobierno corporativo... todas son áreas que están siendo sometidas a un mayor escrutinio normativo. Los proveedores tienen que desarrollar sus propias tecnologías y operar sus propios negocios de manera que apoyen los requisitos de cumplimiento de sus clientes.

Cada vez más, el panorama normativo abarca más que el desarrollo y el uso específicos de la tecnología en sí. La geopolítica y las relaciones comerciales entre estados nacionales también están dando lugar a normativas que exigen transparencia hasta el nivel de los componentes si los proveedores quieren mantener la licencia para operar en mercados internacionales clave.

Se trata de un ámbito en constante evolución y cambio, que requiere diligencia, desarrollo y transparencia constantes en toda la cadena de valor. Para los usuarios de tecnología de seguridad, es una cuestión de confianza. ¿Pueden estar seguros de que todos los eslabones de su cadena de suministro operan de una forma que respalda su propio cumplimiento de la normativa?

5.- "ADOPTAR LA PERSPECTIVA DEL SISTEMA TOTAL"

El impacto de cada aspecto de un sistema de seguridad estará sometido a un escrutinio cada vez mayor, y los vendedores y clientes tendrán que supervisar, medir y, cada vez más, informar sobre una amplia gama de factores. Será esencial adoptar una perspectiva global del sistema.

El consumo de energía es un buen ejemplo. Una videocámara consume por sí misma una cantidad relativamente pequeña de energía. Pero si se tienen en cuenta también los servidores, conmutadores, concentradores y enrutadores a través de los cuales se transfieren los datos, ubicados en grandes centros de datos que requieren refrigeración, el panorama cambia.

Esta perspectiva global del sistema es útil y debe ser bien acogida por el sector. Dará lugar a innovaciones en nuevas tecnologías y cámaras que aporten beneficios a todo el sistema, no de forma aislada. Las cámaras que reducen la tasa de *bits*, el almacenamiento y la carga del servidor con la intención de reducir las necesidades de refrigeración del servidor son un buen ejemplo. El transporte más eficiente de los productos, el embalaje sostenible y el uso de componentes estándar también pueden desempeñar un papel importante. La visibilidad y un mayor control en toda la cadena de suministro son esenciales.

Todos aceptamos que el costo total de propiedad (CTP) es una medida importante, pero los proveedores de seguridad tendrán que considerar cada vez más (y ser transparentes al respecto) el impacto total de la propiedad, teniendo en cuenta aspectos no financieros, como los medioambientales y sociales. Ya no será posible que los proveedores operen aislados de su propia cadena de valor y de la de sus clientes.

No nos cabe duda de que en 2025 se producirán nuevos avances tecnológicos y, con ellos, nuevos retos que todos deberemos afrontar. Como siempre, estamos deseando trabajar con nuestros socios y clientes para garantizar resultados positivos para todos, dentro y fuera del sector. ■

Johan Paulsson, director de Tecnología en Axis Communications. *Más sobre el autor:*

CRNOVA SECURITY

Custodia de Mercancía

Guardia Intramuros

Monitoreo y Rastreo

ISO 9001

ISO 28000

BASC

ISO 18788

ISO 37001

AMESP

ESR

ASIS INTERNATIONAL

crnovaoficial

crnovasecurity

www.crnova.com.mx

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

EL IMPACTO DEL *NEARSHORING* EN LA INDUSTRIA AUTOMOTRIZ

Cada vez más fabricantes y empresas se suman al mercado nacional, lo que incentiva a generar nuevas redes de distribución y almacenamiento con los procesos de seguridad necesarios que garanticen la operación y continuidad del negocio

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

En 2023, China fue el principal país proveedor de autos a México con 237 mil 18 unidades, seguido de Brasil, Estados Unidos, India y Japón, y este año continúa adentrándose en el mercado automotriz nacional. De acuerdo con datos de la Asociación Mexicana de Distribuidores de Automotores (AMDA), los primeros meses del 2023 tuvo un crecimiento anual de 48% respecto al año anterior, actualmente son más de 20 marcas de vehículos de pasajeros, de origen chino en México, siendo las SUV's con mayor demanda.

DFAC DONGFENG SE INTEGRA AL MERCADO AUTOMOTRIZ LATINOAMERICANO

En julio del presente año, de la mano de Grupo Magna y Magma Automotive, DFAC, el mayor fabricante de vehículos comerciales en China y los segundos a nivel mundial, anunció su inicio de operaciones en México y nueve países de Latinoamérica con su gama de vehículos comerciales garantizando excelencia, seguridad y tecnología vanguardista.

Hasta el momento se tienen contemplados 80 centros de atención, distribución y servicio en Latinoamérica, ofreciendo una línea de 11 modelos y 16 versiones distintas de vehículos comerciales entre vanes, *pickups*, minivanes, camiones ligeros y el tractocamión Junfeng H con motor Cummins ISZ.

"México con el *nearshoring* tiene una gran oportunidad que ya se está materializando en el sentido de inversiones directas que van a generar una derrama económica muy importante, principalmente bajo dos aristas. Una, sobre el mercado interno, por generación de trabajo, cadena de valor, entre otras, y, por otro lado, una demanda de ciertos elementos para que esa inversión bajo el ala del *nearshoring* pueda surtir a otros mercados de América del Norte. DFAC Dongfeng es de las principales automotrices chinas, es la marca número uno de vehículos comerciales en China, y el número dos a nivel global por lo que lanzar DFAC en México, es un hito muy importante generando un buen posicionamiento con el *nearshoring*", comentó en entrevista Philipp Heldt, *General Manager* para DFAC Dongfeng México y Grupo Magna México.

Grupo Magna es una empresa dominicana con cinco décadas de trayectoria, se ha consolidado como un referente de excelencia en el sector automotriz, representando exclusivamente prestigiosas marcas internacionales, entre ellas BMW y Hyundai, lo cual genera un gran beneficio al contar con una amplia red de distribución que se caracteriza por ofrecer atención personalizada al cliente, y promete tener un stock que satisfaga la demanda del mercado latinoamericano.

"Los productos que ofrecemos son de calidad, y ahora que se integra la marca líder de China, y la segunda a nivel mundial, lo corrobora, tanto en tecnología como diseño y seguridad. La mayoría de nuestros vehículos tienen motores Cummins, que son reconocidos mundialmente, la transmisión Eaton, Ejes Dana, es decir, son marcas reconocidas que dan como resultado vehículos muy bien hechos, con muy buenas características, y la ventaja con Magna, es que tenemos un enfoque completo en cuanto a servicios, refacciones, asegurarnos que nuestro cliente esté bien respaldado y con una buena posventa", y resaltó Agustín Lama, CEO de Grupo Magna.

Instalar una ensambladora en el país es una de las intenciones que tiene Magna para el siguiente año, pues las ventajas se verán reflejadas en la reducción de costos de flete, en la distribución, la creación de empleos y otras oportunidades de negocio. ■

Fotos: Mónica Ramos / SEA

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

24/365 DÍAS Monitoreo de equipos

Desarrollo de WEB y APP

Telemetría e inteligencia Artificial (IA)

Tecnología 3G/4G/Satelital

Contamos con puntos estratégicos en todo el país

amazon web services

Azure

Infraestructura sustentada por AWS y Azure

AMESIS · AMESP · ANTP · ASIS · CANACAR · COPARMEX · ConaLog

LÍDERES EN SOLUCIONES DE

RASTREO SATELITAL

Más Información:

Contáctanos

55·5374·9320

¡Síguenos en nuestras redes!

trackingsystems.mx

+ de 52,500 Equipos Instalados

24/7 Rastreo Satelital

Recuperación 98.5% Aviso en menos de 30 minutos*

IA

VALIDACIÓN DE IDENTIDAD CON IA

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

ANÁLISIS POR FRECUENCIA DE VOZ

TRUST ID

VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL

LA FORMA MÁS RÁPIDA Y PODEROSA DE CERTIFICAR A TU PERSONAL

UNA SOLUCIÓN DE Grupo UDA · Tracking® Systems

¡Síguenos en nuestras redes!

TRUSTID.MX

Contáctanos

55·4447·0231 · 5374·9320 · EXT 159

atencionaclientes@trustid.mx

Más Información:

TENDENCIAS EN SOLUCIONES DE RASTREO VEHICULAR

La constante mejora en la precisión, la capacidad de análisis de datos, la integración de sistemas y la seguridad representan innovaciones continuas en este campo

Foto:–Freepik

MÉXICO **José Luis Sánchez Gutiérrez**

Realmente muy agradecido por su acostumbrada preferencia estimados lectores; y en esta ocasión tocaremos el tema de las soluciones de rastreo vehicular.

Las soluciones de rastreo vehicular varían en función de las necesidades específicas de seguridad y seguimiento. Les enlisto algunas de las mejores soluciones disponibles en el mercado, cada una con sus propias características y beneficios:

1) **Sistemas de GPS:** estos dispositivos utilizan señales GPS para rastrear la ubicación exacta del vehículo en tiempo real. Pueden ser autónomos o integrados en sistemas de gestión de flotas, permitiendo el seguimiento continuo del vehículo y generando alertas en caso de movimientos no autorizados o desviaciones de ruta.
2) **Dispositivos de seguimiento por radiofrecuencia (RFID):** utilizan etiquetas o transpondedores RFID para rastrear vehículos dentro de áreas específicas cubiertas por lectores RFID. Estos sistemas son útiles para controlar el acceso y la salida de vehículos de áreas restringidas.
3) **Sistemas basados en la Nube:** ofrecen soluciones de seguimiento que se conectan a plataformas en la Nube, permitiendo el acceso remoto a la información del vehículo desde cualquier lugar con conexión a Internet.
4) **Dispositivos de seguimiento satelital:** utilizan comunicación satelital para rastrear vehículos incluso en áreas remotas donde la señal GPS puede ser limitada. Son ideales para flotas que operan en regiones con poca cobertura celular.
5) **Soluciones de seguimiento móvil mediante aplicaciones:** algunas empresas ofrecen aplicaciones móviles que permiten a los propietarios rastrear sus vehículos desde sus teléfonos inteligentes, ofreciendo funcionalidades como alertas de movimiento, límites de velocidad y geocercas.
6) **Sistemas integrados de gestión de flotas:** combinan el rastreo vehicular con herramientas de gestión de flotas, proporcionando análisis detallados sobre el rendimiento del vehículo, mantenimiento, eficiencia de combustible y más.

1. SISTEMAS DE GPS

Los sistemas de GPS (Sistema de Posicionamiento Global) son tecnologías que utilizan una red de satélites para determinar la ubicación precisa de un objeto en la Tierra. En el contexto de seguridad vehicular, los sistemas de GPS se utilizan ampliamente para rastrear y monitorear la ubicación y movimiento de vehículos. Aquí hay detalles sobre estos sistemas:

Componentes y funcionamiento:

- **Receptores GPS:** estos dispositivos recogen señales de al menos cuatro satélites GPS para calcular la ubicación del vehículo.
- **Satélites GPS:** una red de satélites orbita la Tierra emitiendo señales continuamente, las cuales son captadas por el receptor GPS en el vehículo.
- **Comunicación de datos:** la información de ubicación y movimiento se transmite a través de la red celular o por satélite a un centro de monitoreo o plataforma en la Nube.

Características principales:

- **Rastreo en tiempo real:** los sistemas de GPS permiten monitorear la ubicación exacta del vehículo en tiempo real, mostrando trayectorias, velocidad y paradas.
- **Geovallas o Geocercas:** establecen límites geográficos virtuales y emiten alertas si el vehículo entra o sale de estas áreas predefinidas.
- **Alertas de movimiento:** notifican a los administradores o propietarios del vehículo si se detecta movimiento no autorizado o si el vehículo sale de horarios programados.
- **Informes y análisis:** ofrecen informes detallados sobre la actividad


Foto:–Freepik

ALGUNAS EMPRESAS OFRECEN APLICACIONES MÓVILES QUE PERMITEN A LOS PROPIETARIOS RASTREAR SUS VEHÍCULOS DESDE SUS TELÉFONOS INTELIGENTES, OFRECIENDO FUNCIONALIDADES COMO ALERTAS DE MOVIMIENTO, LÍMITES DE VELOCIDAD Y GEOCERCAS

del vehículo, incluyendo tiempos de conducción, paradas, eficiencia de combustible y más.
- **Inmovilización remota:** algunos sistemas avanzados permiten la desactivación remota del motor del vehículo en caso de robo o situación de emergencia.

Beneficios:
- **Seguridad:** permite un seguimiento continuo del vehículo, facilitando su recuperación en caso de robo o pérdida.
- **Gestión de flotas eficiente:** ayuda a optimizar la planificación de rutas, el mantenimiento y el uso de los vehículos.
- **Reducción de costos:** mejora la eficiencia del combustible y reduce el tiempo de inactividad no planificado.

Consideraciones:
- **Costos y suscripciones:** los sistemas de GPS pueden implicar costos iniciales de *hardware* y tarifas de suscripción por el uso de la plataforma y la red de comunicación.
- **Privacidad:** la implementación de estos sistemas debe considerar y respetar la privacidad de los conductores y empleados.
- Los sistemas de GPS son herramientas valiosas para mejorar la seguridad vehicular, la gestión de flotas y la eficiencia operativa, pero es importante elegir el sistema que mejor se adapte a las necesidades específicas de cada caso.

2. DISPOSITIVOS DE SEGUIMIENTO POR RADIOFRECUENCIA (RFID)

Los dispositivos de seguimiento por radiofrecuencia (RFID) son sistemas de identificación que utilizan ondas de radio para identificar y rastrear objetos, incluyendo vehículos, a través de etiquetas o transpondedores RFID. En el ámbito de la seguridad vehicular, estos dispositivos se emplean para controlar el acceso y el seguimiento de vehículos en áreas específicas. Aquí se detallan sus características:

Componentes y funcionamiento:
- **Etiquetas o transpondedores RFID:** estos dispositivos, generalmente pequeños y pasivos, se adhieren a los vehículos y contienen información específica del vehículo o del propietario.
- **Lectores RFID:** Estos dispositivos emiten señales de radiofrecuencia que son recibidas por las etiquetas RFID y recopilan la información contenida en ellas.
- **Sistema de gestión o base de datos:** La información recopilada se almacena y gestiona en un sistema o base de datos para su análisis y seguimiento.

Características principales:
- **Control de acceso:** los lectores RFID -2- instalados en entradas o salidas pueden identificar los vehículos autorizados que ingresan o salen de áreas restringidas.
- **Identificación automática:** las etiquetas RFID permiten la identificación automática y sin contacto, lo que agiliza el proceso de control de acceso.
- **Registro de eventos:** registra automáticamente la presencia del vehículo en áreas específicas, creando un registro de eventos para auditorías y seguimiento.
- **Geocercas virtuales:** al igual que con otros sistemas de rastreo, se pueden establecer geocercas virtuales para generar alertas si un vehículo entra o sale de áreas predefinidas.
- **Seguridad y antifalsificación:** los sistemas RFID avanzados pueden tener medidas de seguridad integradas para evitar la clonación o falsificación de etiquetas.

Beneficios:
- **Control de acceso seguro:** permite restringir el acceso a áreas específicas, aumentando la seguridad del perímetro.
- **Automatización y eficiencia:** agiliza los procesos de entrada y salida de vehículos, reduciendo el tiempo y mejorando la eficiencia operativa.
- **Registro y auditoría:** proporciona registros precisos de la presencia de vehículos para fines de auditoría y seguimiento.

Consideraciones:
- **Costo inicial:** la implementación de sistemas RFID puede implicar costos iniciales de *hardware* y *software*.
- **Alcance de lectura:** la distancia de lectura de los lectores RFID puede variar y verse afectada por obstáculos o interferencias.
- **Privacidad:** la utilización de etiquetas RFID para el seguimiento de vehículos plantea cuestiones de privacidad que deben ser consideradas y respetadas.
- Los sistemas de seguimiento por radiofrecuencia (RFID) ofrecen una manera efectiva de controlar el acceso y rastrear vehículos en áreas restringidas, mejorando la seguridad y la eficiencia operativa. Sin embargo, su implementación debe ser considerada cuidadosamente para asegurar su compatibilidad con las necesidades específicas y los requisitos de privacidad de la organización.


Foto:–Freepik

3. SISTEMAS BASADOS EN LA NUBE

Los sistemas basados en la Nube para el rastreo vehicular son plataformas que utilizan tecnología en la Nube para almacenar, procesar y gestionar datos relacionados con la ubicación y el seguimiento de vehículos. Estos sistemas ofrecen una serie de beneficios y funcionalidades específicas para el monitoreo remoto y la gestión eficiente de flotas. Aquí tienes más detalles:

Características principales:

- **Almacenamiento centralizado:** Los datos sobre la ubicación del vehículo, trayectorias, velocidades y otros parámetros se almacenan en servidores remotos en la Nube.
- **Acceso remoto:** Los usuarios autorizados pueden acceder a la información desde cualquier lugar con conexión a Internet a través de una interfaz web o una aplicación móvil.
- **Seguridad de datos:** Las plataformas en la Nube utilizan protocolos de seguridad avanzados para proteger la información almacenada, como cifrado de datos y autenticación de usuarios.
- **Actualizaciones automáticas:** Las actualizaciones de *software* y nuevas funcionalidades se implementan de manera automática y transparente para los usuarios.
- **Escalabilidad:** Estos sistemas son altamente escalables, lo que significa que pueden adaptarse fácilmente a la cantidad de vehículos y usuarios que necesitan ser monitoreados.

Funcionalidades y beneficios:

- **Rastreo en tiempo real:** proporciona información actualizada sobre la ubicación, velocidad y actividades del vehículo en tiempo real.
- **Análisis y reportes:** genera informes detallados y análisis sobre el rendimiento del vehículo, historial de rutas y eficiencia operativa.
- **Notificaciones y alertas:** emite alertas automáticas sobre eventos predefinidos, como salidas de áreas designadas o excesos de velocidad.
- **Gestión de flotas:** permite una gestión eficiente de flotas al ofrecer información sobre el estado y la ubicación de múltiples vehículos simultáneamente.
- **Integración con otros sistemas:** puede integrarse con sistemas de gestión empresarial o *software* de gestión de flotas para un flujo de trabajo más eficiente.

Consideraciones:

- **Conectividad y acceso a Internet:** la eficiencia del sistema depende de una conexión a Internet estable para la transmisión de datos en tiempo real.
- **Costos y suscripciones:** puede implicar costos recurrentes por el uso de la plataforma en la Nube y la cantidad de datos almacenados.
- **Seguridad y privacidad:** se debe considerar y mantener un enfoque robusto en cuanto a la seguridad de los datos almacenados en la Nube.
- Los sistemas basados en la Nube para rastreo vehicular son herramientas poderosas que ofrecen acceso remoto, análisis detallados y funciones avanzadas para la gestión de flotas. Su eficacia y utilidad dependen de la selección adecuada y de su integración con las necesidades específicas de seguimiento y gestión de vehículos de cada organización.

4. DISPOSITIVOS DE SEGUIMIENTO SATELITAL

Los dispositivos de seguimiento satelital son herramientas de rastreo vehicular que utilizan tecnología de comunicación por satélite para monitorear la ubicación y el movimiento de vehículos en tiempo real, incluso en áreas remotas donde la cobertura celular puede ser limitada. Estos dispositivos ofrecen una serie de características y beneficios específicos:

Características principales:

- **Conectividad satelital:** utilizan comunicación vía satélite para enviar y recibir datos de ubicación y seguimiento del vehículo.
- **Global Coverage:** pueden rastrear vehículos en cualquier lugar del mundo, incluso en áreas sin cobertura celular.
- **Seguimiento en tiempo real:** proporcionan información actualizada sobre la ubicación precisa del vehículo en tiempo real.
- **Funciones de seguridad:** algunos dispositivos ofrecen alertas automáticas en caso de movimientos no autorizados o situaciones de emergencia.
- **Resistencia a interferencias:** la comunicación vía satélite es menos susceptible a interferencias externas, ofreciendo una conexión más estable.

Tipos de dispositivos:

- **Dispositivos autónomos:** son unidades independientes que se instalan en el vehículo y se comunican directamente con los satélites para el seguimiento.
- **Integrados en sistemas de gestión de flotas:** algunos dispositivos de seguimiento satelital se integran en sistemas de gestión de flotas más amplios para una administración más completa.

Beneficios:

- **Cobertura global:** funcionan en cualquier parte del mundo, incluso en áreas remotas o sin cobertura celular.
- **Fiabilidad:** la comunicación satelital ofrece una conexión más estable y menos susceptible a interferencias locales.
- **Seguridad:** permite un seguimiento continuo y confiable de los vehículos, incluso en situaciones de emergencia o robo.
- **Seguimiento en tiempo real:** ofrece información actualizada sobre la ubicación y movimiento del vehículo en tiempo real.

Consideraciones:

- **Costos:** los dispositivos de seguimiento satelital pueden tener costos iniciales más altos que otros sistemas de rastreo.
- **Suscripciones y planes de datos:** pueden requerir suscripciones continuas para el acceso a la red de satélites y la transmisión de datos.
- **Integración:** la integración con otros sistemas de gestión de flotas o *software* empresarial puede ser necesaria para un uso eficiente y efectivo.
- Los dispositivos de seguimiento satelital son una opción robusta para el rastreo vehicular, especialmente en áreas remotas o donde la cobertura celular es limitada. Ofrecen una cobertura global confiable y una capacidad de seguimiento en tiempo real que puede ser crucial en entornos donde otros sistemas pueden no ser efectivos.

Foto:–Freepik

5. SOLUCIONES DE SEGUIMIENTO MÓVIL MEDIANTE APLICACIONES

Las soluciones de seguimiento móvil mediante aplicaciones son herramientas que permiten el rastreo y la monitorización de vehículos a través de dispositivos móviles, como teléfonos inteligentes o tabletas, mediante la instalación de aplicaciones dedicadas. Estas soluciones proporcionan una serie de funcionalidades específicas:

Características principales:

- **Aplicaciones móviles:** se instalan en dispositivos móviles (iOS, Android, etc.) y permiten el acceso a las funciones de seguimiento vehicular.
- **Rastreo en tiempo real:** proporcionan información actualizada sobre la ubicación del vehículo, su velocidad, direcciones y trayectorias en tiempo real.
- **Alertas y notificaciones:** permiten configurar alertas personalizadas para eventos específicos, como ingreso o salida de áreas designadas o límites de velocidad excedidos.
- **Geolocalización:** utilizan GPS integrado en los dispositivos móviles para identificar la ubicación del vehículo con precisión.
- **Informes y análisis:** ofrecen informes detallados sobre el historial de rutas, paradas, tiempos de conducción, eficiencia de combustible, entre otros datos.

Beneficios:

- **Acceso remoto:** permite el monitoreo del vehículo desde cualquier lugar con conexión a Internet a través de dispositivos móviles.
- **Facilidad de uso:** las aplicaciones móviles suelen tener interfaces intuitivas y fáciles de usar para los usuarios.
- **Costo efectivo:** algunas soluciones basadas en aplicaciones pueden tener costos iniciales bajos y requerir menos infraestructura que otros sistemas de seguimiento.
- **Notificaciones instantáneas:** ofrecen alertas en tiempo real sobre eventos específicos, lo que permite tomar acciones rápidas en caso de situaciones inesperadas.

Consideraciones:

- **Conectividad:** la eficacia de estas soluciones puede depender de la calidad de la conexión a Internet y la cobertura de red móvil en el área.
- **Seguridad de la aplicación:** debe garantizarse que la aplicación utilice medidas de seguridad adecuadas para proteger la información y el acceso.
- **Privacidad:** es importante considerar la privacidad de los datos, asegurándose de cumplir con las regulaciones y protecciones necesarias.
- Las soluciones de seguimiento móvil mediante aplicaciones ofrecen una forma conveniente y accesible de monitorear vehículos, proporcionando datos en tiempo real y funcionalidades útiles para la gestión de flotas y la seguridad vehicular. Sin embargo, es fundamental seleccionar la aplicación que mejor se ajuste a las necesidades específicas y garantizar su seguridad y privacidad.

6. SISTEMAS INTEGRADOS DE GESTIÓN DE FLOTAS

Los sistemas integrados de gestión de flotas son soluciones completas que permiten a las empresas monitorear, administrar y optimizar eficientemente sus flotas de vehículos. Estos sistemas utilizan tecnología avanzada para proporcionar una gestión integral y coordinada de todos los aspectos relacionados con la operación de la flota. Aquí se detallan sus características y beneficios:

Características principales:

- **Monitoreo en tiempo real:** proporciona información actualizada sobre la ubicación, el estado y la actividad de los vehículos en tiempo real.
- **GPS y tecnología de seguimiento:** utiliza GPS y otros métodos de seguimiento para rastrear la ubicación precisa y el rendimiento de los vehículos.
- **Informes detallados y análisis:** ofrece informes completos sobre el historial de rutas, tiempos de conducción, paradas, eficiencia de combustible y mantenimiento.
- **Gestión de mantenimiento:** programa y administra el mantenimiento de la flota para optimizar el rendimiento y reducir los tiempos de inactividad no planificados.
- **Optimización de rutas:** calcula las rutas más eficientes, minimizando el tiempo de viaje y los costos operativos.
- **Alertas y notificaciones:** emite alertas automáticas para eventos como exceso de velocidad, desviación de rutas o mantenimiento programado.

Beneficios:

- **Mejora de la eficiencia:** permite una gestión más eficiente de los vehículos, reduciendo costos operativos y mejorando la productividad.
- **Reducción de costos:** optimiza el consumo de combustible, reduce el desgaste de los vehículos y minimiza los costos de mantenimiento.
- **Seguridad mejorada:** permite un monitoreo constante, lo que puede mejorar la seguridad del conductor y del vehículo.
- **Cumplimiento normativo:** ayuda a cumplir con regulaciones y estándares relacionados con el transporte y la seguridad vehicular.

Consideraciones:

- **Costo:** puede implicar costos iniciales de *hardware*, *software* y suscripciones.
- **Capacitación y adopción:** la implementación exitosa requiere que el personal esté capacitado y dispuesto a adoptar y utilizar la tecnología.
- **Privacidad y seguridad:** es fundamental garantizar la seguridad de los datos y el cumplimiento de las regulaciones de privacidad.
- Los sistemas integrados de gestión de flotas son herramientas poderosas para las empresas que poseen y operan flotas de vehículos. Permiten una gestión integral, mejorando la eficiencia operativa, reduciendo costos y optimizando la seguridad y el rendimiento de la flota en general.

Nuevamente; no quiero dejar pasar el análisis *NOVELTY, FEASIBILITY, SPECIFICITY, IMPACT y WORKABILITY* aplicados a las soluciones de rastreo vehicular:

NOVELTY (NOVEDAD):

Las soluciones de rastreo vehicular han existido durante algún tiempo, por lo que su concepto no es completamente nuevo. Sin embargo, la innovación está en constante evolución. Nuevas tecnologías como el GPS, la conectividad satelital, las aplicaciones móviles y los sistemas basados en la Nube han mejorado significativamente estas soluciones. La constante mejora en la precisión, la capacidad de análisis de datos, la integración de sistemas y la seguridad representan innovaciones continuas en este campo.

FEASIBILITY (VIABILIDAD):

Estas soluciones son altamente viables, ya que aprovechan tecnologías establecidas y comprobadas como el GPS, la comunicación por satélite, las aplicaciones móviles y los sistemas en la Nube. Además, se han convertido en una opción más asequible debido a la reducción de costos en *hardware*, conectividad y suscripciones a lo largo del tiempo. La implementación es relativamente sencilla y su uso es intuitivo, lo que facilita su adopción por parte de empresas de distintos tamaños y sectores.

SPECIFICITY (ESPECIFICIDAD):

Las soluciones de rastreo vehicular son altamente específicas en cuanto a la información que proporcionan. Permiten un seguimiento preciso de la ubicación, velocidad, dirección y otros datos relevantes de los vehículos. Además, ofrecen funcionalidades específicas como alertas de eventos, informes detallados, gestión de flotas y monitoreo en tiempo real, lo que las hace altamente especializadas en el control y gestión vehicular.

IMPACT (IMPACTO):

El impacto de estas soluciones es significativo tanto en términos de eficiencia operativa como en la seguridad. Ayudan a reducir costos operativos, mejorar la productividad, optimizar el uso de combustible y minimizar tiempos de inactividad no planificados. Además, tienen un impacto positivo en la seguridad al permitir un monitoreo constante de los vehículos, lo que puede mejorar la seguridad del conductor y la prevención de robos.

WORKABILITY (VIABILIDAD PRÁCTICA):

Estas soluciones son altamente viables en entornos prácticos. Son fáciles de implementar y se adaptan a una variedad de contextos, desde flotas pequeñas hasta grandes empresas. Son escalables y flexibles, lo que las hace adecuadas para empresas con diferentes necesidades operativas y presupuestos.

De cualquier forma te enlisto desde mi observador los pros y contras de las soluciones de rastreo vehicular:

PROS:

- **Mejora la Eficiencia Operativa:** permite una gestión más eficiente de la flota, optimizando las rutas, reduciendo costos operativos y maximizando la productividad.
- **Optimización del Combustible:** proporciona datos precisos sobre el consumo de combustible y el rendimiento de los vehículos, lo que permite tomar medidas para reducir costos.
- **Seguridad Mejorada:** permite un monitoreo continuo de la ubicación y el estado de los vehículos, mejorando la seguridad de los conductores y la prevención de robos.
- **Gestión de Mantenimiento:** facilita la planificación y el seguimiento del mantenimiento preventivo, lo que reduce el tiempo de inactividad no planificado.
- **Informes Detallados:** genera informes completos sobre el historial de rutas, tiempos de conducción, paradas y otros datos relevantes para la toma de decisiones.
- **Cumplimiento Normativo:** ayuda a cumplir con regulaciones y estándares relacionados con el transporte y la seguridad vehicular.

CONTRAS:

- **Costo Inicial:** puede implicar costos iniciales significativos en términos de *hardware*, *software* y suscripciones.
- **Costos Continuos:** aunque inicialmente asequibles, los costos recurrentes como suscripciones de datos y mantenimiento pueden ser altos.
- **Posible Resistencia al Cambio:** algunos conductores pueden resistirse a ser monitoreados, lo que puede generar conflictos y disminuir la eficacia.
- **Dependencia de la Tecnología:** una interrupción en la conectividad o problemas técnicos puede afectar la funcionalidad del sistema.
- **Privacidad de los Conductores:** el monitoreo constante puede plantear preocupaciones sobre la privacidad de los datos y el control del conductor.
- **Capacitación del Personal:** la implementación exitosa requiere que el personal esté capacitado y dispuesto a adoptar y utilizar la tecnología.

Al evaluar todas las soluciones de rastreo vehicular, es crucial considerar factores como la precisión de la ubicación, la capacidad del seguimiento en tiempo real, la duración de la batería (en caso de dispositivos portátiles), el costo, la facilidad de instalación y el soporte técnico ofrecido por cada proveedor. Cada solución tiene sus propias ventajas y limitaciones, por lo que es importante elegir la que mejor se adapte a las necesidades específicas de seguridad y gestión de la flota de cada empresa o usuario.

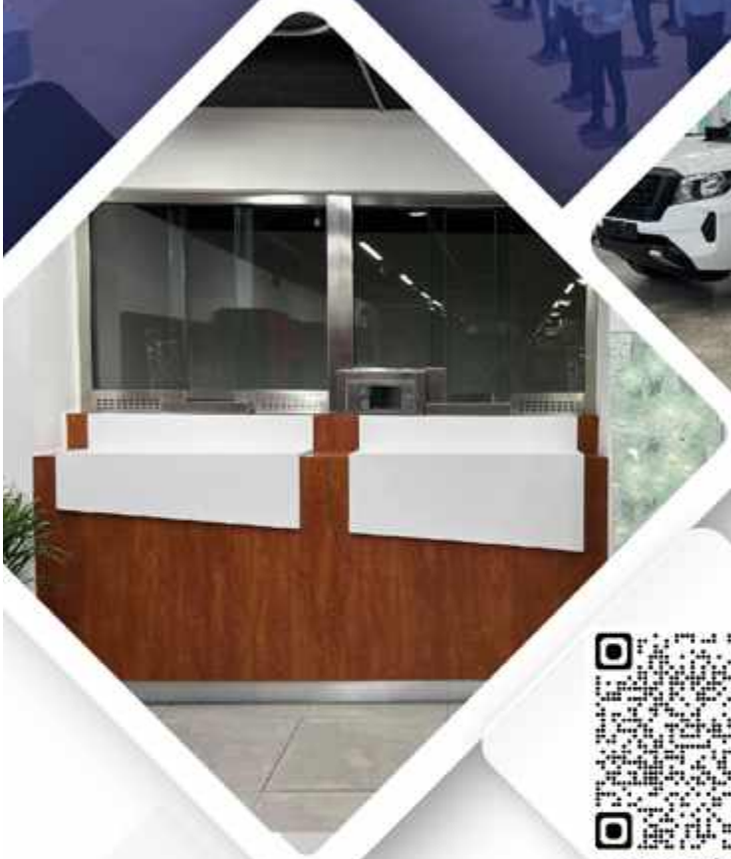
Te reitero nuevamente mi agradecimiento, por permitirme compartir contigo este artículo, esperando sea de tu interés y nos leemos como siempre en la siguiente edición; muchas gracias por tu acostumbrado apoyo y seguimiento a cada artículo aquí escrito. ■


Foto:–Freepik

José Luis Sánchez Gutiérrez, director comercial en Galeam. *Más sobre el autor:*

GSI

FABRIL S.A. DE C.V.®



VER CATÁLOGO

NUESTRA SEGURIDAD BANCARIA ES LA GARANTÍA DE SU TRANQUILIDAD

BLINDAJE

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

SEGURIDAD BANCARIA

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

CAJAS DE SEGURIDAD

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

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

SEGURIDAD EN COMERCIO EXTERIOR:

EL OPERADOR ECONÓMICO AUTORIZADO (OEA) EN ARGENTINA

Impulsor de buenas prácticas y beneficios para el comercio exterior

ARGENTINA **Jorge Gabriel Vitti**

La categorización de Operador Económico Autorizado (OEA), otorgada por la Aduana Argentina, ha llegado para definitivamente quedarse y expandirse. Si bien era fácilmente predecible por tratarse de una iniciativa internacional generada en la Organización Mundial de Aduanas, a través del Marco Normativo para Asegurar y Facilitar el Comercio Mundial (SAFE), venía sufriendo demoras y dilaciones.

Se trata de una categorización para probar el cumplimiento de ciertas medidas relacionadas con la seguridad y buenas prácticas en la cadena de suministro internacional de mercancías, adaptadas por cada nación. Los operadores económicos que cumplan los criterios para obtención del estatus OEA se consideran socios fiables en la cadena de suministro.

EL MARCO SAFE DE LA ORGANIZACIÓN MUNDIAL DE ADUANAS

Actualizado en 2021, el Marco SAFE ofrece, entre otras cosas, las condiciones para asegurar el comercio internacional, favoreciendo y facilitando el tránsito de las mercancías entre las fronteras. Crea, de esta forma, un conjunto de normas internacionales que genera uniformidad y previsibilidad, reduciendo los requisitos de informes múltiples y complejos.

De esta forma, los OEA recibirán un beneficio por su inversión en buenos sistemas y prácticas de seguridad, en particular mediante evaluaciones e inspecciones reducidas de objetivos de riesgo, así como el tratamiento acelerado de sus mercancías (con la reducción de costos que esto conlleva). Los OEA obtendrán beneficios, como el procesamiento más rápido de las mercancías por las Aduanas, con el consiguiente ahorro en tiempo y costos. En el caso de la máxima categoría de Argentina (OEA Seguridad), por ejemplo, la deseada selectividad canal verde.

OEA
Operador Económico Autorizado

LOS ACUERDOS DE RECONOCIMIENTO MUTUO

El Marco SAFE también prevé el reconocimiento mutuo de los controles en determinadas circunstancias, materializados por los Acuerdos de Reconocimiento Mutuo (ARM) entre Aduanas de distintas naciones. Este instrumento permite a las administraciones aduaneras adoptar una visión más amplia y completa de la cadena logística global y ofrecer la oportunidad de eliminar la duplicidad y los múltiples requisitos de informes. Un gran beneficio para los operadores de comercio exterior.

En Argentina, se encuentran vigentes los ARM firmados con:

- Uruguay – noviembre de 2019.
- Mercosur (Argentina, Bolivia, Brasil, Paraguay y Uruguay) – noviembre de 2019.
- ARM OEA Regional (Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, Paraguay, Perú, República Dominicana y Uruguay) – mayo de 2022.

Fotos cortesía: Jorga Gabriel Vitti

Autoridades aduaneras de Argentina, Bolivia, Brasil, Colombia, Costa Rica, Chile, Guatemala, Paraguay, Perú, República Dominicana y Uruguay firmaron el Arreglo de Reconocimiento Mutuo Regional, para el reconocimiento de los Programas del Operador Económico Autorizado (imagen de la página oficial de la Aduana de Bolivia).

Además, se encuentra instrumentado un Plan de Acción (paso previo a ARM) con la República Popular China – 19 de septiembre de 2019.

ADHESIONES EN ARGENTINA

En Argentina, ya pueden adherirse al programa los siguientes operadores:

- Importadores/Exportadores.
- Despachantes de Aduana.
- Agentes de transporte aduaneros.
- Transportistas automotores de carga relacionados con el comercio exterior.

Categorías y requisitos generales (micro-sitio OEA de AFIP)

Todos los demás sujetos relacionados con el comercio exterior e integrantes de la cadena de suministro internacional se irán incorporando gradualmente.

Bayer fue la primera empresa en Argentina en obtener la categorización OEA Seguridad, en noviembre del 2022.

De acuerdo con lo informado oficialmente por la Aduana Argentina, hay ya 79 acuerdos de categorización de empresas OEA materializados (al 22 de junio del 2023): 25 de cumplimiento, 42 de simplificación (categoría intermedia) y 11 de seguridad (máxima categoría). En esa misma oportunidad, fue categorizada en OEA Seguridad, la primera empresa nacional de logística internacional. Previamente un despachante de Aduana también había accedido a la misma categorización.

PARTICULARIDADES DE OEA SEGURIDAD

La decisión de obtener la categorización es de la Alta Dirección, dado que conlleva tareas para todos los sectores de la organización (Compras, RRHH, etc.) Esto es porque todas las tareas o funciones no sólo tienen un responsable designado, sino también designación de responsables de registro, control y producción de informes de retroalimentación para la mejora continua.

La formalidad indica que se deben confeccionar 9 (nueve) manuales donde se detalla el cumplimiento de los requisitos para cada caso expuestos. También se agrega que debe presentarse una matriz de riesgos paso que, evidentemente, debe ser el inicial y el disparador para la confección de los manuales. En tal sentido, y ya proporcionado una experiencia personal, es decisivo NO caer en la tentación de confeccionar los manuales como meros documentos que no se van a implementar, y sólo para cumplir el requisito. Es la receta óptima para el fracaso.

Los procesos reflejados en ellos son auditados y rechazados si no se cumplen, no están completos y no demuestran el enfoque participativo de toda la organización. Esta transición le es mucho más sencilla y llevadera a las organizaciones que desarrollan sus actividades bajo Normas Internacionales ISO 9001, por la dinámica de mejora continua y aplicación del Ciclo de Deming.

Manuales OEA Seguridad

Asimismo, estos cumplimientos que la organización debe instrumentar, debe también exigirlo por parte de sus socios comerciales. Por ello deben verse reflejados en los instrumentos contractuales, otorgando a quien contrata la potestad (y obligatoriedad) de controlar su cumplimiento mediante comprobaciones e inspecciones. Esto explica por qué es importante el alcanzar la categorización para las empresas logísticas, los despachantes de aduana y otros agentes que no reciben un beneficio directo de la selectividad canal verde. El valor agregado es, precisamente, ser un socio comercial adecuado con ventaja competitiva para un categorizado OEA Seguridad.

Por último, el perfil del Responsable OEA Seguridad Corporativo. Por la relevancia y características de la tarea, debe ser realizada por un profesional de la gestión de riesgos, en forma excluyente. Solamente ese perfil puede tener una visión holística y sistémica, con la capacidad de gestionar riesgos, incluidas las previsiones de planes de continuidad de actividades.

