SEGURIDAD®
EN AMÉRICA

Especial:

Mujeres en la seguridad

Seguridad para hoteles

Seguridad en casinos y centros de entretenimiento

Reportaje: Técnicas en pruebas de confianza e investigaciones

Año 24 / No.143
Marzo - Abril

www.seguridadenamerica.com.mx

COBERTURA NACIONAL

A QUIEN VALOR MERECE

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

@MultiprosegOficial @MULTIPROSEGOFICIAL MULTIPROSEG OFICIAL

ALGUNOS DE NUESTROS CLIENTES

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

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

CDMX
CIUDAD DE MÉXICO

CNS
COMISIÓN NACIONAL DE SEGURIDAD

ASIS INTERNATIONAL
CAPÍTULO MÉXICO 217

redconocer
de prestadores de servicios
Entidad de Certificación y Evaluación

ISO

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE

ema
entidad mexicana de acreditación, a.c.

ANERPV
Asociación Nacional de Empresas de Rastreo y Protección Vehicular

COPARMEX

REPSE
Registro de Prestadoras de Servicios Especializados u Obras Especializadas

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

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

Año 24 / No. 143 / Marzo - Abril / 2024

Portada:
SEPSISA

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. 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 INTERNATIONAL · ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD · AMESP · Circulo logistico · ANERPV

EXPERTOS EN
TRASLADOS VIP
Y PROTECCIÓN EJECUTIVA

grip®
global risk prevention

CON GUSTO LO ATENDEREMOS:

55·1391·6570

comercial@grip.mx

www.grip.mx
Global Risk Prevention

NUESTROS SERVICIOS:

- Protección Ejecutiva
- Traslados VIP
- Estudios de confianza
- Análisis de vulnerabilidades
- Vigilancia y detección de vigilancia y contravigilancia
- Capacitación en armas de fuego

CERTIFICADOS ISO 9001:2015

#SOYGRIPER

PODCAST the box IN EXECUTIVE PROTECTION

EDITORIAL

Ecuador vive una de las mayores crisis de seguridad de su historia reciente. Un violento asalto a una canal de televisión, secuestros de policías, fuga de importantes líderes criminales de las cárceles e incursiones de grupos armados en universidades son algunos de los episodios que han golpeado recientemente a este país sudamericano. Esto llevó a su actual presidente, Daniel Noboa, a declarar la existencia de un "conflicto armado interno" en el país, ordenando a las fuerzas militares a restablecer el orden.

En vista de esta situación, ¿qué pueden aprender los otros países latinoamericanos de lo que está sucediendo hoy en Ecuador?

1. MAYOR (Y MEJOR) PRESENCIA ESTATAL

De acuerdo con BBC, una de las cosas más importantes para frenar el avance del crimen organizado es la presencia del Estado en los distintos territorios.

El Observatorio Ecuatoriano de Crimen Organizado (OECO), en un informe sobre caracterización del crimen organizado en Ecuador, asegura que "la pobreza, el desempleo y la desigualdad", que han sufrido un "crecimiento sostenible" en los últimos años, "guardan una relación causal con el nivel de criminalidad y violencia en las ciudades".

2. CONTROL DE LA CORRUPCIÓN

Es importante que los países latinoamericanos entiendan que el crimen organizado siempre opera en la intersección entre agentes estatales, criminales y actores económicos.

En el caso de Ecuador, los investigadores han constatado que las bandas se han hecho omnipresentes en la estructura del país, expandiendo sus tentáculos no sólo en la sociedad civil, sino que también en las propias instituciones. De hecho, a mediados de diciembre de 2023, la fiscalía de Ecuador lanzó una megaoperación contra la corrupción y el narcotráfico, con decenas de redadas en distintos puntos de Ecuador.

3. MEJOR INVERSIÓN EN SISTEMAS CARCELARIOS

En Ecuador, las prisiones son el epicentro de la crisis de seguridad pública. La realidad de otros países de América Latina, como Brasil o Venezuela, no es muy diferente. Y es que las distintas penitenciarías creadas por los Estados para mejorar la seguridad de quienes están fuera de ellas han tenido un efecto inverso al buscado: se volvieron centros de comando de importantes organizaciones criminales.

Frente a esto, una urgencia para los países latinoamericanos es invertir en mejores prisiones, con un mayor sistema de vigilancia.

4. FORTALECIMIENTO DE LAS POLICÍAS

En América Latina, históricamente se ha recurrido con frecuencia a los militares para restablecer el orden ante diversas crisis de seguridad. Ecuador lo está haciendo ahora, pero países como México o Colombia también son un ejemplo de aquello.

Uno de los motivos por el que los gobiernos latinoamericanos han recurrido con tanta frecuencia a esta vía es por la percepción de debilidad de sus policías que se alimenta de casos de corrupción y profundas crisis de representatividad.

5. NO MENOSPRECIAR EL PODER DE LAS PANDILLAS LOCALES

De acuerdo con el presidente de Ecuador, Daniel Noboa, en ese país hoy operan más de 20 bandas criminales que su gobierno califica como "organizaciones terroristas". Éstas libran una lucha interna por el control de las rentables rutas del narcotráfico que existen en territorio ecuatoriano.

Por esto, se debe tener un adecuado control fronterizo y una política vecinal que ayude a ese control. Hoy, con el acceso tecnológico, los modelos de criminalidad exitosos de otros países son fácilmente replicables. ■

SISSA DIGITAL

Haciendo **Check-in** en el Futuro

www.sissadigital.com

Seguridad Electrónica Fábrica de Software Infraestructura de TI

SISSA DIGITAL

CMMI DEV | ML 3 APPRAISED
Appraisal # 67638 | Exp. Dec 22, 2026

RECONOCIMIENTO

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

En la presente edición, el director general de esta casa editorial, Samuel Ortiz Coleman, entregó un reconocimiento a Gigi Agassini, CPP, *International Security Consultant*, quien en generosas ocasiones ha presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

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

Si desea conocer más de la experta, consulte su currículo:

ENTREVISTA EXPRÉS CON

Carlos Rodrigo Roca Petricioli,

CEO de SPEC

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

Sin duda alguna es una gran oportunidad de negocio para el sector, así como un área de nuevos aprendizajes. Como proveedores de seguridad, debemos garantizar y salvaguardar la integridad de todas y cada una de las empresas que se están incorporando a estos proyectos, tanto de su personal como de los bienes materiales. Es nuestro deber demostrar y dar esa seguridad para que más y nuevas compañías volteen a ver a México como un aliado para su crecimiento, dando como resultado nuevos empleos, derrama económica y crecimiento para el país. ■

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

Marzo - Abril

ESR · Great Place To Work. · CRESE · Súper Empresas para Mujeres Expansión 2023 Top Companies · COPARMEX Ciudad de México · ASUME · CCE Consejo Coordinador Empresarial

grupoipsmexico.com

SEGURIDAD ELECTRÓNICA: *NO SÓLO MITIGAR EL RIESGO*

Foto: - Freepik

PERÚ | **Juan Carlos Portilla Gómez**

La seguridad electrónica ha venido evolucionando de manera acelerada conforme lo hacen las tecnologías

1.- INTRODUCCIÓN

A lo largo de nuestra existencia, la necesidad de garantizar la integridad ha sido permanente. La seguridad es un enfoque holístico que requiere la combinación adecuada de tecnologías y medidas físicas. La sinergia entre estos elementos proporciona un entorno más seguro y protegido, tanto a nivel personal como empresarial.

Podemos entender básicamente a la seguridad electrónica, como un conjunto de tecnologías que sirven para brindar apoyo a las operaciones de seguridad física, y en la actualidad se ha transformado en un componente importante para cualquier compañía.

2.- LA SEGURIDAD ELECTRÓNICA

Sobre su significado se han dicho innumerables definiciones, pero la que más apropiada encuentro para describirla es: "Todo sistema electrónico capaz de realizar operaciones de seguridad física" como vigilancia (monitoreo), controlar accesos, reportar alarma o alertar sobre las intrusiones a cualquier instalación.

En resumen, la seguridad electrónica no sólo actúa como una herramienta de prevención y detección, sino que también es esencial para la gestión proactiva del riesgo. Su integración adecuada en estrategias más amplias de seguridad y gestión de riesgos es vital para lograr entornos empresariales más seguros y resilientes.

3.- SINERGIA CON LA SEGURIDAD FÍSICA

No es ninguna novedad que conforme surge la necesidad de garantizar el aseguramiento físico y patrimonial de las distintas empresas y con el auge de la transformación digital, estas industrias están empezando a utilizar los sistemas de seguridad para optimizar operaciones y reducir costos.

Para cada necesidad y servicio que surge existe un tipo de seguridad electrónica diferente, que se ajusta a las múltiples condiciones que presenta el contexto.

En definitiva, la coexistencia de la seguridad electrónica y los mecanismos físicos de control es esencial para proporcionar una protección integral. Al aprovechar las fortalezas de ambas partes y promover la colaboración, se puede lograr un entorno más seguro y resistente frente a diversas amenazas.

4.- ROSI: RETORNO SOBRE LA INVERSIÓN EN SEGURIDAD

Vivimos en una era en la que la eficiencia y la justificación económica son esenciales en todas las áreas de una organización, y la seguridad electrónica no es una excepción.

Al adoptar un enfoque sistemático para justificar las inversiones en seguridad electrónica, las organizaciones pueden tomar decisiones más informadas y garantizar que los recursos se asignen de manera efectiva para mitigar los riesgos y proteger los activos críticos.

ROSI = Mitigación del riesgo monetario – Costo del control.

En resumen, mientras que el ROI evalúa cuánto dinero se ganará por realizar una inversión, el ROSI evalúa cuánto dinero se dejará de perder.

Foto: - Freepik

Para cada necesidad y servicio que surge existe un tipo de seguridad electrónica diferente, que se ajusta a las múltiples condiciones que presenta el contexto

Protectio
Seguridad Logística

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

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

EMPRESA SOCIALMENTE RESPONSABLE

COPARMEX®
CIUDAD DE MÉXICO

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

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

El uso de la IA está impulsando la innovación en la seguridad electrónica, mejorando la capacidad de anticipación, detección y respuesta a amenazas de manera más eficiente y efectiva

5.- EL NUEVO ROL DE LA SEGURIDAD ELECTRÓNICA

La seguridad electrónica ha venido evolucionando de manera acelerada conforme lo hacen las tecnologías. Esta rápida evolución no sólo ha mejorado la eficiencia y la efectividad de los sistemas de seguridad electrónica, sino que también ha ampliado el alcance de lo que es posible lograr en términos de prevención, detección y respuesta a amenazas. Sin embargo, también plantea desafíos, como la necesidad de abordar las preocupaciones de privacidad y ciberseguridad asociadas con estas tecnologías avanzadas.

La adopción generalizada de la IoT en la seguridad electrónica ha llevado a la creación de entornos más inteligentes y conectados, mejorando la capacidad de respuesta y la eficacia de los sistemas de seguridad. Sin embargo, también plantea desafíos en términos de ciberseguridad, que deben abordarse de manera adecuada para garantizar la protección de los sistemas y datos.

El uso de tecnologías en la nube en el ámbito de la seguridad electrónica representa un avance significativo para abordar desafíos cibernéticos y mejorar la eficiencia operativa de los sistemas de seguridad.

El enfoque en la ciberseguridad es crucial para garantizar la confiabilidad y la integridad de los sistemas de seguridad electrónica en un entorno cada vez más conectado. La colaboración entre fabricantes, integradores y usuarios finales es esencial para construir y mantener sistemas seguros.

La eficiencia energética, el PoE y las tecnologías asociadas desempeñan un papel vital en la eficiencia energética de los sistemas de seguridad electrónica. Al reducir el consumo de energía y simplificar la infraestructura, contribuyen a entornos más sostenibles y eficientes desde el punto de vista energético.

Otra innovación de gran valor es el desarrollo de tecnologías sustentadas en la inteligencia artificial. La cual ha sido de gran relevancia en el cumplimiento de diversos procesos, tanto de seguridad como de productividad para la empresa.

El uso de la IA está impulsando la innovación en la seguridad electrónica, mejorando la capacidad de anticipación, detección y respuesta a amenazas de manera más eficiente y efectiva. La incorporación de la IA está llevando a sistemas de seguridad más inteligentes y adaptables, lo que veremos como tendencia que involucra desarrollos muy interesantes en el campo de la IA son:

1) Búsqueda forense instantánea para videos grabados.
2) Sistemas biométricos avanzados (huella, voz, iris, movimiento, rostros, venas de la mano).
3) Detección inteligente de incendio por video.
4) Analíticas avanzadas en videovigilancia.

Estas innovaciones han permitido a las industrias y empresas fortalecer sus medidas de seguridad, adaptándose a un entorno en constante cambio y enfrentando nuevas amenazas. Sin embargo, también es importante tener en cuenta los desafíos y consideraciones éticas asociadas con el uso de estas tecnologías en el ámbito de la seguridad.

Pero, sin duda alguna al combinar la seguridad con iniciativas que impulsen la eficiencia y la productividad, las empresas pueden crear entornos más seguros y operativamente eficientes. Esta sinergia entre seguridad y productividad es fundamental para construir instalaciones inteligentes y resilientes en el contexto empresarial actual.