Asimismo, y como consecuencia de tener que supervisar y dirigir tareas de distintos sectores (RRHH, Compras, Seguridad, Mantenimiento, entre otros), este profesional debe tener autoridad delegada por la Alta Dirección en tal sentido. En una opinión personal, esta función es mucho más eficientemente cubierta por alguien externo a la organización, dada su autonomía en el obrar, sin condicionamientos y no representando intereses de ninguno de los sectores involucrados, respondiendo a la Alta Dirección, y con un planeamiento por objetivos. ■

Jorge Gabriel Vitti, magíster en Inteligencia Estratégica por la Universidad Nacional de La Plata y Licenciado en Seguridad.
Más sobre el autor:

Columna de
Jaime A. Moncada
jam@ifsc.us

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

INSPECCIONES VIRTUALES DE SISTEMAS CONTRA INCENDIOS

Foto:–Freepik

El impacto, luego de la reclusión forzada que sufrimos por los efectos del COVID-19, resultó en cambios importantes en la manera como ejecutamos nuestro trabajo. Por un lado, tuvimos que adaptarnos a las restricciones operativas de muchos proyectos e industrias. Pero, por otro lado, cambiamos al trabajo remoto, que planteó desafíos en términos de adaptación a nuevas tecnologías, mantenimiento de la productividad y garantía de una comunicación efectiva entre los miembros del equipo de trabajo. Mientras sufríamos los efectos de la pandemia, en el mundo de la seguridad contra incendios, se aceleró el interés por los usos y capacidades de las inspecciones remotas. Esta metodología de inspección virtual llegó para quedarse.

Unos pocos años antes de la pandemia ocurrió otro cambio importante en las regulaciones de protección contra incendio, sobre la cual escribí en esta revista[1]. Me refiero a que la normativa de la NFPA, la cual es utilizada como la referencia internacional en seguridad contra incendios, empezó a requerir una Prueba de Sistemas Integrados (PSIx), antes de la apertura de cualquier edificio. Aunque siempre se había requerido que cualquier sistema de protección contra incendio, nuevo o remodelado, debería pasar una prueba de aceptación, los códigos de la NFPA como la NFPA 1, 101 y 5000, así como el Código Internacional de la Construcción (IBC), ahora requieren que todos los sistemas interrelacionados que tienen que ver con la seguridad humana y la protección contra incendios en cualquier edificio o instalación, pasen una prueba concurrente de aceptación, de todos los sistemas contra incendios antes de la apertura del edificio.

INSPECCIONES REMOTAS POR VIDEO

Durante la pandemia, en varios proyectos en los que estaba trabajando a través de Latinoamérica, específicamente para el gobierno de los Estados Unidos, así como para hoteles de cadena internacional, nos llevó, en la compañía donde trabajo, a la ejecución de Inspecciones Remotas por Video (IRV) para llenar el requerimiento de la Prueba de Sistemas Integrados antes mencionada.

Las IRVs, conocidas en la normativa de la NFPA como RVIs por su acrónimo en inglés, son una forma de inspeccionar utilizando ayudas virtuales o electrónicas para permitir que un inspector o un equipo de inspectores observen a distancia la inspección o las pruebas de aceptación. Como se muestra en el pantallazo anexo, a través de una plataforma de videoconferencia, la IRV permite que los ingenieros que lideran el proceso de inspección o aceptación se comuniquen en línea con los contratistas de los diferentes sistemas contra incendios, quienes están en el sitio del proyecto, y los dirijan durante la prueba de aceptación de los sistemas contra incendios.

REGULACIÓN DE LAS IRVS

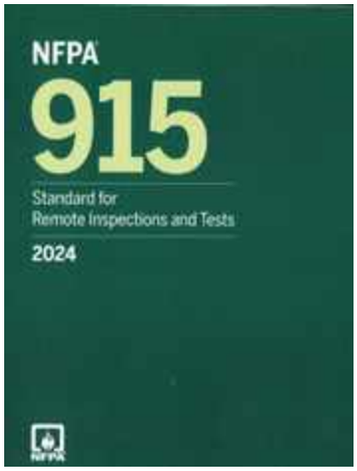
Las IRVs, como todo nuevo procedimiento, tiene una curva de aprendizaje, pero la realidad es que se están ejecutando con mucho éxito. En ingeniería de protección contra incendios, con la limitada disponibilidad de ingenieros calificados e independientes que puedan liderar el proceso de aceptación de proyectos complejos, esta metodología trae grandes beneficios para proyectos a través de Latinoamérica.

Aunque el proceso de prueba virtual es generalmente un poco más largo, estas pruebas pueden tener un costo más económico para el dueño del edificio. La prueba remota permite, que aún en los proyectos más remotos, ingenieros idóneos y calificados, aún a miles de kilómetros de distancia, lideren el proceso de inspección y aceptación. Como se mencionó anteriormente, estas pruebas remotas fueron necesarias durante la pandemia, pero se estima que estas pruebas se van a quedar con nosotros. Es por esto, que la normativa de protección contra incendios las está regulando.

En este sentido, la NFPA ha recientemente publicado una nueva norma, la NFPA 915, Norma sobre Pruebas e Inspecciones Remotas. Tanto NFPA como el ICC, el ente que publica el IBC, han publicado también guías para la ejecución de IRVs.

El propósito de la NFPA 915 es el de proporcionar requisitos mínimos para inspecciones y pruebas remotas. Aunque esta norma regula las pruebas virtuales remotas, también establece requerimientos para lo que muy posiblemente ocurrirá en el futuro cercano, por ejemplo, inspecciones y pruebas automatizadas y monitoreo a distancia. La norma busca regular un resultado equivalente o mejorado que el que se obtendría con otros métodos presenciales de inspección, prueba y monitoreo.

NFPA 915 indica que las IRVs son un método de inspección que permite que el contratista, de manera presencial operando los equipos, y el equipo de inspección, que de manera remota lidera la inspección o prueba, procedan de manera efectiva. NFPA indica que, si bien



esta práctica obtuvo una buena aceptación e implementación durante la pandemia, sus ventajas son tan grandes que probablemente se convertirá en una herramienta popular y rutinaria en el futuro previsible.

CRITERIOS GENERALES PARA LAS IRVS

Para aquellos dueños de proyectos que quisieran utilizar esta metodología para certificar el proceso de aceptación de sistemas contra incendios o que quieran llevar adelante la PSIx, se incluyen a continuación unas recomendaciones básicas pero esenciales:

1) El dueño del proyecto debe elegir y contratar el equipo que participe en las IRVs.

2) Las pruebas deben ser efectuadas en presencia de los contratistas de los distintos sistemas, quienes de manera presencial deben operar los equipos, siguiendo las directrices de un Agente de Prueba Integrada (aPI), quien está presente de manera virtual o remota.

3) El aPI, desde un sitio remoto, debe liderar y ser responsable por las pruebas. El aPI planifica, coordina, documenta, implementa y aprueba las pruebas.

4) El aPI es típicamente una firma de ingeniería de protección contra incendios calificada que pudiera haber sido responsable del proceso de diseño o una revisión por tercera parte del proyecto, aunque esto no es estrictamente necesario.

5) Es importante entender que el aPI debe ser distinto e independiente a cualquier contratista, instalador o vendedor de los sistemas contra incendios.

6) Para la ejecución de las pruebas por video, los miembros del equipo de aPI deben liderar las pruebas dando indicaciones a los contratistas.

7) Siguiendo un Protocolo de Pruebas pre-acordado, el aPI debe indicar al contratista algo así como: "Me puede mostrar la operación de xyz...". Aunque debe haber un diálogo entre el contratista y el aPI, el aPI siempre debe liderar las pruebas, indicando los elementos que se deben probar.

8) Durante la prueba, no sólo es importante verificar la operatividad de los equipos, sino que se debe verificar la secuencia de operación de los sistemas y lo que reporte el panel de alarma.

9) Antes de las pruebas se debe revisar la tecnología que se va a utilizar. Todos los participantes deben tener acceso a la plataforma de videoconferencia. Los miembros del aPI están en sus oficinas y se conectarán por computadora. Los contratistas se conectan a través de celulares con video. Se debe revisar que haya buena señal de video en el sitio del proyecto, ya sea por servicio celular o wifi. El contratista debe tener por lo menos dos celulares operando concurrentemente, uno en el panel de alarma y otro en el sitio donde se esté probando el equipo contra incendios.

Quisiera finalmente reiterar que, si está adelantando la construcción de un proyecto o está instalando sistemas nuevos de seguridad contra incendios en un edificio, es importante que antes de que el proyecto habrá sus puertas o el contratista termine su contrato, se efectúe una Prueba de Sistemas Integrados. Esta prueba se puede efectuar virtualmente de manera costo-eficiente y efectiva, utilizando profesionales calificados y con amplia experiencia en la aceptación de sistemas contra incendios, no importa dónde geográficamente esté el proyecto, o dónde residan los responsables del proceso de aceptación. ■

Referencias:

[1] *¿Dónde son Requeridas las Pruebas de los Sistemas Contra Incendios? Seguridad en América, Enero-Febrero 2023, Vol 136, pags. 44-46.*

Fotos: Cortesía Jaime A. Moncada

MEJORES PRÁCTICAS DE GESTIÓN DE VULNERABILIDADES EN LAS ORGANIZACIONES PARA LA TOMA DE DECISIONES: UN ANÁLISIS COMPLETO

Nuestro colaborador invitado proporciona un análisis completo y detallado de las mejores prácticas para la gestión de vulnerabilidades organizacionales

Foto:–Freepik

MÉXICO **Valente del Angel Santos**

Hoy en día en el contexto de ciberseguridad, cuando nos referimos a los actores de amenaza, todos nos conducen a un mismo camino: esas debilidades o fallas inherentes de un sistema o componente, mejor conocidas como vulnerabilidades, que, si se desencadena o se actúa en consecuencia, podrían casuar un evento de riesgo de los activos valiosos, incluida la información. Por ello la gestión de vulnerabilidades es una estrategia que debe ser incluida en cualquier programa de seguridad.

Toda organización debe tomar la postura para evaluar esa probabilidad de que un evento de riesgo ocurra y tomar esas medidas que se adecuan a su entorno para mitigar o reducir ese riesgo. Recordemos que el riesgo nace de la intersección entre un activo (lo que necesita protección), una vulnerabilidad (la brecha o debilidad) y una amenaza (algo o alguien que tiene como objetivo explotar una vulnerabilidad). Aquí radica esa vital importancia y es donde se entra en ese emocionante campo de batalla de la ciberseguridad, pues los profesionales en ciberseguridad utilizan sus conocimientos y habilidades para determinar cómo usar los datos de riesgo de manera eficiente, trabajar de manera transversal y por supuesto informar de manera digerible sobre los hallazgos a las partes interesadas para la toma de decisiones.

EMPEZAMOS CON UN CICLO COMPLETO Y CONTINUO:

1) **Descubrir:** Es la sección donde se identifican todos los activos de la red, incluidos los sistemas operativos, el *software* y el *hardware*.
2) **Priorizar:** Dividir los activos en grupos y darle un valor según cuán importantes son para tu empresa.
3) **Evaluación:** Llevar a cabo una evaluación de las vulnerabilidades detectadas.
4) **Corrección:** Implementar las soluciones requeridas para reducir las vulnerabilidades.
5) **Verifique:** Asegurarse que las soluciones aplicadas han reducido efectivamente las vulnerabilidades.
6) **Informe:** Mantenga un registro de todo el proceso y los resultados.

¿TODO QUEDA EN AUTOMATIZACIÓN? LA IMPORTANCIA DEL ANÁLISIS HUMANO:

Cuando entramos al terreno de las vulnerabilidades podemos encontrarnos con una gran cantidad de soluciones que permiten automatizar estos procesos, con la finalidad de optimizar las cargas de trabajo, pero hay algo que no se debe desprender de estos procesos: la capacidad analítica humana, que es la que permite la toma de decisiones para cada diversidad de objetivos de cada organización, pues tengamos en cuenta que la priorización de cada vulnerabilidad depende totalmente del apetito del riesgos de la misma organización.

Adoptar formas de trabajo transversales y multidisciplinares que permitan abordar las siguientes pautas:

- **Priorización de vulnerabilidades:** Considerar el contexto empresarial, el apetito al riesgo y el impacto potencial de cada vulnerabilidad en el negocio.


Foto:–Freepik

- **Seleccionar las formas de mitigación adecuadas:** Al evaluar las diferentes opciones, se considera el costo, la complejidad de realizarlo y la compatibilidad con los servicios, *software* y sistemas existentes.
- **Interpretación de los datos y resultados:** El análisis de datos que se obtienen de las pruebas para la verificación e identificación de posibles errores, brechas o falsos positivos, y tomar decisiones sobre las mejores acciones correctivas.

LA RESPONSABILIDAD COMPARTIDA PUEDE REDUCIR EL RIESGO EMPRESARIAL:

La gestión de vulnerabilidades debe tomarse como una responsabilidad compartida que no vive sólo sobre el área de TI y seguridad, pues durante todo el proceso se debe involucrar a cada responsable de un activo y de los servicios asociados al mismo, podemos incluir:

- **Áreas de negocio:** Se debe colaborar en la identificación de activos críticos, la evaluación del impacto potencial de las vulnerabilidades y la toma de decisiones sobre la mitigación de riesgos.
- **Operaciones:** Deben implementar las soluciones de mitigación, realizar pruebas de seguimiento y garantizar la continuidad del negocio en caso de incidentes de seguridad.
- **Gestión de riesgos:** Debe asesorar en la evaluación del apetito al riesgo de la organización y la priorización de las vulnerabilidades.
- **Comunicación:** Las diferentes áreas y partes interesadas deben poder comunicarse de manera efectiva.

RECOMENDACIONES PARA MEJORAR LA ADMINISTRACIÓN DE VULNERABILIDADES:

- **Una política de gestión de vulnerabilidades clara:** La política debe definir los roles y responsabilidades de las diferentes áreas involucradas, así como los procedimientos para la identificación, evaluación, priorización, mitigación y reporte de vulnerabilidades, los plazos para la toma de medidas y las métricas para medir la efectividad del programa.
- **Implementar herramientas de escaneo y análisis de vulnerabilidades confiables:** Seleccionar herramientas que sean adecuadas para el tamaño y la complejidad de la organización, que proporcionen información precisa y actualizada sobre las vulnerabilidades y que se integren con otros procesos de seguridad.
- **Capacitar al personal en la gestión de vulnerabilidades:** Capacitar a los empleados para comprender los riesgos asociados con las vulnerabilidades, utilizar herramientas de escaneo y análisis y participar activamente en el proceso de gestión de vulnerabilidades.
- **Realizar pruebas de penetración regulares:** Contratar a expertos en seguridad para realizar pruebas de penetración regulares que simulan ataques reales con el objetivo de encontrar vulnerabilidades que las herramientas automatizadas no hayan detectado y evaluar la efectividad de las medidas de seguridad implementadas.
- **Considere la integración con otros procesos de seguridad:** La gestión de vulnerabilidades debe integrarse con procesos de gestión de identidades y accesos (IAM), gestión de configuración y respuesta a incidentes para crear un sistema de seguridad completo y proactivo.
- **Medir y monitorear la efectividad del programa:** Establecer métricas y KPIs clave para evaluar la efectividad del programa de gestión de vulnerabilidades, como la cantidad de vulnerabilidades identificadas, el tiempo promedio de respuesta, la tasa de mitigación y el impacto en los riesgos del negocio.
- **Mejorar continuamente el programa:** Revise regularmente el programa de gestión de vulnerabilidades para encontrar áreas de mejora e implementar las acciones necesarias para maximizar su efectividad y adaptarlo a nuevas amenazas y tecnologías.

CONCLUSIÓN

La gestión de vulnerabilidades es un proceso continuo que requiere participación y atención constante. Al implementar las mejores prácticas y recomendaciones mencionadas, las organizaciones pueden aumentar significativamente su nivel de seguridad y proteger sus activos valiosos de ciberataques.

Este artículo proporciona un análisis completo y detallado de las mejores prácticas para la gestión de vulnerabilidades organizacionales. Las organizaciones pueden fortalecer significativamente su postura de seguridad cibernética y reducir el riesgo de sufrir ataques exitosos al comprender la importancia de este proceso, implementar las recomendaciones adecuadas y contar con el compromiso de las diferentes áreas involucradas. ■

Valente Del Angel Santos, analista de vulnerabilidades. *Más sobre el autor:*

Columna de
GEMARC

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

george_rayas@hotmail.com

Jorge Rayas, líder en Seguridad Corporativa.
Más sobre el autor:

SEGURIDAD CORPORATIVA EN LA BANCA Y *RETAIL* EN MÉXICO: FUNDAMENTOS Y CUALIDADES CRÍTICAS PARA UN ENTORNO SEGURO PARA EL 2025

MÉXICO

Foto:-Freepik

La seguridad corporativa y la prevención de pérdidas son áreas críticas para cualquier organización, especialmente en el contexto de negocios digitales. En México, los sectores bancario y *retail* enfrentan desafíos únicos en su transición hacia el entorno digital. Este artículo analiza las acciones que deben tomar las organizaciones que cuentan con un departamento de Seguridad Corporativa y las que no, enfocándose en la preparación para el año 2025.

IMPORTANCIA DE LA SEGURIDAD CORPORATIVA Y LA PREVENCIÓN DE PÉRDIDAS EN EL CONTEXTO DIGITAL

Contexto actual y proyecciones futuras

La transformación digital ha llevado a un incremento significativo en las amenazas cibernéticas y las pérdidas asociadas. Según un estudio de Statista, el 60% de las empresas en México han experimentado algún tipo de ataque cibernético en los últimos dos años. Las instituciones bancarias y el sector *retail* son particularmente vulnerables debido al manejo intensivo de datos sensibles y transacciones financieras.

Instituciones bancarias

Para el caso de las instituciones bancarias están en la primera línea de la batalla contra el fraude y los ataques cibernéticos. La implementación de tecnologías avanzadas, como la banca en línea y las aplicaciones móviles, ha mejorado la accesibilidad y la comodidad para los clientes, pero también ha incrementado la superficie de ataque para los ciberdelincuentes.

Sector *retail*

En referencia al sector *retail* ha adoptado el comercio electrónico a un ritmo acelerado, especialmente tras la pandemia de COVID-19. Aunque esto ha generado nuevas oportunidades de negocio, también han aumentado los riesgos de fraudes y violaciones de datos, afectando la confianza de los consumidores y la integridad de las operaciones.

Después de la pandemia, las organizaciones que sí cuentan con un departamento de Seguridad Corporativa y un área de Prevención de Pérdidas están mejor equipadas para enfrentar estos desafíos. A continuación, se detallan las diferencias y los pasos a seguir para ambas.

Estas organizaciones suelen tener una infraestructura robusta y políticas bien definidas para protegerse contra amenazas y minimizar pérdidas.

- **Ventajas:**
- **Respuesta Rápida a Incidentes:** Equipos dedicados permiten una rápida detección y respuesta a incidentes de seguridad.
- **Capacitación Continua:** Los empleados reciben capacitación constante sobre mejores prácticas de seguridad.
- **Tecnología Avanzada:** Implementación de tecnologías como IA y *blockchain* para proteger datos y transacciones.

- **Desafíos:**

Costos Elevados: Mantener un departamento de Seguridad puede ser costoso.
Evolución de Amenazas: Las amenazas evolucionan constantemente, requiriendo actualizaciones frecuentes de políticas y tecnologías.

ORGANIZACIONES SIN DEPARTAMENTO DE SEGURIDAD CORPORATIVA Y ÁREA DE PREVENCIÓN DE PÉRDIDAS

Las organizaciones sin un departamento dedicado enfrentan mayores riesgos y tienen una menor capacidad para responder a incidentes de seguridad y prevenir pérdidas.

- **Desventajas:**
- **Respuesta Lenta a Incidentes:** La falta de personal especializado puede retrasar la respuesta a amenazas.
- **Menor Capacitación:** Los empleados pueden no estar adecuadamente capacitados en seguridad digital.
- **Mayor Vulnerabilidad:** Sin medidas de seguridad avanzadas, estas organizaciones son más vulnerables a ataques.

• **Desafíos:**

- **Implementación de Medidas Básicas:** Asegurar que todos los empleados sigan prácticas de seguridad básicas.
- **Dependencia de Proveedores Externos:** Muchas veces dependen de proveedores externos para servicios de seguridad, lo cual puede ser menos efectivo y más costoso a largo plazo.

PRINCIPALES ACCIONES PARA MEJORAR LA SEGURIDAD Y LA PREVENCIÓN DE PÉRDIDAS

Evaluación de Riesgos y Planificación Estratégica

La evaluación de riesgos debe ser un proceso integral que combine métodos cualitativos y cuantitativos. Los análisis de impacto y las simulaciones de escenarios pueden ayudar a prever posibles contingencias y planificar respuestas adecuadas.

Evaluación de Riesgos

Las organizaciones deben realizar evaluaciones de riesgos regulares para identificar vulnerabilidades y puntos débiles en su infraestructura de seguridad. Esto incluye tanto amenazas internas como externas.

Planificación Estratégica

La planificación estratégica debe centrarse en la implementación de políticas y procedimientos sólidos, así como en la adopción de tecnologías avanzadas para mejorar la seguridad y la prevención de pérdidas.

Implementación de Tecnologías Avanzadas

La adopción de tecnologías avanzadas es esencial para mejorar la seguridad corporativa en el entorno digital. A continuación, se describen algunas de las tecnologías clave que las organizaciones deben considerar.

Inteligencia Artificial y Análisis Predictivo

La inteligencia artificial (IA) y el análisis predictivo permiten a las organizaciones anticiparse a las amenazas antes de que se materialicen. Estos sistemas pueden analizar grandes volúmenes de datos para identificar patrones inusuales que podrían indicar un ataque inminente.

***Blockchain* y Seguridad de Datos**

El *blockchain* ofrece una forma segura y transparente de gestionar las transacciones y almacenar datos. Su naturaleza descentralizada y cifrada lo convierte en una herramienta valiosa para proteger la información crítica.

Sistemas de Detección y Respuesta

Los sistemas de detección y respuesta a incidentes (IDS/IPS) son fundamentales para identificar y mitigar amenazas en tiempo real. Estos sistemas pueden detectar actividades sospechosas y activar alertas para que el personal de seguridad tome medidas inmediatas.

Desarrollo de Políticas y Procedimientos

El desarrollo y la implementación de políticas y procedimientos sólidos son fundamentales para garantizar la seguridad corporativa. Estas políticas deben ser claras, comprensibles y aplicables a todos los niveles de la organización.

Políticas de Seguridad Cibernética

Las políticas de seguridad cibernética deben cubrir todos los aspectos de la protección de la información, desde el uso de contraseñas hasta la gestión de incidentes. La capacitación regular y la concienciación sobre la ciberseguridad son esenciales para asegurar que todos los empleados comprendan y sigan estas políticas.

Procedimientos de Respuesta a Incidentes

Tener procedimientos de respuesta a incidentes bien definidos permite a las organizaciones reaccionar rápidamente ante cualquier amenaza. Estos procedimientos deben incluir la identificación, contención, erradicación y recuperación de incidentes, así como la comunicación efectiva con las partes interesadas.

Datos Relevantes de la Industria

Las estadísticas oficiales proporcionan una visión clara de la situación actual de la seguridad corporativa en México y ayudan a los directivos a tomar decisiones informadas.

Aumento de Incidentes de Seguridad

Hoy existe un aumento de la inseguridad en México y esto impacta en el aumento de incidentes de seguridad para la operación. Un estudio de PwC México revela que el 58% de las empresas han experimentado un aumento en los incidentes de seguridad en los últimos dos años. Los sectores más afectados son finanzas, manufactura y telecomunicaciones.

Este panorama impacta indudablemente en el costo de la seguridad para

La evaluación de riesgos debe ser un proceso integral que combine métodos cualitativos y cuantitativos. Los análisis de impacto y las simulaciones de escenarios pueden ayudar a prever posibles contingencias y planificar respuestas adecuadas

Foto:-Freepik

Los retos y acciones para las organizaciones que cuentan con un departamento de Seguridad Corporativa, un área de prevención de pérdidas y las que no lo tienen en negocios digitales, especialmente en instituciones bancarias y retail en México para el 2025, son variados y complejos

Foto: Freepik

las organizaciones, según datos del Instituto Nacional de Estadística y Geografía (INEGI), el costo anual de la inseguridad y el delito en el sector empresarial asciende a más de 85 mil millones de pesos. Estos costos incluyen pérdidas por robo, gastos en medidas de seguridad y costos indirectos como la pérdida de productividad.

Es prescindible sensibilizar a los CEO sobre esta situación, y comprender los indicadores clave que reflejan la efectividad de las estrategias de seguridad corporativa. Estos indicadores pueden incluir:

Tasa de Incidentes de Seguridad

- **La tasa de incidentes de seguridad** mide la frecuencia de los incidentes de seguridad dentro de la organización. Un aumento en esta tasa puede indicar vulnerabilidades en el sistema de seguridad.
- **El costo por incidente de seguridad** incluye los gastos directos e indirectos asociados con la gestión de un incidente de seguridad. Este indicador ayuda a evaluar el impacto financiero de los incidentes de seguridad en la organización.
- **El tiempo de respuesta a incidentes** mide el tiempo que tarda una organización en identificar, contener y resolver un incidente de seguridad. Un tiempo de respuesta rápido es esencial para minimizar el daño y recuperar la normalidad operativa lo antes posible. Quiero traer a este artículo tres preguntas que en reuniones con diferentes CEO en LATAM me han hecho y la posible respuesta:

1) **¿Qué es un departamento de Seguridad Corporativa?** Un departamento de Seguridad Corporativa es una unidad dentro de una organización responsable de proteger sus activos, información y operaciones frente a amenazas internas y externas. Este departamento implementa políticas, procedimientos y tecnologías de seguridad para mitigar riesgos.
2) **¿Cómo puede una empresa sin departamento de seguridad mejorar su Seguridad?** Las empresas sin un departamento de Seguridad pueden mejorar su Seguridad mediante la contratación de servicios de seguridad externos, la capacitación de empleados en mejores prácticas de seguridad y la implementación de tecnologías básicas de seguridad como firewalls y sistemas de detección de intrusiones.
3) **¿Cuáles son las principales amenazas de seguridad para 2025?** Las principales amenazas de seguridad para 2025 incluyen ciberataques avanzados, fraudes financieros y violaciones de datos. La evolución constante de las tácticas de los ciberdelincuentes y la creciente dependencia de la tecnología digital aumentan la complejidad de estas amenazas.

CONCLUSIÓN

En resumen, para GEMARC es prescindible abordar estos temas que son cotidianos para todos sus integrantes y además de aportar a las organizaciones para los cuales prestan sus servicios, la respuesta correcta, por ello, nos enfocamos en generar conocimiento y sentar las bases para el continuo profesionalismo que nos caracteriza.

Los retos y acciones para las organizaciones que cuentan con un departamento de Seguridad Corporativa, un área de Prevención de Pérdidas y las que no lo tienen en negocios digitales, especialmente en instituciones bancarias y *retail* en México para el 2025, son variados y complejos. La capacidad de anticipar y responder eficazmente a las amenazas será un diferenciador clave para las empresas que buscan prosperar en un entorno digitalizado y globalizado.

Las organizaciones deben adoptar un enfoque proactivo y holístico hacia la seguridad corporativa, invirtiendo en tecnologías avanzadas, desarrollando políticas y procedimientos sólidos y asegurando la capacitación continua de sus empleados.

Con una planificación estratégica adecuada y un compromiso con la mejora continua, las empresas pueden mitigar los riesgos y garantizar su continuidad operativa en el futuro.

La seguridad corporativa no es sólo una necesidad operativa, sino un componente esencial para la resiliencia y el éxito a largo plazo de cualquier organización en la era digital. ■

LA TECNOLOGÍA
Y EL SOPORTE TÉCNICO
APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA




SEGURIDAD ELECTRÓNICA:

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

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

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

222 141 12 30
gerenciacomer@pem-sa.com

WWW.PEM-SA.COM

LA PARADOJA DE LA VULNERABILIDAD: ¿CÓMO ATREVERSE, ABRAZAR EL INCIERTO Y TRANSFORMAR LA CIBERSEGURIDAD EMPRESARIAL?

La vulnerabilidad en ciberseguridad no debe ser una condición que debe ser evitada, sino una oportunidad que debe ser aprovechada por las organizaciones

COLOMBIA | **Jeimy Cano**

Foto: Freepik

INTRODUCCIÓN

El reto de la ciberseguridad empresarial no inicia en las prácticas y estándares de seguridad y control, inicia en la experiencia de la vulnerabilidad, en la lectura de la inevitabilidad de la falla, en el incierto de cuándo el atacante se va a aprovechar de una debilidad que no conocemos, en la sensación de incertidumbre que genera un estado de inquietud y muchas veces "susto", sobre qué puede pasar cuando el evento adverso que no se quiere, ocurre (Stallings, 2019).

Experimentar vulnerabilidad muchas veces se traduce en sensación de debilidad y de exposición que las organizaciones no quieren experimentar ni conocer, pues la necesidad de certezas es lo que se necesita para tener tranquilidad. Bien anota Brené Brown (2016): "experimentar vulnerabilidad no es opcional: lo único que sí podemos controlar es nuestra respuesta cuando nos enfrentamos a la incertidumbre, al riesgo y a la exposición emocional". Esto es precisamente lo que en el escenario de la ciberamenazas las organizaciones deben desarrollar, capacidad de respuesta y práctica para enfrentar la inevitabilidad de la falla.

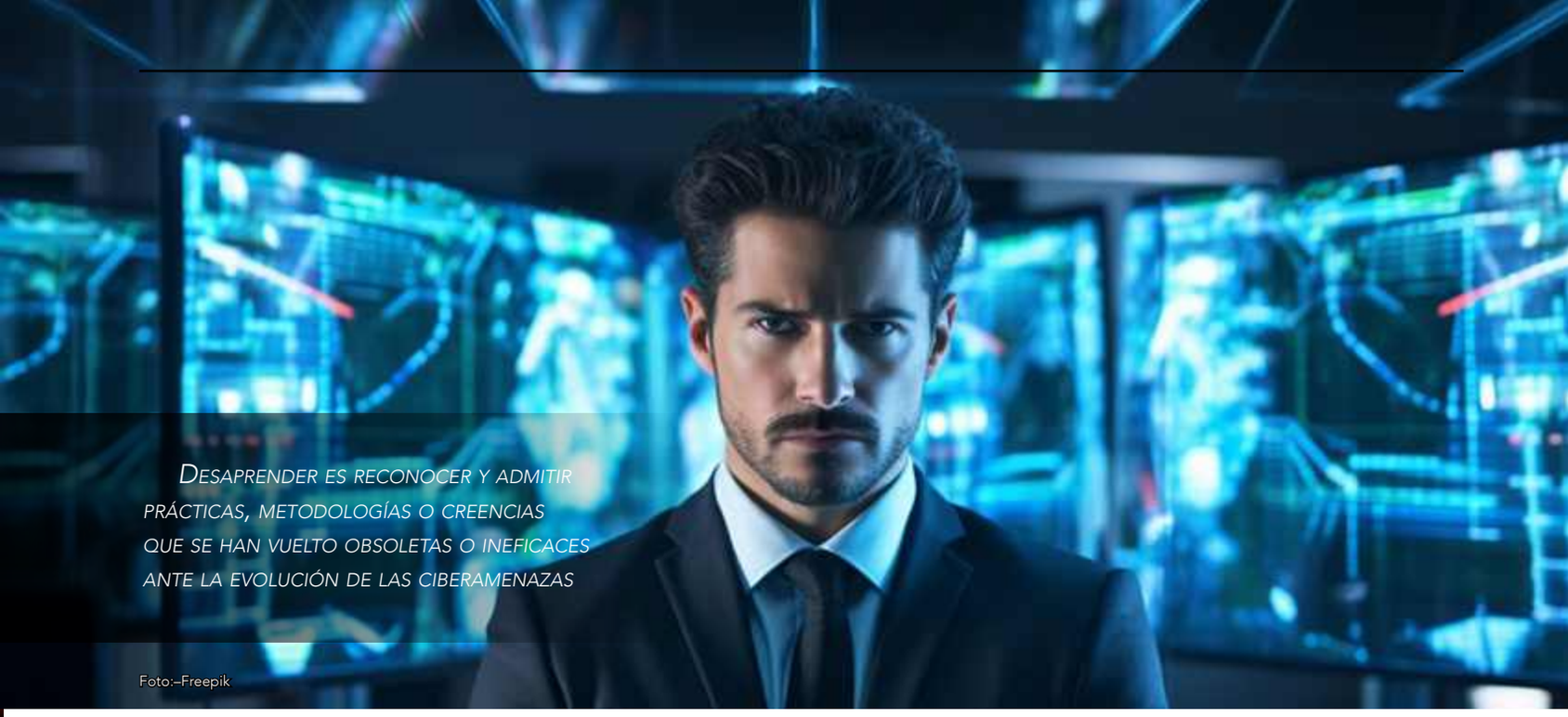
Al iniciar un programa de ciberseguridad la consigna debería ser "seguridad por vulnerabilidad", esto es, reconocer que estamos en un espacio de trabajo donde el adversario tiene algunas jugadas que no es viable descubrir (o al menos detectar con suficiente anticipación) y donde la organización, deberá jugar algunas veces viendo algunas señales débiles y otras, anticipando algunos de sus movimientos. Es un juego desigual donde por lo general la compañía tendrá algunas victorias y en otros momentos, las derrotas se materializan en eventos con efectos inesperados (Cano, 2015).

Cuando se concreta la perspectiva de ciberseguridad desde la vulnerabilidad la empresa se prepara no sólo para asumir una brecha inminente, sino para jugar y retar al adversario en su propio terreno, lo que equivale a reconocer la vulnerabilidad propia y deteriorar la inteligencia del adversario, esto es, aumentar el incierto en el modelo de riesgo del atacante. De esta forma, la empresa no sólo no tiene una postura de víctima, sino que sale al encuentro de su propia amenaza para retar sus saberes previos y lecciones aprendidas, con el fin de encontrar nuevas formas para aprender de la inseguridad.

La vulnerabilidad mantiene a la organización fuera de la zona cómoda, de la falsa sensación de seguridad, para mantener una postura vigilante que le permite estar reconociendo su entorno, entendiendo las señales contradictorias de las acciones del adversario, y sobremanera revisando todo aquello que se sale de las líneas base previamente definidas. La vulnerabilidad por definición no debe ser una postura de debilidad, sino una oportunidad para explorar nuevas formas de mejorar y avanzar para enfrentar al adversario y sus asimetrías, esas que generan inestabilidad, incierto y muchas veces caos.

ABANDONAR EL PERFECCIONISMO EN LA GESTIÓN DE CIBERSEGURIDAD EMPRESARIAL

No existe la seguridad perfecta, esto es, ni riesgo cero ni seguridad ciento por ciento. Por tanto, buscar la perfección o lograr el 100 en seguridad es una postura nociva y antinatural en las prácticas de seguridad y control. Es un ejercicio que niega la existencia de la falla y so-



Desaprender es reconocer y admitir prácticas, metodologías o creencias que se han vuelto obsoletas o ineficaces ante la evolución de las ciberamenazas

Foto:–Freepik

bremanera, lleva a las personas a alcanzar un estado que técnicamente no existe: "ser seguros". De acuerdo con René Brown (2016), estas son algunas de las características del perfeccionismo:

- Es un sistema de creencias adictivo y autodestructivo que fomenta un pensamiento primario y muchas veces infantil: "Si hago todo perfecto, puedo evitar o minimizar los sentimientos dolorosos de vergüenza, crítica y culpa".
- Es una meta inalcanzable, que se basa más en la percepción que en la motivación interna.
- Es un acto defensivo, que se traduce en un escudo que arrastramos, pensando que nos protege cuando en realidad evita que nos vean.

Al revisar estas características básicas del perfeccionismo en la práctica de la ciberseguridad empresarial, revelan las encrucijadas de los oficiales de seguridad y ciberseguridad de las organizaciones, cuando les piden alcanzar un nivel de seguridad y control que raya en la perfección, esto es, cero ciberataques exitosos o brechas de seguridad en la empresa, como una métrica de su trabajo, lo que resulta en términos prácticos y a largo plazo, algo que no se puede lograr.

Si se interpretan las características anteriores en la práctica de los ejecutivos de ciberseguridad se podrían tener las siguientes lecturas:

- Tenemos que asegurar que tenemos todos los puntos cubiertos y monitoreados para que el adversario no nos sorprenda. Es nuestro deber mantener una vigilancia permanente que no descanse ni tenga brechas para lograr el mayor nivel de confianza con los ejecutivos.
- Es importante trabajar en la percepción de la seguridad y fortaleza de nuestras defensas, como una lectura de tranquilidad para que los ejecutivos nos puedan ayudar y mantener su apoyo ahora y en el futuro.
- Debemos cerrar todas las vulnerabilidades conocidas para asegurar que estamos preparados y enviar un mensaje de protección y aseguramiento que es lo que esperan los ejecutivos.

Si se revisan todas estas reflexiones se envía un mensaje de invulnerabilidad y blindaje que no es sostenible en el tiempo, no sólo por el esfuerzo que esto implica, sino por la imperfección natural de las herramientas, las prácticas y estrategias que se tienen implementadas en las organizaciones. Bien afirma René Brown (2016): "nuestra naturaleza consiste en ser imperfectos, tener sentimientos y emociones inclasificables, fabricar o hacer cosas que no necesariamente tienen sentido", esto es, no es viable anular la dinámica natural de un entorno volátil e incierto, ni se puede evitar las emociones que una brecha de seguridad genera. Negar la existencia un ataque exitoso, es negar la existencia de puntos ciegos en la dinámica de la ciberseguridad empresarial.

APRENDER, DESAPRENDER Y REAPRENDER. EL RETO DE LA CIBERSEGURIDAD EMPRESARIAL

Las personas aprenden cuando elaboran nuevos significados, cuando retan sus saberes previos (Petty, 2023), en este sentido, el área de ciberseguridad será más efectiva en la medida que logra construir y reconstruir de forma permanente sus propias experiencias, y de esta manera alcanza una perspectiva más fina y activa de las actividades de los atacantes. Dicho aprendizaje se traduce en cambios en la manera como reconocen el entorno, la forma como detallan patrones de eventos y en la estrategia para atender los incidentes. En pocas palabras, en la forma como logran sorprenderse y conectar puntos inconexos en sus análisis.

Desaprender es reconocer y admitir prácticas, metodologías o creencias que se han vuelto obsoletas o ineficaces ante la evolución de las ciberamenazas. Este paso requiere una evaluación crítica de las medidas de seguridad existentes para identificar las áreas que necesitan ser renovadas o abandonadas (Gundu, 2024). Es un ejercicio de desconexión de las prácticas actuales en sus diferentes componentes, para observar los nuevos patrones de amenaza que se advierten en el entorno, y desde allí, ver cómo recomponer la dinámica de las metodologías y renovar los constructos de la ciberseguridad, ahora enriquecidos con las novedades del entorno.

Reaprender es desarrollar la capacidad de amortiguación, adaptación y evolución frente a los nuevos retos de los atacantes (Gundu, 2024). Es movilizar los esfuerzos fuera de la zona de protección, asociado con los riesgos conocidos, y movilizar la estrategia de ciberseguridad al ejercicio de defensa y anticipación, que busca distraer, disuadir, demorar y confundir al adversario, para ganar tiempo y así,

La ciberseguridad empresarial no es un deporte de individualidades, es un reto de conjunto donde cada uno de los participantes suma y se fortalece cada vez que reconoce aspectos novedosos del entorno que son de interés para la organización y se enmarcan

Foto: Freepik

tener la oportunidad de interceptarlo antes de que tenga éxito. Esto es, innovar y transformar los mecanismos de seguridad y control para "pensar fuera de la caja" y hacer menos predecible la inteligencia del adversario sobre la infraestructura de la organización.

Por tanto, la organización no sólo recibe nuevos conocimientos frente al reto de la ciberseguridad empresarial, sino que queda habilitada para aplicar estos nuevos aprendizajes en la dinámica de los procesos y el aseguramiento de su promesa de valor (Petty, 2023). En este sentido, todo lo aprendido es viable reutilizarlo para profundizar en las nuevas formas de ciberamenazas las cuales, permiten a la organización, no sólo experimentar la vulnerabilidad natural que conlleva reconocer estos aspectos, sino comenzar a preparar lo pertinente para defenderse frente a estos nuevos escenarios y formarse en aquello en donde carece de los conocimientos o saberes requeridos.