Foto: - Freepik

6.- CONCLUSIONES

Entender la conexión entre seguridad electrónica y negocios es esencial en la era de la Industria 4.0. Aquellos que reconocen y adoptan estas tecnologías no sólo mejoran su seguridad, sino que también abren oportunidades para la eficiencia operativa, la innovación y el crecimiento sostenible. ■

Juan Carlos Portilla Gómez,
Prosegur Tecnología.
Más sobre el autor:

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 INTERNATIONAL CAPITULO MEXICO XXI

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

LA TECNOLOGÍA PARA VIDEOVIGILANCIA AVANZA, PERO... ¿Y EL FACTOR HUMANO?

La Tecnología, por más avanzada y sofisticada que sea, nunca podrá ir más allá de su diseño y su programación. Esto significa, que nunca podrá manejar condiciones y situaciones no previstas en su diseño y su programación. Sólo el Factor Humano puede hacer frente a condiciones y situaciones imprevistas, porque sólo este factor puede reconocer, adaptarse y enfrentar condiciones y situaciones inéditas

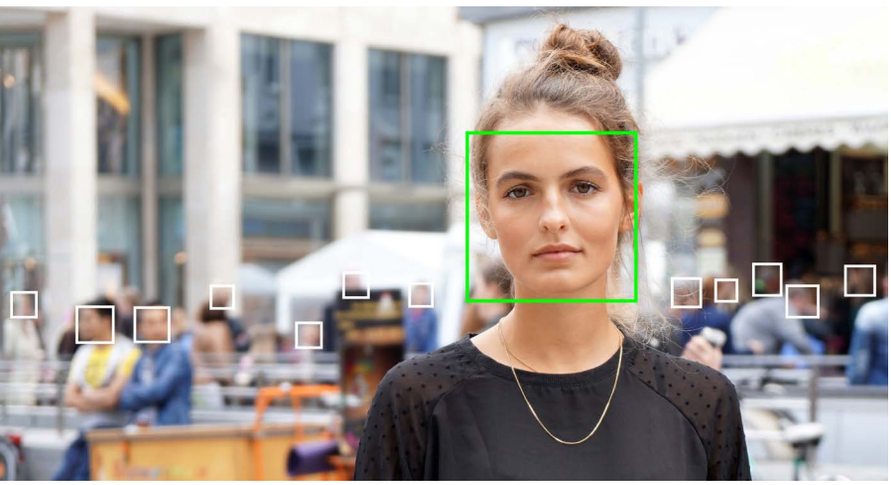


Foto: - Freepik

MÉXICO | **David Chong Chong**

En toda aplicación de la tecnología siempre se configura un binomio Hombre-Máquina. HM (o MM, por Man-Machine), en el cual los avances y la cada día mayor sofisticación en las funcionalidades por los avances tecnológicos, han ido cubriendo más y más de las tareas que antaño desempeñaba el Factor Humano, pero con mayor eficiencia, ya que lo hace más rápido, sin distracciones y prácticamente sin cometer errores, al grado de suponer que cada día se hace menos relevante el papel de este Factor, hasta que en algún momento, ya no sea necesario.

Hoy en día, con las nuevas funcionalidades en los Sistemas de Videovigilancia, es posible identificar y detectar no sólo personas y vehículos, sino con éstos en movimiento, identificar y detectar sus matrículas, identificar personas a distancia por reconocimiento facial de su fisonomía, e incluso detectar "conductas sospechosas". Y lo puede hacer con mayor rapidez, precisión y sin errores que cualquier elemento humano.

UMBRAL DE COINCIDENCIA

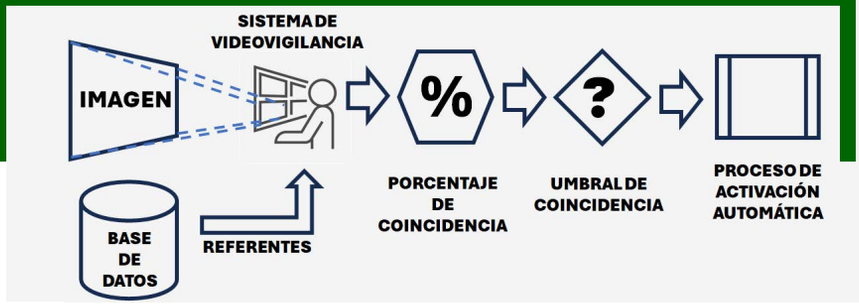
En principio, las tareas que pretenden desempeñar estas nuevas funcionalidades en los Sistemas de Videovigilancia son las que corresponden al personal de monitoreo en el marco del Proceso de Seguridad, esto es, Detectar y Alertar condiciones de riesgo que se muestren en el contenido de las imágenes proyectadas.

Pero, dado que todos estos avances y sofisticaciones funcionales se sustentan en tecnología de procesamiento de datos, sólo puede identificar y detectar los referentes que se le proporcionen. Esto porque la forma en que operan estos sistemas es comparando la imagen captada contra los referentes en su Base de Datos para determinar un porcentaje de coincidencia entre la imagen y algún referente. Y si este porcentaje supera el establecido en un "umbral de coincidencia" se puede activar una acción automática.

Los sistemas con estas capacidades proyectan un alto nivel de eficiencia, lo que ha propiciado su proliferación como solución a los problemas de inseguridad, desplegando una gran cobertura por medio de sistemas de videovigilancia, pero sin incrementar el número de elementos humanos, los monitoristas, bajo el supuesto de que las funcionalidades automatizadas pueden cubrir con mayor eficiencia el desempeño del elemento humano. Sin embargo, a pesar del alto nivel de eficiencia de este mecanismo en el desempeño de las tareas de Detección, e incluso de Alertamiento, muy superior al del elemento humano, paradójicamente su potencial de efectividad se puede ver comprometido por ciertas condiciones que sí pueden ser superadas por el elemento humano de alguna manera. Estas condiciones pueden ser, de manera enunciativa más no limitativa, las siguientes:

Si un referente no se alimenta a la Base de Datos, o no existe, el sistema no puede detectarlo, porque su capacidad de deducción e inferencia a partir de los referentes disponibles y los hechos ocurridos es limitada o inexistente. Mientras que el elemento humano sí tiene esa capacidad de deducción e inferencia para detectar referentes no disponibles previamente, o bien resultado de situaciones inéditas.

Si la imagen no tiene la calidad adecuada para distinguir detalles, la comparación que realice el sistema podría quedar por debajo del umbral de coincidencia, y por tanto no procederá al alertamiento correspondiente, en contraposición con el elemento humano, que aún con imágenes de menor calidad, podría detectar condiciones de riesgo.



Si la imagen no tiene la calidad adecuada para distinguir detalles, la comparación que realice el sistema podría quedar por debajo del umbral de coincidencia, y por tanto no procederá al alertamiento correspondiente, en contraposición con el elemento humano, que aún con imágenes de menor calidad, podría detectar condiciones de riesgo

Los referentes existentes se derivan de conocimientos previos, es decir eventos conocidos, por lo que su actuación se vuelve predecible. Y dado que la delincuencia, también cada día más sofisticada, suele infiltrarse para conocer las previsiones de Seguridad, es muy probable que pueda "enmascarar" sus acciones para quedar debajo de los umbrales de coincidencia, o incluso crear situaciones "detectables" como distractores para el sistema.

Las imágenes proyectadas desde un sistema de videovigilancia, aún con funcionalidades avanzadas y más sofisticadas, son reproducciones imprecisas de una supuesta realidad, tanto, por un efecto de degradación derivado de la concurrencia de resolución de las cámaras, ancho de banda del medio de transmisión y calidad de la reproducción en el destino, así como porque no hay certeza de que la imagen recibida por el sistema sea la misma que captaron las cámaras.

CARENCIAS, DEFICIENCIAS E INSUFICIENCIAS (CDI)

En virtud de la naturaleza heterogénea de la Seguridad, y dado que el estado natural es el de Latencia ("el riesgo está latente"), siempre existe la probabilidad que se manifiestan una o más de estas condiciones, de tal suerte que se anularía la efectividad y el alto nivel de eficiencia del sistema. En este contexto, el panorama para hacer frente a estas condiciones es que el sistema opera bajo un enfoque maniqueísta (sí o no) respecto a sus referentes, y no puede ir más allá de sí mismo, mientras que el elemento humano si puede recurrir a apoyos ajenos y externos al sistema, ya sea para subsanar su Perfil de Carencias, Deficiencias e Insuficiencias (CDI), o bien para verificar con una certeza razonable las condiciones y situaciones que le parezcan cuestionables. Y esta propensión a subestimar y menospreciar la contribución del elemento humano, propiciada por el espejismo de las posibilidades de los avances tecnológicos, ha sido la causa de que no se cumplan las expectativas creadas.

Foto: - Freepik

Las imágenes proyectadas desde un sistema de videovigilancia, aún con funcionalidades avanzadas y más sofisticadas, son reproducciones imprecisas de una supuesta realidad, por un efecto de degradación derivado de la concurrencia de resolución de las cámaras, ancho de banda del medio de transmisión y calidad de la reproducción en el destino

Foto: - Freepik

Por ello, en ese binomio HM/MM que se configura en toda aplicación de Tecnología, el Fator Humano debe ser el elemento consciente del sistema, responsable en última instancia de todas las acciones de discernimiento y decisión, porque sólo el elemento humano es capaz de valorar y tomar decisiones con información incompleta, confusa y muchas veces aparentemente contradictoria. De aquí se proyecta la conveniencia de preparar al Factor Humano para aprovechar de mejor manera los avances tecnológicos, porque la Tecnología ayuda a hacer el trabajo, pero no hace el trabajo, que es una responsabilidad de este factor. Una preparación con base en programas de capacitación y adiestramiento permanentes, acordes a los perfiles de Complejidad, Diversidad y Heterogeneidad (CDH) de las condiciones y dinámica del entorno que se pretende vigilar. ■

Con buen personal, hasta con el peor de los sistemas se puede tener éxito.
Con mal personal, hasta el mejor de los sistemas puede fracasar.

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

GARANTIZAR LA TRANQUILIDAD EN EL SECTOR HOTELERO CON SISTEMAS DE SEGURIDAD INTEGRALES

La industria hotelera, con su constante flujo de huéspedes y actividades, se enfrenta a desafíos significativos en términos de seguridad

Los directores de seguridad de los grandes hoteles deben estar preparados para abordar diversas amenazas, desde robos, hasta situaciones de emergencia en las que se ha de actuar rápidamente.

Para garantizar la tranquilidad de los huéspedes y del personal, es esencial implementar sistemas de seguridad avanzados. Para ello, es muy importante tener claras las principales amenazas a las que se enfrenta cualquier responsable de seguridad y conocer cómo las soluciones de videovigilancia, control de accesos, integración de sistemas e, incluso, la inteligencia comercial, pueden ayudar a reducir todos y cada uno de los riesgos.

La afluencia constante de personas hace que los hoteles sean blancos atractivos para los delincuentes. Desde las pertenencias de los huéspedes, hasta suministros de cocina, los robos pueden ocurrir en cualquier parte del establecimiento

AMENAZAS EN EL MUNDO HOTELERO: ¿A QUÉ SE ENFRENTA UN DIRECTOR DE SEGURIDAD?

En primer lugar, los hurtos y robos. La afluencia constante de personas hace que los hoteles sean blancos atractivos para los delincuentes. Desde las pertenencias de los huéspedes, hasta suministros de cocina, los robos pueden ocurrir en cualquier parte del establecimiento.

Junto a ello, otro de los riegos a los que se enfrentan los departamentos de seguridad de los hoteles son los actos vandálicos y los daños materiales. Estamos ante un sector enfocado a ofrecer servicios y el mejor bienestar para sus clientes, por lo que se tiene que evitar ante todo este tipo de situaciones y, en el caso de que se den, poder reaccionar de la forma más rápida posible.

Otra de las principales amenazas son los accesos no autorizados. Mantener el control sobre quién tiene acceso a áreas restringidas es crucial. Los accesos no autorizados pueden resultar en situaciones peligrosas o incluso en la pérdida de información confidencial.

En último lugar, una de las cuestiones a las que se enfrentan diariamente los departamentos de seguridad son las denuncias fraudulentas por parte de huéspedes o visitantes. Para evitar estas situaciones y tener controladas todas las áreas del hotel es necesario disponer de grabaciones e información para poder acreditar la veracidad de las declaraciones.

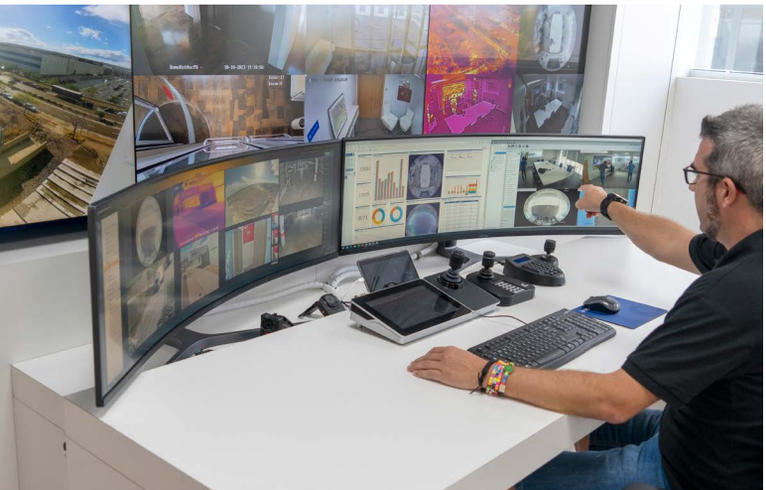
Los accesos no autorizados pueden resultar en situaciones peligrosas o incluso en la pérdida de información confidencial