La vulnerabilidad natural de los nuevos entornos y apuestas de los atacantes deben motivar reflexiones y preguntas claves por parte de todos los participantes de la organización para formarse una idea y explorar nuevas posibilidades de amenazas. De igual forma, las inquietudes permiten conectar diferentes lecturas de la realidad y así detallar de forma situada las posibles debilidades que la organización puede tener y que debe atender de cara al reto del riesgo cibernético. El debate constructivo permite aumentar la capacidad de respuesta y la comprensión de la inevitabilidad de la falla.

REPENSANDO LA CIBERSEGURIDAD EMPRESARIAL DESDE LA VULNERABILIDAD

El reto de las organizaciones actuales es tratar de identificar el "cuándo", no "sí" van a tener un ciberataque. Esta condición nativa habla del ejercicio imperfecto de la ciberseguridad que recaba en la vulnerabilidad como estado natural pero no necesariamente "normal" de la función de ciberseguridad. Lo anterior, se traduce en un apetito de riesgo cibernético que la organización define y acepta, como la base de sus retos estratégicos, donde el ejecutivo de seguridad y control revela cómo puede acompañar dicho apetito y cómo deberá prepararse la organización cuando el atacante tenga éxito (Martin, 2024).

Aceptar la vulnerabilidad debe activar los mecanismos de aprendizaje, desaprendizaje y reaprendizaje como fundamento de la acción organizacional frente al riesgo cibernético. Es movilizar a la organización en la zona de prototipos y simulaciones que no siempre dejarán respuestas claras a las preguntas de los efectos de los posibles movimientos de los atacantes (Petty, 2023), un ejercicio que revela el incierto que la organización debe asumir frente a los nuevos escenarios que se tienen en el contexto de su negocio. Un juego donde todos los participantes de la organización suman para explicar un modelo imperfecto de defensa, que no sólo es responsabilidad del área de ciberseguridad.

En este sentido, la vulnerabilidad que genera las nuevas capacidades de los adversarios no debe motivar respuestas concretas, sino preguntas que permitan ir afinando el mapa estratégico incompleto de la gestión de la ciberseguridad desde preguntas claves que abran espacios para un debate informado que rete los modelos de seguridad y control vigentes de la organización. Entre las preguntas a realizar se tienen:

- ¿Qué podemos aprender de los adversarios?
- ¿Qué tienen en común y qué los diferencia?
- ¿Qué capacidades tienen y que puedan hacernos daño?

De esta manera la organización reconoce la vulnerabilidad como el espacio natural para reconocer las amenazas, sin miedo o susto, sino con entusiasmo y postura proactiva, con el fin de establecer el grado de preparación que tiene para dar cuenta con estas capacidades del adversario, y cómo debe prepararse para enfrentarlo y en el mejor de los casos, superarlo si es del caso. En este sentido, la vulnerabilidad no se convierte en debilidad de la organización, sino en motivación para conocer, explorar y aprender de la inevitabilidad de la falla como una fuente natural del ejercicio de defensa, alineado con el apetito de riesgo cibernético de la empresa (Siegel & Sweeney, 2020).

La ciberseguridad empresarial no es un deporte de individualidades, es un reto de conjunto donde cada uno de los participantes suma y se fortalece cada vez que reconoce aspectos novedosos del entorno que son de interés para la organización y se enmarcan dentro de la dinámica de las ciberamenazas. Esto implica un trabajo colaborativo y cooperativo donde aplicar lo que se ha aprendido y reflexionar en ello de forma situada, permite crear un constructo de ciberseguridad por vulnerabilidad que no es un saber superficial basado en los impactos, sino un aprendizaje profundo integrado en y desde la dinámica organizacional.

CONCLUSIONES

La ciberseguridad empresarial es un ejercicio de confianza imperfecta, donde la organización sabe que se va a equivocar, que va tener una falla, o que el atacante aprovechará una vulnerabilidad conocida u oculta, y por lo tanto, la promesa de una vida tranquila y sin ataques no será posible. En este sentido, la empresa no sólo debe declarar su apetito de riesgo cibernético de cara a su estrategia corporativa, sino prepararse

ISIS SEGURIDAD INTEGRAL

Creamos entornos seguros

Servicios:

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

AFAC
AGENCIA FEDERAL DE AVIACIÓN CIVIL

BASC

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

ASIS INTERNATIONAL

mesis

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

Si la organización decide superar su apetito de riesgo cibernético, deberá actuar para mitigar los efectos de la materialización de este riesgo, lo que hará que aumente la vulnerabilidad natural de la empresa, llevando las reflexiones previas realizadas a lugares inexplorados y las estrategias planteadas a escenarios donde no es posible anticipar cómo serán sus desempeños

Foto:–Freepik

para responder frente a la inevitabilidad de un ciberataque, que entre otras cosas, no sólo afecta su infraestructura sino a sus diferentes grupos de interés, incluidos los reguladores.

En este contexto, experimentar vulnerabilidad debe ser el referente natural que la compañía debe tener para mantener una postura vigilante. Esta lectura de la realidad, centrada en la inseguridad y limitación de la infraestructura, los procesos y las personas, debe motivar una reflexión permanente de los ejecutivos para actualizar el panorama de riesgos cibernéticos que pueden afectar a la empresa. En línea con lo anterior, los directivos deben razonar y conectar la estrategia de la organización como una amalgama de retos empresariales e iniciativas digitales que podrán hacer la diferencia en la experiencia de sus diferentes clientes para asegurar la promesa de valor y crear nuevas fuentes de ingresos.

La ciberseguridad por vulnerabilidad es reconocer que la organización cuenta con puntos ciegos en su dinámica de negocios, infraestructura y personas, los cuales hacen parte de lo que ella representa, y al mismo tiempo, configura la postura vigilante y humilde que le permite trabajar y desafiar lo que he aprendido para configurar una estrategia de ciberseguridad flexible y adaptable, que no se acomoda con lo conocido, sino que se lanza a encontrarse con el incierto para renovar su caja de herramientas y tratar de disuadir, demorar y distraer al adversario.

Si la organización decide superar su apetito de riesgo cibernético, deberá actuar para mitigar los efectos de la materialización de este riesgo, lo que necesariamente hará que aumente la vulnerabilidad natural de la empresa, llevando las reflexiones previas realizadas a lugares inexplorados y las estrategias planteadas a escenarios donde no es posible anticipar cómo serán sus desempeños. La ciberseguridad por vulnerabilidad demanda una cultura organizacional de seguridad de la información que hable e interrogue desde un entorno psicológicamente seguro, donde las ideas y debates permitan elaborar nuevos mapas de un territorio desconocido y configuren nuevos constructos de defensa desde la comprensión y cierre de sus propias vulnerabilidades.

La vulnerabilidad en ciberseguridad no debe ser una condición que debe ser evitada, sino una oportunidad que debe ser aprovechada por las organizaciones. Es un ejercicio que lleva consigo la posible materialización de una falla, la incomodidad de no saber lo que pasa. De esta forma, una compañía podrá sobrevivir a los impactos que esto genera, si reconoce que no se sabe, que quiere aprender y declara como maestra a la inevitabilidad de la falla, un desafío de confianza digital imperfecta como camino para hacerse más resistente a los ataques. ■

Referencias:

- *Brown, R. (2016). El poder de ser vulnerable. ¿Qué te atreverías hacer si el miedo no te paralizara? Barcelona, España: Editorial Urano.*
- *Cano, J. (2015) Modelo PERIL. Repensando del gobierno de la seguridad de la información desde la inevitabilidad de la falla. Memorias Congreso Iberoamericano de Seguridad Informática 2015. 6-13. https://www.researchgate.net/publication/292984005_Modelo_PERIL_Repensando_el_gobierno_de_la_seguridad_de_la_informacion_desde_la_inevitabilidad_de_la_falla*
- *Gundu, T. (2024). Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. Proceedings of The 19th International Conference on Cyber Warfare and Security. 19(1). https://doi.org/10.34190/iccws.19.1.2177*
- *Martin, P. (2024). Insider Risk and Personnel Security. An Introduction. Oxon, UK: Routledge.*
- *Petty, G. (2023). Educación basada en evidencias. Cómo enseñar aún mejor. España: SM.*
- *Siegel, C. & Sweeney, M. (2020). Cyber strategy. Risk-Driven Security and Resiliency. Boca Raton, Fl. USA: CRC Press.*
- *Stallings, W. (2019). Effective cybersecurity. Understanding and using standards and best practices. Upper Saddle River, NJ. USA: Addison-Wesley.*

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:*

EMPRESA DE SEGURIDAD ELECTRÓNICA INTEGRADOR

SYSTEM AI

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

ALAS Asociación Latinoamericana de Seguridad · ASIS International · AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C. · CPP Certified Protection Professional · NFPA · ICAI ICADE Comillas · COPARMEX · IMEI · CNSP · American Chamber Mexico

Totalmente conectado a ti

comexa_seguridad · comexa · ComexaSeguridad

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

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

55 5685 7830 t 55 5685 7837 • 800 2 COMEXA

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

Columna de ALAS COMITÉ NACIONAL MÉXICO

comite.mexico@alas-la.org

Carlos Román Martínez Sánchez, director general de Multisoluciones en Seguridad Integral TI y presidente de ALAS Comité Nacional México.
Más sobre el autor:

LA IMPORTANCIA RESPECTO A LA IMPLEMENTACIÓN DE TECNOLOGÍA EN LAS EMPRESAS DE SEGURIDAD PRIVADA

MÉXICO

Foto:–Freepik

No es ningún secreto la situación crítica que actualmente se presenta como un gran reto para las empresas de seguridad privada en México; la falta de personal, la constante rotacion (sin mencionar las pérdidas económicas que esto conlleva) y la falta de empatia por parte de algunos usuarios respecto a el impacto de costos derivado de las regulaciones actuales, por mencionar algunos factores. Han llevado a este sector a confrontar un gran reto que pareciera no tener solución. Todas las empresas viven de su rentabilidad y en ocasiones los presupuestos asignados por parte de los usuarios finales, no necesariamente contempla estos incrementos tan importantes para obtener el servicio que se requiere.

¿CÓMO ENFRENTAR ESTOS RETOS?

¿Cómo optimizo la permanencia de mi personal y disminuyo la rotación? Todas estas estrategias que las empresas de calidad implementan son muy eficientes, pero no son suficientes hoy en día. Es aquí donde la magia de la implementación de la tecnología puede generar un impacto bastante benéfico tanto para el empresario de seguridad privada como para el cliente. La rentabilidad de los servicios se puede incrementar en mas del treinta por ciento dependiendo de la eficiencia y calidad de la tecnología a implementar, recordemos que cada cliente es un traje a la medida considerando las consignas específicas de cada cliente o instalación.

Sin embargo, en esta nueva era tecnológica y el uso de un correcto razonamiento e implementacion de estas herramientas, nos puede entregar implementaciones inimaginables. Hoy día son pocas las soluciones que no se pueden llevar a cabo. Un gran avance que ha permitido esto ha sido la visión que han tenido algunos fabricantes y desarrolladores de herramientas tecnológicas que han tenido la visión de integrar diferentes marcas y equipos lo que permite entregar una solución específica para el cliente.

Esto se puede traducir a la implementacion de un "guardia virtual", que puede ejecutar un sinfín de funciones con una eficiencia extraordinaria, controles de acceso, validaciones de identidad, comunicación y validaciones con centros de monitoreo, etc. Las opciones de implementación son infinitas. Cabe recalcar esta pregunta que siempre todo mundo hacemos: ¿Esto sustituye al factor humano? La respuesta es "no", pero la integración del factor humano con la tecnología generan servicios más eficientes y efectivos.

Sólo para dejar la duda en la mesa, he tenido la oportunidad de ver implementadas estas soluciones donde, de manera remota, un elemento de seguridad gestiona hasta ocho diferentes sitios residenciales o de portería. Invito a los empresarios de seguridad a que vean estas herramientas como un aliado y no como un enemigo tecnológico. Recordemos que "si fuera sencillo cualquiera lo haría" y te aseguro, lector, que si estás leyendo este artículo es porque tienes ese valor y la visión de dar ese paso. ■

#SiLoCreesLoCreas

RENTA DE BLINDADOS

COLEMAN

Tel.: 557672.4992

krauda@seguridadenamerica.com.mx

www.rentadeblindados.com.mx

TRUST GROUP:
EXCELENCIA Y PASIÓN POR MÉXICO

Su constante labor y la adaptación a nuevos retos, son algunas de las claves para que la empresa de seguridad privada mantenga altos estándares de calidad y se posicione en la industria

Con una trayectoria de más de 20 años en el sector de la seguridad privada, **Trust Group** se ha establecido como una empresa de alto nivel que cuenta con los permisos de la Secretaría de Seguridad y Protección Ciudadana, así como de la Secretaría de la Defensa Nacional en todas las modalidades para la portación de armas de fuego en todo el territorio nacional y ahora con la nueva empresa del grupo: **Incident Prevention and Response Private Security (IPR)** que también cuenta con las licencias de portación de armamento en todas sus modalidades, el grupo se fortalece para ofrecer operaciones y servicios de alto impacto a clientes específicos que requieran este tipo de cobertura.

Y como lo comenta el **licenciado Pedro Sanabria, CPP**, socio director de Trust Group, "No es fama de sólo cinco minutos, han sido años de constante evolución y trabajo lo que nos ha permitido materializar el éxito, así como la pasión por México y por servir a la sociedad, nos ha permitido trascender a través del desarrollo de la profesión de la seguridad, lo que también nos ha llevado a lograr un círculo virtuoso de colaboración con cada uno de los integrantes de la empresa para impactar positivamente en las experiencias que ofrecemos día a día a nuestros clientes y así establecernos como un referente en el mercado como una empresa de calidad y confianza".

De tal manera, la reputación de Trust Group como una empresa integral de seguridad privada que ofrece servicios de excelencia ha sido resultado de su constante labor y adaptación a nuevos

retos en estos veinte años y es que para el grupo establecer nuevas metas siempre ha sido importante para mantener el éxito, pero sobre todo tener una visión extremadamente clara de hacía dónde hay que dirigirse y contar con los procesos adecuados para ello, pues ante la situación de inseguridad que se vive en el país, es importante que las empresas y dependencias gubernamentales cuenten con servicios de protección integral que vayan de acuerdo con sus necesidades, siendo esencial contar con el apoyo de expertos que conozcan a la perfección esta problemática.

LÍNEAS DE NEGOCIO

Por ello, Trust Group cuenta con especialistas con una vasta experiencia que los respalda para lograr esos objetivos establecidos a través de sus diferentes líneas de negocio:

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

Hoy Trust Group cuenta con cerca de mil colaboradores a nivel operativo y administrativo, con lo que garantiza y refuerza su dominio en temas de seguridad nacional, pública y privada sobresaliendo con éxito en un entorno cada día más competitivo para seguir siendo considerados como un aliado de seguridad estratégico que aporta un valor agregado a las operaciones de sus clientes y manteniendo la calidad en la capacitación que ha sido el eje central de su éxito, elevando así la función de la seguridad privada e influyendo en el éxito organizacional para seguir construyendo una empresa con alto sentido de responsabilidad social y humana. ■

Trust Group
Por eso, en seguridad "Nadie Conoce México como Nosotros".

Fuente y fotos: Trust Group

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

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

Foto:–Freepik

MÉXICO **Hermelindo Rodríguez Sánchez**

PROCEDIMIENTO DE EMERGENCIAS OPERATIVAS

¿Qué es una emergencia en seguridad privada? Se consideran emergencias operativas a todos aquellos sucesos o novedades que ocurren de manera no prevista en los servicios y que, de acuerdo con su gravedad e importancia, requieran solución inmediata y adecuada.

EL PERSONAL DE SEGURIDAD DEBE:

1) Tener el máximo conocimiento de las instalaciones de la empresa que vigila.
2) Identificar los equipos contra incendios y verificar que se le den mantenimiento.
3) Conocer el manejo y ubicación de los sistemas de alarma.
4) Conocer las salidas de emergencia y puntos de reunión de seguridad.
5) Tener contacto con Protección Civil y brigadas internas para conocer el plan de emergencias.
6) Tener directorio telefónico interno y de los cuerpos de emergencia actualizado.
7) Identificar actos y condiciones inseguras en las instalaciones y personal de la empresa.
8) Informar siempre por medio de reportes las anomalías que se presenten.
9) Proponer medidas preventivas.
10) Vigilar el cumplimiento de las normas y procedimientos contra riesgos en la empresa.

DESPUÉS DE UNA EMERGENCIA EL PERSONAL DE SEGURIDAD DEBE:

Inspeccionar las instalaciones, área de emergencia para garantizar la seguridad del personal y el patrimonio de la empresa.

- Verificar que los equipos de emergencia queden listos para funcionar.
- Evaluar los acontecimientos y proponer acciones correctivas y preventivas a la empresa para evitar que suceda de nuevo otro evento igual.
- Preparar un reporte de novedades en el que se detallen los hechos.

1.- ASALTO A MANO ARMADA

- No oponer resistencia en caso de ser sorprendido.
- Conservar la calma (controla tus acciones utiliza un tono de voz tranquilo).
- Si el oficial está armado y es sorprendido por los asaltantes deberá rendirse y hacer todo lo que le pidan evitando poner en peligro su vida y la de los demás. Sólo en caso de estar seguro de someter a los delincuentes se utilizarán las armas buscando únicamente amedrentarlos y disparar en caso de ser necesario para salvar su vida y la de los demás.
- Memorizar las características de los asaltantes tales como media filiación (color de piel, color de cabello, color de ojos, estatura, complexión física, sexo, su acento al hablar), vestuario (color, moda, tipo, etc.), forma de actuar (tranquilo, nervioso, seguro, etc.).

- Si los asaltantes te preguntan, contesta (da respuestas concretas, no mientas ni des más información de la que te solicitan).

2.- ROBO

- Mantenga la calma, actúe de acuerdo con el plan de contingencia.
- No permita el ingreso de personas al área donde ocurrió el robo. Revisar el lugar, analizar bien los hechos y buscar pistas. Informar de inmediato al representante de la empresa y al supervisor en turno.

3.- INCENDIO

- Mantenga la calma, actúe de acuerdo con el plan de contingencia.
- Dar la voz de alarma.
- Evacúe el edificio con precaución y orden, no corra, no grite, diríjase a las zonas de seguridad establecidas como puntos de reunión.
- Si detecta fuego no abra puertas ni ventanas (el fuego se alimenta e incrementa con el oxígeno).
- No accione los interruptores de luz ni encienda llamas de ninguna especie (puede haber fugas de gas), cierre las llaves de gas y de cualquier otro líquido inflamable y peligroso.
- No grite, no corra, no empuje, puede provocar pánico general.
- Si el incendio no es grande, tranquilícese. Busque el lugar más seguro para protegerse.
- No utilice los elevadores, escaleras eléctricas, aléjese de los objetos que se puedan caer o romper (estanterías no fijadas, bardas o paredes exteriores, ventanas, cables de luz y de alta tensión, tanques de gas estacionarios y cualquier sustancia inflamable).
- Si el fuego es de origen eléctrico no intente apagarlo con agua. Tratar de extinguirlo por sí mismo empleando el equipo contra incendio adecuado.

4.- TEMBLOR

Mantenga la calma, actúe de acuerdo con el plan de contingencia, si el temblor no es fuerte tranquilícese, busque el lugar más seguro para protegerse (una columna, debajo de un escritorio), no utilice los elevadores, escaleras eléctricas, aléjese de los objetos que se puedan caer o romper (estanterías no fijadas bardas o paredes exteriores ventanas, cables de luz y de alta tensión tanques de gas estacionarios y cualquier sustancia o líquido inflamable).

5.- INUNDACIÓN

- Mantenga la calma. Actúe de acuerdo con el plan de contingencia de la empresa.
- Si hay lluvia intensa no salga, no trate de caminar o nadar a través de caminos inundados, el nivel del agua puede aumentar inesperada y rápidamente.
- No use el automóvil, es difícil conocer las condiciones de un camino inundado.
- Manténgase lejos de la corriente, ésta puede contener árboles, piedras y objetos que pueden golpearte o arrastrarte.
- No te acerques a postes de electricidad con cables colgando.

6.- SECUESTRO

- Informar de inmediato al representante de la empresa y al supervisor en turno.
- Denunciar el secuestro.
- No dejarse influenciar por rumores ni tomar decisiones precipitadas.
- Considerar que el secuestro, en su mayoría de veces, es por dinero y no por venganzas personales.


Foto: Freepik

7.- AGRESIÓN O RIÑA

Mantenga la calma, actué de acuerdo con el plan de contingencia. Intervenir conciliatoriamente para evitar que las personas pasen a los golpes o uso de armas. En caso de que pasen a los golpes tratar de separarlos sin exponerse a ser golpeado. En caso de que las personas intenten usar o usen armas no se exponga busque el apoyo de una patrulla o llame al 060. En caso de existir agresión física o verbal al personal de seguridad no le hará caso ni responderá la agresión. En caso de insistencia de agresión por parte del o las personas, póngase a cubierto en la caseta de seguridad.

8.- ACCIDENTE DE TRABAJO O ENFERMEDAD DE UN EMPLEADO DE LA EMPRESA

- Mantenga la calma, actúe de acuerdo con el plan de contingencia.
- En caso de enfermedad común no grave, tomar las medidas necesarias para que la enfermera o médico de turno lo atienda.
- En caso de enfermedad grave y al ser informado de la emergencia, tomará las medidas necesarias para que la enfermera o médico de turno lo auxilien en caso de no haber enfermera ni médico.
- Se solicitarán los servicios de auxilio médico por teléfono, mientras tanto si está capacitado le brindará los primeros auxilios poniendo especial atención a lo siguiente: póngase a un costado de la persona, muévala suavemente de los hombros mientras le pregunta ¿está usted bien? Si la persona no responde asuma que está inconsciente y en peligro de muerte observe que no tenga obstrucción de las vías respiratorias con su propia lengua.


Foto: Freepik

Sólo en caso de estar seguro de someter a los delincuentes se utilizarán las armas buscando únicamente amedrentarlos y disparar en caso de ser necesario para salvar su vida y la de los demás

No permita el ingreso de personas al área donde ocurrió el robo. Revisar el lugar, analizar bien los hechos y buscar pistas. Informar de inmediato al representante de la empresa y al supervisor en turno


Foto: Freepik

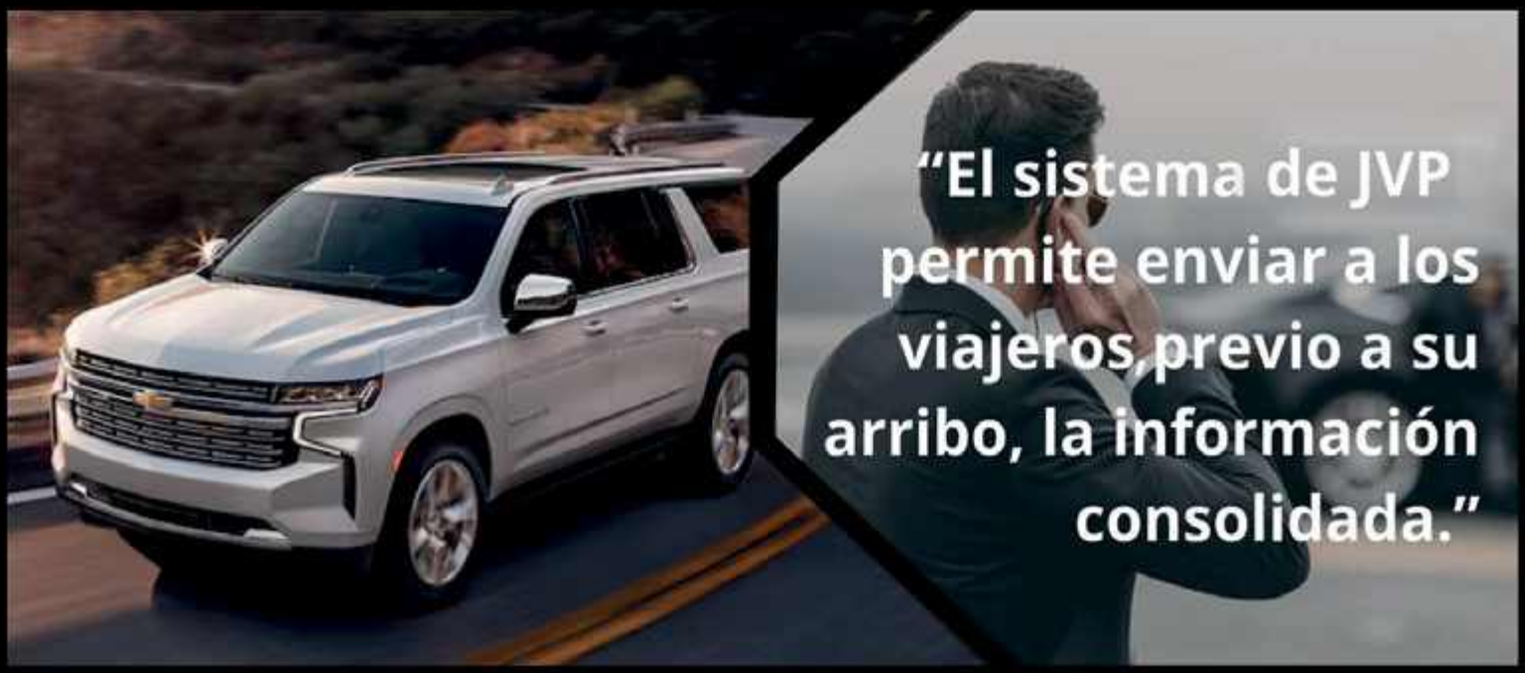
Revise sus signos vitales como pulso y respiración, si la persona se encuentra inconsciente, no respira, no tiene pulso, necesita atención inmediata no le dé líquidos, no le ponga alcohol, no la levante y en caso de no estar capacitado seguirá las instrucciones del radio operador de emergencias que está en la línea del teléfono mientras espera a que lleguen los servicios de emergencia.

- Informar de inmediato al representante de la empresa y al supervisor de seguridad en turno.

9.- INTRUSIÓN

- Tomar precauciones, ya que el intruso puede estar armado.
- Si se detecta que está armado, tratar de que no lo vea, y pedir apoyo a seguridad pública e informar a la comandancia, así como a la administración.
- Seguir ocultándose, pero sin perder de vista al intruso ni de todos los movimientos que haga.
- Estar al pendiente de la llegada de los refuerzos de la policía, y de la supervisión.
- Cuando estos lleguen, indicar en dónde está el intruso e informarles de los movimientos de éste.
- Si llega primero la supervisión debe esperar a la policía para que sean éstos quienes actúen; los oficiales de vigilancia y el servicio de supervisión sólo apoyarán.
- Si el intruso no está armado, el oficial deberá preguntarle quién es y a dónde va, así como el motivo por el cual se introdujo a las instalaciones, si el sospechoso contesta calmado, indicarle que abandone las instalaciones de inmediato.
- Si insiste en permanecer en el interior de las instalaciones, indicarle que de ser necesario se llamará a una patrulla policíaca para desalojarlo.
- Si reincide y se pone agresivo, no hacerle caso, deben alejarse de él, sin perderlo de vista y pidiendo auxilio a las supervisiones. Cuando llegue la supervisión estos deberán invitarlo a rendirse pacíficamente, si accede tomar sus datos y desalojarlo de la empresa.
- Si se pone agresivo, pedir apoyo a la policía para retirarlo del lugar, de preferencia sin golpearlo. ■

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



@JVPLOGISTICA

CONTACTO: 55 8108 0587

¿CUÁL ES EL MEJOR PERFIL DEL GUARDIA DE SEGURIDAD?

Un modelo integral

MÉXICO | **Gabriel Esteban Escobar González**

Foto: Freepik

Es muy notorio que poco a poco se busca integrar a la tecnología para sustituir tareas humanas y eso incluye al guardia de seguridad, por ejemplo, la gran China, referente tecnológico en el mundo, hoy en día utiliza robots que fungen como anfitriones en la recepción de visitantes en edificios corporativos y su alcance no tiene límites

Esta pregunta normalmente se formula al momento de buscar un colaborador destinado a la protección de activos y para el profesional de seguridad no cabe duda que es necesario evaluar y analizar una serie de factores que van desde el puesto, ubicación, responsabilidades, controles, aplicación de reglamentos, procesos, protocolos, herramientas tecnológicas, capacidad de comunicación, interacción con clientes internos, externos, entre otros. Al final se logra establecer un perfil con cierto grado de idoneidad.

Antes de continuar, debemos comprender que el guardia de seguridad forma parte de un conjunto que se integra para poder realizar las funciones de seguridad para la protección de activos y personas de una organización: "…la seguridad es un conjunto de elementos técnicos (tecnología), administrativos (procedimientos, protocolos, etc.) y humanos (personal con funciones propias a la seguridad), destinados a la prevención, disuasión y/o reacción cuyo propósito es evitar pérdidas y/o daños en las personas, bienes y/o activos de una organización" (Lic. J. Rubén Fajardo Correa).

Esta definición nos permite comprender que, la tecnología por sí sola no logra el éxito en la seguridad. El Ing. David Chong Chong, secretario general de CEAS México, documenta en sus múltiples aportaciones, que, la tecnología ayuda a hacer el trabajo más no hace el trabajo y enfatiza que el ser humano es el elemento consciente con capacidad de discernimiento para la toma de decisiones, incluso explica que la tecnología se suma al humano formando un binomio, pero para lograr el éxito en seguridad, se debe integrar lo que definimos como factor administrativo (procedimientos, protocolos, etc.). Entonces debemos concluir que, el factor humano no puede ser sustituido.

Cabe señalar que, el Ministerio de Industria y Tecnología de la Información (MIIT) de China anunció a finales del 2023, la intención de comenzar para 2025 la producción en masa de robots humanoides con el objetivo de que estos sean capaces de realizar tareas laborales y convertirse en "un importante motor económico" del país

Foto:–Freepik

GUARDIAS ROBOTS

Es muy notorio que poco a poco se busca integrar a la tecnología para sustituir tareas humanas y eso incluye al guardia de seguridad, por ejemplo, la gran China, referente tecnológico en el mundo, hoy en día utiliza robots que fungen como anfitriones en la recepción de visitantes en edificios corporativos y su alcance no tiene límites. Según Juan Luis Moreno, *Chief Innovation Officer* de The Valley, los robots humanoides no necesariamente reemplazarán el trabajo humano, ya que su aplicación dependerá de varios factores como el nivel de automatización, las necesidades de las empresas, las políticas laborales, la legislación y cuestiones éticas. En muchos casos, estos robots colaboran con los trabajadores en lugar de sustituirlos, realizando tareas repetitivas, peligrosas o físicamente agotadoras, lo que permite a los empleados concentrarse en actividades más complejas que requieren creatividad y habilidades interpersonales. (nota publicada en La Vanguardia Barcelona el 07/11/23).

Cabe señalar que, el Ministerio de Industria y Tecnología de la Información (MIIT) de China anunció a finales del 2023, la intención de comenzar para 2025 la producción en masa de robots humanoides con el objetivo de que estos sean capaces de realizar tareas laborales y convertirse en "un importante motor económico" del país (nota publicada el 13/11/2023 en el Economista por Miguel Terán Haughey, redactor de tecnología).

Revisemos datos relevantes de México para analizar cómo se forma un enlace tecnología – guardia de seguridad. En lo que concierne a las empresas de seguridad privada (debidamente registradas y validadas ante las autoridades competentes), según Agrupaciones de Seguridad Unidad por México, Sociedad Nacional de Industrias de la Seguridad Privada, A.C., con sus 32 asociaciones que representa y 980 empresas del gremio; existen más de 947 mil 200 trabajadores relacionados a la industria, esta cifra evidentemente representa una necesidad descomunal en México.

Del mismo modo existen necesidades para poder subsanar la demanda, un factor relevante es la alta rotación de personal que cada vez se vuelve más complejo debido a la oferta laboral fuera del gremio y es aquí donde la tecnología embona perfectamente para dar una solución, es decir, integrar a la tecnología para sustituir tareas humanas, lo que incluye al guardia de seguridad. Esta convergencia tendrá beneficios operativos, pero también con enfoque financiero ante la organización. No es sorprendente que los gastos en materia de seguridad suelen ser vistos como "la seguridad cuesta y molesta", pero al integrar tecnología, se generan inversiones y se disminuyen los gastos, lo que será mejor visto financieramente hablando.

Retornando a la pregunta inicial: ¿Cuál es el mejor perfil del guardia de seguridad? Es evidente que se requiere un modelo integral que incluye:

- Humanos.
- Tecnología.
- Procedimientos, protocolos, etc.

El conjunto de estos, sin duda darán como resultado el éxito en las tareas de seguridad.

Con la colaboración de Georgina Rodríguez, *Security Manager*. ■

Gabriel Esteban Escobar González, director corporativo de Seguridad en Grupo Armstrong.
Más sobre el autor:

RETOS DE SEGURIDAD DEL *NEARSHORING* EN LA INDUSTRIA AUTOMOTRIZ

Ante el incremento de este modelo de negocio, uno de los riesgos probables es la falta de mano de obra, mismo que puede prevenirse con estrategias de seguridad

Foto: Freepick

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Una de las interrogantes ante este crecimiento exponencial de la industria automotriz, es si México podrá ajustarse a la demanda de mano de obra, así como a los recursos hídricos y de infraestructura que se requiere. Sin lugar a dudas esto representa un gran reto para el país, quien vive una situación crítica de seguridad, aspecto que los inversionistas no pueden dejar de lado, es por ello que Guillermo Hassey, *National Security Officer* en Daimler Truck México, presentó una interesante ponencia en el *roadshow* organizado por **Seguridad en América**, y de donde se extrae la siguiente información.

El *nearshoring* está definido como la práctica de trasladar procesos empresariales o servicios, a un país cercano al mercado principal, en el caso de México, hacia Estados Unidos y Canadá, y quien se ha visto más interesado en la industria automotriz del país, no sólo por la expansión de este modelo de negocio, sino también por lo bien recibidos que han sido sus vehículos y la oportunidad de ampliar su mercado hacia el norte y América Latina, es China.

México es atractivo por su posición geográfica que permite una logística más eficiente y, por ende, una reducción de tarifas de transportación. También los costos laborales son competitivos, además cuenta con acuerdos comerciales como el T-MEC (Tratado entre México, Estados Unidos y Canadá), y debido al incremento del *e-commerce*, su infraestructura se ha mejorado.

De acuerdo con el análisis de Guillermo Hassey, los siguientes aspectos representan los principales retos ante el crecimiento del *nearshoring* en la industria automotriz:

- **Seguridad física y protección.** La violencia relacionada con el crimen organizado y el narcotráfico, pueden representar un riesgo significativo para las empresas que trasladan sus operaciones a ciertos estados de la república, esto incluye robo de mercancías, cobro de piso, secuestros, extorsiones. Por ello se recomienda realizar la inversión en seguridad con base en las necesidades de cada compañía de forma particular.
- **Cadena de suministro.** El robo en tránsito o vandalismo, pueden afectar la eficiencia y la capacidad de cumplir con los plazos de entrega. El mayor reto actual en esta etapa, es crucial y consiste en asegurar la integridad de los productos desde el punto de origen hasta el destino final.
- **Ciberseguridad.** Con la creciente dependencia de la tecnología y las comunicaciones digitales, las empresas deben protegerse contra ataques cibernéticos como el robo de datos, *ransomware*, y otros tipos de ataques, que pueden dañar no sólo la información delicada de la compañía, sino también su reputación.
- **Corrupción y sobornos.** En algunas regiones, la corrupción puede ser un desafío preocupante. Las empresas pueden verse obligadas a pagar sobornos para asegurar contratos, proteger sus operaciones, o simplemente operar sin interrupciones.
- **Marco legal y cumplimiento normativo.** Cumplir con las leyes y regulaciones locales, que pueden ser complejas y cambiar frecuentemente, pero es necesario estar al margen de la ley para operar adecuadamente.

- **Infraestructura.** Si está deficiente puede afectar la operación y la seguridad. Por ejemplo, si las carreteras no son adecuadas y además la red de comunicación es débil, los riesgos pueden aumentar y la respuesta por parte de los equipos de emergencia o de recuperación de mercancía pueden verse afectados y sin poder actuar de manera rápida y eficiente.
- **Relaciones laborales.** Es importante garantizar condiciones de trabajo seguras. Evitar las disputas, las cuales pueden derivar en huelgas o protestas, afectando la continuidad e imagen del negocio.

ESTRATEGIAS PARA LA FALTA DE MANO DE OBRA

Para que México continúe siendo atractivo para la inversión extranjera, debe mejorar las condiciones de seguridad del país, de las regiones donde la industria se instale, así como su infraestructura y las condiciones laborales de los empleados, misión que comparte con las propias compañías.

Guillermo Hassey enumeró algunas estrategias que pueden servir para la falta de mano de obra:

- **Capacitación y Desarrollo de Habilidades.** Invertir en programas de capacitación, asociaciones con instituciones educativas, programas de formación técnica, y cursos especializados en las habilidades necesarias para las operaciones específicas de la empresa. Esto motivará a los y las empleadas, les dará recursos para aprender y desarrollarse, alejándolos de intenciones de robo o fraude.
- **Colaboraciones con instituciones educativas.** Una estrategia que ha funcionado bastante bien, es establecer alianzas con universidades, colegios técnicos, y escuelas vocacionales para desarrollar currículos que se alineen con las necesidades de la industria. A cambio, las empresas pueden ofrecer prácticas profesionales, y programas de aprendizaje a estudiantes.
- **Mejorar las condiciones laborales.** Atraer y retener a los colaboradores ofreciendo salarios competitivos, beneficios atractivos reales, y un entorno de trabajo seguro y saludable. Generar oportunidades de trabajo profesional y un buen equilibrio entre trabajo y familia.
- **Reclutamiento de talento internacional.** Puede considerar atraer talento de otros países considerando apoyar con el trámite de VISA, y permisos de trabajo ofreciendo incentivos para que sea atractiva la oferta de trasladarse a otro país, muy acorde al objetivo del *nearshoring*.
- **Automatización y tecnología.** Estas herramientas son necesarias para fortalecer las estrategias de seguridad, las tecnologías de automatización permiten reducir la dependencia de la mano de obra humana en ciertas tareas. Esto puede ser útil en procesos repetitivos y de baja cualificación.
- **Políticas de retención de talento.** Desarrollar políticas efectivas para retener al talento existente, como programas de reconocimiento, planes de carrera, y beneficios adicionales que fomenten la lealtad de los empleados.
- **Fomento de la movilidad laboral interna.** Facilitar la reubicación de los trabajadores dentro del país, ofreciendo apoyo para la mudanza y programas de integración para aquellos que se trasladen de una región a otra.
- **Programas gubernamentales.** Utilizar programas y subsidios gubernamentales destinados a fomentar el empleo y la formación profesional.
- **Mejorar la infraestructura local.** Trabajar con autoridades locales para mejorar la infraestructura, así como el transporte y la vivienda, en las áreas donde se establecerán las operaciones.
- **Estrategias de reclutamiento innovadoras.** Utilizar plataformas digitales y redes sociales para llegar a una audiencia más amplia de candidatos potenciales. ■

Guillermo Hassey es Licenciado en Economía y cuenta con una Maestría en Administración Internacional por la Universidad de Thunderbird en Arizona, USA. Desde hace más de 15 años ha trabajado en el sector de Seguridad en distintas posiciones; en consultoría y como responsable de Seguridad de empresas multinacionales.

Es miembro de varias asociaciones de Seguridad como GEMARC y ASIS. Como parte de su responsabilidad, Guillermo lidera los proyectos e implementaciones de Seguridad Electrónica en las instalaciones de Daimler Truck México, que incluyen plantas de manufactura de vehículos, centros de distribución y oficinas corporativas.

Tiene amplia experiencia en la seguridad del Sector Automotriz, es un experto certificado en la seguridad de la Cadena de Suministro por TAPA y como CPP de ASIS International.

SEGURIDAD EN LA INDUSTRIA FARMACÉUTICA

Vulnerabilidad de todos los sistemas de IT, mercancía en tránsito y robo interno como los principales retos de seguridad

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La industria farmacéutica enfrenta diferentes retos de seguridad, ya no sólo aquellos que tienen que ver con las instalaciones, la producción, y transportación, sino también aquellos que dañan su reputación y que pueden tener daños irreversibles, como lo es un ataque cibernético o el robo de información confidencial. Es por ello que realizamos una serie de entrevistas a especialistas en la materia para conocer cuáles son las mejores estrategias y tecnología en seguridad para cumplir con el objetivo de esta tan importante industria: que el producto llegue al paciente en las mejores condiciones y así contribuir con la mejora y cuidado de su salud.