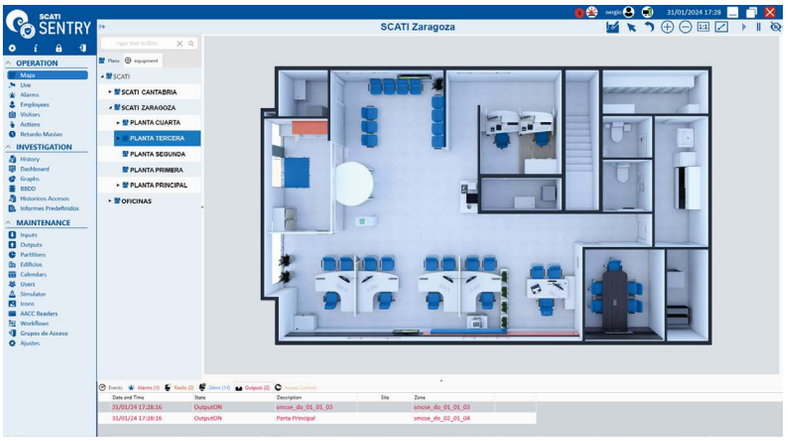
Con el fin de mitigar todos estos riegos, los departamentos de seguridad del sector hotelero cada vez están innovando más en lo que a soluciones de seguridad se refiere y con una doble finalidad: por una parte, se quiere disponer de sistemas capaces de predecir y evitar incidentes antes de que ocurran de una forma discreta y, por otra parte, este mismo sistema ha de ser capaz de anticiparse a las necesidades de los clientes para ofrecer servicios que mejoren su estancia y su satisfacción. Por ello, la única solución es instalar un sistema inteligente de seguridad integral, que cubra las cuatro cuestiones a tener en cuenta:

En primer lugar, la videovigilancia avanzada. La instalación de sistemas de video modernos proporciona una vigilancia constante en áreas clave del hotel. Las cámaras de alta resolución y la tecnología de análisis de video permiten la detección temprana de comportamientos sospechosos, brindando a los directores de seguridad la capacidad de responder de manera rápida y efectiva.

En segundo lugar, implementar sistemas de control de acceso avanzados asegura que sólo personal autorizado y huéspedes tengan accesos a áreas específicas. La tecnología de tarjetas magnéticas o incluso biometría, aumenta la seguridad y reduce el riesgo de accesos no autorizados.

Por otra parte, podemos decir que la clave de cualquier sistema de seguridad efectivo reside en la integración de sistemas.





La videovigilancia, el control de accesos y cualquier sistema de seguridad deben trabajar en conjunto. Esto no sólo mejora la eficiencia operativa, sino que también proporciona una visión más completa de la seguridad del hotel.

En último lugar, pero sin ser menos importante, los sistemas de seguridad no deben verse como un gasto para asegurar el área perimetral de la instalación: se puede sacar mucho más partido de ellos. Con esto nos referimos al aprovechamiento de los datos que ofrecen los sistemas de seguridad para mejorar el negocio, es decir, al Business Intelligence.

Con la gran cantidad de información de dichos sistemas, se pueden identificar patrones, prevenir incidentes, dar trato preferencial a algunos clientes, controlar al personal…. En definitiva, optimizar la gestión de recursos en todos y cada uno de los departamentos del hotel.

En conclusión, la seguridad en grandes hoteles es un desafío multifacético que requiere un enfoque integral. La combinación de videovigilancia avanzada, control de accesos, integración de sistemas y la aplicación de inteligencia comercial crea un entorno más seguro para los huéspedes y el personal. Los directores de seguridad deben estar siempre atentos a las últimas tecnologías y mejores prácticas para garantizar que sus establecimientos sigan siendo lugares seguros y acogedores. ■

Fuente y fotos: SCATI

LA TECNOLOGÍA LPR EN AMÉRICA LATINA: AVANCES, DESAFÍOS Y OPORTUNIDADES

La tecnología de reconocimiento de placas (LPR), también llamada reconocimiento automático de matrículas (ALPR), tiene la capacidad de capturar imágenes, convertirlas en texto y otros metadatos útiles para las autoridades

Foto: - Freepik

MÉXICO **David Sánchez**

Imagina una ciudad latinoamericana donde los desafíos de seguridad y control de acceso de vehículos se superan de manera automática y eficiente, en un entorno donde los autos ingresan sin contratiempos a los estacionamientos y donde las autoridades los puedan rastrear y localizar con precisión y en tiempo récord en caso de hurto o de fuga.

Para lograr estos beneficios, el sistema de reconocimiento de matrículas LPR emerge como una solución clave para ser tomada en cuenta por profesionales de TI y expertos en seguridad. Este artículo explora cómo esta tecnología aborda desafíos específicos, proporcionando una visión centrada en las demandas de los especialistas en seguridad.

Desde sus inicios, en 1976, la LPR ha sido empleada para el control del tráfico en entornos urbanos, su capacidad para capturar automáticamente imágenes de matrículas de vehículos, convertirlas en texto o metadatos y proporcionar información en tiempo real ha demostrado ser fundamental para mejorar la fluidez vehicular y facilitar las operaciones de las autoridades en la identificación de vehículos de interés.

Ahora bien, en la actualidad la aplicación de esta tecnología se extiende a diversas áreas, como la gestión de estacionamientos y la automatización de peajes. Además, se utiliza para fortalecer la seguridad pública, como en el caso innovador de Bogotá, Colombia, donde se implementó para mejorar la eficacia en la reacción ante hechos delictivos.

En combinación con una herramienta de análisis en tiempo real, los operadores o investigadores forenses pueden identificar vehículos de interés rápidamente, así como asistir en el procesamiento de pruebas. Además, están en capacidad de generar reportes que den cuenta de los movimientos de un vehículo en particular durante un período de tiempo específico, incluyendo miniaturas de video y detalles sobre el tiempo de detección.

¿CÓMO FUNCIONA LA LPR?

La lectura efectiva de una placa depende crucialmente de la calidad de la imagen, influenciada por diversos factores como el tipo de cámara de vigilancia (sensor, obturador, lente, etc.), la dirección y velocidad del vehículo, la iluminación, las condiciones climáticas y posibles obstrucciones. En un escenario ideal, la obtención de imágenes de alta calidad se lograría mediante cámaras de seguridad con lentes óptimas, instaladas estratégicamente y operando en entornos bien iluminados.

La adopción de un *software* de gestión de video (VMS) robusto y de plataforma abierta se vuelve fundamental. Incluso frente a imágenes de calidad inferior, sólo los sistemas más avanzados cuentan con la capacidad para integrar analíticas de diversos fabricantes de cámaras y pueden seleccionar de manera automática los fotogramas más efectivos. Estos VMS aplican métodos de mejora y verifican los números de matrícula con bases de datos gubernamentales, optimizando así los procedimientos de control de acceso y estacionamiento.

En casos de baja calidad extrema, entra en juego el aprendizaje automático, una herramienta que, aunque demandante en términos de recursos digitales y tiempo, ha demostrado ser eficaz en la resolución de crímenes de alto perfil en la vida real. Este método implica un proceso meticuloso de ajuste de propiedades de imagen, análisis manual de resultados y la enseñanza al sistema sobre los cambios que mejoran su calidad.

AVANCES EN LA TECNOLOGÍA LPR

Las cámaras y la tecnología de reconocimiento de placas (LPR) se pueden integrar en un *software* de gestión de video (VMS) o funcionar como una solución independiente. La integración de LPR en el VMS es preferible, puesto que permite aprovechar las capacidades del *software*, como alertas, notificaciones, mapas, etc.

Por otro lado, las soluciones independientes de LPR basadas en la nube pueden tener sus propias cámaras e interfaz, pero actúan como un sistema dispar. El beneficio de utilizar LPR en un *software* de gestión de video de plataforma abierta es la capacidad de ejecutar soluciones integradas y de terceros de manera simultánea. La incorporación de LPR en el VMS aprovecha toda su funcionalidad y evita sistemas aislados y flujos de trabajo desarticulados.

Los avances más significativos en la tecnología LPR incluyen la mejora de la precisión y la capacidad de extraer atributos adicionales de los vehículos; la precisión se ha mejorado mediante el uso de algoritmos de aprendizaje profundo y el aumento de la resolución de las cámaras. Los atributos adicionales que se pueden extraer incluyen el color del vehículo, el tipo de vehículo y la dirección de viaje.

Algunos sistemas también pueden leer otras etiquetas y marcas, como placas de peligro y etiquetas de envío/carga. Este alcance más amplio de información legible, junto con una mayor precisión, brinda a la industria muchas capacidades sólidas de búsqueda y análisis.

LOS NUEVOS USOS DE LA TECNOLOGÍA LPR

La tecnología LPR está encontrando aplicación en una variedad de ámbitos e industrias. Casi cualquier organización que gestione una instalación puede beneficiarse del análisis forense de incidentes y la mitigación proactiva al identificar vehículos de interés. Desde casinos hasta bancos y grandes propiedades privadas, la tecnología se ha vuelto universal para gestionar vehículos conocidos frente a desconocidos.

Más allá de la gestión del tráfico en las ciudades, esta tecnología encuentra utilidad, por ejemplo, en instalaciones de atención médica para la gestión de estacionamientos y en instituciones educativas para el control de acceso.

De igual manera, las empresas de transporte y logística utilizan la tecnología LPR para automatizar la facturación y el peaje, así como para rastrear y gestionar flotas de vehículos. Asimismo, los operadores de estacionamientos la utilizan para controlar el acceso, cobrar las tarifas e identificar vehículos que han excedido el tiempo permitido. En el sector de las gasolineras, la solución se puede integrar con listas negras y puede cerrar automáticamente surtidores en caso de que se detecte una matrícula asociada a actividades como el no pago del combustible.

DESAFÍOS Y REQUISITOS DE DISEÑO

En el contexto latinoamericano, la implementación exitosa de sistemas LPR enfrenta desafíos específicos y requisitos de diseño particulares. Es crucial contar con una infraestructura de red sólida y confiable para garantizar el funcionamiento eficiente y se requieren fuentes de alimentación e iluminación adecuadas para las cámaras, aspectos fundamentales para superar las condiciones variables de las ciudades en la región y maximizar la efectividad de la tecnología.

Al implementar sistemas, los integradores deben cumplir con los requisitos específicos de tecnología de LPR en cuanto a la posición de la cámara, la iluminación y la calidad de la imagen. Se necesita suficiente resolución, contraste y un ángulo directo para capturar claramente las placas en movimiento.

Foto: - Freepik

Adicionalmente, puede ser necesario el uso de iluminación infrarroja u otra para la legibilidad las 24 horas del día. El campo de visión debe estar controlado de manera rigurosa para cumplir con los requisitos de densidad de píxeles por el *software* de LPR. Por lo tanto, los integradores no deben esperar que esta tecnología funcione con cámaras existentes posicionadas para la vigilancia general, a menudo, se necesitan cámaras dedicadas para capturar imágenes de alta calidad de las placas en puntos clave. Comprender estos factores es fundamental para que los integradores entreguen soluciones de LPR de alto rendimiento.

Además, se deben tener en cuenta las regulaciones locales y nacionales relacionadas con la privacidad y la protección de datos.

En conclusión, la tecnología LPR tiene el potencial de transformar la seguridad y la eficiencia del tráfico en América Latina, entre otras aplicaciones. A medida que más ciudades y empresas adoptan esta tecnología, se puede esperar ver mejoras significativas en estos aspectos, con su capacidad para integrarse con los sistemas de gestión de video existentes y su creciente precisión y funcionalidad, la tecnología LPR está bien posicionada para liderar el camino hacia ciudades más inteligentes y seguras. ■

David Sánchez, gerente de Ventas de Milestone Systems para la región norte de México. *Más sobre el autor:*

TRES INNOVADORAS TENDENCIAS EN EL CONTROL DE ACCESO FÍSICO EN AMÉRICA LATINA

La importancia creciente de soluciones sostenibles, el acceso móvil y las identificaciones en billeteras digitales está remodelando cómo las organizaciones y los jefes de seguridad en la región gestionan la accesibilidad

Foto: - Freepik

MÉXICO **Alejandro Espinosa Figueroa**

En un contexto donde la seguridad y la accesibilidad se entrelazan de manera cada vez más dinámica, el campo del control de acceso se encuentra en plena evolución en América Latina. La búsqueda constante de soluciones que aborden no sólo los desafíos de seguridad, sino también la responsabilidad ambiental, ha llevado a una serie de tendencias significativas que impactan la forma en que las organizaciones abordan estos aspectos. Este artículo explorará estas tendencias emergentes, que son cruciales para las decisiones de los jefes de seguridad en la región.

Dichas tendencias, que enfatizan en el auge del acceso móvil, la comodidad de las identificaciones en billeteras digitales y la sostenibilidad de las credenciales de acceso, no sólo marcan el rumbo de la seguridad y la accesibilidad, sino que también configuran la forma en que organizaciones y usuarios finales abordan estos desafíos en entornos tanto físicos como digitales. Así las cosas, este será un recorrido por las transformaciones más notables en el ámbito del control de acceso de la actualidad.

Tras un análisis de las conversaciones en todo el mundo sobre seguridad y control de acceso, se revelan tres tendencias en este ámbito:

1. EL AUGE DEL ACCESO MÓVIL

Dispositivos como los *smartphones*, tabletas o *smartwatch* desempeñan un papel cada vez más importante en el control de acceso. Las aplicaciones móviles permiten, entre otras funciones, abrir puertas sin necesidad de tarjetas físicas, reduciendo así la huella de carbono. Pero más allá de la mera apertura de puertas, el acceso móvil se integra en la infraestructura de edificios, brindando comodidad y seguridad en múltiples espacios, desde ascensores hasta áreas de trabajo.