DESAFÍOS DE LA INDUSTRIA

En México existen problemas de seguridad que afectan de forma general a las industrias, entre los más comunes están: el robo hormiga, robo al transporte de carga, extorsiones o amenazas del crimen organizado, y aquellos que son fortuitos, como un huracán; y existen otros como la piratería, falsificación de productos y actualmente la vulneración de los sistemas de IT, así como el robo de propiedad intelectual, que pueden causar afectaciones muy graves en la industria farmacéutica, pues la falsificación de un medicamento puede provocar la muerte del paciente.

De acuerdo con el análisis y experiencia de Octavio García Peregrina, CPP, gerente de Seguridad y Protección en Farmacéuticos Maypo, la industria farmacéutica enfrenta una serie de problemas de seguridad en sus instalaciones, laboratorios y almacenes, que incluyen tanto, temas de seguridad, ciberseguridad como operativos. Algunos de los más importantes son:

Contaminación y Control de Calidad.

- Contaminación cruzada: los medicamentos pueden contaminarse entre sí, lo que pone en riesgo la seguridad del paciente y la eficacia de estos.
- Control de calidad inadecuado: fallas y desviaciones en los procesos de fabricación de medicamentos, lo que puede resultar en productos con afectaciones en la calidad.

Seguridad del Personal.

- Exposición a sustancias peligrosas: los trabajadores pueden estar expuestos a productos químicos peligrosos o agentes biológicos durante el proceso de fabricación.
- Accidentes laborales: riesgos relacionados con el manejo de maquinaria pesada y procesos automatizados.

Ciberseguridad.

- Robo de propiedad intelectual: información sobre fórmulas y procesos de fabricación es un objetivo valioso para *hackers*.
- Interrupciones en la cadena de suministro digital: ataques cibernéticos pueden afectar los sistemas de control y gestión de la producción, provocando retrasos o interrupciones.

Seguridad en la Cadena de Suministro.

- Falsificación de productos: medicamentos falsificados pueden entrar en la cadena de suministro, poniendo en riesgo la salud pública.
- Robo y desvío de productos: productos pueden ser robados o desviados durante el transporte o almacenamiento.

Regulaciones y Cumplimiento.

- Incumplimiento de normativas: fal-

"Debemos involucrarnos con las diferentes áreas internas de la compañía, como un socio estratégico del negocio, que coadyuva a cumplir con el suministro de los medicamentos y que estos lleguen a todos los pacientes que los necesitan", Jesús Islas

"Hay que trabajar en conjunto con las asociaciones de la industria para generar campañas de concientización sobre la falsificación y el uso de medicamentos de dudosa procedencia", Alan Vara

"Un gran reto es el disminuir el robo con tendencia a cero, ya que el medicamento robado es pérdida total y trae costos ocultos de destrucción si es que se recupera", Eduardo Téllez

ta de adherencia a las regulaciones gubernamentales y estándares internacionales pueden llevar a sanciones y retirada de productos del mercado.
- Auditorías y documentación: errores en la documentación y auditorías pueden comprometer la integridad del proceso de fabricación y la trazabilidad del producto.

Desastres Naturales y Emergencias.
- Planes de contingencia inadecuados: falta de preparación para desastres naturales, incendios u otras emergencias pueden interrumpir la producción y afectar la seguridad de los empleados.

Seguridad del Entorno de Producción.
- Control ambiental: problemas en el control de la temperatura, humedad y presión en áreas críticas pueden afectar la estabilidad y eficacia de los productos.
- Mantenimiento de equipos: fallos en el mantenimiento preventivo de equipos pueden causar interrupciones en la producción y riesgos de seguridad.

Ante estos riesgos de seguridad, los especialistas están en constante actualización sobre la tecnología y estrategias que pueden fortalecer sus sistemas de seguridad. Jesús Islas, *Protective Security Lead* en Novartis, nos compartió los siguientes aspectos a considerar para contrarrestar esos riesgos:
- Combinación adecuada de los medios de seguridad humanos, tecnológicos y físicos en las etapas de la cadena de suministro. Elementos de seguridad privada seleccionados y capacitados adecuadamente, procedimientos y protocolos bien definidos para ejecutar durante la operación, centros de monitoreo, mapas georreferenciados, GPS, comunicaciones, y contacto con autoridades, y control de accesos en los almacenes.
- Emplear todos los esfuerzos y acciones con un sólo objetivo: ¡Los pacientes! Involucrarse con las diferentes áreas internas de la compañía, como un socio estratégico del negocio, que coadyuva a cumplir con el suministro de los medicamentos y que estos lleguen a todos los pacientes que los necesitan.
- Continuar con la estrategia de capacitación y concientización de las autoridades, responsables de aduanas y entidades médicas, sobre los riesgos existentes para la salud pública en la falsificación de medicamentos y cómo detectarlos para evitar consecuencias adversas en los pacientes y daño reputacional a las compañías.

Respecto a la falsificación de medicamentos, Alan Vara, *Country Security & SHE Sr. Manager* en Roche México, externó la importancia de trabajar en conjunto para disminuir esta mala práctica en el mercado negro. "Una estrategia para combatir la piratería, es teniendo implementada una mentalidad en nuestra organización sobre el impacto positivo que podemos tener hacia nuestros pacientes si todos nuestros esfuerzos y operaciones se rigen con la ética que nos guía día a día. Por otro lado, trabajamos en conjunto con las asociaciones de la industria para generar campañas de concientización sobre la falsificación y el uso de medicamentos de dudosa procedencia".

Por su parte, Luis Guillermo Iturbe, *Regional Security Officer* en Merck, agregó las siguientes recomendaciones para la seguridad en el transporte:
- Empresas de transporte serias y certificadas.
- Planes de mantenimiento preventivos a las unidades.
- No más de cinco años de antigüedad.
- Operadores verificados en exámenes de confianza.
- Manejo de información adecuado.
- Identificación de riesgos carreteros y evitar lugares de parada peligrosos y/o reportados previamente.
- Buen sistema de monitoreo remoto híbrido, es decir, GPRS y satelital.
- Protocolos de reacción eficientes con una buena relación con la autoridad buscando evitar los robos y/o recuperación oportuna del producto.

Y precisamente en la transportación de los medicamentos, Eduardo Téllez, *Chief Security Officer* en Laboratorios Liomont, encuentra grandes retos para los responsables de Seguridad. "El disminuir el robo con tendencia a cero, ya que el medicamento robado es pérdida total y trae costos ocultos de destrucción si es que se recupera, volver a conseguir la materia prima para refabricar,

"No podemos dejar de lado, los riesgos que se presentan en el resguardo de información de fórmulas y componentes de los medicamentos; así como los procesos de destrucción y disposición de lotes de producto no conforme", Luis Iturbe

"Ante el robo de medicamentos en ruta, después del Protocolo de reacción y recuperación, se deben revisar y evaluar las medidas de seguridad actuales en el transporte de medicamentos y hacer mejoras basadas en las lecciones aprendidas del incidente", Octavio García Peregrina

"Nos dedicamos a vender salud, a brindar alternativas que mejoran la calidad de vida de los pacientes, es por eso que todas las actividades que realizamos deben ser cuidando todos los detalles", Rebeca Anguiano

tiempo en las máquinas de producción alterando el programa anual de ésta y se tiene que refabricar para satisfacer la demanda programada, más las horas hombre para volver a producir lo robado o dañado, costos de volver a distribuir, imagen con el cliente, tiempo del área de Ventas para explicar al cliente y volver a sacar pedido, y un muy largo número de etcéteras", señaló.

Sobre la imagen con el cliente, Alfredo Jiménez, *Director Corporate Security* en Teva, explicó que, aunque no le corresponde de manera directa al área de Seguridad la imagen de las farmacéuticas o los laboratorios, sí puede contribuir a que ésta no sea dañada.

"Más allá de comentarios de carácter político, no he tenido conocimiento de que la seguridad afecte la reputación del sector, sin embargo como parte de las labores diarias del área de Seguridad Corporativa de las compañías farmacéuticas en conjunto con otras áreas de control es proteger la reputación de la compañía, con acciones preventivas que se traducen en toda una cultura cimentada en la ética, integridad, concientización, capacitación, buenas prácticas, respeto y sobre todo estricto apego y cumplimiento de la ley".

Rebeca Anguiano, *Security Manager LATAM* en Bausch Health, también comparte la idea de que el área de Seguridad contribuye a la buena imagen de las farmacéuticas al cuidar cada detalle de la operación. "Considero que la industria farmacéutica es uno de los giros que más cuida todos sus procesos, por lo delicado que es, nos dedicamos a vender salud, a brindar alternativas que mejoran la calidad de vida de los pacientes, es por eso que todas las actividades que realizamos deben ser cuidando todos los detalles, es importante contar con los mecanismos que te ayuden a detectar cualquier situación que pueda generar un riesgo o amenaza; y en caso de sufrir algún incidente acudimos a la instancias competentes para denunciar el hecho".

PROTOCOLOS DE ACTUACIÓN

El robo al transporte de carga desafortunadamente ha ido en aumento y no se ha podido controlar, las empresas de cualquier industria tienen que asegurar que tanto la carga y el transportista lleguen a su destino totalmente seguros, pero cuando un incidente se presenta, una reacción planeada y adecuada contribuirá a que los daños sean los menos posibles.

Octavio García Peregrina compartió los pasos a seguir ante un robo de transporte de medicamentos:

- Notificación Inmediata:
  - Contactar a las autoridades: informar inmediatamente a la policía local y proporcionar todos los detalles disponibles sobre el robo, incluyendo la ubicación, descripción del vehículo y cualquier otra información relevante.
- Notificar a la empresa: informar al departamento de Seguridad de la empresa y a la gerencia sobre el incidente.
- Bloqueo y Rastreo del Vehículo:
  - Sistema de rastreo GPS: si el vehículo está equipado con un sistema de rastreo GPS, activar el seguimiento en tiempo real para ayudar a las autoridades a localizar el vehículo robado.
- Inmovilización remota: si es posible, activar la función de inmovilización remota del vehículo para evitar que continúe en movimiento.
- Activación del Protocolo de Seguridad:
  - Equipo de respuesta rápida: activar el equipo de respuesta rápida de la empresa para coordinar las acciones necesarias y apoyar a las autoridades en la recuperación de los medicamentos.
- Comunicación interna: informar a todos los departamentos relevantes sobre el robo para que estén al tanto y puedan tomar medidas adicionales si es necesario.
  - Evaluación del Impacto:
- Inventario de lo robado: realizar un inventario preliminar para deter-

minar la cantidad y tipo de medicamentos robados.
  - Análisis de riesgos: evaluar el impacto potencial del robo en la cadena de suministro y en los pacientes que dependen de esos medicamentos.
- Notificación a las Autoridades Reguladoras:
- Informe a las autoridades sanitarias: notificar a las agencias reguladoras de salud pertinentes (como la FDA, EMA u otras) sobre el robo, proporcionando detalles del incidente y de los productos robados.
- Plan de Recuperación y Mitigación:
- Reabastecimiento de productos: iniciar el proceso de reabastecimiento de los productos robados para minimizar las interrupciones en el suministro.
  - Investigación interna: llevar a cabo una investigación interna para identificar cualquier posible fallo en los procedimientos de seguridad y mejorar los protocolos para evitar futuros incidentes.
- Comunicación Externa:
  - Aviso a distribuidores y clientes: informar a los distribuidores y clientes afectados sobre el incidente y las medidas que se están tomando para asegurar el suministro continuo.
  - Advertencia pública: si es necesario, emitir un aviso público para alertar sobre la posible distribución de medicamentos robados y falsificados en el mercado.
- Revisión y Mejora de la Seguridad:
  - Evaluación de seguridad: revisar y evaluar las medidas de seguridad actuales en el transporte de medicamentos y hacer mejoras basadas en las lecciones aprendidas del incidente.
  - Capacitación adicional: proporcionar capacitación adicional al personal sobre cómo manejar situaciones de emergencia y mejorar la seguridad en el transporte.
- Seguros y Compensaciones:
  - Reclamación de seguro: iniciar el proceso de reclamación de seguro para recuperar las pérdidas financieras causadas por el robo.
  - Compensación a clientes: si el robo afecta el suministro a clientes clave, evaluar la necesidad de ofrecer compensaciones o soluciones alternativas.

FALSIFICACIÓN DE MEDICAMENTO Y MERCADO NEGRO

En la experiencia de Luis Iturbe, uno de los principales problemas de esta industria es el crimen de producto, como la piratería. "La venta en mercado negro, la distribución de producto robado, falsificación y contrabando son los temas más preocupantes en el sector, sin dejar de lado los riesgos en el resguardo de información de fórmulas y componentes de los medicamentos; así como los procesos de destrucción y disposición de lotes de producto no conforme", indicó.

Por su parte, Jesús Islas explicó que ante este problema han implementado varias medidas que fueron adoptando para garantizar que sus productos no lleguen al mercado negro, por ejemplo, mantener interacción permanente con las autoridades, organizaciones regulatorias del sector y sus socios terceros involucrados en el plan de seguridad general de la cadena de suministro, con el fin de evitar el robo de producto, así como la detección de aquel de dudosa procedencia.

"Por más de 10 años, hemos colaborado con las autoridades y con los entes regulatorios, en participar en eventos y foros como el que hoy **SEA** organizó, para hablar del tema, de los riesgos del sector e intercambiar conocimientos y experiencias con nuestros colegas de seguridad, así como con los responsables de aduanas, hospitales y médicos para la detección temprana de medicamentos falsos", platicó.

La creación de una cultura de seguridad en la sociedad, es una estrategia efectiva para enfrentar este problema, sin embargo, aún hace falta mucha disposición tanto de las autoridades, como de los usuarios que no se informan o no prestan atención en el medicamento que requieren.

"Los problemas de seguridad en la industria farmacéutica, desde mi punto de vista, tienen como principal motor el mercado negro de medicamentos, que es potencializado por el desabasto, falta de información de los pacientes o sus familiares y el negocio que representa para la delincuencia, lo que genera la problemática de robo de productos principalmente en carretera, CDT (Falsificación, Desviación y Manipulación), venta ilícita (Medios Electrónicos y Comercio Informal) y también la aparición de distribuidores irregulares que han sido denunciados por la industria ante las autoridades", puntualizó Alfredo Jiménez.

TECNOLOGÍA EN SEGURIDAD: UNA NECESIDAD MÁS QUE UN GASTO

Los especialistas tienen presente que además de la capacitación al personal, la creación de una cultura de seguridad, de ciberseguridad entre su personal, la tecnología es fundamental para complementar la seguridad de esta industria, y precisamente este análisis lo compartieron en el desayuno que da pie a este reportaje especial, en donde no sólo dialogaron sobre los retos del sector, sino también conocieron dos marcas que ofrecen soluciones tecnológicas para esta industria.

Gabriel Apel, director comercial;

y Alejandro Rojas, *Account Manager* para Convergint México, junto con Omar Murillo, *Senior Sales Director Mexico & Andina* de Motorola Solutions, interactuaron y escucharon las inquietudes de los especialistas de la industria farmacéutica para comprender los retos y oportunidades que deben abordarse al avanzar hacia soluciones más robustas que satisfagan las necesidades de seguridad.

Convergint, como integrador y en colaboración con sus socios, identifica las necesidades de los clientes, personaliza las soluciones y selecciona la tecnología adecuada para implementar con un equipo capacitado y certificado. Su propuesta incluye soluciones basadas en avances tecnológicos, como la inteligencia artificial aplicada al análisis de video, conectividad a la Nube y la integración con otros sistemas completos de seguridad que permite optimizar de manera segura la toma decisiones efectivas para la detección y prevención de incidentes. Además, la implementación de soluciones integradas no sólo mejora la seguridad operativa, sino también mantiene la vinculación y respaldo para la toma de decisiones de otras áreas como Finanzas, Comercial y *Marketing*, lo que a su vez mejora el retorno de inversión.

Alan Vara comentó que algunas de las soluciones tecnológicas que recomienda es el uso de sistemas de seguridad electrónicos como el control de accesos, la videovigilancia y tecnología biométrica; así como uso de geolocalización en las unidades de transporte, protocolos de establecimiento rutas y horarios.

Cada vez más las compañías hacen uso de las nuevas herramientas tecnológicas y con la llegada de la Inteligencia Artificial, es necesario conocer tanto sus beneficios como estar un paso delante de la delincuencia, pues ellos también hacen uso de ésta, algunos casos ya se han presentado, usurpando la identidad de altos mandos.

Eduardo Téllez considera que hoy en día la tecnología debe ser el principal aliado de esta industria y eliminar lo más posible el factor humano, así como contar con políticas claras y adaptarlas a la modernidad. "Por ejemplo, los códigos de conducta rara vez tocan el tema de redes sociales, tampoco incluyen el tema cada vez mayor cantidad de personas que no se identifican con hombre o mujer (actualmente hay 137 diferentes formas conocidas), todo eso se tiene que contemplar y modificar", señaló.

No obstante, los retos del sector van cambiando y además de resiliencia, se requiere de actualización en todo, estrategias y tecnología. "La seguridad es dinámica, si bien existe un estándar y procedimientos estos deben de adaptarse diariamente a diferentes aspectos, desde el clima hasta aspectos sociales. Como en todas las profesiones es indispensable estar actualizados y saber lo que pasa en el momento, anticipándote a cualquier evento que pueda representar un riesgo para todo tu entorno", concluyó. ■

Fotos: Mónica Ramos / SEA

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

Este reportaje se llevó a cabo gracias al patrocinio de Convergint y Motorola Solutions.

convergint®

MOTOROLA SOLUTIONS

MEXSEPRO

SEGURIDAD Y PROTECCIÓN DE MÉXICO

EMPRESA **A FAVOR** DE LOS **DERECHOS** Y **JORNADAS DIGNAS LABORALES**

[SEGURIDAD | inteligente]

Nos enorgullece y compartimos la visión y el camino que está tomando nuestra industria, en **beneficio** de todos los trabajadores en cuanto a la **dignificación**, **jornadas** y **profesionalización** de la **seguridad privada.**

ORGULLOSAMENTE **MEXICANOS**

MEXSEPRO S. DE R.L. DE C.V. Artemio Alpizar Ruz no. 341, Int. 02, San Miguel, C.P. 09360, Iztapalapa, CDMX
Web: mexsepro.com | **Correo:** ventas@mexsepro.com | **Oficinas:** (55) 6585 4448 | **Whatsapp:** (55) 4141 85 73

ISO AMESP AMEXS ASIS COPARMEX CIUDAD DE MÉXICO REPSE

IV ENCUENTRO DE SEGURIDAD BANCARIA

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

IV ENCUENTROS DE SEGURIDAD Bancaria

Más de 150 responsables de seguridad conocieron los principales riesgos de la banca, entre ellos, ciberataques y fraude con Inteligencia Artificial

Seguridad en América llevó a cabo el IV Encuentro de Seguridad Bancaria el pasado 26 de junio en el Hotel Courtyard by Marriott Mexico City Revolución. En esta ocasión se presentaron dos paneles de especialistas quienes expusieron los riesgos de seguridad a los que se enfrenta ese sector y las diferentes estrategias que han implementado para contrarrestarlos. El Encuentro se llevó a cabo gracias al patrocinio de las marcas: SCATI, Dorlet, Genetec, Multiproseg, SALTO, Motorola Solutions, GSI Fabril, y Verint; mismas que expusieron sus soluciones y tecnologías más innovadoras para la seguridad de la banca.

Samuel Ortiz Coleman, director general de **Seguridad en América**, agradeció la participación tanto de los asistentes, como de los patrocinadores y conferencistas, y los invitó a seguir contribuyendo no sólo con la seguridad de las instituciones a las que representan, sino también en estos foros que tienen como objetivo compartir conocimientos, experiencias y mejores prácticas, así como las tendencias tecnológicas que favorecen la seguridad.

PRIMER PANEL

Después de dar la bienvenida, Samuel Ortiz Coleman presentó a los participantes del primer panel que llevó por título "Transformación de la seguridad bancaria en el siglo XXI", integrado por Maribel Cervantes Guerrero, *Head Protective Security Mexico & LAM* en HSBC; Luis Meza Cepeda, director de Seguridad en Citibanamex; Hugo Montes Campos, director de Seguridad y Prevención en CI Banco; Víctor Hugo Ramos Ortiz, director ejecutivo de Prevención en Grupo Financiero Santander México, y como moderador del panel, Ciro Ortiz Estrada, director general de Seproban.

Los especialistas comenzaron por enumerar los principales riesgos de seguridad a los que se enfrenta el sector bancario, siendo el robo en ATM (cajeros automáticos), lo que continúa representando un alto

riesgo para los usuarios, mismos que plasmaron esta preocupación en la más reciente Encuesta Nacional de Seguridad Pública Urbana (ENSU marzo 2024), realizada por el Instituto Nacional de Estadística y Geografía (INEGI).

Cifras que compartió Maribel Cervantes, siendo el 69.4% de la población quien manifestó sentirse insegura en los cajeros automáticos localizados en la vía pública; seguido del 63.9%, en el transporte público; 53.9%, en la carretera y 53.5%, en el banco. Por lo que la especialista externó este problema al que se enfrentan y la necesaria participación de las autoridades para coadyuvar en la mitigación del mismo.

Otro de los temas que se tocaron fue el del fraude bancario y los ataques cibernéticos, demostrando por qué es necesario integrar a la ciberseguridad en las instituciones bancarias y también la creación de una cultura de seguridad y ciberseguridad entre personal y usuarios de la banca electrónica, puesto que la digitalización del servicio es inevitable, y por el contrario, va en aumento.

Una de las herramientas de la que se han apoyado los panelistas para situaciones de riesgo e inseguridad, ha sido Seproban (Seguridad y Protección Bancarias), la Sociedad de Apoyo de las Instituciones de Crédito, que se encarga de recibir las señales de alarmas emitidas por las instituciones bancarias, y las apoya coordinándolas con las autoridades de Seguridad Ciudadana, y Procuración de Justicia, en la investigación y persecución de los delitos que afecten a la institución bancaria.

SEGUNDO PANEL

El segundo panel del día que llevó el mismo nombre, pero con diferentes participantes, estuvo moderado por Pedro Villanueva Meléndez, director de Investigación y Prevención de Fraudes en Seproban, y participaron Selene Molina Arenas, subdirectora de Seguridad en BanCoppel; Diego de la Torre Díaz, subdirector de Seguridad en Banco del Bajío; Eduardo Arellano Vázquez, director de Seguridad en Banorte; y Fernando Gómez Villarreal, director de seguridad en Compartamos Banco.

Este panel se enfocó más en las amenazas digitales que enfrentan los bancos y cómo deben estar preparados para saber reaccionar y sobre todo para prevenirlos. También mencionaron los constantes ataques al sistema SPEI de la banca, y cómo la delincuencia está utilizando la Inteligencia Artificial para fraudes con la ursurpación de identidad a través de audio e imagen. Pedro Villanueva recomendó tener claros los protocolos de actuación de manera interna ante estos riesgos de ciberseguridad.

CONFERENCIAS COMERCIALES

La primera compañía que se presentó en el IV Encuentro fue SCATI, empresa española con más de 25 años en el mercado que ha desarrollado sus propias plataformas de: Integración de Sistemas, Videovigilancia y Control de Accesos; con lo último en Inteligencia Artificial y gestión del Big Data, con los máximos estándares de IT y ciberseguridad.

Alberto Pérez Aparicio, *Sales Director* LATAM en SCATI, fue el encargado de brindar la charla titulada "Inteligencia de Negocios. De la imagen al rendimiento: cómo la analítica de video impulsa la gestión del negocio", en la que habló sobre la transformación digital que ha tenido la Banca y cómo los usuarios de ésta han cambiado la forma en que la usan y migrado a la banca digital. Alberto Pérez habló de los beneficios de usar analíticas de video, de instalar plataformas que ayuden a la automatización de procesos y cómo el *Big Data* mejora la seguridad. SCATI ya cuenta con clientes y experiencia ofreciendo soluciones de seguridad especializadas para la banca, por ejemplo, Suite Vision, una plataforma completa para la gestión de la videovigilancia, robusta, estable y segura.

El siguiente ponente en pasar fue José de Jesús Arellano, *Vertical Sales Manager* de Genetec, quien habló sobre "Ciberseguridad y Operación Eficiente desde un Sistema de Seguridad Unificado". Genetec es una compañía global líder en soluciones unificadas de seguridad en redes IP, con 25 años de experiencia, más de dos mil empleados y más de 42 mil clientes en 159 diferentes países.

José de Jesús destacó la importancia de crear e implementar estrategias de ciberseguridad en las instituciones bancarias, siendo ya una necesidad, y comentó que, en el año 2023, el 42% de las organizaciones incrementaron sus implementaciones de herramientas de ciberseguridad en respuesta a las ciberamenazas en comparación con el 29% en 2022. Una de las soluciones que ofrece Genetec para la banca es Security Center, la plataforma de seguridad abierta, intuitiva y unificada en un solo sistema para control de acceso, video, ALPR, comunicaciones, intrusiones, entre otras.

Y una de las soluciones de seguridad que no puede faltar, es la seguridad privada, para ello, Pedro Arellano, gerente de Proyectos de Multiproseg, realizó una ponencia fuera de lo tradicional. Mostró a los asistentes un cuestionario que ellos pudieron resolver desde sus dispositivos móviles, en los que se tocaron temas sobre la seguridad en bancos, tecnología y sus observaciones sobre la seguridad privada en bancos.

El siguiente turno fue de SALTO Systems, fabricante reconocido a nivel mundial por especializarse en cerraduras y control de accesos, y fue Jorge Olmedillo, *Regional Sales Manager* para México en SALTO, quien mostró las diferentes soluciones que ofrece para este sector, con la charla "Revolucionando la Seguridad Bancaria: Implementación de Cerraduras Inalámbricas Avanzadas". Olmedillo comentó que la firma es líder mundial en crecimiento de cerraduras electrónicas y pioneros en el sector de la seguridad con el primer sistema *data-on-card*, el primer sistema inalámbrico, y el primer sistema de cerradura en la Nube.

SALTO Systems tiene más de 20 años en el mercado, ha instalado más de siete millones de cerraduras en todo el mundo, y tiene más de 41 oficinas operando. Jorge Olmedillo mostró los beneficios de la Solución SALTO 360, específicamente tres soluciones par aña banca: SALTO KS, solución en la Nube para sucursales bancarias; SALTO SPACE, solución *on-permise* para oficinas corporativas; y SALTO Homelock, gestión de llaves puertas descentralizadas para inmuebles bancarios.

Por su parte, Motorola Solutions representada por Edgar López, *Regional Sales Manager* de la firma, habló sobre la transformación digital de la banca, impulsada por la Inteligencia Artificial. El expositor comentó que la firma desarrolla redes y dispositivos de comunicaciones críticas que funcionan excepcionalmente en las condiciones más duras y están comprobados

para ayudarlo a mantenerse conectado y comunicarse con claridad. Motorola Solutions ofrece un portafolio unificado con soluciones para la banca.

La siguiente compañía que pasó a presentar sus soluciones fue GSI Fabril, empresa mexicana líder en metalmecánica de transformación de acero y diversos materiales enfocada en atender profesionalmente los requerimientos en los sectores de almacenamiento, exhibición, mobiliario, equipos de blindaje a vehículos de traslado de valores y línea arquitectónica con más de 30 años de experiencia en el mercado. GSI Fabril cuenta con dos plantas de producción, una en Lerma, y la otra en Huehuetoca, Estado de México.

Durante todo el Encuentro estuvo presentándose un video informativo de Dorlet, especialista en control de accesos e integración de sistemas de seguridad.

La última compañía que pasó a exponer, fue Verint Systems, representada por José Machado, *Regional Sales Manager–Latin America & Caribbean, S. Florida Fraud and Security Solutions,* quien habló sobre cómo Verint ayuda a los bancos a transformarse gracias a su plataforma abierta y la incorporación de la Inteligencia Artificial a las diferentes innovaciones tecnológicas que ofrece. ■

Fotos: Mónica Ramos / SEA

DORLET

GSI FABRIL S.A. DE C.V.

MOTOROLA SOLUTIONS

Genetec

SCATI

SALTO inspiredaccess

Multiproseg A quien valor merece

VERINT

SEGURIDAD EN LA INDUSTRIA ALIMENTARIA

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Cambios en las preferencias de los consumidores, sustentabilidad, trazabilidad, normatividad e inflación, así como seguridad en los procesos de producción, son de los principales retos de este sector que registró un Producto Interno Bruto de 6.26 billones de pesos este año

La industria alimentaria en México representa el 7.6% del Producto Interno Bruto (PIB), aunque en el primer trimestre del año presentó una caída del 0.29% con respecto al trimestre anterior, algunos de los sectores que la integran también han reflejado un decrecimiento comparado con el mismo periodo, pero del año anterior, por ejemplo, el sector agrícola en México se situó en torno a los 471 mil 138 millones de pesos (25 mil 565 millones de dólares)[1].

Los especialistas coinciden en que esta industria enfrenta diferentes retos como el cambio climático, sostenibilidad, tecnología e innovación, acuerdos comerciales, normatividad, y por supuesto retos de seguridad, generales y específicos de acuerdo a las características de cada alimento o producto. Es por ello que realizamos una serie de entrevistas a especialistas en la materia quienes nos compartieron la situación actual de la industria, los retos, riesgos y mejores estrategias y tecnología para contrarrestar todo aquello que ponga en peligro la producción, distribución y sobre todo llegue en las condiciones adecuadas al usuario final.

"Los lectores faciales son un gran aporte a los temas de seguridad alimentaria, al evitar el contacto de las manos con equipos y tarjetas"

LORENZO SANCHO LÓPEZ, GERENTE DE SEGURIDAD PATRIMONIAL EN ALPURA

SEA: ¿Cuáles considera que son los retos de seguridad de la industria alimentaria en México?

Lorenzo Sancho (LS): Existen diferentes retos que van cambiando de acuerdo con el contexto social, mundial, local y dependen también de la materia o producto de cada empresa. Algunos de los retos de seguridad, específicos de nuestra industria que ubico en la actualidad, son los siguientes:

- **El control de la cadena logística del producto en toda su extensión.** En nuestro caso, desde la recepción en el rancho hasta la entrega al cliente final, para prevenir acciones sobre el mismo, que impliquen daño de marca a parte del patrimonial.
- **Y el control del auto robo por parte de colaboradores.** El robo interno continúa siendo un reto importante.

SEA: ¿Cómo contribuye a la creación de una cultura de seguridad entre los colaboradores de la empresa?

LS: A través de la inclusión de una exposición sobre recomendaciones básicas de seguridad en el *onboarding*, a las nuevas incorpo-

raciones de personal, acompañadas de campañas con mensajes sobre el tema, en los correos internos, que permitan identificar peligros que se estén desarrollando en el periodo.

SEA: ¿Qué tecnología recomienda para el control de accesos de una planta de la industria alimentaria?

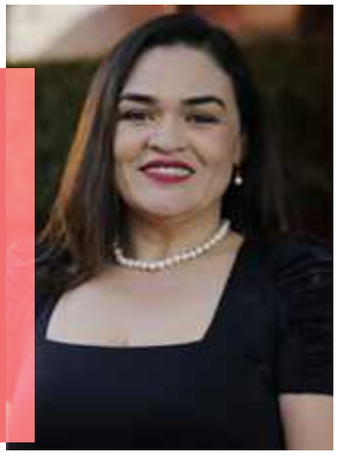
LS: Los lectores faciales son un gran aporte a los temas de seguridad alimentaria, al evitar el contacto de las manos con equipos y tarjetas.

SEA: ¿Considera importante la ciberseguridad en la industria alimentaria?

LS: Sí, en la actualidad es importante establecer un área de Ciberseguridad, ya que el riesgo es muy grande ante un fallo donde, por ejemplo, se produzca un secuestro de datos, con la exposición de estos, o la pérdida de control del proceso, generando un daño desmesurado en la cadena de producción.

De igual manera, el control de la calidad del producto tiene base en ciertos procesos basados en sistemas, y que podrían ser alterados, afectando a la sociedad y a la marca.

"La Seguridad Corporativa juega un papel crucial en la identificación de riesgos al trabajar en estrecha colaboración con las diversas unidades de negocio"



DORA ELENA CORTÉS, *ASSOCIATE DIRECTOR – REGIONAL & PHYSICAL SECURITY LATAM, GLOBAL SECURITY* EN CARGILL

SEA: ¿Cuáles son los riesgos de seguridad que enfrenta la industria alimentaria en México?

Dora Elena Cortés (DEC): Existen diferentes riesgos dependiendo, algunos específicos y otros de acuerdo a cada proceso de la industria. Desde el campo hasta que el alimento llega a nuestra mesa, hay diversos riesgos a los que la industria se enfrenta, por ejemplo, el productor que está en el campo, está expuesto a robos, cobros de cuota o derechos de piso, inseguridad por la presencia de grupos de delincuencia organizada, así como riesgos durante el transporte.

En las etapas de transformación o producción, están los robos y mermas, y durante la distribución: el robo al transporte de carga, o bien, el tren si así es el caso. Así mismo, el control que buscan ejercer grupos al margen de la ley en ciertas zonas del país sobre ciertos productos específicos (pollo, limón, aguacate, por mencionar algunos). También existen riesgos para las personas (específicamente personal de Ventas o técnicos) que visitan a los agricultores y productores en zonas de alto riesgo, distribuidos en toda la geografía.

SEA: ¿Cuáles son las estrategias de seguridad que mejor te han funcionado para contrarrestar esos riesgos?

DEC: La Seguridad Corporativa juega un papel crucial en la identificación de riesgos al trabajar en estrecha colaboración con las diversas unidades de negocio. Esta colaboración permite a la Seguridad Corporativa entender mejor las operaciones del negocio, los procesos y las áreas de vulnerabilidad. Al estar inmersos en el negocio, pueden identificar proactivamente los riesgos potenciales, ya sean físicos, digitales o legales, y desarrollar estrategias de mitigación adecuadas. Sin embargo, la Seguridad Corporativa no puede trabajar de manera aislada. La identificación de riesgos es un esfuerzo conjunto que requiere la participación de todas las partes interesadas. Los empleados en todos los niveles de la organización deben estar capacitados para reconocer y reportar posibles amenazas. Además, la alta dirección debe estar comprometida con la promoción de una cultura de seguridad y la implementación de políticas y procedimientos de seguridad. De esta manera, la Seguridad Corporativa y el negocio trabajan juntos para proteger los intereses de la organización.

En México, específicamente hablando, existen dos factores que son determinantes a la hora de establecer medidas de protección: La Granularidad y la Volatilidad.

La granularidad se refiere a que no puedes comparar los problemas de seguridad que se enfrenta en Tamaulipas con Oaxaca, por ejemplo. Incluso, dependiendo de la operación, puede ser necesario llegar a un análisis a nivel de calle. Puede ser que de un lado de la colonia opere un grupo y al otro lado, otra banda. Y cada uno tenga "reglas" diferentes. Así que si es una operación de entrega de distribución de pollo a tiendas (por ejemplo), se tiene que saber la dinámica para entender los riesgos específicos.

La volatilidad tiene que ver con que la situación de seguridad es altamente sensible a desarrollar episodios de violencia sin previo aviso. Bloqueos, enfrentamientos armados y similares, pueden cambiar la dinámica de un sitio de forma repentina y abrupta por lo que es necesario adaptarse rápidamente para proteger los activos que estén en riesgo en ese momento específico.

"La Seguridad contribuye con otras áreas, con una gestión de los riesgos internos, derivados del factor humano con la aplicación de protocolos, que nos permiten contar con los controles adecuados, para prevenir las incidencias en general"

ALEJANDRO RODRÍGUEZ, GERENTE DE SEGURIDAD PATRIMONIAL EN GRUPO BACHOCO

SEA: ¿Cuáles son los riesgos de seguridad en la cadena de suministro de la industria alimentaria?

Alejandro Rodríguez (AR): Los riesgos en la cadena de suministros se identifican desde sus áreas de acción como los son:

- **Complicaciones en la producción, transporte o almacenamiento de mercancías o productos.**

Por ejemplo, retrasos en la entrega, fallas en la calidad de los productos, inconvenientes con proveedores. Falta de cumplimiento de las regulaciones normativas, ambientales, sociales y gubernamentales.

- **Factores externos:** amenazas de robos, ataques cibernéticos, daños a la propiedad, o desastres naturales que pueden afectar la cadena de suministro.

SEA: ¿Cuáles son las estrategias de seguridad que mejor te han funcionado para contrarrestar esos riesgos?

AR: Algunas de las estrategias son:

La correcta identificación y evaluación de los riesgos, para establecer el plan de acción mismo que mantendrá el control y mitigar el impacto.

La prevención aplicada a cada uno de los procesos, utilizando las herramientas tecnológicas actuales, para administrar los riesgos y la superación de las crisis; consecuentemente es primordial hacer una revisión del estado actual de estas contingencias, a fin de plantear las acciones suficientes, las cuales fortalecerán las áreas que contribuyen a la disminución de los riesgos, así como el registro adecuado de los acontecimientos para mantener actualizada la memoria de los riesgos.

SEA: ¿Cómo se relaciona o colabora el área de Seguridad con las demás áreas de la empresa?

AR: Con una constante y estrecha comunicación con las diferentes áreas administrativas y de operación, en donde se diseña un plan estratégico para cada cliente con la viabilidad de negocio. La Seguridad lleva una cadena de colaboración para asegurar que los productos lleguen a las instalaciones de nuestros clientes. Esta interacción es primordial para favorecer al cliente con propuestas y proyectos que hagan una viabilidad de funcionamiento adecuado, el cual se diseña de acuerdo con los objetivos de la Dirección General.

SEA: ¿Cómo contribuye o influye el área de seguridad en la imagen de la marca?

AR: Contribuye con una gestión adecuada de los riesgos internos, derivados del factor humano con la aplicación de protocolos, que nos permiten contar con los controles adecuados, para prevenir las incidencias en general, alteración de reportes, conflictos de intereses, apoyados en la ética y conducta de los colaboradores, de igual formar generando los canales idóneos de denuncias, que permitan identificar cualquier anormalidad en los procesos. Así como gestionando auditorías a los procesos sensibles, y con el área de Calidad.

"Mitigar estos riesgos requiere la implementación de buenas prácticas de manufactura, sistemas robustos de trazabilidad, auditorías regulares y el uso de tecnologías avanzadas para monitorear y gestionar la cadena de suministro"

ADALBERTO BARRALES, *DIRECTOR GLOBAL SECURITY & ASSET PROTECTION (GSAP) PARA NORTH LATAM* (MÉXICO Y CENTROAMÉRICA) EN *THE COCA-COLA COMPANY*

SEA: ¿Cuáles son los riesgos de seguridad que involucran directamente al consumidor de la industria alimentaria?

Adalberto Barrales (AB): Los riesgos de seguridad en la cadena de suministro de la industria alimentaria son numerosos y variados, afectando tanto a la calidad del producto como a la seguridad del consumidor. Aquí hay algunos de los principales riesgos:

Contaminación:

- **Contaminación biológica:** Involucra bacterias, virus, parásitos y hongos que pueden causar enfermedades transmitidas por alimentos. Ejemplos incluyen Salmonella, E. coli y Listeria.
- **Contaminación química:** Ocurre debido a la presencia de pesticidas, herbicidas, residuos de medicamentos veterinarios y contaminantes industriales.
- **Contaminación física:** Involucra la presencia de objetos extraños como vidrio, metal o plástico en los productos alimentarios.

Fraude alimentario:

- **Adulteración:** Inclusión intencionada de sustancias no autorizadas o sustitución de ingredientes de menor calidad para reducir costos.
- **Etiquetado incorrecto:** Información falsa o engañosa sobre el origen, contenido o naturaleza de los productos alimentarios.

Problemas de almacenamiento y manipulación:

a) **Condiciones inadecuadas de almacenamiento:** Temperaturas inadecuadas, humedad y prácticas de almacenamiento deficientes pueden llevar a la degradación de los productos alimentarios.

SEA: ¿Qué estrategias recomienda para prevenir esos riesgos?

AB: Mitigar estos riesgos requiere la implementación de buenas prácticas de manufactura, sistemas robustos de trazabilidad, auditorías regulares y el uso de tecnologías avanzadas para monitorear y gestionar la cadena de suministro, por ejemplo:

Implementación de sistemas de gestión de seguridad alimentaria (FSMS):

- **Certificaciones internacionales:** Adoptar estándares reconocidos como ISO 22000, BRC, IFS o FSSC 22000 que proporcionan un marco estructurado para gestionar la seguridad alimentaria.
- **HACCP (Análisis de Peligros y Puntos Críticos de Control):** Utilizar el enfoque HACCP para identificar, evaluar y controlar los peligros que son significativos para la inocuidad de los alimentos.