Además, el personal de seguridad puede proporcionar y revocar credenciales al aire, mejorando la administración del control de acceso con una plataforma digital basada en la nube, por ejemplo.

El acceso móvil gana también reconocimiento en el concepto de multiaplicación, puesto que un sólo producto o solución puede ejecutar múltiples operacio-

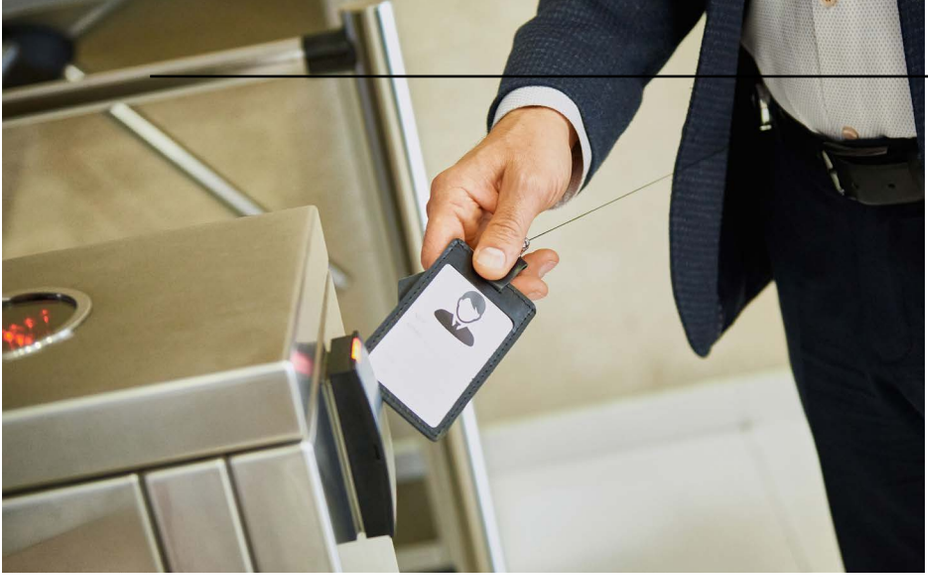


Foto: - Freepik

nes. Esta experiencia digital no sólo aumenta la eficiencia operativa, sino que también ayuda a reducir el número de tarjetas de plástico que los usuarios utilizan y pierden, lo que repercute positivamente en la seguridad y sostenibilidad.

Para citar un ejemplo en la región, podemos mencionar Davivienda, entidad bancaria que cuenta con un equipo de trabajo que suma alrededor de 18 mil personas y llega a más de 22 millones de clientes en varios países de América Latina y Estados Unidos, el banco actualizó su sistema de control de acceso incorporando credenciales móviles con la tecnología de acceso móvil y la plataforma de gestión de credenciales en la nube, lo que generó una serie de beneficios significativos para la entidad como un notable aumento en la seguridad y resultados positivos en términos de productividad y experiencia del personal.

2. IDENTIFICACIONES EN BILLETERAS DIGITALES: COMODIDAD Y SEGURIDAD

La billeteras digitales también han ganado terreno en América Latina. Esta opción permite a los usuarios acceder a lugares físicos y entornos digitales utilizando una única aplicación, lo que permite un acceso cómodo y ágil a los lugares de trabajo.

Además, esta solución ofrece seguridad a gran escala, dado que las identificaciones electrónicas pueden incorporarse directamente en las billeteras digitales que los usuarios ya utilizan para sus transacciones diarias.

La integración de la solución HID Mobile Access con las billeteras digitales simplifica el control de acceso en los edificios y mejora la experiencia del usuario. En lugar de presentar tarjetas de identificación físicas, los empleados pueden identificarse ante sus empleadores utilizando sus *smartphones* o relojes inteligentes. Simplemente, deben activar la identificación en su aplicación de billetera digital y, a partir de entonces, podrán acceder no sólo a su lugar de trabajo, sino también a las aplicaciones corporativas habilitadas. Para utilizar esta forma de autenticación sencilla y digital, todo lo que las organizaciones requieren es un lector con tecnología NFC (Comunicación de Campo Cercano).

Además del control de acceso, la identificación digital de empleado puede utilizarse en otras aplicaciones, como en computadores portátiles y estaciones de trabajo, impresión segura, acceso especial a áreas restringidas, estaciones de carga e incluso estacionamientos.

La credencial del empleado alojada en estos dispositivos se integra sin problemas con los sistemas de control de acceso y es fácil de gestionar por parte del personal interno, lo que agiliza y mejora la eficiencia de la implementación inicial.

3. CREDENCIALES SOSTENIBLES: UN ENFOQUE ECOAMIGABLE

Si bien es cierto que las credenciales móviles ganan terreno en la actualidad, en situaciones donde se requiere una tarjeta física, las organizaciones están tomando una ruta más sostenible. Cada vez es más evidente que las tarjetas fabricadas con materiales respetuosos con el medio ambiente emergen como una alternativa atractiva al plástico convencional, sin comprometer la seguridad.

Un ejemplo concreto de esta tendencia es la adopción de credenciales de control de acceso fabricadas con materiales sostenibles, las cuales están diseñadas para cumplir con los objetivos de responsabilidad ambiental al utilizar recursos renovables y contar con certificaciones que respaldan su origen ecoamigable. Este enfoque cobra cada vez más relevancia en la región, puesto que las organizaciones están en búsqueda de soluciones de control de acceso que no sólo cumplan con los estándares de seguridad, sino que también contribuyan a la reducción del impacto ambiental, demostrando así su compromiso con la sostenibilidad.

Este tipo de credenciales sostenibles son aptas para tecnologías de última generación, lo que les permite funcionar de manera eficiente con una amplia gama de sistemas y aplicaciones de control de acceso. No obstante, es importante destacar que no todas las credenciales cuentan con esta virtud. En el mercado, existen fabricantes reconocidos con la capacidad de crear credenciales de estos materiales que son compatibles con las tecnologías de vanguardia. Además, el enfoque en la seguridad proporciona una protección de datos de identidad de múltiples capas, garantizando que la información sensible esté resguardada contra accesos no autorizados. De manera similar, su versatilidad y capacidad de adaptación a diversas aplicaciones las convierten en una opción valiosa para organizaciones que buscan una solución de control de acceso segura y respetuosa con el medio ambiente.