Trazabilidad y transparencia:

- **Sistemas de trazabilidad:** Implementar sistemas de trazabilidad robustos para rastrear todos los ingredientes y productos a lo largo de la cadena de suministro. Esto permite una rápida identificación y retirada de productos en caso de contaminación.
- ***Blockchain*:** Utilizar la tecnología *blockchain* para asegurar la transparencia y la integridad de los datos a lo largo de la cadena de suministro.

Capacitación y concientización:

- **Formación continua:** Capacitar regularmente a los empleados y proveedores sobre buenas prácticas de manufactura, higiene, manipulación de alimentos y procedimientos de seguridad. Crear una cultura de seguridad.

SEA: Puede compartirnos algunas recomendaciones para preservar la buena imagen de una marca, basándose en las políticas de seguridad necesarias.

AB: Para preservar la buena imagen de una marca basándose en políticas de seguridad, es fundamental implementar medidas que aseguren tanto la protección de la información como la integridad de los productos y servicios. Aquí tienes cinco recomendaciones clave:

Implementar políticas de ciberseguridad robustas:

1) **Protección de datos:** Asegúrate de que todos los datos sensibles, tanto de clientes como de la empresa, estén protegidos mediante encriptación y accesos restringidos.
2) **Actualizaciones y parches:** Mantén todos los sistemas y *software* actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas.
3) **Educación y concienciación:** Capacita a los empleados regularmente sobre las mejores prácticas de ciberseguridad, incluyendo cómo reconocer y evitar ataques de *phishing*.
4) **Fomentar la transparencia y la comunicación efectiva:**
5) **Transparencia en la cadena de suministro:** Mantén una comunicación abierta y honesta sobre la procedencia y el procesamiento de los productos. Utiliza tecnologías como *blockchain* para asegurar la trazabilidad y transparencia.

"Un líder debe tener entre sus objetivos ser parte de ese cambio en general y ser parte del equipo que obligue al cambio por adaptarse"

GONZALO ENRIQUE ALAMILLO, DIRECTOR DE SEGURIDAD EN WALMART MÉXICO Y CENTROAMÉRICA

SEA: ¿Cuáles considera que serán las tendencias en seguridad en los próximos años en la industria alimentaria?

Gonzalo Enrique Alamillo (GEA): Considero que como responsables de Seguridad debemos considerar tres puntos clave para los siguientes años en la industria alimentaria. El primero, es el desarrollar especialistas en Seguridad en nuestros equipos que contemplen el ciclo de vida del producto en toda su cadena, incluyendo la cadena de suministro, que sean capaces de establecer una estrategia tomando en cuenta las variables de seguridad de acuerdo al tipo y escenario, que se puedan actualizar y capacitar de manera frecuente, de otra manera se corre el riesgo de quedar desactualizados o con expectativas subjetivas en nuestros análisis y reportes anuales.

El segundo, corresponde a tener la posibilidad de contar con aliados comerciales que consideren lo relevante a veces más allá de los contractual del aspecto de la seguridad en toda su contribución al proceso, esquemas de auditoría a la calidad nos garantizan este punto de manera general

Y, en tercer lugar, desestimar procesos que no integren la tecnología y aplicativos que garanticen la supervisión y monitoreo cada vez más específicos No podemos permitir procesos de seguridad con más de cinco años de antigüedad. sin actualización regular que involucre la mejora al proceso idealmente por una metodología.

SEA: ¿Cómo contribuye un líder a la creación de una cultura de seguridad entre los colaboradores de la empresa?

GEA: Con el ejemplo de ser el portavoz de programas que cada vez se ajusten a nuevas generaciones, sin duda es una obligación en los esquemas de cultura la adaptación a nuevas generaciones y sus particularidades. Es un gran error pretender que la cultura se asimila a pesar de los años, la cultura caduca y debe ser adaptable al ambiente sin olvidar su esencia en sus valores. Un líder debe tener entre sus objetivos ser parte de ese cambio en general y ser parte del equipo que obligue al cambio por adaptarse.

SEA: ¿Considera importante la aplicación de la ciberseguridad en la industria alimentaria? ¿Por qué?

GEA: Sí, aunque pareciera que se ha usado en manera excesiva el nombre de ciberseguridad, los responsables de Seguridad debemos ser cercanos a términos más allá de la transgresión de plataformas que impliquen un robo o fraude por suplantación de identidad o por "asaltos" a plataformas que permitan el colocar destinos diferentes de la mercancía o producto o coloquen ya nula la necesidad de la violencia al colocar datos incorrectos y a favor de ladrones tecnológicos.

Es una prioridad para los años inmediatos que en nuestros equipos se cuente con un gerente de Riesgos con la capacidad de evaluar y colocar lo necesario para mitigar riesgos de este tipo y que futuros directores tengan en sus áreas de conocimiento esta necesidad como básica.

"El mayor riesgo que tenemos son las extorsiones presenciales o cobros de piso que pueden darse en lugares muy focalizados siendo estas ejercidas de igual forma por grupos locales"

EDUARDO PLIEGO MORENO, GERENTE DE SEGURIDAD INTEGRAL EN ALSEA

SEA: ¿Cuáles son los riesgos de seguridad en un restaurante?

Eduardo Pliego (EP): Sin duda el sector restaurantero principalmente el que se encuentra a pie de calle, es decir aquellos que no están dentro de una plaza comercial presentan una dinámica delictiva diferente, en estos el robo de oportunidad se da con mayor frecuencia

y lo que observamos es que hoy se utiliza mayor violencia en este delito, el tema de carteristas como un fenómeno recurrente a lo largo de los años ha transmutado al desapoderamiento con violencia, siendo el robo de dinero, relojes y llaves de vehículo los más hurtado.

Otros factores de preocupación para el sector son las intrusiones nocturnas y extorsiones telefónicas, mismas que muestran dinámicas delictivas que involucran necesariamente un mayor acercamiento con las autoridades locales, en este punto es relevante que, como sector restaurantero, participemos no sólo con la información de videograbaciones, sino que realmente se presenten las denuncias y ratificaciones correspondientes ante la autoridad. Dentro de estos dos factores el mayor riesgo que tenemos son las extorsiones presenciales o cobros de piso que pueden darse en lugares muy focalizados siendo estas ejercidas de igual forma por grupos locales que no en pocas ocasiones utilizan el nombre de alguna organización delictiva para generar un mayor miedo.

SEA: ¿Cuáles son las estrategias de seguridad que mejor te han funcionado para contrarrestar esos riesgos?

EP: Sin duda pensar fuera de la caja, como bien dice uno de mis mejores maestros en la seguridad privada, Enrique Alamillo, esto no significa que para cada caso y cada momento se debe considerar acciones concretas alcanzables; ejemplo de ello fue la implementación hace cuatro años de guardias más dinámicos en donde participen más con la operación retirando ese viejo esquema del guardia parado sin mayor actividad, con ello registramos una disminución de cerca del 95% de los incidentes de robo sin violencia principalmente en el corredor Reforma-Centro, así como en ciudades como Guadalajara y Cancún, constituyendo todo un éxito su implementación.

Otra estrategia que nos ha funcionado es la relación de reciprocidad con la autoridad, en especial con las áreas de Inteligencia y Policía Turística en donde el intercambio de información ha sido valioso para la contención de estos grupos de criminales que ingresan, pero también para observar su zonas de confort para su seguimiento y aseguramiento, esto nos ha permitido sacar a no menos de 20 objetivos que nos afectaban en dichas zonas.

SEA: ¿Considera importante la sinergia con las autoridades para la disminución de delitos en los restaurantes?

EP: Sí, la vinculación con autoridades, principalmente las con las áreas de Prevención del Delito resulta esencial para crear esta simbiosis entre seguridad y operación si algo hemos notado es que este tipo de talleres con las áreas de Prevención del Delito, terminan con una mejor respuesta ante las emergencias.

"Vemos como pilar fundamental la capacitación de las personas en conocimientos de procesos de seguridad, la auto protección, el cuidado personal y de activos"

ROBERTO VELIZ, PREVENCIÓN Y GESTIÓN DE RIESGOS EN JUGOS DEL VALLE SANTA CLARA

SEA: ¿Cuáles son las estrategias de seguridad que recomienda para los riesgos actuales en esta industria?

Roberto Veliz (RV): Sin duda alguna, la prevención. Preferimos prevenir a estar gestionando riesgos, sabemos que toda acción de seguridad tiene un riesgo inherente, por varias condiciones, nuestra meta es trabajar en planes concretos y definidos para tener un riesgo residual cada vez más bajo, el cero es posible y mantener los estándares para la continuidad del negocio es clave.

¿Cómo lograrlo? Enfocándonos en el uso de las tecnologías de seguridad, estando a la vanguardia y actualizándonos constantemente. Vemos como pilar fundamental la capacitación de las personas en conocimientos de procesos de seguridad, la auto protección, el cuidado personal y de activos. En general, creamos cultura de prevención desde el día uno que los colaboradores, propios y terceros requieren al ingreso a nuestras operaciones.

SEA: Mencione algunas particularidades o características de la industria alimentaria que el área de Seguridad siempre debe tomar en cuenta para la seguridad en la cadena de suministro.

RV: Apoyar la cadena de suministro y cadena de valor desde sus inicios, asegurando el correcto abasto con la mejor calidad y al mejor costo.

Se debe lograr que los accesos tanto de entrada como de salida sean lo más ágiles y seguros posibles, los tiempos bajos de recibo, estancia y salidas generan ahorros y es imperativo mantenerlos bajos.

Asegurar los planes de *Food Defense* y Contra Sabotaje de las Unidades Operativas y de negocio, invirtiendo en tecnologías y capacitación.

Garantizando la seguridad de nuestro producto terminado a la salida de nuestros CeDis y Plantas, desde todos los frentes, legal, alimenticio, de seguridad. Buscando la seguridad de las personas y que el producto final llegue a clientes y consumidores con máxima calidad.

El cuidado de la marca y nuestro talento personal al reclutar. Todo lo que conlleva la cultura de la empresa, apostando por un Código de Ética sólido y de estricto cumplimiento y tratando a nuestros colaboradores propios y terceros como parte integral de nuestras políticas y procesos.

- Salvaguardar los activos de ataques externos y robos.
- Implementación de usos de tecnología para resguardo de información y de materias primas.
- Mantener y Cumplir los temas regulatorios y legales con los clientes y lugares que correspondan y donde se tengan relaciones comerciales.
- Contribuir al cuidado del medio ambiente y asegurar el cuidado de la marca, además de ser amigables con el planeta.

TECNOLOGÍA COMO ALIADO INHERENTE

Gabriel Apel, director comercial de Convergint México, se reunió con Alejandro Aguirre, *National Sales Manager México & CCA National*; y Alejandra Guerrero, *Key Account Manager* de Axis Communications, y los especialistas en seguridad alimentaria. Durante esta reunión, abordaron preocupaciones y necesidades de seguridad específicas para el sector. Convergint, como líder integrador, ofrece soluciones de seguridad electrónica diseñadas especialmente para cubrir las demandas de dicho mercado. Su enfoque personalizado y experiencia en el sector garantizan la máxima protección y eficiencia en las operaciones, proporcionando tecnología de vanguardia adaptada a estas necesidades críticas como los son:

- **Sistema de Control de Acceso Avanzado:** Mejora la seguridad al restringir el acceso a áreas sensibles, proteger datos confidenciales y gestionar eficientemente al personal.
- **Videovigilancia y Monitoreo Remoto:** Permite supervisión en tiempo real, prevención de pérdidas y respuestas rápidas ante incidentes.
- **Sistemas de Intrusión y Detección de Incendios Integrados:** Protege contra amenazas internas y externas, con detección rápida de intrusiones no autorizadas.
- **Integración de Sistemas de Seguridad:** Optimiza la gestión y proporciona mayor visibilidad en tiempo real.
- **Soluciones de Gestión de Video y Análisis Inteligente:** Ofrece eficiencia operativa mediante análisis de video y optimización de recursos.

Estas soluciones consideran aspectos como adaptabilidad a normativas, escalabilidad, integración con sistemas existentes, soporte post-implementación y análisis de costo-beneficio.

A través de socios como Axis Communications, es posible personalizar proyectos para satisfacer las necesidades específicas de los clientes. Algunas soluciones generales impulsadas por Axis incluyen el cumplimiento de normas ISO 31000, apoyo en la implementación de CTPAT/OEA, monitoreo de temperaturas en cámaras de refrigeración y protección perimetral.

Los beneficios para los clientes incluyen:

- Amplia oferta de productos, incluyendo opciones para cumplir con ISO 22000.
- Garantía de calidad de cinco años.
- Plataforma abierta.
- Ciberseguridad.
- Analíticas integradas en los productos.
- Capacitación.
- Herramientas de diseño.
- Programa de préstamo de equipo.
- Soporte técnico.
- Ecosistema amplio de socios tecnológicos e integradores.
- Enfoque en sustentabilidad.

Finalmente, tanto Convergint como Axis recomiendan a los ejecutivos de seguridad considerar los siguientes consejos antes de adquirir soluciones tecnológicas:

- Verificar la compatibilidad con normativas y estándares.

- Evaluar la escalabilidad y flexibilidad.
- Considerar la integración con sistemas existentes.
- Asegurar soporte post-implementación.
  Analizar el costo-beneficio. ■

Fotos: Mónica Ramos / SEA

Referencias:

1 Industria alimentaria. Data México. Gobierno de México 2024 https://www.economia.gob.mx/datamexico/es/profile/industry/food-manufacturing

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

Este reportaje se llevó a cabo gracias al patrocinio de Convergint y Axis Communications.

25 ANIVERSARIO
DE SEGURIDAD EN AMÉRICA

Fuente de conocimiento y actualización

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

"El éxito no se logra sólo con cualidades especiales. Es sobre todo un trabajo de constancia, de método y de organización", Víctor Hugo.

Hace 25 años surgió la revista especializada **Seguridad en América**, exactamente el 28 de septiembre de 1999, con una primera edición que sólo contaba con cuatro pliegos de información, es decir, 52 páginas en tamaño carta; hoy en día, **SEA**, fuente de conocimiento y actualización, se ha posicionado, no sólo como un medio de comunicación veraz, sino como una herramienta de aprendizaje, de profesionalización y consulta, en la que más de 50 especialistas en seguridad y sus vertientes, comparten su *expertise* y las mejores prácticas que día con día los lleva a ser los mejores líderes de esta industria.

"**Seguridad en América** no es sólo una revista informativa, es una plataforma para muchos de nuestros colaboradores y socios comerciales. Hemos desarrollado diferentes estrategias que involucran esquemas virtuales y presenciales, con la pandemia aprendimos a ser resilientes y bajo nuestro compromiso de mantenerlos siempre informados, realizamos diferentes *webinars online* que hasta la fecha continúan siendo un referente a distancia. Retomamos los Encuentros presenciales y fomentamos cada vez más la interacción en redes sociales y la web, siempre en tendencia, innovando y pensando en que la actualización es parte fundamental en esta industria", expresó Samuel Ortiz Coleman, director general y fundador de **SEA**.

Más de 500 colaboradores nacionales e internacionales han compartido sus conocimientos nacionales, reafirmando que en Seguridad no hay competencia cuando el objetivo es el mismo: salvaguardar vidas y contribuir con el bienestar del país.

"Agradecemos a nuestros socios comerciales, que confían en nosotros y la relevancia del medio en el sector. Estos 25 años son muestra de constancia, esfuerzo, y trabajo en equipo. Es un cuarto de siglo en el que he conocido grandes amigos, y sobre todo contribuir desde mi trinchera con la seguridad de todos", enfatizó Samuel Ortiz Coleman.

Gracias a quienes se tomaron el tiempo de compartir esta celebración:

t-Risk
Método de Avaliação de Riscos

TÁCITO AUGUSTO SILVA LEITE, CEO DE T-RISK–SOFTWARES PARA GESTIÓN DE RIESGOS (BRASIL)

Tengo el honor de colaborar con **Seguridad en América**, una de las revistas pioneras en el ámbito de la seguridad en América Latina. Mi experiencia con esta prestigiosa publicación ha sido sumamente enriquecedora y gratificante. **Seguridad en América** no sólo es una fuente de información invaluable sobre nuevas tendencias, tecnologías, productos y servicios en el sector de la seguridad, sino que también ha jugado un papel crucial en la profesionalización de nuestra industria.

Como colaborador y autor de artículos sobre gestión de riesgos, he tenido la oportunidad de compartir conocimientos y experiencias con una amplia audiencia de directores, gerentes y responsables de la protección de activos tanto del sector privado como público. La dedicación de **Seguridad en América** a la difusión de información relevante y actualizada ha sido fundamental para el crecimiento y la profesionalización del sector de la seguridad en nuestra región.

Es inspirador ver cómo la revista ha evolucionado a lo largo de los años, adaptándose a los cambios y necesidades del mercado, y ampliando su alcance con la versión digital que permite a más profesionales acceder a su valioso contenido. Mis deseos para **Seguridad en América** son de continuo éxito y expansión, manteniendo siempre su compromiso con la excelencia y la innovación en la industria de la seguridad.

Agradezco profundamente la oportunidad de formar parte de este proyecto y espero seguir contribuyendo al desarrollo del conocimiento y la práctica de la gestión de riesgos a través de este medio. **Seguridad en América** seguirá siendo un pilar fundamental para todos nosotros que trabajamos en pro de una sociedad más segura y protegida.

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

COSEPRI

Estimados Amigos SEA

Para mi es un gusto poder compartir con ustedes esta historia que tengo con ustedes, mi relacion con la revista se basa a hace 23 años que inicie la lectura de las revistas que me llegaban a la oficina, fueron importantes reportajes los que me ayudaron a mi trayectoria profesional, temas de seguridad patrimonial e industrial me ayudaron mucho en mi gestión que iniciaba como gerente en la empresa que trabajaba y fueron con mis actividades y con mis clientes donde pude realizar mis trabajos y asi por lo mismo a través de los años que pasaron más de 20 años, me fui al extranjero y regrese y continúe en la lectura de la revista.

Ya en los eventos de Asis y demás, me hice amigo de Samuel Coleman, la historia con él fue sorprendente, porque siempre igual que todos mis amigos de la industria, siempre ha sido muy cordial su amistad y me ha tratado genial y hemos platicado de muchos esquemas de la seguridad, para ser un confidente y amigo de la seguridad, un colega como pocos que existen en el medio, después de muchos años pero muchos fuimos haciendo la amistad más y más sólida entre los dos y hasta hoy seguimos siendo buenos compañeros.

¿Y todo empezó en el 2022 cuando me hicieron mi nombramiento de LIDER MUNDIA 2022 y le llame a SAM para contarle y me dijo, te hare una publicación en la revista, quieres??? Me pregunto y le dije si claro... mi me dio mucho gusto escuchar eso y de inmediato al próximo mes salió mi publicación de la revista y con mis fotos y el texto me agrado tanto la publicación que le pregunte si podía interactuar con la revista para hacer un artículo y una publicación y como siempre era el conmigo, me dijo si claro que si ponte en contacto con Tania flojo y adelante así inicio mi colaboración con la REVISTA SEGURIDAD EN AMERICA CON QUIEN YA CUMPLI 2 AÑOS, 2 años de otorgar todo mi expertise y mis conocimientos en varias modalidades del sector, muchos pero muchos artículos han salido de mi desarrollo, han sido dirigidos para Directores, Empresarios, Supervisores, Oficiales de Seguridad, Suplly Chain, Capacitación, habilidades para el oficial.

Seguiré colaborando más por el solo hecho de apoyar a mi gran amigo y la fabulosa ayuda de Tania que ha sido muy gratificante su apoyo en todo, agradezco mucho a la revista por su gran atención a mi persona, Felicidades por cumplir 25 años no es fácil y mucho menos sencillo, mi amigo ha sido muy exitoso y les deseo más y más triunfos y un gran camino por venir y sigan con sus Road Shows presencial que me dejan mucho, LES CUENTO QUE AUN TENGO UNA REVISTA DE HACE 23 AÑOS...gracias.

Un cordial saludos y sus órdenes.

Hermelindo Rodriguez Sánchez CPO CSSM DSI DSI DES
CEO / FUNDADOR
DIRECTOR GENERAL
CONSULTORIA EN SEGURIDAD Y PROTECCION INTEGRAL (COSEPRI)

JOSÉ LUIS SÁNCHEZ GUTIÉRREZ, DSE, DIRECTOR COMERCIAL EN GALEAM

Estimados colegas de la Revista **Seguridad en América**:

Es un honor y un verdadero placer dirigirme a ustedes en esta ocasión tan especial para felicitarles por su 25 aniversario. Como director de Seguridad Corporativa, he tenido la oportunidad de seguir y beneficiarme de su invaluable contribución al campo de la seguridad a lo largo de estos años.

Desde sus inicios, la revista **Seguridad en América** ha sido una fuente inestimable de información, análisis y tendencias en el sector de la seguridad. Su compromiso con la excelencia editorial y su dedicación para mantener a los profesionales de la seguridad informados y preparados han sido fundamentales para el crecimiento y la profesionalización de nuestra industria.

SEA no sólo ha sido un recurso educativo, sino también una plataforma que ha fomentado el intercambio de ideas y mejores prácticas entre expertos de toda la región. Gracias a su incansable labor, hemos podido afrontar con mayor eficacia los desafíos de seguridad que enfrentan nuestras organizaciones y comunidades.

En este hito de su 25 aniversario, quiero expresar mi más profundo agradecimiento y admiración por todo lo que han logrado. Su visión y liderazgo han dejado una huella indeleble en el campo de la seguridad y continúan inspirándonos a todos a seguir mejorando y adaptándonos en un mundo en constante cambio.

Muchas gracias por permitirme compartir diferentes artículos de interés para nuestros lectores, gracias por permitirme aprender de los excelentes colaboradores de esta revista especializada y número uno en el sector, gracias por permitirme exponer experiencias en los diferentes foros en los que he tenido la oportunidad de participar, simplemente gracias.

Les deseo muchos más años de éxito y prosperidad, y espero seguir viendo cómo continúan innovando y elevando los estándares de nuestra profesión. ¡Felicidades por este cuarto de siglo de excelencia y dedicación!

Con el mayor respeto y admiración.

ALEJANDRO PULIDO, CPP

Estimado Samuel:

Deseo expresar mi saludo de felicitación al alcanzar la revista 25 años de historia. Considero imperioso y oportuno resaltar el fundamental papel que ha desempeñado por un cuarto de siglo la publicación de seguridad más importante en América Latina. **Seguridad en América** es el medio donde se han acrisolado el conocimiento y la experticia de personas profesionales en busca de unificar conceptos y difundir de manera eficiente los avances, tendencias y novedades de la profesión.

Se ha convertido **SEA** gracias a un denodado trabajo, en un obligado referente para quienes buscan estar actualizados, catapultar su imagen institucional, realizar negocios corporativos o simplemente sentir el orgullo de contribuir como autor que es mi humilde caso. El derrotero se vislumbra aún mejor tutelado por el eximio grupo humano que lideras y mis mejores deseos para que sigan brillando.

RAQUEL ELÍAS GUTIÉRREZ, *MARKETING MANAGER* EN SCATI

Desde SCATI, queremos felicitar a la revista **Seguridad en América** por su 25° aniversario. Este hito significativo refleja su compromiso y dedicación al sector de la seguridad.

A lo largo de estos años, hemos tenido el privilegio de colaborar estrechamente con la revista en numerosas iniciativas que han fortalecido el sector de la seguridad. La revista **Seguridad en América** se ha consolidado como un referente informativo, proporcionando información de alta calidad y contribuyendo al crecimiento y desarrollo de nuestra industria.

En SCATI, nos dedicamos a ofrecer soluciones inteligentes de seguridad y hemos encontrado en **Seguridad en América** un aliado estratégico. Hemos participado activamente en sus eventos, patrocinado encuentros clave, contribuido en *webinars*, y publicado artículos y reportajes que reflejan nuestro compromiso con la innovación y la excelencia. Nuestras inserciones publicitarias en la revista han sido una herramienta crucial compartir nuestras innovaciones y soluciones tecnológicas con un público especializado y exigente.

Estamos orgullosos de ser parte de su comunidad y de apoyar iniciativas que promueven la seguridad y la protección. Esperamos seguir colaborando en los próximos años, impulsando juntos la innovación y la excelencia en la seguridad.

VIOLETA E. ARELLANO OCAÑA, GERENTE DE SEGURIDAD CORPORATIVA EN CIE

JAVIER NERY ROJAS BENJUMEA, MBA, CPP, *BOARD CERTIFIED IN SECURITY AND RISK MANAGEMENT*

El aniversario de un negocio es una fecha especial que merece ser celebrada y reconocida. Expresar buenos deseos en el aniversario del negocio es una forma de mostrar gratitud hacia todos aquellos que han sido parte de su crecimiento y éxito a lo largo del tiempo. Es una manera de agradecer a los clientes, empleados, socios y demás colaboradores por su apoyo y confianza.

El éxito de un negocio se sustenta en la combinación perfecta de talento, dedicación y trabajo en equipo. La habilidad y destreza de cada persona que forma parte de la empresa son clave para alcanzar metas y sobresalir en la industria, especialmente en la tarea principal de revista **SEA** que la construcción de conocimiento.

En estos 25 años los aportes de **SEA** para la industria de la seguridad en la región LATAM han sido evaluables, felicitaciones y muchos éxitos en los años por venir.

ASOCIACIÓN MEXICANA DE BLINDAJES AUTOMOTORES (AMBA)

"La AMBA y sus asociados envían a la revista **Seguridad en América** y a todos sus integrantes una cordial felicitación por estos 25 años informando y publicando acerca de la seguridad privada en sus diversos ámbitos, enhorabuena y que vengan muchos más".

CONSEJO NACIONAL DE LA INDUSTRIA DE LA BALÍSTICA (CNB)

JESÚS VARGAS, ASESOR INDEPENDIENTE Y ESPECIALISTA EN SEGURIDAD BANCARIA

Trabajé más de 30 años en Investigaciones Especiales y Seguridad en la Banca, iniciando en Banamex, posteriormente en Banco del Atlántico, continuando en Banca Serfin y culminando mi trayectoria en Banco Santander, actualmente estoy en proceso de jubilación y realizando asesorías a particulares.

Gracias a **Seguridad en América**, sigo actualizado y en contacto con todos los viejos colegas y conociendo nuevos especialistas en Seguridad. Felicidades por estos primeros 25 años de su revista.

Saludos a todos.

JULIETA MUÑOZ CORNEJO, CPP, DSE, *LOSS PREVENTION MANAGER* EN ONEST SMART LOGISTICS

Quise compartir unas palabras para esta hermosa revista porque, desde que ingresé hace 22 años en el mundo de la seguridad, siempre ha sido para mí un referente de información valiosa para mi crecimiento profesional y aprendizaje de los diferentes ramos de nuestra industria, referente de eventos, patrocinadores, asociaciones, siempre buscando sumar al gremio y mantenernos informados de una amplia gama de especialidades.

Agradezco también que, con todo este tiempo, he tenido la oportunidad de conocer a todo el equipo de trabajo de **SEA** y en ellos siempre he visto un *staff* que se entrega a su trabajo y siempre con amplia sonrisa y ánimo de aportar desde su responsabilidad.

No me resta más que desear a Samuel Ortiz Coleman y a todo su equipo, que sigan siempre siendo referentes para todos, que sigan los éxitos y que cumplan muchísimos años más. Enhorabuena equipo **SEA** y qué privilegio haber podido colaborar con ustedes cada que nos brindan esta increíble oportunidad de aportar en sus publicaciones, a nuestra industria. ¡Feliz aniversario!

JORGE AQUINO PALOMINO, ACCIONA

"Estimado Samuel:

Muchas felicidades por los 25 años de tu gran revista, por medio de la cual me mantengo actualizado de la diversidad de noticias del mundo de la seguridad".

CHRISTUS MUGUERZA
Sistema de Salud

FRANCISCO VILLEGAS, CPP, *CHIEF SECURITY OFFICER* EN CHRISTUS MUGUERZA

Felicitamos a la Revista **Seguridad en América** por su 25 aniversario. Nos llena de orgullo reconocer su destacada trayectoria como un referente en el ámbito de la seguridad en México. Les deseamos muchos más años de éxito y dedicación en su invaluable misión de mantener a nuestro sector bien informado. ¡Que sigan los éxitos!

OMAR BALLESTEROS, DIRECTOR EJECUTIVO EN BALLESTEROS Y BARRERA SERVICIOS DE PROTECCIÓN

¡Saludos, amigos!

¿Cómo están? Es un placer como siempre comunicarme con ustedes a través de esta magnífica revista que es **Seguridad en América**.

Les quiero compartir una anécdota que me sucedió la vez que tuve que ir a la Ciudad de México para recibir mi reconocimiento como partícipe de mis columnas, sucedió entonces que llegando a la Ciudad me detuvo una patrulla de la policía, y me hizo la observación de que tenía placas foráneas, para entonces yo ya había entrado desde las 08:00 de la mañana a la Ciudad de México, sin embargo por mis placas debería haber entrado hasta después de las 11:00 am, lo cual no sabía, por esa razón me querían multar y en su caso hasta me querían quitar la unidad.

Como suele pasar, se me ofreció una alternativa y fue que me pidieron una mordida, para que no me quitaran mi camioneta. Cuando llegué a la revista tuve una entrevista con el gran amigo Samuel y le comenté lo que me había sucedido, le dije que me habían desplumado, algo muy habitual cada vez que voy a la Ciudad de México, porque con esa ocasión ya eran tres veces, Samuel amablemente se ofreció a apoyarme y le agradecí con el corazón, porque en realidad me había quedado sin dinero.

Cuando te pasan esas cosas solamente te queda reír, agradezco enormemente a la revista **Seguridad en América** que me dé la oportunidad de participar con ellos con mis dos columnas: "El Silencio Habla" y "El Tigre Tiene Rayas".

Les mando todas mis bendiciones y les deseo siempre el mayor de los éxitos a todos sus colaboradores y en especial a su director general, el Lic. Samuel Coleman Coleman.

GA Gigi Agassini

GIGI AGASSINI, CPP, INTERNATIONAL SECURITY CONSULTANT

Con sumo placer y profunda gratitud, me permito expresar mi más sincero agradecimiento a **Seguridad en América** por la oportunidad brindada de colaborar en la producción de contenido especializado para la industria de la seguridad.

A lo largo de nuestra colaboración, ha sido un honor contribuir con artículos que abordan las temáticas más relevantes y emergentes en el ámbito de la ciberseguridad, privacidad, la seguridad física y la gestión integral de riesgos empresariales. Este medio digital se ha distinguido por su compromiso inquebrantable con la excelencia editorial y la difusión de conocimientos críticos que promueven la resiliencia y la seguridad en un entorno global cada vez más complejo.

Deseo destacar que la experiencia de trabajar con un equipo editorial tan profesional y dedicado

ha sido verdaderamente gratificante. La sinergia creada ha permitido no sólo la elaboración de contenido de alto valor, sino también el fortalecimiento de un espacio de intercambio y crecimiento continuo para todos los involucrados.

Es para mí un honor ser parte del crecimiento y desarrollo de **Seguridad en América**, y celebro con entusiasmo el aniversario que conmemora su trayectoria y aportes significativos a la industria.

Confío en que nuestra colaboración continuará prosperando, y reitero mi disposición a seguir contribuyendo con el mismo fervor y dedicación que nos han caracterizado hasta ahora.

Con mi más sincero reconocimiento y estima.

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

GABRIEL BERNAL GÓMEZ, PRESIDENTE DE AMESP

Samuel Ortiz Coleman:

Para la Asociación Mexicana de Empresas de Seguridad Privada (AMESP) es motivo de celebración el 25 aniversario de tan prestigioso medio de comunicación como lo es la revista **Seguridad en América** que usted dirige con admirable profesionalismo.

En este tiempo, la revista se ha consolidado como un medio con credibilidad, objetividad y confiabilidad en el periodismo especializado en un tema tan importante como lo es la seguridad. Sean extensivas nuestras congratulaciones a todo el equipo que colabora en **Seguridad en América** y a quienes a través de estos años han hecho posible el éxito de la revista.

¡Enhorabuena y que vengan muchos años más de éxito!

Para la AMESP es un orgullo representar a una industria cuya actividad equivale al 1.5% del PIB y emplea a más de 800 mil personas y, a la vez, hacer sinergia con la revista más importante del sector.

GABRIEL ESTEBAN ESCOBAR GONZÁLEZ, DIRECTOR EJECUTIVO DE SEGURIDAD CORPORATIVA EN GRUPO ARMSTRONG

A nuestra querida revista: ¡Feliz aniversario 25!

Es un honor y orgullo formar parte de algunas de tantas anécdotas, experiencias, eventos, encuentro con colegas, entrevistas, artículos, crónicas, y un sinfín de momentos captados en nuestra revista a lo largo de 25 años y los que vienen.

Gracias a todo el equipo que lidera nuestro querido amigo Samuel Ortiz Coleman, un gran visionario y profesional de la seguridad que impulsa cada vez más la integración del gremio y que lo hace desde un enfoque de intercambio de opiniones, con alternativas de interacción con calidad humana.

SEA se congratula como un medio vigente y vanguardista ¡Enhorabuena!

MERCEDES ESCUDERO CARMONA, DIRECTORA ELECTA DEL BOARD EJECUTIVO DE LA INTERNATIONAL CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

Metepec, Estado de México, a 11 de julio del 2024.

Estimado Samuel Ortiz Coleman DSE
Presidente de la Revista Seguridad en América

Presente

Querido amigo, me es grato felicitarte a ti y a todo el equipo de trabajo que hace posible cada edición de tan importante medio de comunicación, que ha logrado llegar a ser un gran referente de la información del sector de la Seguridad en México y Latinoamérica.

No solo se conmemoran 25 años de servicio, sino también de pasión, dedicación y compromiso. Gracias por crear un espacio que construye conexiones, deja un legado y huellas en los corazones. Agradecida y honrada por pertenecer al grupo de colaboradores que comparten conocimiento y experiencias en Seguridad en América.

Que sean muchos años más. Felicidades.

Dra. H.C. Mercedes Escudero Carmona
Presidente de CPTED México ICA Chapter y
Directora General del CESCH MX

cpted.mexico@gmail.com y centro.scsh@gmail.com

CARLOS MARTÍNEZ, PRESIDENTE DE ALAS COMITÉ NACIONAL MÉXICO

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD | Comité Nacional MÉXICO

Ciudad de México a 28 de septiembre del 2024

Revista Seguridad en América

Director General, Lic. Samuel Ortiz Coleman,

Presente.

Por medio de la presente y en nombre ALAS Internacional (Asociación Latinoamericana de Seguridad) comité México queremos enfocar una Felicitación a la revista Seguridad en América por este veinticinco aniversario, así como extender una felicitación a su líder y director general Lic. Samuel Ortiz Coleman y su equipo de profesionales quienes a lo largo de todos estos años han logrado ser un referente en la industria de la seguridad.

Quiero agradecer el gran apoyo que en todo momento hemos recibido de su parte como medio aliado y la difusión que siempre han dado a nuestros eventos así como la difusión de noticias trascendentales y tendencias de innovación, brindado siempre un espacio para compartir opiniones como asociación líder en la industria de la seguridad electrónica en nuestro país México, lo cual nos ha ayudado a lograr de manera muy eficiente y satisfactoria ampliar la red de asociados y compartir los logros y novedades de una manera más puntual y efectiva.

Particularmente para mí, es un honor el poder extender esta carta de felicitación en un aniversario tan importante. Muchos triunfos, logros, éxitos y todas para siempre en Seguridad en América. Que continúen los éxitos a sumar muchos años más aportando a este tan amado gremio de la seguridad. ¡Muchas felicidades! en hora buena.

Atentamente.

Carlos Martínez Sánchez

Presidente comité México 2024

RICARDO NAVA RUEDA, "*LOST BOY*", DIRECTOR DE DIFUSIÓN Y RELACIONES PÚBLICAS DE LA ASOCIACIÓN MEXICANA DE NIÑOS ROBADOS Y DESAPARECIDOS, A.C.

Antes que nada y como siempre muchas gracias por la oportunidad de colaborar en la revista SEGURIDAD EN AMÉRICA.

Hace años tenía el sueño de compartir o plasmar las experiencias personales y recomendaciones en prevención y reacción para el tema de personas desaparecidas, Dios me cumplió mis sueños, a través de la revista SEGURIDAD EN AMÉRICA, las experiencias acumuladas a lo largo de 34 años en el grupo NUESTRO OBJETIVO ES BRINDAR AYUDA, la ASOCIACIÓN MEXICANA DE NIÑOS ROBADOS Y DESAPARECIDOS, el PROYECTO ENCUENTRA ME DE SEGURIDAD POR MÉXICO y el CONSEJO CIUDADANO DE LA COMISIÓN DE BÚSQUEDA DEL ESTADO DE MORELOS, entre otros me ha permitido compartir a través de la prestigiada revista a lectores mis ideas, de igual manera el compartir los artículos con grupos relacionados a la búsqueda de personas, autoridades correspondientes y al público en general estos temas, mismos que han servido para tomar acciones preventivas, lo más agradable es el que me feliciten, hace unos días fui a la ACADEMIA DE FORMACIÓN ESPECIALIZADA DE ESCOLTAS Y GUARDA ESPALDAS (AFEEG), para ver unos temas y me mostraron un ejemplar donde viene una colaboración mía, les dio gusto doble, por el tema de la colaboración y porque también formo parte de la AFEEG.

Nuevamente gracias SAMUEL ORTIZ COLEMAN, SEGURIDAD EN AMÉRICA por la oportunidad de colaborar.

"ESTA LUCHA NO TIENE SIGLAS, NO TIENE COLORES Y NO TIENE RELIGIÓN, LA BÚSQUEDA ES DE TODOS".

Dr.H.C.Ricardo Nava Rueda.

"LOST BOY"

Dr. H.C. Ricardo Nava Rueda LOST BOY

Firma Dr H.c.c Ricardo nava

MARTHA BEATRIZ MANRIQUE GÓMEZ, SOLUCIONES BALÍSTICAS

El 15 de enero de 1998, comencé a trabajar en lo que antes era el Distrito Federal. Íbamos a iniciar la empresa de BETA, Blindajes Especializados Tame, S.A. de C.V. (BETA). No recuerdo muy bien la fecha exacta, pero casi segura que era final de mayo cuando llegaron a la planta en la Calle de Urbina en Naucalpan, Estado de México, Lino Monroy y Samuel Ortiz Coleman. Los dos trabajaban en Ventas para otra empresa de blindaje, ULTRA, propiedad del señor Kociankowski, lo recordaré siempre por su forma "intimidante" de vender seguridad.

Estuvimos hablando de varias cosas, proyectos, la situación en Colombia y ellos me comentaban de la situación de la ciudad y el país hasta ese momento. Éramos jóvenes, ellos aún más que yo, y poco nos importó el que aún no tuviera la planta equipada con una oficina donde poder sentarnos.

Samuel comentó la idea de crear una revista especializada en seguridad, y creo que, para la siguiente visita, ese mismo año, ya pude ver unos bocetos de la misma y luego su primer ejemplar.

Con el tiempo fue creciendo y para el 2004 con la primera edición de mi evento, LAS AMERICAS SECURITY SHOW, el directorio del evento, formaba parte de la revista, después, se manejó como un inserto para los siguientes eventos. Siempre tuve su apoyo incondicional como persona y equipo y le estaré inmensamente agradecida.

Su consolidación en el mercado de las Revistas de Seguridad, la ha llevado a la vanguardia de las mismas y hoy día su presentación y contenido, reflejan la evolución, el avance y trabajo de Samuel y su equipo.

¡Muchísimas felicidades **SEA** y que festejen muchos años más!

VIVOTEK

¡Enhorabuena a **Seguridad en América** por sus 25 años de excelencia! Celebramos un cuarto de siglo de compromiso inquebrantable con la seguridad y la protección en nuestro continente. Son una fuente veraz y oportuna de información sobre nuevas tecnologías, soluciones y servicios que contribuyen a mejorar un entorno seguro para la sociedad. Gracias por la visión vanguardista y dedicación a la industria de la seguridad en América. ¡Por muchos años más de éxito e innovación informativa!

BOLIDE

BOLIDE TECHNOLOGY GROUP

En **Bolide Technology Group**, reconocemos la importancia de mantenernos informados y actualizados en el siempre cambiante mundo de la seguridad electrónica y la tecnología de la información. Por ello, queremos expresar nuestras más sinceras felicitaciones a revista **Seguridad en América** por sus **25 años** de arduo trabajo, dedicación y compromiso con la difusión de información relevante y de alta calidad.

Durante estos años, **Seguridad en América** ha demostrado ser un pilar fundamental en la industria, brindando a sus lectores artículos de profundidad, análisis detallados, y una visión clara de las tendencias y avances tecnológicos que moldean el futuro de nuestra seguridad. Su contribución ha sido invaluable para profesionales y empresas que buscan mantenerse a la vanguardia, garantizando que estemos mejor preparados para enfrentar los desafíos del mañana. Compartimos su pasión por la innovación y la excelencia. Nos sentimos honrados de ser parte de esta comunidad y de poder colaborar con una publicación tan prestigiosa. Estamos seguros de que los próximos años traerán aún más éxitos y contribuciones significativas a nuestra industria.

Felicitamos nuevamente a todo el equipo de **Seguridad en América**, en especial a **Samuel Ortiz Coleman**, **Presidente** de la revista, por este logro monumental y esperamos seguir viendo su impacto positivo en el sector durante muchos años más.

Alex Salinas
Vice President
Bolide Technology Group

www.bolideco.com

ARMANDO GARCÍA SÁNCHEZ, DSI, SFC, GERENTE DE CONSULTORÍA EN TIMUR LATINOAMÉRICA

¡Feliz 25 Aniversario, **Seguridad en América**!

Quiero felicitar afectuosamente a la Revista **Seguridad en América** por otro año de éxito y dedicación. A lo largo de estos años, han sido un pilar fundamental en la difusión de información actual y relevante para el gremio de la seguridad privada, ya que a través de sus artículos, entrevistas e información destacada podemos conocer personas expertas en diversas ramas de la seguridad e información que resulta un verdadero valor agregado para quienes nos dedicamos a esta bella profesión de la Seguridad integral.

La primera edición que leí fue una del año 2011, una edición de Seguridad en Aeropuertos, y desde entonces no dejé de leerla. Gracias por su compromiso inquebrantable con la excelencia y por ser una fuente confiable de conocimiento y actualización para todos los profesionales del sector. Su labor ha sido esencial para mantenernos informados y preparados ante los desafíos de la seguridad en nuestro país.

¡Les deseo muchos más años de éxitos y logros! Que continúen siendo un referente en la industria y sigan inspirando a todos con su pasión y profesionalismo.

¡Felicidades Samuel Ortiz Coleman y, por supuesto, a todo tu equipo tan apasionado, que sigan los éxitos! ■

GSI
SEGURIDAD PRIVADA

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

Profesionales en Seguridad Privada

Oficiales de Seguridad

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

SOMOS GRUPO GSI,
Orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx

atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

ESR Empresa Socialmente Responsable · redconocer · DNV · AMESP · Empresas de GSI Grupo Seguridad Integral · BAC

FRAUDE BANCARIO EN AUMENTO. ¿CÓMO PREVENIRLO?

En 2023 hubo 8 millones de quejas referentes a fraudes financieros, de las cuales 71% fueron por engaños realizados en Internet, y el 29%, por defraudaciones de forma tradicional

Foto: Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

En marzo del presente año, un hombre de 32 años y una mujer de 30, acompañados de sus dos hijos menores de edad, fueron detenidos por la Policía Municipal de Nezahualcóyotl, Estado de México, ya que se dedicaban a colocar trampas en los cajeros automáticos de sucursales bancarias de la zona centro de dicho municipio.

El *modus operandi* consistía en que el hombre ingresaba a los cajeros y colocaba reglas metálicas en el dispensador de los billetes, mientras la mujer y sus hijos lo esperaban en la puerta para prevenirlo en caso de la presencia de las autoridades. Precisamente uno de los empleados de estas sucursales bancarias, quien fue víctima de los dichosos delincuentes, fue quien dio aviso a las autoridades, las cuales comenzaron con una detallada investigación hasta realizar el operativo que culminó en la captura de Luis Enrique "N", y Brisa Itzel "N"[1].

De acuerdo con la Encuesta Nacional de Seguridad Pública Urbana (ENSU) del primer trimestre de 2024, el 61.0% de la población a nivel nacional de 18 años y más, consideró inseguro vivir en su ciudad. En cuanto a la "percepción de inseguridad en espacios físicos específicos", el 69.4% de los habitantes, manifestó sentirse inseguro en los cajeros automáticos localizados en la vía pública; 63.9 %, en el transporte público; 53.9 %, en la carretera y 53.5 %, en el banco[2].

Cada vez son menos los robos dentro de sucursales bancarias, de hecho, año con año ha habido una notoria reducción de estas malas prácticas; información de T Research International, agencia especializada en estudios de opinión, en enero-febrero ocurrieron 29 robos a bancos disminuyendo 12% en comparación al mismo periodo del año anterior.

Así como otras industrias se han traslado y adaptado a la tecnología actual y la demanda de los servicios en línea, la banca también lo ha hecho, y tanto ahí como en los ATM (*Automated Teller Machines*–Cajeros Automáticos), en donde está presentando los mayores riesgos de seguridad.

PRINCIPALES AMENAZAS

En marzo del presente año, la Asociación de Bancos de México (ABM), con base en información de la Comisión Nacional Bancaria y de Valores (CNBV), informó que, hasta ese periodo, se registraron 87 millones de usuarios de banca móvil en el país, presentando un crecimiento de 200% en los últimos seis años.

"En la actualidad, los principales riesgos en materia de seguridad son los delitos cibernéticos, cada vez son más frecuentes los casos de transferencias bancarias no reconocidas por *phishing*, así como los casos de robo o secuestro de información a las instituciones financieras por *ransomware*, y a nivel doméstico, los casos de fraudes o robos en cajeros automáticos y la usurpación de identidad", comentó en entrevista Pedro Villanueva, director de Prevención de Fraudes en Seguridad y Protección Bancaria, S.A. de C.V. (SEPROBAN).

Por su parte, Selene Molina, gerente *Sr.* de Seguridad en BanCoppel, agregó que los principales riesgos y problemáticas que han estado analizando los especialistas en seguridad desde finales de 2023 y 2024, son los relacionados con información sensible que vive en el ciberespacio, así como el desconocimiento de los usuarios de la banca y el cómo proteger dicha información.

Foto: Freepik

"Las instituciones financieras son el sector más afectado a nivel mundial según datos de Deloitte, y en el último año, el 70% de estos ataques han tenido éxito", Selene Molina

"El principal problema o riesgo de seguridad en los cajeros automáticos en México, es el robo de la tarjeta mediante el engaño por la delincuencia organizada", Pedro Villanueva

pvillanueva@seproban.com.mx www.seproban.com.mx
www.linkedin.com/in/pedro-villanueva-melendez-94b66662/

ESTRATEGIAS DE SEGURIDAD EN ATM'S

Una de las estrategias que ayudan a reducir riesgos, no sólo a este sector sino en general, es fomentar la cultura de seguridad en colaboradores. "Hoy en día, el principal problema o riesgo de seguridad en los cajeros automáticos en México, es el robo de la tarjeta mediante el engaño por la delincuencia organizada que intercambia la tarjeta y engaña a los clientes y o usuarios, afectando su patrimonio", indicó Pedro Villanueva, y compartió las siguientes recomendaciones para los usuarios de los ATM's:

1) No perder de vista la tarjeta o dispositivo con el cual están realizando su operación en el cajero automático.
2) No permitir el apoyo, asesoría o distracción de cualquier persona ajena a la institución bancaria.
3) Verificar que en el cajero automático no existan objetos extraños que impidan ingresar la tarjeta o retirar dinero.
4) Validar que en el cajero automático existan cámaras de videovigilancia y realizar sus operaciones, en medida de lo posible, en horarios diurnos.

Selene Molina señaló que, de acuerdo con datos oficiales de la incidencia a nivel banca de 2023 y 2024, los principales el robo a cuentahabiente, y los constantes "desplazadores", sujetos que utilizan diversos métodos de engaño para confundir al usuario de cajeros automáticos e intercambiar o robar su tarjeta y su información personal para posterior a esto, vaciar sus cuentas.

"De acuerdo con los datos en enero 2024, tuvimos un aumento del 26% de eventos de robo a tarjetahabientes comparado con enero de 2023, en ese mismo sentido tuvimos un decremento en los eventos de asalto bancario (-28%), robo ATM's (-59%), y robo a cuentahabiente (-31%), lo que nos confirma que los eventos de robo de tarjetas e información de usuarios cuando hacen uso de los cajeros automáticos va en aumento; esto también relacionado con lo complicado que se vuelve para la institución involucrada y la autoridad, poder hacer ejercicios de la acción penal en contra de estos sujetos, ya que necesitamos la denuncia del titular del plástico y/o afectado que en la mayoría de los casos no le interesa interponer una denuncia penal, lo que favorece a los delincuentes".

Y externó que a nivel banca, cuentan estrategias de monitoreo e identificación de estas bandas, mientras que a los usuarios les hacen llegar recomendaciones para evitar estos robos y fraudes, mediante trípticos, anuncios y carteles con leyendas como: "No aceptar ayuda de un extraño", "no compartir información de NIP o claves con nadie", "si identificas alguien en el cajero que te resulte sospechoso, no realices tu retiro y repórtalo a la institución y/o autoridad", entre otras.

CIBERDELINCUENCIA

Pedro Villanueva cuenta con una larga trayectoria en temas de fraudes y ciberdelitos en la banca, actualmente considera que las amenazas de *ransomware* y *phishing* son las más frecuentes y de alto impacto, por ello se deben realizar respaldos de la información con mayor frecuencia y crear mecanismos de prevención y alertamiento en las áreas operativas y hacia a los clientes y usuarios de la banca móvil para evitar fraudes cibernéticos.

De acuerdo con información de la Condusef (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros), en su reporte "Fraudes (financieros) cibernéticos y tradicionales", emitido a través del Portal de Fraudes Financieros[3], las quejas por este tipo de robo, llegaron a 5 millones 762 mil 195, un aumento de 20.1% con respecto al año anterior.

El mismo portal refiere a que en 2023 hubo 8 millones de quejas referentes a fraudes financieros, de las cuales 71% fueron por engaños realizados en Inter-

Foto:–Freepik

net, y el 29%, (alrededor de 2.3 millones de reclamaciones), por defraudaciones de forma tradicional.

"Las instituciones financieras son el sector más afectado a nivel mundial, según datos de Deloitte, y en el último año, el 70% de estos ataques han tenido éxito. Esto claramente ha ido en aumento desde 2019 donde la pandemia por COVID-19, obligó a todos los sectores y personas en el mundo a digitalizarse. Tomando este evento como punto de inflexión, los bancos han tenido que obligarse a una transformación digital, que permitan al usuario utilizar todos los servicios que antes se brindaban únicamente en una sucursal física", comentó Selene Molina, y compartió, de acuerdo con su *expertise*, las principales amenazas cibernéticas para las instituciones financieras:

1) Generación, transferencias, resguardo y almacenamiento de datos personales y confidenciales de los usuarios.
2) Uso de tecnologías emergentes con el objetivo de mejorar la experiencia del cliente en la banca móvil, ya que son un arma de doble filo, mejoran y hacen novedosa la experiencia del cliente, pero pueden ser puertas potenciales para terceros maliciosos.
3) Robo de datos por *hackers*, esto genera desconfianza a nivel mundial de los usuarios, un ataque de *ransomware* a un banco, en la mayoría de los casos, tiene el objetivo de exigir un pago a la institución para su devolución íntegra, algo como un secuestro virtual de datos.

Referente a las entidades bancarias, los especialistas hacen las siguientes recomendaciones en dado caso de enfrentar un ataque cibernético:

- **Preventivas**

1) Conocimiento de vulnerabilidades y puntos fuertes en cuanto a la seguridad previo a cualquier evento consumado o tentativa.
2) Capacitación del personal interno y del usuario de la banca.
3) Actualización constante de sistemas y *software* y cifrado de datos.
4) Contar con un *Business Continuity Plan* y llevar a cabo prácticas o simulacros constantes mínimo cada cuatro meses
5) Establecer y sesionar con un "Comité de Crisis" donde esté plenamente definido e identificado el rol de cada uno ante un evento que pudiera poner en riesgo la continuidad del negocio.

- **Reactivas**

1) Reacción inmediata.
2) Respaldo de la información.
3) Cadena de custodia del incidente cibernético.
4) Alertamiento y denuncia a las autoridades.
5) Protección perimetral de la infraestructura de TI.

IDENTIFICACIÓN DE RIESGOS Y NUEVAS AMENAZAS

En Seguridad cada día es diferente y los riesgos van cambiando, la delincuencia va construyendo nuevas herramientas y estrategias para lograr sus cometidos, es por eso que los responsables de esta área se encuentran en constante capacitación para estar a la altura de los problemas.

"La preparación y colaboración entre expertos de seguridad de las instituciones es muy importante, así como estar al día con las necesidades y tipos de incidencias en nuestro país y a nivel internacional, donde en muchos de los casos, países como España, Estados Unidos y Brasil siempre llevan la delantera en soluciones y buenas prácticas por tipos de incidencias para usuarios de la banca digital y física", comentó Selene Molina.

Y agregó que la colaboración entre expertos de seguridad bancaria es una estrategia que en el país

han trabajado mucho, siempre apegados a las diferentes normativas que los regulan, esto ha contribuido a identificar las diferentes problemáticas de la banca en la actualidad, colaborando y reforzando esas áreas de oportunidad, trabajando en conjunto para investigación, detención y judicialización de los delincuentes, lo que los ha llevado a mejorar la reacción y disminuir el tipo de delitos, así como para prevenir y reaccionar ante cualquier evento que afecte a usuarios de los servicios financieros sin importar la institución a la que pertenezca.

Pedro Villanueva también recomendó que, para identificar nuevas amenazas, es importante realizar un adecuado análisis de riesgos para evaluar la probabilidad e impacto, así como su debida atención a las nuevas tendencias tecnológicas que podrían afectar en los procesos y servicios de la banca.

Y precisamente sobre las tendencias tecnológicas, fue necesario tocar el tema del uso de la Inteligencia Artificial para realizar fraudes bancarios, a lo cual los especialistas comentaron que, la IA es la realidad actual de la civilización humana, y no es algo a lo que podamos resistirnos o negarnos, es algo inminente.

"Toda acción o movimiento diario que tenemos implica un riesgo que debemos asumir en diferentes medidas y situaciones, por lo que lo único en lo que podemos enfocarnos es en conocer esos riesgos y estar preparados para atenderlos y que su impacto sea el menor posible. A nivel banca, el riesgo aumenta y está enfocado en los datos y patrimonio de los usuarios por lo que es muy importante que todos los participantes, tanto del banco como el usuario, se capaciten y tengan conocimiento de los riesgos, y sepan qué se debe hacer en caso de un evento y qué no debe hacer", indicó Selene Molina.

QUE NO TE PASE

La pandemia por COVID-19 aceleró el uso de la banca digital, pero no por ello, los usuarios han comprendido o tienen en cuenta los riesgos a los que están involucrados si no se informan sobre temas de seguridad. Los especialistas enumeran las siguientes medidas para el uso correcto del SPEI (transferencia electrónica):

1) Uso responsable, no compartas tus datos de cuentas con cualquier persona, toma precaución al dar de alta o realizar transacciones a personas desconocidas.
2) Contar con antivirus.
3) Actualización de su banca en línea cuando sea necesario.
4) No utilizar redes públicas cuando se pretenda utilizar su *app*.
5) Atender las recomendaciones de seguridad de cada institución que hace llegar por diversos medios.
6) Si tienes cualquier duda o sospecha, detente y llama a tu banco.
7) Validar que las operaciones de transferencia electrónica, se realicen desde el origen y hacia al destinatario correcto.
8) Usar un doble o múltiple factor de autenticación de sus transferencias.


Foto: Freepik

SEPROBAN

La colaboración entre especialistas de seguridad de las instituciones financieras, autoridades y otras instituciones como SEPROBAN, contribuye a la seguridad de la banca. "La Sociedad de Apoyo de Seguridad y Protección Bancaria es el enlace con estas entidades para mitigar, prevenir fraudes y delitos de alto impacto que pueden afectar a las Instituciones Financieras en el país. Por lo cual es un elemento importante de enlace con las instituciones financieras, al igual que con las autoridades, para la denuncia y la atención inmediata de las incidencias o amenazas que se puedan presentar. Un punto clave en el que estamos trabajando para identificar, prevenir y mitigar este tipo de vulnerabilidades, es la constante búsqueda y alertamiento de riesgos potenciales y emergentes para el sector financiero", finalizó Pedro Villanueva. ■

Referencias:

1 "Se dedicaban a robar en cajeros automáticos acompañados de sus hijos en Edomex", María de los Ángeles Velasco. Excélsior, 21/03/2024 https://www.excelsior.com.mx/comunidad/robo-cajeros-automaticos-hijos-nezahualcoyotl-edomex/1642426

2"Encuesta Nacional de Seguridad Pública Urbana (ENSU)", INEGI, 18/04/2024 https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/ENSU/ENSU2024_04.pdf

3 Portal de Fraudes Financieros. Condusef. https://phpapps.condusef.gob.mx/fraudes_financieros/informate.php

NUEVO PERFIL DE GUARDIAS Y PROTECCIÓN EJECUTIVA

Comunicación asertiva, trabajo en equipo, conocimientos generales de seguridad, respuesta a emergencias, conocimientos de softwares maliciosos y ciberseguridad, son sólo algunas características del EPE actual

Foto:–Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Actualmente existen 7 mil quinientas cincuenta y cinco empresas de seguridad privada registradas en el Instituto Mexicano del Seguro Social (IMSS), y el número de empleos generados por esta industria son aproximadamente 915 mil, de los cuales la mitad son ocupados por guardias (450 mil). A su vez, este sector aporta el 1.9 por ciento al Producto Interno Bruto del país, y dada la inseguridad que se vive en la actualidad, se prevé que continúe creciendo.

A lo largo de los años, la delincuencia se ha organizado y actualizado, hasta capacitado, respecto a nuevas estrategias y tecnologías para robar, secuestrar, extorsionar y defraudar a los ciudadanos, por lo que, tanto guardias, como elementos de protección ejecutiva, cada día buscan soluciones que ayuden a contrarrestar estos problemas, uno de ellos, la capacitación y actualización.

EL AGENTE DE PROTECCIÓN EJECUTIVA Y EL PRINCIPAL

La Protección Ejecutiva involucra no sólo al personal operativo, sino también al principal y a quien lo envía, así como ciertas consideraciones sobre su familia, círculo social, trabajo, motivo de la visita, entre otras. Pero en quien recae la seguridad de los involucrados, es directamente en el elemento de protección ejecutiva.

Héctor Robles Conde, *President of Latam and VP of Global Operations* en FirstCall CSS, cuenta con una larga trayectoria y experiencia reconocida en esta vertiente de la seguridad privada, recientemente impartió una conferencia magistral en uno de los *roadshows* que organiza **Seguridad en América Academy**, en la que explicó cuál es el perfil, requisitos, habilidades y conocimientos que debe tener un elemento de Protección Ejecutiva, información que compartimos en este reportaje y que está basada en el perfil que presenta la IFPO (Fundación Internacional para Oficiales de Protección - http://ifpo.es/recursos-para-reclutadores/).

"La Protección Ejecutiva es un esfuerzo colaborativo que involucra tanto al principal como a su equipo de seguridad. La comunicación y coordinación regulares son esenciales para un programa de seguridad exitoso. Es recomendable involucrar a expertos en seguridad en el proceso de capacitación para garantizar un programa y política corporativa de seguridad completa y eficaz", explicó.

En principio, el especialista considera que, para tener un servicio de protección ejecutiva exitoso, se debe partir de crear programas y políticas corporativas de seguridad que van a regir el desarrollo de éste, y eso lo debe conocer el principal y su equipo.

Héctor Robles Conde mostró cuáles son los requisitos para ser especialista en protección de personas, algunos de ellos son:

- Experiencia comprobada y específica, en cargo de: protector/ escolta/ resguardo/ especialista en protección a ejecutivos.
- Experiencia general en seguridad, que incluye uso de tecnología y equipos relevantes, planificación de informes, y respuesta a emergencias.
- Conocimientos como generalista de Seguridad.
- Conocimiento y dominio de los protocolos y procedimientos de seguridad.
- Conocimiento de las pautas legales para la protección a ejecutivos.
- Buena comunicación, habilidades interpersonales; toma ética de decisiones, comprometido y confiable.

"Hay que partir desde los conocimientos generales de seguridad, es decir, no ser especialistas en cada uno, pero sí manejar con asertividad estos temas: manejo de riesgos, legalidad y normatividad, seguridad del personal y continuidad del negocio, seguridad física,

Enrique Tapia Padilla, MA, CPP, socio director en Altair, Security Consulting & Training

Héctor Robles Conde, President of Latam and VP of Global Operations en FirstCall CSS

ciberseguridad, gestión de crisis, investigaciones, administración de casos, conocer de globalización y conciencia cultural, gobernanza, cómo respeto las políticas de la empresa. No todo es contravigilancia y avanzada. El objetivo de la protección ejecutiva es asegurar la integridad y la disponibilidad de nuestros ejecutivos, y para ello debe tener presente todos estos temas", puntualizó.

Comentó que las acciones que cada persona tenga, soportan todos sus conocimientos, lo que has hecho, haces y vas a hacer; por ello la capacitación y sobre todo en temas de seguridad, es sumamente relevante, no cualquier persona puede tiene las habilidades que se requieren, ni los conocimientos y destrezas, y ejemplificó algunas de estas últimas:

- Conocer los fundamentos de seguridad.
- Conocer los fundamentos empresariales.
- Tener pensamiento crítico y analítico.
- Aunque parezco algo obvio, no se puede dejar de lado tener la certeza de que el elemento sabe leer y escribir.
- Alfabetización STEM (Ciencia, Tecnología, Ingeniería, Matemáticas).
- Trabajo en equipo.
- Planificación y organización.
- Pensamiento estratégico.
- Resolución de problemas y toma de decisiones.
- Trabajo con herramientas y tecnología.
- Visión para los negocios.

"Existe también otro aspecto que debe tener el elemento de protección ejecutiva (EPE), actitudes generales de seguridad: por un lado, interpersonales y, por otro, saber trabajar en equipos de seguridad; integridad, profesionalismo, a veces es mejor permanecer callados y sonreír más; tener iniciativa, adaptabilidad y flexibilidad, confiabilidad, confidencialidad, empatía, diplomacia, conciencia cultural, y muy importante saber cómo tener una comunicación eficaz".

Explicó también algunos de los conocimientos del EPE actual:

- Seguridad del personal y continuidad del negocio.
- Trabajo de avanzada adecuado.
- Conocer las regulaciones y leyes por jurisdicción, las pautas sobre el uso de la fuerza.
- Aplicar los estándares éticos de la industria.
- Conocer y contar con tecnología de seguridad (GPS, rastreo, electrónica), vigilancia y contravigilancia.
- Saber y mantenerse actualizado en temas de ciberseguridad e inteligencia artificial.

La seguridad nunca es igual al día anterior, y siempre enfrenta retos diferentes conforme todos los factores a su alrededor suceden. El nuevo perfil del EPE requiere actualizarse no sólo en técnicas y estrategias de protección, de prevención, avanzada, sino también en temas sociales, políticos, contextuales sobre su principal y los lugares donde el servicio se llevará a cabo, así como de su círculo social y familiar. De acuerdo con el especialista, los siguientes aspectos son ahora fundamentales para tener éxito:

- Administrar equipos pequeños o individuales.
- Técnicas de recopilación de información.
- Evaluación de riesgos de PE (Protección Ejecutiva).
- Mantener la información segura.
- Prácticas de transporte / vehículo seguro.
- Principios de prácticas de operaciones tácticas.
- Respuesta médica primaria.
- Movimientos para mantener la seguridad.
- Gestión de incidentes.

Héctor Robles Conde enfatizó en la importancia de mantener una comunicación asertiva y constante con el principal, ya que esto ayudará con la seguridad de ambos. No se requiere establecer más lazos, sólo una comunicación directa y coordinada. Algo que se debe saber del principal son los riesgos personales y familiares; hacerle saber de estos y crear en él una consciencia situacional personal de seguridad, así como una sensibilidad cultural. Y el EPE debe contar con una buena condición física y estar saludable, así como realizar actualizaciones de forma regular.

Foto:–Freepik

LA PROTECCIÓN EJECUTIVA EN ENTORNOS DIGITALES

Actualmente el uso de medios tecnológicos como computadoras o teléfonos celulares son parte de la vida cotidiana de las personas, así como las redes sociales y otras plataformas de entretenimiento que puedes visualizar desde este dispositivo inteligente, los elementos no son ajenos al uso de estas, es por ello que es importante sensibilizarlos sobre los riesgos a los que están expuestos en los medios tecnológicos, proporcionando sencillas medidas de prevención y actuación, evitando así ser víctimas de la delincuencia.

"Nadie puede proteger a un tercero, si no se sabe proteger a sí mismo", comentó Enrique Tapia Padilla, MA, CPP, socio director en Altair, Security Consulting & Training, en otra de las charlas magistrales del *roadshow* sobre el tema. El especialista, quien cuenta con más de 25 años de trayectoria, indicó que no se puede impedir que les lleguen ataques o virus cibernéticos a los EPE y/o principales, pero que, con diferentes estrategias y capacitación, sí van a ayudar a que estos sepan reaccionar y no caigan en fraudes virtuales.

"La base en la formación de una cultura de prevención, está en enseñar a la sociedad a auto protegerse. El ejecutivo está protegido de manera física y debe contar con medidas de protección digitales, ya que a través de los celulares, por ejemplo, se realiza la comunicación con quien lo protege, ahí se comparte información sensible, lo mismo que el protegido.

Sin embargo, debido a la falta de una cultura de seguridad, de conocimiento, de sensibilización y prevención, los ataques cibernéticos exitosos han aumentado de forma significativa en Latinoamérica", indicó.

Y agregó que no es un tema de alarmar, es un tema de alertar. Saber cuáles son los retos de seguridad en los cuales están dentro del ambiente en el que operan día a día, y cuáles son las recomendaciones de seguridad.

Algunos de los delitos cibernéticos más frecuentes son:

- Robo de información.
- Suplantación de identidad.
- Espionaje cibernético.
- Fraude cibernético.
- Ataques a infraestructuras tecnológicas.
- Extorsiones.
- Secuestros.
- Trata.

Modalidades de ataque a la ciudadanía:

- ***Phishing.*** Consiste en engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito, números de cliente, entre otros, y con esto cometer delitos.
- ***Pharming.*** Es un cibercrimen muy similar al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial.
- ***Vishing.*** Es una estafa que pretende suplantar la identidad del afectado a través de VoIP (Voice over Internet Protocol), recreando un sistema semejante al de las entidades bancarias, cuando en realidad son delincuentes.
- ***Smishing.*** Emplea mensajes de texto dirigidos a los usuarios de telefonía móvil solicitando datos, o que llamen a cierto número, o entren a una dirección web fraudulenta.
- ***Ransomware.*** Es un programa de software malicioso que infecta las computadoras y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Puede bloquear la pantalla de la computadora, o cifrar archivos importantes predeterminados con una contraseña.
- ***Grooming.*** Es una técnica empleada por ciertos adultos para ganarse la confianza de menores de edad y conseguir su simpatía con fines de satisfacción sexual.
- **Uso de Inteligencia Artificial.** Se requiere una pronta regulación de la IA, ya que se está utilizando y se utilizarán para: amenazas y ataques, robo de información, sesgos y discriminación, clonación de audio y video, suplantación de identidades, seguridad en IoT comprometida, dependencia excesiva a la IA, uso en el ámbito militar.

El especialista explicó que hay ciertas reglas que los EPE deben seguir, y en general todos los usuarios de Internet y redes sociales, por ejemplo: Todo lo que subas a Internet, considéralo público. Aquí es importante establecer filtros de seguridad en las redes sociales, cuidar la privacidad de uno y de los demás. Tener un uso racional de las redes. Importante capacitar y sensibilizar tanto al principal como a los elementos de seguridad, puesto que, de acuerdo con unos ejercicios experimentales realizados, en redes sociales, el 90% de las personas cae en engaños de otras personas.

Para concluir la ponencia, Enrique Tapia dejó un Decálogo de Prevención, reiterando la importancia de compartirlo con los EPE y en cada organización, así como con el principal y equipo de trabajo, hasta con su familia, puesto que la ciberseguridad y la cultura de seguridad es algo necesario para la vida actual, es parte del nuevo perfil del guardia.

1) Mantener dispositivos seguros / soluciones de seguridad.
2) Contraseñas fuertes y únicas / autenticación múltiple.
3) Verificar las fuentes de información/ transacciones.
4) No compartir información sensible.
5) Actualizarse en temas de Inteligencia Artificial.
6) Privacidad en redes sociales.
7) Proteger los dispositivos IoT.
8) Evitar el uso de IA no verificados.
9) Contar con preguntas o palabras claves para identificar situaciones de riesgo.
10) Conciencia situacional, uso del sentido común.

"La seguridad no es un departamento, es un comportamiento de todos y cada uno de nosotros, en la medida que sensibilicen, concienticen y los exhorten a realizar políticas y estén convencidos de que las deben realizar para estar más seguros, ellos y sus protegidos. En un servicio de Protección Ejecutiva de calidad, el 90% es prevención; 5%, disuasión; 3%, reacción, y 2%, suerte", concluyó. ■

Referencias:
https://ifpomexico.com/

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

CUANDO LOS MUNDOS CHOCAN

Conflictos entre las perspectivas de negocio

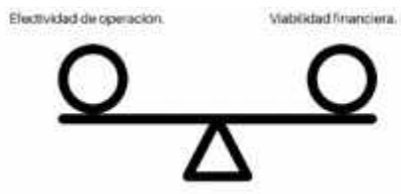
MÉXICO | **David Chong Chong**

Foto: Freepik

Toda empresa, por su naturaleza de "organización de negocio con fines lucrativos" enfrenta una dicotomía de objetivos que en ocasiones llegan a entrar en conflicto: la efectividad de operación enfocada al logro de su "objetivo de negocio" para permanecer y posicionarse en el mercado, y la viabilidad financiera, enfocada a permanecer e incluso prevalecer en el mercado. Conflictos que surgen cuando se altera el necesario equilibrio que debe existir entre los dos objetivos, debido fundamentalmente a la diferencia entre sus perspectivas de "éxito".

En general, la presencia de una empresa en un mercado se sustenta y justifica a partir de la definición de su objetivo de "negocio", lo que constituye su misión, su razón de ser (¿qué se quiere hacer?). Y su perspectiva de posicionamiento está determinada por su nivel de efectividad en la operación de ese "negocio", de tal suerte que, a mayor efectividad mejor perspectiva de posicionamiento y viceversa.

Pero, dado que para lograr cualquier objetivo se requiere de algún tipo de recursos, lo que, de acuerdo con la premisa de que nada es gratuito, todo tiene alguna forma de costo (dinero, esfuerzo, tiempo), se proyecta un segundo objetivo, simbiótico con la efectividad, que es la viabilidad financiera, la cual determina las posibilidades de permanencia e incluso prevalencia de la empresa en su mercado, de tal suerte que por esta simbiosis de ambos objetivos, es imprescindible un equilibrio entre ambos para, a su vez, posibilitar el éxito en el logro del objetivo de "negocio" proyectado.



VIABILIDAD FINANCIERA

La causa principal de los posibles desequilibrios entre estos dos objetivos es la diferencia entre sus perspectivas de "éxito", de hacer más y lo mejor posible para la efectividad, y de erogar lo menos posible para la viabilidad financiera. En este contexto, si se privilegia la efectividad por sobre la viabilidad financiera, se puede mejorar la posición de la empresa, pero se puede comprometer hasta la misma existencia de la empresa, al perder la rentabilidad, y en consecuencia, el logro del objetivo de "fines lucrativos".

Por otro lado, si se privilegia la viabilidad financiera sobre la efectividad operativa, probablemente a corto plazo se obtengan mejores beneficios financieros, pero también eventualmente se podrían perder posiciones en el mercado ante sus competidores, en un virtual efecto de "cascada", y acabar perdiendo tales beneficios financieros hasta comprometer su propia existencia por un efecto que se puede describir como "inanición" por la reducción de los ingresos.

Este segundo tipo de desequilibrio es el más frecuente, en especial en ámbitos de alta competencia y márgenes de utilidad reducidos, y el que provoca las crisis, incluso hasta la extinción, de algunas empresas, y de ello hay muchos casos, uno muy reciente e ilustrativo es el de la compañía Boeing. La compañía Boeing es una de las más importantes en la industria aeronáutica, en una posición no sólo de prevalecía sino, en un momento, de dominancia en el mercado cuando absorbió a su entonces principal competidor, la empresa McDonnell Douglas en 1996.

Y esta posición la alcanzó con base en una gran efectividad de negocio, produciendo productos de calidad, sobre todo seguridad, que es un factor crucial, incluso crítico, por las vidas en juego a bordo de las aeronaves, lo cual lograron asegurando la calidad en la mayoría de la fabricación y ensamblaje de sus partes, ubicándolas en sus propias instalaciones (*in house*) y con cercanía física, lo que les permitía aplicar mecanismos de supervisión directa y frecuente, manteniendo un equilibrio razonable en la dicotomía de objetivos.

Pero el éxito y la dominancia distorsionaron su visión, y en aras de mejorar su viabilidad financiera susti-

tuyeron este modelo de cultura corporativa, dispersando físicamente sus instalaciones técnicas y gerenciales, y tercerizando una gran parte de su producción, con lo que propició que sus mecanismos de supervisión y control de calidad, se volvieron más laxos y menos rigurosos.

Este cambio redujo la calidad de sus equipos, y provocó una crisis a la empresa derivado de los accidentes de la versión MAX-8 de su modelo 737, el más vendido de su historia que provocó un debilitamiento de su posición en el mercado de la industria aeronáutica, un ámbito de muy alta competencia y márgenes reducidos y volátiles de utilidad, ante su principal competidor en la actualidad, la compañía europea Airbus.



Las empresas en el mercado de los servicios de Seguridad Privada en México, es un ámbito con gran número de competidores y márgenes de utilidad reducidos y muy volátiles, en su mayor parte están ubicadas en el segmento de las micro, pequeñas y medianas (MIPyMES), que enfrentan un ámbito de mercado condicionado primordialmente por la demanda (los prestatarios o clientes), y criterios de elección entre las opciones disponibles "a la baja", es decir, con preferencia por el menor de los costos, lo que se puede considerar como la "cultura del mercado".

Estas condiciones colocan a estas empresas en una posición de desequilibrio hacia la viabilidad financiera, sacrificando significativamente la efectividad de operación en detrimento de la calidad de los servicios provocando un efecto de "cascada" en un "círculo vicioso" de degradación progresiva de la efectividad y calidad. Asimismo, se tiene que, si bien estas condiciones son predominantes, no son exclusivas de este sector de empresas, sino que se extienden, al menos parcialmente, a las grandes empresas con algunos de sus clientes que no consideran prioritario los aspectos de efectividad y calidad, que necesariamente representan mayores costos.

La priorización de la viabilidad financiera sobre la efectividad de negocio en el mercado de los servicios de Seguridad Privada se ha convertido en la base de la "cultura corporativa" de estas empresas, y se debe más a razones de asegurar la rentabilidad para propósitos de sobrevivencia de la empresa en el negocio, derivado del enfoque preferencial de costos reducidos sobre la calidad de los servicios que priva en la "cultura del mercado".

La repercusión más significativa de este desequilibrio suele reflejarse como una degradación de las condiciones laborales del personal operativo, que representan el mayor concepto de los costos de la empresa, lo cual, a su vez, provoca una secuencia progresiva en "cascada", esto es un "círculo vicioso", que inducirá presiones sobre la viabilidad financiera.

El desequilibrio por la prevalencia de la viabilidad financiera sobre la efectividad operativa constituye un conflicto con potencial de cataclismo, de un evento a nivel de extinción, en este caso la empresa, toda proporción guardada, equivalente a lo que ocurre cuando los mundos chocan, por la confrontación entre las dos perspectivas de negocio.

El problema de fondo es que la solución a este conflicto no se puede dar al interior de las empresas, sino en el exterior, en la "cultura del mercado", que si bien no comparten las grandes empresas prestatarias (clientes) que entienden la conveniencia de la efectividad y están dispuestos a sufragar los costos, si predominan en el resto de empresas que se ubican en el sector de MIPyMES, lo mismo que la mayoría de las empresas prestadoras. Y este cambio sólo se podrá lograr por medio de un esfuerzo unificado de concientización y sensibilización de las empresas prestatarias por parte de las prestadoras, con una visión de coexistencia competitiva, ya que con ello "todos saldremos ganando" en el sector de los Servicios de Seguridad Privada. ■

Fotos: Cortesía David Chong Chong

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

INVESTIGACIONES DE SEGURIDAD EN EL ÁMBITO CORPORATIVO

Las mejores técnicas de investigación requieren de frecuentes evoluciones y verificaciones

Foto: Freepik

COLOMBIA

Javier Nery Rojas Benjumea

Una definición comúnmente aceptada de investigación es la evaluación sistemática y completa de algo o alguien (la recolección de hechos e información) y el registro de tal evaluación dentro de un reporte. El propósito principal de cualquier investigación (particularmente en el área organizacional o corporativa) generalmente cae dentro de una o más de las siguientes categorías:

- Documentar incidentes de manera completa.
- Identificar las causas de situaciones no deseadas.
- Documentar y relacionar hechos alrededor de cualquier situación o alegato.
- Identificar sospechosos involucrados en un crimen o un acto de mala conducta.
- Compilar información que pueda aprobar o desaprobar un alegato o que implique o exonere a un individuo sospechoso de cometer un crimen.
- Permitir una decisión, usualmente con respecto al nivel de confianza o determinación de un individuo.

5 ATRIBUTOS QUE CARACTERIZAN UNA INVESTIGACIÓN EFECTIVA Y CONFIABLE

1) **Objetividad:** El proceso investigativo involucra tanto ciencia como arte. Muchas investigaciones tienen sus bases en hipótesis, las cuales pueden ser desarrolladas al final o posteriormente a la investigación y pueden cambiar una o muchas veces. La hipótesis es apropiadamente usada como una herramienta mientras permanezca dentro de las barreras de la objetividad.

   El no corroborar la evidencia es un error común de los investigadores inexpertos, pero puede pasarle a cualquiera. El objetivo general es permitir que los hechos hablen por sí mismos de manera concisa, acertada y profesional. Para ayudar a mantener la objetividad el investigador debe reconocer conscientemente sus prejuicios personales y neutralizar los efectos de estos detrás de las actividades investigativas, incluyendo la formación de hipótesis.

   El investigador profesional debe asegurarse que los hallazgos investigativos formen las bases de sus impresiones, no al contrario. Además, el enfoque y conducta del investigador es de crítica importancia para un resultado exitoso del caso.

2) **Entereza:** Seguir todas las pistas relevantes hasta su conclusión lógica y concentrarse en corroborar todos los hallazgos investigativos clave.

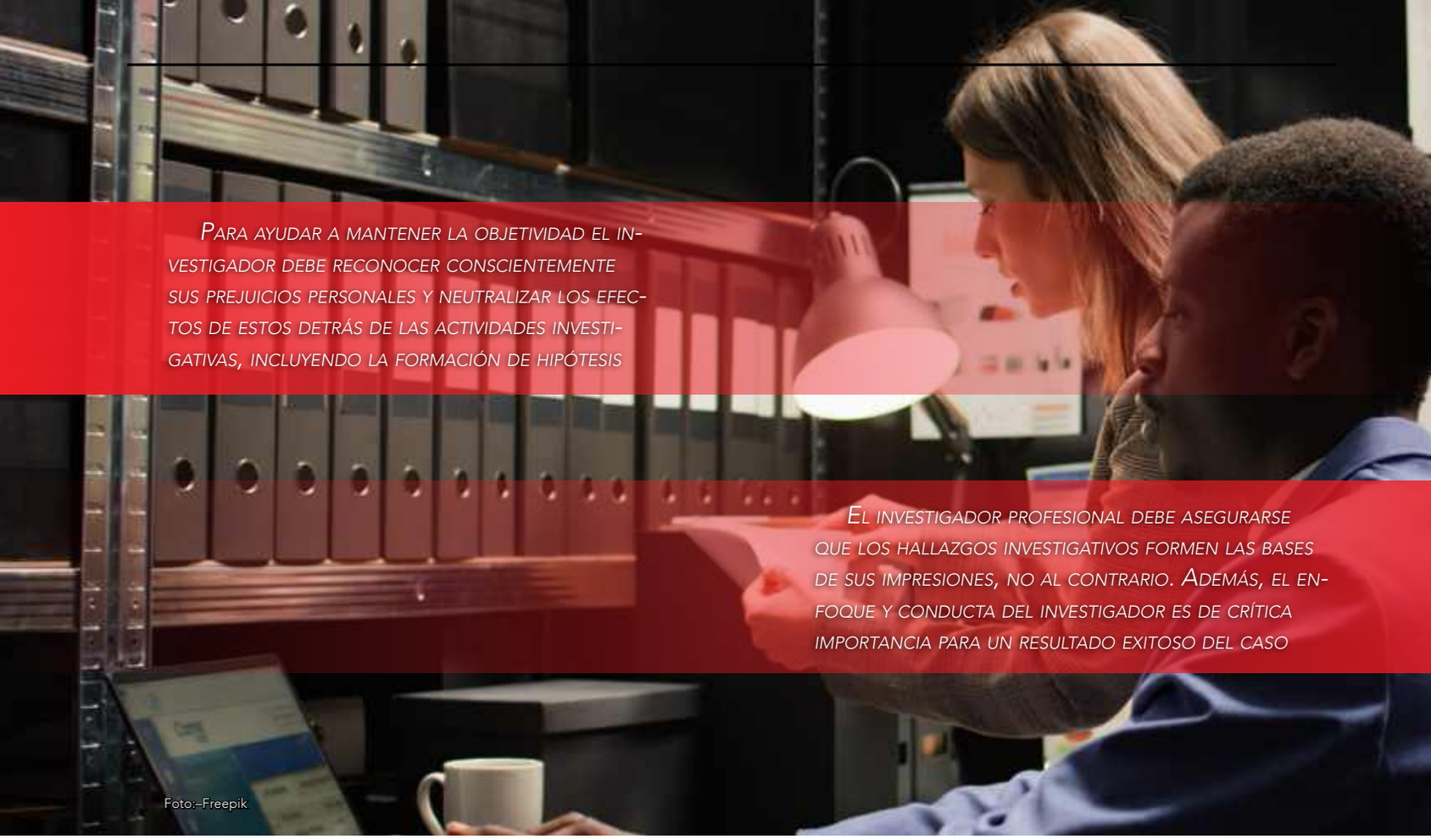
3) **Relevancia:** Significa que la información en cuestión es pertinente al sujeto de investigación de alguna manera y es de nivel de detalle apropiado.

   Es trabajo del investigador determinar la relevancia y el nivel de detalle necesario. El espectro de detalles es pertinente para determinar qué tan amplia debe ser una red de investigación para poder reunir toda la información relevante.

   Es posible que aparezcan relaciones similares de causa y efecto y volverse extremadamente relevantes en cualquier tipo de investigación. La declaración de los hechos realizada por testigos esta entre las formas menos acertadas de formación investigativa. "Dada la naturaleza de la memoria, el testimonio de testigos nunca podrá ser totalmente acertado o confiable".

   Las mejores técnicas de investigación requieren de frecuentes evoluciones y verificaciones. Esto es similar a una auditoría financiera donde la evaluación de la certeza, tiempos y competencia de los registros de transacciones corporativas es crítica. Si los datos son susceptibles a una medición física, entonces deben ser medidos.

4) **Certeza:** Toda información investigativa debe ser cuidadosamente evaluada. No debe ser aceptada con una simple observación casual, incluso si a primera vista parece ser certera. Por ejemplo, la fecha y hora de las computadoras, cámaras, o máquinas. Pueden tener sus relojes internos mal calibrados. Similarmente, un sistema de control de accesos que indica que un individuo en particular



Para ayudar a mantener la objetividad el investigador debe reconocer conscientemente sus prejuicios personales y neutralizar los efectos de estos detrás de las actividades investigativas, incluyendo la formación de hipótesis

El investigador profesional debe asegurarse que los hallazgos investigativos formen las bases de sus impresiones, no al contrario. Además, el enfoque y conducta del investigador es de crítica importancia para un resultado exitoso del caso

Foto:–Freepik

entró hacia la puerta en un momento determinado puede ser considerado como sospechoso.

La credibilidad de una fuente, ya sea evidencia humana, física, o electrónica o el resultado de observación o vigilancia.

En las investigaciones, es importante:

- Abrir una investigación tan pronto como sea posible.
- Completar una investigación tan rápido como sea posible.
- Evitar cerrar una investigación prematuramente.

Aún cuando estos aspectos pueden sonar contradictorios, una vez más el balance es la llave, respecto a un comienzo rápido, "las investigaciones deben realizarse tan pronto como se reporte o descubra un incidente". La razón más importante para realizar esto es que el valor de evidencia física o electrónica disminuye rápidamente.

Además, los testigos y otras personas que poseen información relevante proporcionan la mejor cuando el incidente está sus memorias. Al paso del tiempo, comúnmente comienzan a fallar, o la información que proporcionan puede empezar a tener fallas en sus racionalizaciones que tienen que pensar más sobre el incidente que tiene aplicación de sus respuestas a las preguntas del investigador.

5) **Oportunidad:** La habilidad de completar una investigación rápidamente, pero al mismo tiempo resistir la presión de fuerzas externas que desean apresurar inapropiadamente el caso, evitando un daño a la calidad de los resultados. Finalmente, una investigación rápida y decisiva refleja el profesionalismo de las investigaciones del personal de seguridad, por lo tanto, mejorando su efectividad general. Sin embargo, debe tenerse cuidado de no apresurar una investigación a expensas de su calidad, entereza o certeza.

Los investigadores pueden ser apresurados a cerrar el caso debido a tiempo o a limitaciones de los recursos o debido a publicidad o factores políticos. Debe evitarse ver estas presiones en medida de lo posible. El jefe de la unidad investigativa o director de Seguridad puede necesitar educar a la alta dirección sobre los impactos adversos potenciales de apresurar una investigación, incluyendo la posibilidad de incrementar los riesgos de responsabilidades.

Además, los encargados de tomar las decisiones y ejecutivos corporativos deben estar conscientes que no en todos los casos puede alcanzarse una resolución. No pueden asumir que cada caso será resuelto rápidamente o en su totalidad. Tal cosa puede llevar a expectativas poco realistas de una unidad de investigación o departamento de Seguridad.

Las comunicaciones regulares y oportunas entre directivos de Seguridad y los encargados de tomar las decisiones organizacionales ayudarán a minimizar el problema de expectativas poco realistas. ■

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

DIRECTOR DE SEGURIDAD GLOBAL: LIDERAZGO Y SERVICIO

Foto:–Freepik

Los nuevos retos y seguridades requieren y exigen, cada vez con mayor urgencia, una actualización del modelo de Dirección de Seguridad

ESPAÑA

Manuel Sánchez Gómez-Merelo

Los nuevos retos y exigencias de seguridad requieren, cada vez con mayor urgencia, una actualización del modelo de aptitudes y actitudes exigibles a un director de Seguridad.

Es preciso generar el perfil de un nuevo líder, basado en la excelencia, el servicio y la gestión eficaz, para generar en sus equipos confianza, valores y una cultura de seguridad acompañada de una amplia formación especializada. La experiencia nos ha enseñado que los Departamentos de Seguridad son sostenibles, flexibles y eficaces cuando se dispone del líder adecuado.

Recordando que la seguridad, con independencia de los eventos que se hayan de gestionar, está bien o mal interpretada con base en la madurez y el estado de ánimo de quienes la enfrentan, podemos decir que lo más importante es asegurar una equilibrada percepción de la realidad, por lo que el buen líder en seguridad es el que tiene "talento para gestionar el riesgo y la visión correcta de las circunstancias que lo rodean". Para ello, el conocimiento y la mentalidad del buen líder en seguridad tiene que incorporar una visión holística.

Cuando estamos hablando de liderazgo en seguridad lo hacemos desde el concepto y la perspectiva del "*servant leadership*", es decir, un liderazgo enfocado al servicio.

Un director de Seguridad Global debe ser un líder orientado al servicio que tiene claro, en primer lugar, que la visión de la seguridad debe ser integral e integrada, lo que le permitirá construir espacios para la gestión del riesgo en los que todos los elementos en juego y las diferentes percepciones involucradas puedan ser evaluados y comprendidos, teniendo en cuenta que todo el conocimiento adquirido y todo el talento para el liderazgo que posea la persona elegida va acompañado de una auténtica voluntad de servicio, orientada al afrontamiento[1] de cualquier incidencia o circunstancia, por más compleja que parezca.

En un entorno de integración y digitalización como el que vivimos, la pujante incorporación de la IA acelera la velocidad del cambio, haciendo que los tiempos para la reacción sean cada vez más breves. Los profesionales de la seguridad tienen que ser capaces de evolucionar y adaptarse y, para ello, necesitan una enorme capacidad de autogestión y permanente especialización.

HACIA UNA NUEVA SEGURIDAD Y LIDERAZGO

Una moderna organización y dirección de Seguridad debe estar estructurada actualmente en torno a valores, y su liderazgo debe ser una consecuencia de la expresión de estos.

No podemos pretender tener organizaciones seguras y resilientes si las personas que forman parte de las mismas no lo son. Por ello, debemos trabajar en la resiliencia individual proactiva, aprovechando los recursos y experiencia de los que ya disponemos, aplicando los buenos resultados ya obtenidos con ellos y apoyándonos en los valores de los modelos de éxito ya implantados.

De manera especial, es necesario cambiar las estrategias de protección de las infraestructuras esenciales, Críticas y Estratégicas, hacia un enfoque holístico de la seguridad integral e integrada (prevención + protección) que incluya una adecuada gestión de riesgos inherentes a éstas (físicos, lógicos y humanos) en todo el ciclo, desde una cultura de prevención.

En un entorno de integración y digitalización como el que vivimos, la pujante incorporación de la IA acelera la velocidad del cambio, haciendo que los tiempos para la reacción sean cada vez más breves

El líder, el director de Seguridad Global ha de ser creativo, intuitivo e inclusivo, a fin de estar preparado también para reestructurar inercias, modelos mentales y paradigmas ya obsoletos, enfocando el futuro hacia un pensamiento cuántico

Foto: Freepik

Sin duda hoy hay que dar respuesta con base en una Seguridad Global, única con mayúscula, Integral e Integrada, Pública y Privada. Con la aplicación de esta capacidad ya conseguida para absorber las situaciones de crisis y reorganizarse, al tiempo que experimentamos el cambio dentro esencialmente de las mismas funciones, haremos que estructura, identidad y retroalimentación participen de forma especial, reforzando la creatividad, el carácter proactivo y la innovación en las organizaciones.

Por y para ello, hemos de destacar y desarrollar el papel y la necesidad de esta nueva forma de liderazgo, a fin de promover la resiliencia dentro de los sistemas de formación y capacitación, a partir de cinco conceptos clave: formación holística, autoconocimiento, transparencia en las relaciones, perspectiva ética y procesamiento riguroso de la información.

El líder, el director de Seguridad Global ha de ser creativo, intuitivo e inclusivo, a fin de estar preparado también para reestructurar inercias, modelos mentales y paradigmas ya obsoletos, enfocando el futuro hacia un pensamiento cuántico[2].

Resumiendo, diría que mi visión tiende hacia la consecución, a través del trabajo en la selección y la formación, de un tipo de líder con mentalidad diferente, más abierta y global con un mejor autoconocimiento. Precisamos de un cambio permanente que deje ver ese espacio que se abre a los nuevos retos y demandas de seguridad que, del mismo modo, presentan infinitas posibilidades. La transformación es necesario desarrollarla con especial proactividad, y la innovación tecnológica es la base de la especialización en valor compartido.

Los nuevos retos y seguridades requieren y exigen, cada vez con mayor urgencia, una actualización del modelo de Dirección de Seguridad. Es preciso generar el perfil de un nuevo líder, basado en la excelencia, el servicio y la gestión eficaz, para hacer crecer la confianza, los valores y el marchamo empresarial distintivo de una cultura propia. Líderes sólidos, empáticos, con amplios conocimientos y que mantengan la motivación.

Para todo ello, las organizaciones deben modernizarse e invertir en la gestión del conocimiento. El objetivo es asegurar la disponibilidad inmediata de una capacitación que ha de facilitar a sus miembros, así como la implementación de una formación y puesta al día continuada que pueda incorporar el conocimiento externo más fiable.

Hoy, más que nunca, necesitamos líderes para la seguridad que integren y gestionen con especial visión esa hoja de ruta de Análisis - Convergencia - Integración - Resiliencia - Consecuencia - Trascendencia, con la que venimos trabajando proactivamente. ■

Referencias:

[1] *Conjunto de esfuerzos conductuales y cognitivos que realiza el individuo para hacer frente a las situaciones estresantes, así como para reducir el estado de malestar que produce el estrés (Diccionario Médico).*

[2] *El pensamiento cuántico es holístico y unifica, contempla y relaciona todos los datos e integra los procesos del pensamiento en serie y asociativo.*

Manuel Sánchez Gómez-Merelo, consultor internacional de Seguridad. *Más sobre el autor:*

PROS Y CONTRAS
EN LAS TÉCNICAS EN PRUEBAS DE CONFIANZA E INVESTIGACIONES

Las técnicas de prueba de confianza son valiosas para evaluar la confiabilidad de individuos que tienen acceso a activos patrimoniales y pueden ser aplicadas de manera ética y efectiva. Sin embargo, es esencial equilibrar los beneficios con preocupaciones éticas y legales, como la privacidad y la no discriminación

Foto:–Freepik

MÉXICO **José Luis Sánchez Gutiérrez**

Como es habitual, estimados lectores, realmente muy agradecido por su acostumbrada preferencia; y en esta ocasión tocaremos el tema de las Técnicas en pruebas de Confianza e Investigaciones.

Tomando en cuenta a todo profesional de seguridad patrimonial, seguridad corporativa y seguridad física de una empresa en México y el Mundo, las pruebas de confianza son una herramienta importante para evaluar la integridad y confiabilidad de los empleados. Las técnicas de pruebas de confianza son un conjunto de procedimientos y métodos utilizados en el campo de la seguridad patrimonial y de recursos humanos para evaluar la confiabilidad y la integridad de los empleados, contratistas o individuos que tienen acceso a información sensible o activos críticos de una organización. Estas técnicas están diseñadas para identificar posibles riesgos y detectar cualquier comportamiento o antecedente que pueda poner en peligro la seguridad o los activos de la organización. Las mejores técnicas en pruebas de confianza se centran en la identificación de posibles riesgos y la protección de los activos patrimoniales de una organización.

Aquí tienes el top 10 que considero, son las mejores técnicas a incorporar:

1) **Evaluación de Antecedentes:** Realizar una revisión exhaustiva de los antecedentes laborales y personales de los empleados, incluyendo verificación de referencias y antecedentes penales. Esto ayuda a identificar posibles banderas rojas.
2) **Evaluación de Finanzas Personales:** En algunos casos, examinar las finanzas personales de los empleados puede revelar posibles motivaciones para cometer actos fraudulentos o de mala conducta.

c) **Evaluación de Historial de Viajes:** Analizar el historial de viajes de los empleados, especialmente si tienen acceso a información confidencial o activos valiosos, para detectar comportamientos inusuales.

d) **Entrevistas de Revisión de Comportamiento:** Realizar entrevistas estructuradas con empleados para evaluar su comportamiento, motivaciones y actitudes hacia la organización y sus políticas.

e) **Monitoreo de Comportamiento en el Trabajo:** Utilizar sistemas de monitoreo para observar el comportamiento de los empleados en el entorno de trabajo, especialmente en áreas de alto riesgo.

f) **Pruebas de Drogas y Alcohol:** Realizar pruebas regulares de drogas y alcohol, especialmente para empleados en roles críticos, para garantizar que no estén bajo la influencia, mientras desempeñan sus funciones.

g) **Evaluación de Riesgo de Desgaste:** Evaluar el riesgo de "desgaste" o agotamiento emocional entre los empleados que pueden estar experimentando estrés o problemas personales que afecten su confiabilidad.

h) **Evaluación de Conexiones Externas:** Examinar las conexiones externas de los empleados, incluyendo amistades y relaciones, para identificar posibles conflictos de intereses o influencias externas.

i) **Capacitación en Conciencia de Seguridad:** Proporcionar capacitación en conciencia de seguridad a los empleados para aumentar su comprensión de los riesgos y la importancia de mantener la confidencialidad.

j) **Revisión Continua:** La evaluación de la confianza no debe

Las mejores técnicas en pruebas de confianza se centran en la identificación de posibles riesgos y la protección de los activos patrimoniales de una organización

ser un proceso estático. Debe ser continuo y adaptable a medida que cambian las circunstancias y se identifican nuevos riesgos (sugiero sea realizado mínimo anualmente —de manera preferente semestralmente—).

Es importante destacar que las pruebas de confianza deben realizarse de manera ética y respetando las leyes y regulaciones laborales aplicables. Además, deben estar respaldadas por políticas y procedimientos claros y comunicados a los empleados. La privacidad y la equidad son fundamentales en la implementación de estas técnicas. También, desde mi observador les comparto los Pros y Contras para las técnicas en pruebas de confianza en el ámbito de la seguridad patrimonial, seguridad corporativa y seguridad física:

PROS DE LAS TÉCNICAS EN PRUEBAS DE CONFIANZA

- **Identificación de Riesgos:** Las pruebas de confianza permiten identificar posibles riesgos de seguridad interna, lo que ayuda a prevenir incidentes y pérdidas financieras.
- **Mejora de la Seguridad:** Al evaluar la confiabilidad de los empleados, se fortalece la seguridad de la organización, reduciendo el riesgo de actos de mala conducta o fraude interno.
- **Detección de Problemas de Recursos Humanos:** Estas pruebas pueden ayudar a identificar problemas en el ámbito de los recursos humanos, como conflictos internos, descontento laboral o problemas de integridad.
- **Cumplimiento Legal:** En algunos sectores, las pruebas de confianza pueden ser un requisito legal o regulatorio para garantizar la seguridad de las operaciones.
- **Disuasión:** El conocimiento de que se realizan pruebas de confianza puede disuadir a los empleados de cometer actos de mala conducta, actuando como medida preventiva.

CONTRAS DE LAS TÉCNICAS EN PRUEBAS DE CONFIANZA

- **Violación de la Privacidad:** Las pruebas de confianza pueden percibirse como una invasión de la privacidad de los empleados, lo que podría afectar negativamente la moral y la confianza en la organización.
- **Falsos Positivos:** Las pruebas de confianza no siempre son precisas y pueden dar lugar a "falsos positivos", es decir, acusaciones incorrectas o infundadas que pueden dañar la reputación de los empleados.
- **Costos:** Implementar pruebas de confianza puede ser costoso en términos de tiempo y recursos, incluyendo la contratación de expertos y la inversión en tecnología.
- **Potencial de Discriminación:** Existe el riesgo de que las pruebas de confianza se utilicen de manera discriminatoria o sesgada, lo que puede dar lugar a problemas legales y éticos.
- **Dificultad de Interpretación:** La interpretación de los resultados de las pruebas de confianza puede ser subjetiva y complicada, lo que dificulta la toma de decisiones basada en dichos resultados.
- **Posible Resistencia de los empleados:** Los empleados pueden resistirse a las pruebas de confianza, lo que podría generar desconfianza y tensiones en el lugar de trabajo.

Es fundamental equilibrar los beneficios de las pruebas de confianza con las preocupaciones éticas, legales y de privacidad. La implementación de estas técnicas debe llevarse a cabo con cuidado y de manera transparente, respetando los derechos de los empleados y garantizando que se sigan las leyes y regulaciones aplicables.

Y como siempre entrando, más a detalle, no quiero dejar pasar el análisis *novelty, feasibility, specificity, impact* y *workability* aplicados a las técnicas en Pruebas de Confianza:

NOVELTY (NOVEDAD): CONSIDERADA CON UNA PUNTUACIÓN ALTA

Las técnicas de prueba de confianza no son novedosas en sí mismas, ya que han sido utilizadas durante décadas en seguridad y recursos humanos. Sin embargo, la novedad radica en la evolución constante de estas técnicas, como la aplicación de tecnología avanzada en pruebas de confianza, incluyendo análisis de datos, herramientas de tecnología forense y sistemas de monitoreo. Esto permite una mayor precisión y eficacia en la evaluación de la confiabilidad.

FEASIBILITY (VIABILIDAD): CONSIDERADA CON UNA PUNTUACIÓN ALTA

Las técnicas de prueba de confianza son altamente viables y factibles en una variedad de entornos organizacionales. Las organizaciones pueden implementar estas técnicas utilizando recursos internos o contratando servicios especializados. La viabilidad se ve reforzada por la disponibilidad de herramientas tecnológicas y capacitación especializada.

Foto: Freepik

Foto:-Freepik

Estas técnicas de investigación deben llevarse a cabo de manera profesional, ética y confidencial. La integridad y la transparencia son esenciales en todo el proceso de investigación, y la colaboración con expertos legales o forenses puede ser crucial en casos más complejos

SPECIFICITY (ESPECIFICIDAD): CONSIDERADA CON UNA PUNTUACIÓN ALTA

Las técnicas de prueba de confianza son altamente específicas en su enfoque. Están diseñadas para evaluar aspectos muy específicos relacionados con la confiabilidad y la integridad de los individuos, como antecedentes laborales, comportamiento en el trabajo, historial financiero y relaciones externas. Esto permite a las organizaciones abordar riesgos de manera precisa y enfocada.

IMPACT (IMPACTO): CONSIDERADA CON UNA PUNTUACIÓN MODERADA

El impacto de las técnicas de prueba de confianza puede ser significativo. Cuando se aplican adecuadamente, estas técnicas pueden ayudar a prevenir incidentes de seguridad, mejorar la toma de decisiones en recursos humanos y proteger los activos patrimoniales de la organización. Sin embargo, también existe el riesgo de impactos negativos, como la violación de la privacidad o la generación de desconfianza entre los empleados si no se manejan adecuadamente.

WORKABILITY (VIABILIDAD PRÁCTICA): CONSIDERADA CON UNA PUNTUACIÓN ALTA

Las técnicas de prueba de confianza son prácticas y se pueden integrar de manera efectiva en los procesos de seguridad patrimonial y recursos humanos. Las organizaciones pueden adaptar estas técnicas según sus necesidades y recursos disponibles. La implementación exitosa depende de contar con políticas y procedimientos claros, así como de la capacitación de personal adecuada.

En general, las técnicas de prueba de confianza son valiosas para evaluar la confiabilidad de individuos que tienen acceso a activos patrimoniales y pueden ser aplicadas de manera ética y efectiva. Sin embargo, es esencial equilibrar los beneficios con preocupaciones éticas y legales, como la privacidad y la no discriminación.

Y ahora veremos a detalle lo concerniente a las Técnicas de Investigaciones; que son una parte esencial de mantener la seguridad y proteger los activos patrimoniales de una organización. Las mejores técnicas en investigaciones se basan en la recopilación de información precisa y la toma de decisiones informadas. Aquí tienes 13 de las mejores técnicas a considerar:

- **Preservación de Escenas del Crimen/Evento:** Al investigar incidentes, garantiza la preservación adecuada de la escena del crimen/evento para recopilar pruebas valiosas, como fotografías, videos y documentación.
- **Entrevistas Efectivas:** Realiza entrevistas exhaustivas con testigos, empleados y cualquier persona involucrada en el incidente. Utiliza técnicas de entrevista que fomenten la cooperación y la obtención de información precisa.
- **Revisión de Documentación:** Examina registros, informes, correos electrónicos y otros documentos relacionados con el incidente para identificar evidencia relevante.
- **Uso de Tecnología Forense:** En casos que involucren tecnología, como ciberseguridad, recurre a expertos en tecnología forense para analizar dispositivos y sistemas en busca de pruebas.
- **Colaboración con Autoridades:** Trabaja en estrecha colaboración con las autoridades locales o agencias de aplicación de la ley cuando sea necesario, siguiendo los procedimientos legales.
- **Análisis de Datos:** Utiliza herramientas de análisis de datos para identificar patrones o tendencias que puedan revelar información importante.
- **Vigilancia y Monitoreo:** En situaciones en las que sea legal y ético, considera el uso de vigilancia y monitoreo para obtener información sobre actividades sospechosas.
- **Capacitación en Entrevistas y Técnicas de Interrogatorio:** Proporciona a tu equipo de seguridad patrimonial capacitación en técnicas de entrevista y de interrogatorio éticas y efectivas.
- **Recopilación de Pruebas Físicas:** Recolecta evidencia física, como huellas dactilares, muestras de ADN o muestras de productos, cuando sea necesario.
- **Auditorías Internas:** Realiza auditorías internas para detectar posibles vulnerabilidades o áreas de mejora en los procesos y procedimientos de seguridad.
- **Comunicación con las Partes Interesadas:** Mantén una comunicación constante con las partes interesadas, como la alta dirección y otros departamentos, para garantizar una respuesta coordinada a la investigación.

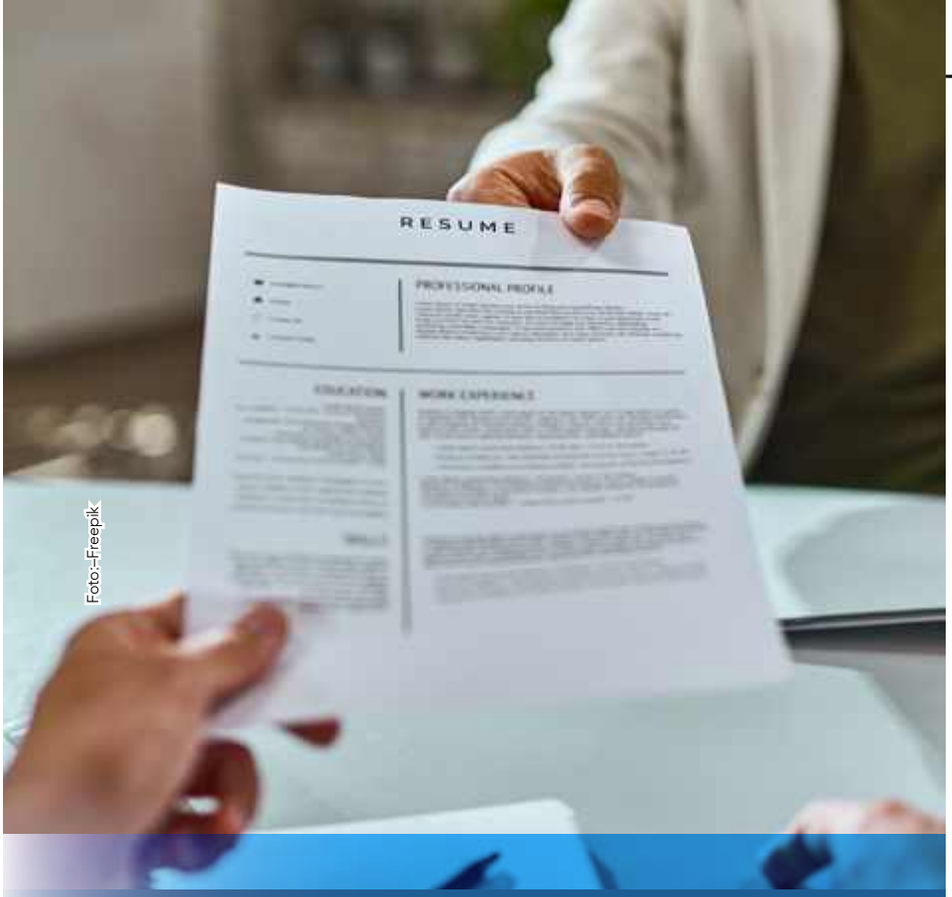


Foto:-Freepik

Estas técnicas son esenciales para identificar amenazas, prevenir incidentes, recopilar pruebas y tomar decisiones informadas

- **Informe de Resultados:** Presenta informes claros y concisos que resuman los hallazgos de la investigación y las acciones recomendadas.
- **Cumplimiento Legal y Ético:** Asegúrate de que todas las investigaciones se realicen de manera legal y ética, respetando los derechos de las personas y siguiendo las regulaciones aplicables.

Estas técnicas de investigación deben llevarse a cabo de manera profesional, ética y confidencial. La integridad y la transparencia son esenciales en todo el proceso de investigación, y la colaboración con expertos legales o forenses puede ser crucial en casos más complejos. También, desde mi observador les comparto los pros y contras para las técnicas investigaciones en el ámbito de la seguridad patrimonial, seguridad corporativa y seguridad física:

PROS DE LAS TÉCNICAS EN INVESTIGACIONES

- **Identificación de Incidentes:** Las técnicas de investigación ayudan a identificar incidentes, amenazas y actividades sospechosas que podrían poner en peligro los activos patrimoniales de la organización.
- **Recopilación de Pruebas:** Las investigaciones permiten recopilar pruebas sólidas que pueden respaldar acciones disciplinarias, legales o correctivas.
- **Mejora de la Seguridad:** Al descubrir y abordar vulnerabilidades, las investigaciones mejoran la seguridad general de la organización.
- **Prevención de Futuros Incidentes:** Al comprender las causas subyacentes de los incidentes, se pueden implementar medidas preventivas para evitar que vuelvan a ocurrir.
- **Cumplimiento Legal:** Las investigaciones pueden garantizar que la organización cumple con las leyes y regulaciones relacionadas con la seguridad y la protección de activos.

CONTRAS DE LAS TÉCNICAS EN INVESTIGACIONES

- **Posible Violación de la Privacidad:** Las investigaciones pueden verse como una invasión de la privacidad de los empleados o individuos investigados, lo que puede generar preocupaciones éticas y legales.
- **Costos Elevados:** Las investigaciones pueden ser costosas en términos de tiempo, recursos y contratación de expertos externos.
- **Falsas Acusaciones:** Existe el riesgo de que las investigaciones conduzcan a acusaciones infundadas o incorrectas que pueden dañar la reputación de individuos o empleados.
- **Resistencia y Desconfianza:** Los empleados pueden resistirse a las investigaciones, lo que podría generar desconfianza en el lugar de trabajo y tener un impacto negativo en la moral.
- **Complicaciones Legales:** Las investigaciones mal gestionadas pueden dar lugar a problemas legales, incluyendo demandas por prácticas de investigación inapropiadas.
- **Posibles Conflictos de Intereses:** Los investigadores internos pueden enfrentar conflictos de intereses o presiones para no revelar información perjudicial para la organización.

Es esencial llevar a cabo investigaciones de manera ética, transparente y profesional, respetando los derechos de las personas y siguiendo las leyes y regulaciones aplicables. La privacidad y la integridad deben ser consideraciones centrales en todo proceso de investigación. Las técnicas de investigación en el ámbito de la seguridad patrimonial son métodos y enfoques utilizados para recopilar información, analizar datos y resolver problemas relacionados con la seguridad y la protección de los activos patrimoniales de una organización. Estas técnicas son esenciales para identificar amenazas, prevenir incidentes, recopilar pruebas y tomar decisiones informadas.

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

José Luis Sánchez Gutiérrez, director comercial de Galeam. *Más sobre el autor:*

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

SOCIO DIRECTOR, ALTAIR, SECURITY CONSULTING & TRAINING

LA IMPORTANCIA DE LA CULTURA DE SEGURIDAD EN LAS ORGANIZACIONES

LATINOAMÉRICA

Imaginen el poder de una mentalidad consciente en seguridad. Ahora imaginen el poder de una conciencia situacional colectiva. ¡El potencial sería inimaginable!

La seguridad en las organizaciones es fundamental y es una responsabilidad compartida. Así también, el cambio cultural es fundamental para cualquier transformación.

La cultura de seguridad se refiere a los valores, creencias, percepciones y actitudes compartidos por los miembros de una organización en relación con la seguridad. Es el conjunto de comportamientos y prácticas que una organización promueve y sigue para garantizar un ambiente seguro para sus empleados, clientes y cualquier otra persona que pueda verse afectada por sus operaciones.

La cultura de seguridad es un aspecto fundamental de la administración empresarial, ya que influye en la salud, el bienestar y la productividad de todos los miembros de la organización. Además, es importante destacar que la cultura de seguridad también influye en la eficiencia operativa y tiene un impacto significativo en los ingresos y en la imagen de las organizaciones.

Para reforzar la cultura de seguridad, es fundamental:

- Contar con el compromiso de la alta dirección.
- Establecer políticas y procedimientos claros.
- Capacitar constantemente a los empleados.
- Fomentar una comunicación abierta y honesta sobre los problemas, los retos y las preocupaciones relacionadas con la seguridad.

Una cultura de seguridad bien desarrollada no sólo protege a las personas, sino también a los activos, la imagen y la continuidad de las operaciones del negocio. Además, beneficia a la empresa económicamente y mejora su posicionamiento en el mercado, coadyuvando en la certidumbre y el éxito de la misma.

¿CÓMO COMENZAMOS?

Una cultura de seguridad comienza con la sensibilización. Entender que, como organización, debemos evolucionar hacia una conciencia situacional colectiva es fundamental.

Cuando cada individuo es consciente de su entorno y de los riesgos que podrían implicar sus acciones o las de otros, estamos en el camino correcto. Por eso, es crucial:

- Informar estratégicamente sobre los retos de seguridad y el modo de operación de los adversarios. De esta forma, en lugar de generar una paranoia vacía y nociva, fomentamos una conciencia activa y colectiva.
- Entender que la mayoría de los riesgos se pueden prevenir o disminuir siguiendo sencillas medidas de seguridad. La solución está en las manos de todos y cada uno de nosotros.
- Comprender cómo se materializan las amenazas y el impacto que pueden tener en la seguridad personal y la de nuestros colaboradores. Esto desarrolla un sentido de responsabilidad y corresponsabilidad. Comprometernos con las medidas de seguridad necesarias para asegurarnos y promover una participación activa en su implementación.

Involucrar a toda la organización y alentar permanentemente a la mejora continua en seguridad. La seguridad es una tarea de todos. Juntos podemos crear un entorno más seguro y más tranquilo para todos. ■

¿En tu organización se vive una Cultura de Seguridad?

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

Fotos: Cortesía Enrique Tapia Padilla

Asistencia Legal

ALES

Gestoría jurídica en materia de

Seguridad Privada

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

Asumimos la responsiva de su empresa en los siguientes rubros:

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

LicDanteGarciaMtz@outlook.com

Cel: +52 477 828 1291

ES UN GRAN PELIGRO CUANDO FALLAN LOS SERVICIOS DE INTELIGENCIA

La criminalidad sigue en aumento y se presentan nuevas formas y modalidades

Foto: Freepik

PERÚ

César Ortiz Anderson

Los errores en la inteligencia del Estado suelen ser hechos recordados en la historia por las graves consecuencias que generan. En el presente artículo nuestra intención es hacer un recuento y un breve diagnóstico de los servicios de inteligencia en el Perú durante las últimas décadas, analizando los factores que la relacionan con la inestabilidad política y la crisis social que atraviesa el país.

Desde Aprosec (Asociación Pro Seguridad Ciudadana del Perú), podríamos afirmar que las actuales crisis de Seguridad Ciudadana y Política respectivamente tienen un punto de inflexión que se presenta en algún momento del gobierno de Pedro Pablo Kuczynski, y que no son responsabilidad exclusiva de ese gobierno, sino que en cambio son el resultado de una serie de errores de la inteligencia peruana en los más altos niveles en un periodo que va desde inicio de la década del 2000 hasta la actualidad, en la que no parece que los servicios de inteligencia peruanos hayan recuperado el nivel de efectividad y anticipación que tuvieron en décadas anteriores.

ERRORES DE INTELIGENCIA Y SEGURIDAD CIUDADANA

En cuanto a la crisis actual en Seguridad Ciudadana, el contexto de la criminalidad en el Perú presenta a la fecha un escenario de guerra entre las bandas criminales peruanas y las bandas criminales venezolanas principalmente relacionadas al "Tren de Aragua". Durante el gobierno de Pedro Pablo Kuczynski entre el 2016 y el 2018, el Perú abrió sus fronteras a la migración venezolana. Ese ha sido uno de los errores más grandes de la inteligencia peruana durante la era Republicana, al no saber anticiparse al accionar de la delincuencia extranjera en el Perú.

Hoy, años después, vemos desbordada a la Policía y a las autoridades nacionales luego de haberse decretado el Estado de Emergencia en los distritos limeños de Comas y San Juan de Lurigancho con resultados totalmente contrarios a los esperados: la delincuencia y la cifra de homicidios aumentó. El gobierno de turno que preside la señora Dina Boluarte no ha querido reconocer este fracaso.

ERRORES DE INTELIGENCIA Y CRISIS POLÍTICA

La inteligencia peruana tampoco funcionó al anticipar la actual crisis socio-política que vive el país —que empezó con la renuncia al gobierno del presidente Pedro Pablo Kuczynski en el 2018 y que se extiende por seis años de inestabilidad política que ya afectan a la economía, llegando al ritmo de cambiar un presidente por año— y que ha llevado al banquillo o a la cárcel a casi todos los ex presidentes del Perú, desprestigiando la institucionalidad nacional que se ha visto afectada en su legitimidad como autoridad democrática.

La mayoría de acusaciones penales en contra de los ex presidentes peruanos proviene del caso Lava Jato, proceso que se inició en el extranjero y que continuó en el Perú como en un efecto dominó, arrastrando a autoridades de los tres niveles del Estado: nacional, regional y local; habiendo entre alcaldes y gobernadores la mayor cantidad de funcionarios involucrados.

Pero en el caso Lava Jato no sólo han sido involucrados altos funcionarios públicos, ex presidentes y ministros, sino también la mayoría de los partidos políticos, las principales empresas y corporaciones de la industria peruana de la construcción, los grupos privados de comunicación social, de radio, prensa y televisión, los más importantes estudios jurídicos, etc. Debido a la cantidad de contratos entre el Estado peruano y las empresas investigadas en el caso Lava Jato, el país se encuentra prácticamente paralizado, al menos en las grandes obras de infraestructura pública que se estaban ejecutando al momento de abrirse el caso: hidroeléctricas, carreteras, etc. Cabe recordar que la pandemia del COVID-19 encontró al país económicamente ya paralizado y en plena crisis política debido al caso Lava Jato.

Las consecuencias del caso Lava Jato han sido mucho más graves en el Perú que en cualquier otro país, incluyendo Brasil. Desde el punto de vista de la inteligencia, el caso Lava Jato representa no uno, sino varios errores de los servicios peruanos que no pudieron anticipar los efectos derivados del hecho fundamental del cual se desprende todo: Operaciones financieras de la empresa Odebrecht provenientes del pago de sobornos en el sistema bancario de los Estados Unidos.

LA CAÍDA DE FUJIMORI Y LA DESACTIVACIÓN DEL SIN

En Aprosec, hemos analizado desde el punto de vista de la inteligencia del Estado el efecto del caso Lava Jato en el Perú y hemos llegado a algunas hipótesis como que la crisis política actual se origina 23 años atrás con la caída del régimen de Alberto Fujimori y la desarticulación de sus servicios de inteligencia, los cuales fueron desmantelados, pasando a la clandestinidad y prestando servicios a intereses privados. En lo sucesivo, la inteligencia peruana dependió del gobierno de turno, tal como lo vamos a describir más adelante. No hubo una política de Estado a nivel de inteligencia, sólo políticas de turno. Desde el punto de vista de la inteligencia del Estado, ese sería el origen de la actual crisis.

"Tras la difusión del video Kouri-Montesinos el 14 de septiembre del año 2000, el gobierno de Fujimori entró en crisis. Una de las principales acciones tras aquel evento fue la desactivación del Servicio de Inteligencia Nacional (SIN) —aún durante el gobierno de Fujimori—, y luego la reforma del sistema, durante el gobierno de transición de Paniagua en el año 2001".

"Por diversas presiones y perspectivas políticas, en ese periodo fueron despedidos, cesados, desactivados o reasignados un gran contingente de analistas, operativos, agentes e informantes: cerca de dos mil personas terminaron su relación con el Sistema de Inteligencia Nacional. Como parte de una investigación sobre la transformación de la inteligencia peruana: a) Describir el contexto de la desactivación y la reforma para entender los objetivos y causas del despido y desactivación de este contingente de agentes y analistas; b) Determinar el rango numérico de agentes y analistas que fueron despedidos, cesados o desactivados entre la desactivación del año 2000 y la reforma del año 2001; c) Determinar el destino y funciones de los agentes y analistas despedidos y desactivados en los años posteriores a 2001, lo que muestra una relación con el desarrollo de empresas de seguridad, sistemas privados de inteligencia, inteligencia empresarial y un mercado de compra-venta de interceptaciones telefónicas durante los últimos catorce años".

"Este estudio se sostiene en el cruce de tres tipos de datos: fuente abierta provista por la normativa, informantes clave que participaron en el proceso de los años 2000 y 2001, y datos primarios de actores que actualmente son miembros de empresas de seguridad e inteligencia privada" (en: "La desactivación del Servicio de Inteligencia Nacional. De la salida del personal de inteligencia al desarrollo de las agencias privadas de inteligencia en el Perú". Jaris Mujica. Pontificia Universidad Católica del Perú PUCP. 2014).

ERRORES DE INTELIGENCIA EN LA HISTORIA

Los servicios de inteligencia y la comunidad de inteligencia son parte del concepto clásico de inteligencia, desde la perspectiva del concepto clásico como organización. Esos servicios son organismos de la administración pública, cuya finalidad es obtener información, que no pueden obtener otros organismos, y transformar esta información en inteligencia para prevenir así posibles amenazas y facilitar la toma de decisiones del gobierno.


Foto:–Freepik

Los servicios de inteligencia se han constituido a lo largo del tiempo en los diferentes países del mundo, hasta el punto de que casi cualquier país tiene su propio servicio de inteligencia. Algunos ejemplos son la CIA en Estados Unidos, el Mosad en Israel o el MI5 en Reino Unido. España tiene el Centro Nacional de Inteligencia (CNI) (Secretos de Estado y Servicios de Inteligencia. Eduardo García Novoa, Universidad de Salamanca 2020).

Un error en la inteligencia de los Estados Unidos en 1941 permitió el ataque de Pearl Harbor, desencadenante de la entrada de EE.UU. en la Segunda Guerra Mundial. Otro error de la inteligencia de ese país, se pudo observar en el atentado de las Torres Gemelas, el 11 de septiembre del 2001. En octubre de 2023, fallaron los servicios de inteligencia israelíes que no pudieron anticipar los demenciales ataques terroristas del Hamás y que degeneraron en la guerra que hoy contemplamos horrorizados en el Medio Oriente: falló el servicio de inteligencia israelí compuesto por dos agencias, el Mossad, a cargo de la seguridad exterior; y el Shinbet, la agencia de inteligencia encargada de la seguridad interior, el territorio, la seguridad del Estado y la población.

CRONOLOGÍA DE LA INTELIGENCIA EN EL PERÚ 1960–2021

Los servicios de inteligencia son fundamentales en los temas de seguridad de un país tanto dentro de sus fronteras como fuera de éstas.

Los servicios de inteligencia suponen una pieza fundamental tanto para la política exterior como para la política interior, teniendo dos preocupaciones principales: "El enemigo exterior, que pone en peligro los intereses legítimos del Estado y el enemigo interior, que trata de subvertir el propio régimen constitucional y quebrantar los valores reconocidos y protegidos por el Estado en su constitución" (Secretos de Estado y Servicios de Inteligencia. Eduardo García Novoa, Universidad de Salamanca 2020).

Estos fallos en las inteligencias de países que se encuentran a la vanguardia mundial de la seguridad del Estado, nos deben hacer reflexionar en la situación en la que se encuentra nuestro servicio de inteligencia nacional. Antes del gobierno de Fujimori, el SIN tenía un buen nivel de inteligencia que le daba al Perú un rol preponderante en la región. Al llegar Fujimori al poder, junto a su asesor presidencial Vladimiro Montesinos, el SIN fue usado para otros fines, como el seguimiento de opositores políticos, periodistas, comunicadores sociales y empresarios.

Para reflexionar acerca de la actual situación de la inteligencia peruana hagamos una breve cronología: el 27 de enero de 1960 el presidente Manuel Prado Ugarteche creó mediante Decreto el Servicio de Inteligencia Nacional (SIN). Posteriormente, el 04 de noviembre de 1970 durante el gobierno de Velasco Alvarado se constituyó el Sistema de Inteligencia Nacional (SINA), y en 1984 —segundo gobierno de Belaúnde Terry— fue expedido el Decreto Legislativo N.° 271 que incluyó como labor de inteligencia, a los campos o dominios no militares de la seguridad.


Foto: Freepik

En el mes de julio de 1992, en el primer gobierno de Fujimori, entró en vigencia el Decreto Ley N.° 25635 y su Reglamento (DSN.° 065-DE-SG), dispositivos que especificaban que el Servicio de Inteligencia Nacional era el organismo central y rector del Sistema de Inteligencia Nacional, tiene rango ministerial, depende del presidente de la república y se encarga de producir, integrar, dirigir, coordinar, controlar y realizar actividades de inteligencia y contrainteligencia requeridas por la Seguridad y la Defensa Nacional.

En octubre de 2000, el servicio fue desactivado por el presidente Fujimori luego que su jefe Vladimiro Montesinos fuera descubierto pagando sobornos a importantes personajes de la política. Luego de la desactivación del SIN, el 05 de junio de 2001 se expidió la Ley n.° 27479 que creó el Consejo Nacional de Inteligencia–CNI y la Dirección Nacional de Inteligencia Estratégica–DINIE. Estos organismos fueron también disueltos con la dación de la Ley N.° 28664.

El 04 de enero de 2006, al finalizar el gobierno de Alejandro Toledo, fue publicada la Ley N.° 28664–Ley del Sistema de Inteligencia Nacional–SINA y de la Dirección Nacional de Inteligencia–DINI. Dicha norma creó el nuevo sistema de inteligencia y dio nacimiento a la Dirección Nacional de Inteligencia. El 11 de diciembre de 2012, con el presidente Ollanta Humala, fue publicado el Decreto Legislativo N.° 1141 según el cual el SINA es el conjunto de principios, normas, procedimientos, técnicas, instrumentos, organismos y órganos del Estado funcionalmente vinculados, que bajo la dirección y coordinación de la Dirección Nacional de Inteligencia–DINI, como ente rector, producen Inteligencia Nacional, Inteligencia Militar e Inteligencia Policial, y ejecutan medidas de contrainteligencia en las áreas de su responsabilidad. El Sistema de Inteligencia Nacional–SINA forma parte del Sistema de Defensa Nacional y mantiene relaciones técnicas de coordinación con la Secretaría de Seguridad y Defensa Nacional–SEDENA.

El 09 de enero de 2017 se promulgó la Ley N.° 30535, mediante la cual se modificó el Decreto Legislativo N.° 1141 con la finalidad de ampliar los controles al sistema de inteligencia nacional, incluyendo a la DINI, por parte del Congreso de la República y la Contraloría General de la República. Asimismo, la nueva norma reorientó la labor de la DINI hacia una de inteligvencia estratégica más que operativa.

En el año 2021, cuando Pedro Castillo asumió el poder, realizó un mal manejo del sistema de inteligencia nacional y policial. Hoy por ejemplo se está produciendo inteligencia contra la criminalidad que hoy nos acecha, se está buscando a los sobrinos y funcionarios de Pedro Castillo, y qué está pasando con Vladimir Cerrón que se burla vía redes de que el general Oscar Arriola no lo puede capturar.

SITUACIÓN DE LA INTELIGENCIA EN EL PERÚ

Nuestra preocupación se centra en la situación en la que se encuentran hoy nuestros sistemas de inteligencia, ya que el relajamiento de estos servicios está trayendo más de una negativa sorpresa para el país.

Es lamentable hablar sobre la situación de la inteligencia en el Perú, hemos retrocedido, porque no hay inteligencia predictiva ni inteligencia estratégica para la toma de decisiones del gobierno, por lo tanto, no hay dirección, como tampoco hay unidad de inteligencia, ni inteligencia operativa. En Seguridad Ciudadana esto es notorio al no haber una política de Estado o de largo plazo en este tema sino políticas de gobiernos de turno que utilizan el problema para mantenerse en el poder.

En el caso de la Policía Nacional, tampoco se hace inteligencia, sino que se trabaja con base en el pago de informantes. Esto conlleva a la corrupción, porque ¿cómo se controla ese pago y las recompensas? Eso demuestra que no hay un trabajo planificado. Plata para los informantes hay, lo que no hay es control, existe plata para la corrupción.

LA POLICÍA DE INVESTIGACIONES DEL PERÚ

Actualmente la Policía Nacional no puede enfrentar los diferentes y nuevos tipos de crímenes que se presentan porque desde hace 30 años se suprimió la especialización en investigaciones. Todas las Policías del mundo tienen investigaciones, menos en el Perú.

La criminalidad sigue en aumento y se presentan nuevas formas y modalidades. La Policía no está preparada para tantas formas de criminalidad. Por ejemplo, ahora hay una especie de "turismo criminal", porque quienes quieren asesinar a alguien contratan sicarios extranjeros que ingresan, perpetran el crimen y se regresan inmediatamente, no dejan pistas, desaparecen. Una prueba de ellos es que ciudades fronterizas como Tacna, Tumbes y Madre de Dios presentan mayor cantidad de casos de sicariato. Estas características del crimen hacen que la lucha de la Policía sea más complicada porque la información con la que cuenta no puede ser comprobada al haber escapado el sicario al país vecino cruzando la frontera. Venezolanos, colombianos, brasileños contratados, cometen el delito y regresan a su país. Este tipo de crímenes se están viendo cada vez más.

Estos nuevos tipos de delito están apareciendo porque la Policía no está capacitada. Nuestra Policía no cuenta con investigaciones. No se hace investigación. Todas las policías del mundo se especializan dividiéndose en preventiva e investigaciones. Ya van a ser 30 años de labor policial —desde que se disolvió la PIP Policía de Investigaciones del Perú— sin especialización en investigaciones, lo que ha sido una mala experiencia para el país, tiene que haber prevención e investigaciones, como en todas las policías del mundo. Por otro lado, la presidenta Dina Boluarte tiene asesores teóricos y no asesores con conocimiento de campo, en las calles. Es decir, los asesores en temas de seguridad ciudadana de la presidenta de la república son asesores de libro, de gabinete o de biblioteca, no son asesores de campo, que conocen las acciones del crimen en las calles, con experiencia en combate contra el crimen en la acción y no en la teoría. ■

César Ortiz Anderson,
presidente de Aprosec (Asociación Pro Seguridad Ciudadana del Perú).
Más sobre el autor:

BASC, DENTRO DE MI TRAYECTORIA EN EL ÁREA DE SEGURIDAD

Arturo Guido Báez
Head of Corporate Security
México & Latam
Zurich

"EN MI HUMILDE OPINIÓN, BASC SE HA VUELTO UN REFERENTE EN LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LAS ORGANIZACIONES. HA AYUDADO A PERMEAR LA CULTURA DE SEGURIDAD EN TODOS LOS NIVELES DE ESTAS INCLUYENDO LA PROVEEDURÍA CRÍTICA"

En mi viaje por el mundo de la seguridad, el cual inició hace más de 25 años en lo que en aquel momento era una de las plantas de manufactura electrónica más importantes de la región, precisamente en el área de lo que hoy se conoce como Supply Chain Security. En aquel entonces, los procesos se implementaban a prueba y error, y sí, al final logramos implementar un sistema de seguridad robusto.

¿Por qué platico esto? Porque ahí es donde entra BASC, una asociación empresarial que tenía definido un sistema de gestión claro y robusto para la seguridad en la cadena de suministro, pero que no tenía presencia en el occidente de México. Han pasado ya más de 20 años desde que, en conjunto con otros colegas, nos propusimos formar el Capítulo BASC en el Occidente. En aquel entonces, existía solamente en Ciudad de México y Monterrey. Veinte años después, BASC Occidente es un Capítulo nacional y referente para la Organización Mundial BASC.

Convencer a los directores generales de nuestras empresas para la conformación del Capítulo fue el primer reto, pero todos se subieron al proyecto ya que tenían claros los beneficios de trabajar bajo procesos de un sistema de gestión. Además, BASC es un sistema de gestión 360°, es decir, que involucra a todos los actores que tienen que ver con los procesos de la seguridad de la cadena de suministro y asegura que la visión y el enfoque en la seguridad sean compartidos.

En mi humilde opinión, BASC se ha vuelto un referente en los sistemas de gestión de seguridad de las organizaciones. Ha ayudado a permear la cultura de seguridad en todos los niveles de estas, incluyendo la proveeduría crítica. Cuando las empresas, principalmente proveedores o empresas que no tienen un área de seguridad debidamente conformada, me preguntan ¿por qué certificarse en BASC y qué beneficios tiene?, siempre hago esta analogía: para mí, BASC es como cursar la escuela desde primaria hasta la preparatoria. Es decir, te va formando y llevando de la mano para lograr un sistema de gestión de seguridad robusto y sólido, traduciendo esto en beneficios tangibles para el negocio, como puede ser la obtención de nuevos clientes para las empresas de servicio o evitando pérdidas o contaminación de mercancías que conllevan, además del impacto económico, un impacto reputacional y/u operacional por incumplimientos de contratos al no entregar sus mercancías en tiempo y forma.

En un ambiente tan globalizado, los retos que hoy enfrentan las organizaciones son enormes y muy complejos, por decir lo menos, aunado a una situación de inseguridad e impunidad, lo que obliga a las organizaciones a ser muy eficientes con cada peso invertido. BASC es ese aliado que les guiará en todo momento a implementar procesos de seguridad, maximizando la inversión en seguridad a través de la prevención.

BASC
OCCIDENTE DE MÉXICO

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

LA TECNOLOGÍA SE PUEDE Y DEBE APLICAR PARA LA BÚSQUEDA DE PERSONAS DESAPARECIDAS

Cámaras y biometría como apoyo

MÉXICO | **Ricardo Nava Rueda**

Foto: Freepik

La tecnología tiene que ser aprovechada en todos sus rubros para la búsqueda de personas desaparecidas o no localizadas. Podemos empezar con los datos biométricos de cada una de estas personas, las fotos y datos como huellas dactilares, ADN y más, desde luego que esto se tiene que hacer desde las autoridades correspondientes y la iniciativa privada, entre otras.

Hoy en día existen miles de cámaras en todo el país, cámaras de los C5, C4 o C2, algunas con buena resolución y otras con menos, vamos a pensar que las Comisiones de Búsqueda y las Fiscalías Especializadas recopilarán los datos de una manera más técnica y en esto participen empresas o negocios que tengan cámaras con gran resolución para guardar en un sistema o *software* las fotos, tiendas de conveniencia, centros comerciales, terminales de autobuses, terminales aéreas y estaciones del tren o metro, donde al detectar a través de los datos ya contenidos a una persona desaparecida y a su vez mandará la señal a un Centro de Comando los datos de donde fue captada la persona en proceso de búsqueda, a su vez estos datos a los C5, C4 o C2 y las cámaras cercanas les dieran seguimiento y su pronta localización a través de patrullas, para ser trasladadas a las instancias que las están buscando o simplemente enviar datos de la zona o polígono donde se les captó.

PROPUESTA DE *APP*

Hace unos meses envié una propuesta a la jefa de Gobierno de la Ciudad de México, Dra. Claudia Sheinbaum Pardo (hoy presidenta electa de la república mexicana), con un proyecto propiamente para LOCATEL (acrónimo con el que se conoce el Servicio Público de Localización Telefónica), en la que sugiero una aplicación para celulares en la que a través de una *app* se envíen unas tres o cuatro fotos de un familiar desaparecido; la propuesta está bien fundamentada, cuando una persona se desaparece o extravía y se reporta a LOCATEL, la operadora se va a imaginar por una llamada de una manera correcta, a la persona que se describe por su ausencia o extravío, la altura, edad, complexión, señas particulares y color de piel, entre otros datos, lo cual describe y envía información a los hospitales, juzgados cívicos y otras instancias para saber si la persona desaparecida se encuentra ahí.

Probablemente la persona se encuentra ahí y quien recibe la información la pueda ver de otra manera, más alta, de más edad y no con los datos proporcionados, se jugaría "al teléfono descompuesto", naturalmente negará que la persona se encuentre ahí; con los datos de una *app*, serán más exactos y la persona desaparecida más fácil de localizar. Al mismo tiempo LOCATEL enviaría al teléfono el folio que regularmente proporciona a quien solicita el servicio o apoyo, si a esto le agregamos que pueda tener mayor alcance, como un ejemplo: la persona se desaparece o extravía, se manda la información, esta a su vez es capturada de manera inmediata y se envía a un centro receptor de la misma, se comparte con C5, C4 o C2 y se ve la persona caminando por las calles cercanas al lugar de donde extravía cuando tiene pocos minutos del evento, desde luego que puede ser localizada prontamente y reintegrada a su familia.

Como lo he comentado a través de este medio, hay muchas personas desaparecidas en situación de calle, el problema que no hay argumento legal para que puedan ser fotografiadas o solicitar sus huellas dactilares, esto ayudaría mucho para ser ubicadas y reintegradas si ellas lo desean al núcleo familiar, lo que está claro que hay que le-

Ricardo Nava Rueda, "Lost Boy", director de Difusión y Relaciones Públicas de la Asociación Mexicana de Niños Robados y Desaparecidos, A.C. *y líder del proyecto Encuéntrame de Seguridad por México (Iniciativa Chapultepec, A.C.). Más sobre el autor:*

17° CONGRESO INTERNACIONAL DE CENTROS DE ATENCIÓN DE EMERGENCIAS

23 AL 25 DE OCTUBRE DE 2024

HOTEL PARADISUS. CANCÚN, MÉX.

NENA THE 9-1-1 ASSOCIATION MEXICO

Te presentamos a nuestros patrocinadores

promad · CITYSHOB · SeguriTech · OnStar

CARBYNE · HIKVISION · INTRADO

HEMAC · NGA Next Generation Advanced · ISS Intelligent Video · PULSIAM

ADISES Advanced Integrated Security Solutions · MOTOROLA SOLUTIONS · THINKSAFE INGENIERIA

servitron · AVAYA · Genetec · sermex EXPERTOS EN SEGURIDAD

Integraciones Electromecánicas · teltronic · TECNETIK

IRISITY powered by Agent Vi · SISTEMAS MER · Bamba "Tu Aliado Tecnológico" · ho1a Innovación · Priority Dispatch · VIPER

nena_911mx · Nena 9-1-1 Mx · www.911latinoamerica.org · Nena 9-1-1 México

DODECÁLOGO DE ASPECTOS LEGALES ANTE LA RECIENTE MODIFICACIÓN DE LA "LEY DE TRATA"

Recomendaciones frente a los cambios más relevantes a esta reforma de ley

Foto: Freepik

MÉXICO

Dante García Martínez

Ante la modificación del 07 de junio del presente año, en la Ley General para Prevenir, Sancionar y Erradicar Los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos (Ley de Trata), es importante considerar, para no caer en el supuesto legal de esta ley, lo siguiente:

1 Actualizar los contratos individuales de trabajo, definiendo perfectamente la jornada laboral del contratado, así como su identificación de horarios.

2 Se deben identificar, en los contratos laborales, con suma precisión, los horarios de alimentos y el sitio destinado a ellos; ante eventuales auditorías, supervisiones o conflictos legales, la rastreabilidad y acreditación de horarios de ingreso y egreso, incluyendo aquellos de los alimentos, deben estar preferentemente firmados por el trabajador, no basta que existan medios electrónicos ni análogos (la firma y huella del trabajador, acreditan o no dicho cumplimiento a la norma).

3 Crea e identifica, nuevas jornadas laborales, evita que excedan más de 48 horas por semana, sin importar las combinaciones, en beneficio mutuo de los contratantes.

4 Actualiza los Contratos de Prestación de Servicios, la prestataria, debe estar consciente y conforme con la identificación de los nuevos esquemas laborales de protección y vigilancia, evitando incurrir en afectaciones al trabajador.

5 Las horas extras, que se puedan generar, legalmente (sólo nueve horas por semana), se deben "consentir", en cláusula específica, con la voluntad del contratado, debiendo ser precisado el eventual supuesto en el mismo contrato laboral. Nunca en adendos.

6 Actualizar el Reglamento Interno de Trabajo de la Empresa, aquí radica una importante revisión, pues es la directriz, del desarrollo de las actividades y jornadas, así como la clara identificación de los contratados, en acuerdo entre el Patrón y el Representante de los Trabajadores (si es el caso, de un contrato colectivo, es indispensable contar con la asistencia del Sindicato correspondiente).

7 Los contratos identificables que requieran terceros (autoridades), deben ser la duplica de lo que existe en el expediente laboral de la empresa; evita crear "Documentación que sí cumple".

8 Los menores de edad, o que no tenga la capacidad de comprender el significado del hecho (analfabeto), así como adultos mayores de sesenta años, pertenecientes a pueblos y comunidades indígenas y afro mexicanas, mujeres embarazadas, personas con lesiones, enfermedades o discapacidad física que sean contratados, en materia de seguridad, bajo ningún pretexto, deben de laborar en jornadas nocturnas o mixtas, por lo que sólo deberán de estar en jornadas diurnas y nunca más de ocho horas diarias.

9 La contratación del personal, debe ser clara y determinante en cuanto a sus responsabilidades y derechos, por ser una consideración de Orden Público, por ende, no cabe la interpretación o dejar cláusulas ambiguas, que entrañen un detrimento al contratado.

10 La capacitación, debe otorgarse en jornadas laborables, nunca en horas extras.

11 La mejor recomendación administrativa, en la nueva realidad laboral, es el pago nominal, por semana.

12 La investigación penal, requieren el claro acreditamiento del incumplimiento laboral, independiente de las infracciones aplicables por la autoridad laboral. No es potestativa la negociación, es una situación disyuntiva, evita infringir el marco legal. ■

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

amesis MR

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

SIAMES C5

Uso exclusivo de la plataforma, para comunicación con las autoridades

TOTAL ACCESO

Consulta a reportes de estadísticas de robos

24/365 DÍAS

Atención personalizada de nuestro centro de monitoreo

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

SOCIOS ACTIVOS

Tracking Systems · Satel · Holkan · skyguardian · skymeduza · ADS LOGIC · SECURE ARTNESS · INFO TRAX · TECNO LOGISTIX · RAINDE · SEGURIDAD 2.0 · ATLANTIDA · TTC · ISIS · GEOTRUCKS · GRUPO ALFIL · SOLUCIONES · GPSMonitor · GRUPO PRYSE · DUMAX · PROTECZONE

SOCIOS ADHERENTES

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

¡Síguenos en nuestras redes!

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

COMUNÍCATE
55 3334 4707

LA RESPONSABILIDAD SOCIAL EMPRESARIAL EN LAS *STARTUPS*

Alinearse con los valores de RSE puede mejorar la reputación corporativa y generar un impacto positivo en la percepción de la marca

Foto:–Freepik

MÉXICO **Rafael E. Vera**

En el mundo de los negocios contemporáneos, la idea de Responsabilidad Social Empresarial (RSE) se ha establecido como un elemento fundamental para que las organizaciones logren un éxito sostenible. Esta filosofía empresarial se enfoca en el impacto positivo que una empresa puede tener en la sociedad y en el medio ambiente, más que sólo buscar beneficios económicos. Aunque normalmente ha estado relacionado mayormente con grandes corporaciones, su importancia se extiende también a las *startups*, donde su adopción temprana puede marcar la diferencia no sólo en su camino, sino también en el entorno que los rodea.

PROMOVER UNA CULTURA DE VALORES

Dado su carácter innovador y ágil, los *startups* tienen la posibilidad de integrar la responsabilidad social en su ADN desde el inicio. Al definirlo, no sólo establecen su propósito más allá de la rentabilidad, sino que también construyen una cultura empresarial sólida fundamentada en valores éticos y morales. Además de atraer empleados comprometidos y clientes leales, contribuye también a una reputación positiva que puede ser un activo invaluable en un mercado cada vez más consciente.

GENERACIÓN DE IMPACTO POSITIVO

El compromiso con la RSE permite a las *startups* ser agentes de cambio en sus comunidades y en el mundo en general. Mediante prácticas sostenibles, voluntariado corporativo y asociaciones con organizaciones sin ánimo de lucro, estas nuevas empresas pueden enfrentar activamente los problemas sociales y ambientales. Las *startups* pueden generar un impacto positivo palpable que va más allá de su negocio, ya sea reduciendo su huella de carbono, promoviendo la diversidad y la inclusión o invirtiendo en proyectos de desarrollo comunitario.

PROMOCIÓN DE LA INNOVACIÓN SOCIAL

Los *startups* deben aprovechar la innovación para abordar desafíos sociales, no limitarse a cumplir con ciertas obligaciones éticas. Estas empresas pueden descubrir nuevas oportunidades de mercado, desarrollar productos y servicios que satisfagan necesidades sociales no cubiertas y catalizar el cambio a través de la tecnología y la creatividad al integrar la responsabilidad social en su modelo de negocio. Esta mentalidad innovadora puede generar beneficios económicos y contribuir de manera significativa al bienestar social en general.


Foto:–Freepik

En la búsqueda de soluciones integrales para los desafíos de seguridad y justicia en las regiones, surge el modelo de atención de Misiones Regionales de Seguridad A.C. (MRS), concebido sobre tres ejes fundamentales: seguridad integral y justicia, igualdad e inclusión social y fortalecimiento institucional

Finalmente, los *startups* que buscan construir un futuro sostenible y próspero no tienen otra opción más que participar activamente en la responsabilidad social empresarial, ya que es una necesidad ética. En un mundo cada vez más interconectado y consciente, todas las empresas, sin importar su tamaño o antigüedad, deben operar de forma ética y contribuir al beneficio colectivo. Al asegurarse un lugar en el mercado al hacerlo, también dejan un legado duradero que trasciende de los límites de sus propias operaciones.

EL MODELO DE ATENCIÓN DE MISIONES REGIONALES DE SEGURIDAD, A.C.

En la búsqueda de soluciones integrales para los desafíos de seguridad y justicia en las regiones, surge el modelo de atención de Misiones Regionales de Seguridad, A.C. (MRS), concebido sobre tres ejes fundamentales: seguridad integral y justicia, igualdad e inclusión social y fortalecimiento institucional. Abordar las complejidades de la seguridad desde diversas perspectivas es el enfoque holístico, reconociendo la interconexión entre seguridad, justicia y bienestar social.

El eje inicial se enfoca en la prevención del delito, la investigación criminal y la administración de justicia. MRS colabora con autoridades locales y organizaciones civiles para implementar estrategias efectivas que disminuyan la delincuencia y fomenten la seguridad ciudadana. Mediante programas de formación y concienciación, se promueve una mayor participación ciudadana y se inculca una cultura de legalidad y respeto a los derechos humanos.

Su enfoque es la mejora de la capacidad y eficiencia de las instituciones responsables de asegurar la seguridad y justicia. MRS trabaja en colaboración con entidades gubernamentales para llevar a cabo reformas institucionales, potenciar la capacitación de las fuerzas policiales y reforzar el sistema de justicia penal.

Se fomenta la transparencia, la rendición de cuentas y el respeto a los derechos humanos en todas las actividades realizadas. Sin abordar las causas subyacentes de la delincuencia y la violencia, no se puede lograr la seguridad, hecho reconocido en el segundo eje igualdad e inclusión social.

MRS está promoviendo la equidad de género, la inclusión de grupos vulnerables y el acceso igualitario a oportunidades de desarrollo para generar condiciones de vida más justas y equitativas, se llevan a cabo programas de empoderamiento comunitario, educación y empleo digno.

El eje de fortalecimiento institucional se centra en mejorar las condiciones laborales en los lugares de trabajo, promover la responsabilidad social empresarial y proporcionar asesoramiento sobre seguridad integral.

Animamos a las empresas que están comenzando sus operaciones a unirse a esta iniciativa mediante la RSE, ya que ésta no se limita a cumplir con las normativas legales y éticas, sino que también implica contribuir al bienestar de las comunidades en las que operan. Las empresas pueden desempeñar un papel activo en la construcción de sociedades más seguras, justas e inclusivas al participar en iniciativas de MRS.

Además, alinearse con los valores de RSE puede mejorar la reputación corporativa y generar un impacto positivo en la percepción de la marca. ■


Foto:–Freepik

El eje inicial se enfoca en la prevención del delito, la investigación criminal y la administración de justicia. MRS colabora con autoridades locales y organizaciones civiles para implementar estrategias efectivas que disminuyan la delincuencia y fomenten la seguridad ciudadana

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

Omar A. Ballesteros, director general y CEO de Ballesteros y Barrera Servicios de Protección.
ballesteros.barrera@hotmail.com

LOS SECRETOS DEL LENGUAJE NO VERBAL

MÉXICO

El lenguaje no verbal es el conjunto de gestos, tonalidades y movimientos que participan en la comunicación complementando o calificando su sentido. Juega un papel clave en la comunicación, puesto que supone un porcentaje muy elevado del mensaje que se emite, y es crucial para transmitir las propias ideas e interpretar lo que nos dicen los demás.

La lista de herramientas de que disponemos para utilizar en el lenguaje no verbal es muy amplia: desde gestos y posturas a una expresión facial determinada o al contacto visual, así como la comunicación a través de objetos, ya sea la ropa o el peinado.

Según el tipo de lenguaje no verbal que se utilice, una misma frase puede adquirir sentidos completamente diferentes y puede llegar a describir el tipo de relación existente con la otra persona.

ASPECTOS DEL LENGUAJE NO VERBAL

Existen tres aspectos a tener en cuenta dentro del lenguaje no verbal que operan al mismo tiempo para transmitir una impresión global que proporciona significado a lo que manifestamos verbalmente, así como a nuestra asertividad.

- **La paralingüística o lenguaje paraverbal:** Se refiere a los códigos sonoros que acompañan la emisión del lenguaje verbal, como el tono, el volumen, el timbre de voz, la entonación, la velocidad del discurso, las pausas o los carraspeos, entre muchos otros. Estos sonidos transmiten información adicional, matizan, reafirman o incluso pueden llegar a contradecir el discurso verbal.
- **La kinésica o gestos y movimientos del cuerpo:** Se realizan a lo largo del discurso. Con ello, nos referimos a las expresiones faciales, las muecas, la sonrisa, la dirección de la mirada, el contacto visual, la duración de la mirada, los movimientos de los brazos y las posturas.
- **La proxémica:** Es el manejo del espacio personal y la distancia con los interlocutores. El espacio entre ambos interlocutores varía de una cultura a otra y de un contexto a otro.

Es importante no analizar un gesto o una reacción de forma aislada. El conjunto de varias conductas será los que nos pueda llevar a sacar alguna conclusión sobre el mensaje que desea transmitir el emisor.

El éxito en la comunicación depende del funcionamiento correcto y adecuado de todos los componentes del sistema de comunicación. La comunicación no verbal necesita ser congruente con la comunica-


Foto: Freepik

La psicología del vestir es una rama que se enfoca en estudiar la relación entre la ropa y el comportamiento humano. Esta disciplina se centra en analizar cómo la ropa influye en nuestra forma de pensar, sentir y actuar

ción verbal y viceversa para que en su totalidad resulte comprensible y sincera.

LO QUE DEBES SABER

- Gestos, miradas, incluso la ropa o el peinado forman parte del llamado lenguaje no verbal.
- Es crucial para transmitir lo que pensamos y poder interpretar lo que los demás nos dicen.
- Para que resulte comprensible y sincera necesita ser congruente con la comunicación verbal.
- Siempre recomiendo ver más allá de lo que expresa el cuerpo en el movimiento de articulaciones, un experto en lenguaje corporal debe ser también otro factor que es la ropa.

PSICOLOGÍA DEL VESTIR: DEFINICIÓN Y SIGNIFICADO

La psicología del vestir es una rama que se enfoca en estudiar la relación entre la ropa y el comportamiento humano. Esta disciplina se centra en analizar cómo la ropa influye en nuestra forma de pensar, sentir y actuar.

La ropa es una herramienta de comunicación no verbal que utilizamos para transmitir información sobre nosotros mismos a los demás. A través de la elección de nuestra ropa, podemos expresar nuestra personalidad, nuestro estado de ánimo, nuestra profesión, nuestra cultura y muchos otros aspectos de nuestra identidad.

Además, la ropa también puede afectar nuestro estado emocional y nuestra autoconfianza. Por ejemplo, vestirnos con ropa elegante y sofisticada puede hacernos sentir más seguros y poderosos, mientras que vestirnos con ropa cómoda y relajada puede hacernos sentir más relajados y cómodos.

En resumen, la psicología del vestir nos ayuda a entender cómo la ropa puede influir en nuestra psicología y en nuestras relaciones con los demás. Al comprender cómo la ropa afecta nuestro comportamiento y nuestras emociones, podemos utilizarla de manera más efectiva para lograr nuestros objetivos y mejorar nuestra calidad de vida.

INFLUENCIA DE LA ROPA EN LA ACTITUD PERSONAL

La ropa que utilizamos en el día a día puede tener un gran impacto en nuestra actitud y comportamiento. Muchas veces, la forma en que nos vestimos puede influir en cómo nos sentimos y cómo interactuamos con los demás.

Cuando vestimos ropa que nos hace sentir cómodos y seguros, es más probable que nos sintamos más confiados y seguros de nosotros mismos. Por otro lado, si usamos ropa incómoda o que no nos gusta, puede afectar negativamente nuestra autoestima y hacernos sentir menos seguros.

Otro aspecto importante es la percepción que los demás tienen de nosotros según la ropa que usamos. Si vestimos de manera profesional en el trabajo, es más probable que se nos tome en serio y se nos vea como alguien competente. Por otro lado, si usamos ropa demasiado casual, es posible que los demás nos vean como poco serios o desinteresados.

En definitiva, la ropa que utilizamos puede influir en gran medida en nuestra actitud y comportamiento, así como en la percepción que los demás tienen de nosotros. Por lo tanto, es importante elegir prendas que nos hagan sentir cómodos, seguros y que se ajusten al entorno en el que nos encontramos.

La ropa que elegimos usar no sólo nos protege del clima, sino que también puede afectar nuestra psicología y comportamiento. Desde la elección de colores hasta la calidad de los materiales, cada detalle puede enviar un mensaje sobre nosotros mismos y nuestra personalidad. Por ejemplo, vestir de colores brillantes puede hacernos sentir más felices y confiados, mientras que los tonos oscuros pueden transmitir seriedad y autoridad.

Además, la ropa también puede tener un impacto en cómo nos perciben los demás. Si usamos prendas elegantes y bien ajustadas, es más probable que nos traten con respeto y consideración. Por otro lado, si vestimos de manera descuidada o inapropiada para la ocasión, es posible que se nos juzgue como poco profesionales o poco confiables.

Por lo tanto, es importante ser conscientes de la ropa que elegimos usar y cómo puede influir en nuestra psicología y en cómo nos ven los demás.

La próxima vez que te prepares para salir de casa, piensa en el mensaje que quieres transmitir y elige tu ropa en consecuencia. Recuerda que, en última instancia, la forma en que te vistes puede tener un impacto significativo en cómo te sientes y en cómo te tratan los demás. ■

SEGURIDAD EN LA VÍA PUBLICA

Sufrir de un asalto en la calle, es uno de los principales temores de la población en México, tan sólo en el primer trimestre de este año, el 61% de sus habitantes indicó que se sienten inseguros (as) en su ciudad. Fresnillo, Naucalpan de Juárez y Zacatecas, son las localidades que más presentan este sentimiento (95.4%, 89.6%, 89.3%, respectivamente). Los robos y asaltos (49%) son las situaciones que ocupan el segundo lugar entre la cotidianeidad de los y las mexicanas; es por ello que le compartimos los siguientes Tips de Seguridad para transitar con prevención en la calle, extraídos del Blog "Manual de Seguridad" de David Lee (con datos del INEGI en abril 2024).

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Manténgase siempre alerta y con un perfil bajo.** No se distraiga y conserve una mirada periférica del entorno. Procure bajar su perfil en la calle, si va a caminar no utilice joyería llamativa, sobre todo collares y relojes, mantenga su bolsa sujeta todo el tiempo.
2) **Evite utilizar su teléfono celular** para hablar o enviar mensajes mientras camina, y no lleve puestos sus audífonos en los oídos o colocados en el cuello.
3) **Equípese ante un posible asalto**, lleve una cartera falsa y resguarde la verdadera por debajo del pantalón o camisa. Porte un silbato profesional para pedir ayuda en casos donde considere que puede hacerlo y cuando no haya sido sometido aún por un delincuente. Si considera utilizar productos de defensa personal, infórmese sobre su funcionamiento modo de uso y restricciones.
4) **Camine con seguridad.** Camine en contrasentido de los vehículos para evitar ser abordado de manera sorpresiva por un auto, motocicletas o asaltantes. Utilice calzado cómodo que le permitan caminar y hasta correr si es necesario.
5) **Identifique sospechosos.** Los delincuentes son, por lo general, hombres entre 17 y 45 años que no suelen estar acompañados de niños o adultos mayores. Confíe en sus instintos y esté alerta en todo momento, si alguna situación o individuos no le generan confianza, aléjese de ellos o pida ayuda. ■


Foto=Freepik

FOMENTE LA CULTURA DE LA SEGURIDAD

Consulte la revista digital en www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

ÍNDICE DE ANUNCIANTES

ASIS INTERNATIONAL | CAPÍTULO MÉXICO 217

5 afiliarte

30 Años de trabajo

1 — ***ASIS Capítulo México es el tercer capítulo más grande del mundo,*** *agrupa a más de 400 profesionales de la seguridad en México.*

30 AÑOS PROFESIONALIZANDO

Networking

2 — *Nuestra membresía está conformada por* ***directores de seguridad de empresas privadas, CEO´s, usuarios finales del sector público y privado.***

Vínculo con ASIS Internacional

3 — ***Obtén acceso exclusivo*** *a las Guías & estándares de ASIS Internacional y* ***a la base de datos de más de 34 mil profesionales de seguridad alrededor del mundo.***

Crecimiento profesional

4 — ***Obtén ascenso en tu carrera profesional*** *a través de nuestros webinars, cursos, talleres, comunidades temáticas, bolsa de trabajo.*

sin costo

Reuniones Mensuales

5 — ***Evento que reúne a los profesionales de la seguridad*** *para abordar temas relacionados con la seguridad, protección, management y liderazgo,* ***así como intercambiar experiencia y establecer una red de networking.***

Linktree

ASIS MÉXICO 217
$5,650 MXN

ASIS INTERNACIONAL
$125 USD

MAYOR INFORMACIÓN

55 3437 6890
55 1321 1289
55 1233 3446
55 3578 6160
socios@asis.org.mx

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

incluye gastos de envío

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. **(Marque así X)**

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ **Depósito en Banco Barnorte, SEA MEDIA GROUP, S. de R. L. de C. V. Cuenta: 1095 5437 37**

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: **Clabe: 0721 8001 0955 4373 78**

_____
Firma

DATOS DEL CLIENTE (para el envio de la revista):

Nombre: _____

Compañia: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envio de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato via: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2024

ALLIED UNIVERSAL®
SECURITY SERVICES
There for you.

COMPROMETIDOS CON LA SEGURIDAD DE NUESTROS CLIENTES Y LA CALIDAD EN EL SERVICIO

Allied Universal® es la empresa líder global en servicios de seguridad e instalaciones. Ofrecemos servicios de seguridad proactivos, tecnología de vanguardia y soluciones a medida para permitir a los clientes centrarse en su negocio principal.

Nuestros servicios

- **Profesionales de Seguridad Altamente Capacitados y Experimentados**
  - Investigaciones Corporativas
  - Respuesta a Emergencias
  - Protección Ejecutiva y Servicios de Inteligencia
  - Monitoreo
- **Servicios de Tecnología**
  - Videovigilancia
  - Controles de Acceso
  - Diseño, Ingeniería e Implementación de Servicios
- **Asesoría y Consultoría de Riesgos**
  - Investigaciones e Inteligencia
  - Respuesta a Emergencias
  - Monitoreo y Centro de Control

Contáctanos **www.ausecurity.mx/esp** **(+52) 55 5337 0444**

Allied Universal® ha encargado y publicado el primer **Informe Mundial sobre Seguridad.** Esta investigación innovadora documenta las opiniones y preocupaciones de 1,775 jefes de seguridad de 30 países. El informe completo, las principales conclusiones, las opiniones de los expertos en seguridad y los videos están disponibles en **https://www.worldsecurityreport.com/**


2 ANIVERSARIO
2004 - 2024
SEPSISA®
SEGURIDAD PRIVADA
"Somos gente cuidando a la gente y lo más valioso para ti"
Guardias, guardias armados, custodias, custodias blindadas y custodias armadas.
Cobertura a nivel nacional.
www.sepsisa.com.mx
comercial@sepsisa.com.mx
55 5351 0402
REPSE
AMESP
COPARMEX