En conclusión, la evolución del control de acceso en América Latina está siendo impulsada por tendencias que abordan la comodidad, la seguridad y la protección del medioambiente. La importancia creciente de soluciones sostenibles, el acceso móvil y las identificaciones en billeteras digitales está remodelando cómo las organizaciones y los jefes de seguridad en la región gestionan la accesibilidad. En un mundo en constante cambio, la adaptación hacia estas tendencias juega un papel crucial en la construcción de un futuro respetuoso con el medioambiente y más seguro para todos. ■

Alejandro Espinosa Figueroa,
director de Ventas de Control de Acceso de HID para México.
Más sobre el autor:

Foto: - Freepik

ABRIENDO UNA NUEVA ERA:
BIOMETRÍA REDEFINE LA SEGURIDAD Y REVOLUCIONA EL SECTOR DE LA EDUCACIÓN

Cuando los alumnos se sienten seguros, naturalmente quieren participar activamente en el proceso de aprendizaje

MÉXICO | **María Kazhuro**

A medida que el mundo conmemoró el sexto Día Internacional de la Educación el 24 de enero de 2024 con el tema "Aprender para una paz duradera", nuestra búsqueda de herramientas educativas transformadoras adquiere una gran importancia. A la luz de los problemas globales urgentes, como los conflictos violentos, la discriminación, el racismo, la xenofobia y el discurso de odio, la educación es un faro de esperanza que generará cambios.

Al analizar el mundo de la biometría, especialmente la tecnología de reconocimiento facial, empezamos a ver no sólo las formas en que puede influir en el acceso y la seguridad, sino que también descubrimos cómo ha contribuido a garantizar la paz a través del conocimiento y la inclusividad. La biometría, siendo una parte de estas relaciones simbióticas, brinda el camino hacia un sistema de educación segura, más accesible y armonizado.

Hoy en día, la tecnología biométrica se utiliza ampliamente en la industria de la educación. Sus múltiples aplicaciones transforman la seguridad y conveniencia de los estudiantes y profesores. Los protocolos modernos han reducido incluso los riesgos asociados con el uso de las técnicas biométricas tradicionales. Las tecnologías biométricas más usadas en las instituciones educativas son el reconocimiento facial y el reconocimiento sin contacto de huellas dactilares o palma.

Debido a su utilización, la biometría está ganando cada vez más confianza. Las juntas examinadoras y las instituciones educativas también pueden usar tecnología de reconocimiento facial, de voz, iris o huellas dactilares para confirmar las identidades de las personas que rinden el examen. De hecho, se ha demostrado que esto mejora la integridad académica.

Foto: - Freepik

En el mundo de la tecnología educativa que cambia rápidamente, los sistemas de reconocimiento facial representan una fuerza revolucionaria en relación con la accesibilidad, la seguridad y la inclusividad dentro de estas instituciones

BENEFICIOS DEL USO DE BIOMETRÍA EN ESCUELAS

Una de las formas más favorables y eficientes de la biometría en la educación es el monitoreo de asistencia. Los administradores pueden identificar problemas de absentismo escolar más fácilmente con la función de monitoreo biométrico automático de asistencia, que también elimina la molestia de pasar listas innecesarias antes de los cursos. Verificando a cada persona que intenta ingresar a una universidad o escuela con control de acceso biométrico puede mejorar significativamente la seguridad.

El acceso biométrico restringido también se puede utilizar para proteger áreas que están fuera del alcance de los estudiantes. La biometría puede desempeñar un papel muy importante en el seguimiento de la actividad. De hecho, se puede aplicar para rastrear varias actividades. Por otro lado, emplear procedimientos de informes manuales para registrar actividades puede llevar mucho tiempo. Los instructores pueden usar datos biométricos para mantener un diario de actividades y crear informes rápidos según sea necesario.

Sin embargo, la naturaleza sin contacto y fácil de usar de la tecnología de reconocimiento facial lo convierte en una modalidad biométrica superior en comparación con otras, como las huellas dactilares. El carácter impecable y la propiedad no intrusiva del reconocimiento facial lo hace una alternativa mucho más conveniente e higiénica para su uso en una instalación educativa.

La principal diferencia entre los escáneres de huellas dactilares y el reconocimiento facial consiste en que este último proporciona una experiencia sin contacto de acuerdo con los requisitos contemporáneos, lo que incrementa la satisfacción general del usuario. La escalabilidad, así como su simplicidad de implementación y adaptabilidad hacen que el reconocimiento facial sea una mejor opción para transformar la seguridad y la accesibilidad dentro de los entornos educativos brindando una seguridad y comodidad superior.

En el mundo de la tecnología educativa que cambia rápidamente, los sistemas de reconocimiento facial representan una fuerza revolucionaria en relación con la accesibilidad, la seguridad y la inclusividad dentro de estas instituciones. La seguridad de los estudiantes y el personal es una cuestión que las instalaciones educativas de todo el mundo tienen en común.

Los sistemas biométricos, incorporados en los puntos de acceso de dormitorios y laboratorios, agregan otra capa de seguridad. Usando biometría facial, la autenticación de los estudiantes en línea también se vuelve más fácil. Esta es una bendición para una gran cantidad de instituciones educativas que proporcionan cursos remotos que hacen que la educación sea más accesible para quienes viven en áreas remotas o tienen problemas de movilidad. Esto brinda una alternativa de bajo costo para los estudiantes que no pueden mudarse para completar su educación superior.

En lugar de una fortaleza, un campus seguro habilitado por la tecnología de reconocimiento facial evoluciona para hacerse un entorno enriquecedor donde el aprendizaje prospera. En este sentido, los establecimientos educativos equipados con medidas de seguridad tecnológicamente avanzados crean un ambiente de seguridad que impregna todas las partes creando un espacio donde ambos, los estudiantes y profesores, se sienten seguros. Una gran infraestructura de seguridad no es sólo un escudo, sino que también un acelerador de la positividad. En un escenario desprovisto de preocupaciones de seguridad, la actitud positiva se instala, estableciendo un ambiente excelente para estudiar y trabajar juntos.

Además de la sensación inicial de protección, una atmósfera de aprendizaje positiva llega a todas partes. Esto sirve como una base para el bienestar, la participación y el rendimiento académico de los estudiantes. Cuando los alumnos se sienten seguros, naturalmente quieren participar activamente en el proceso de aprendizaje.

Por lo tanto, esta participación activa constituye un catalizador por el cual mejoran los rendimientos académicos de los estudiantes, ya que es probable que asimilen y retengan los conocimientos en un entorno más adecuado para el desarrollo general. Básicamente, la combinación de las estrictas medidas de seguridad posibles gracias a la tecnología de reconocimiento facial y una mayor inclusividad da como resultado un espacio educado que no sólo protege, sino que también empuja a los estudiantes hacia el éxito académico y el desarrollo persona. ■

María Kazhuro, gerente de Desarrollo de Negocios, LATAM, RecFaces.
Más sobre la autora:

BASTA EL TOQUE DE UN DEDO PARA HACER FRENTE A LOS DESAFÍOS DE ACCESO Y SEGURIDAD DEL MUNDO REAL

La biometría de huellas dactilares ofrece una solución más precisa, eficiente y segura para que las organizaciones de América Latina enfrenten los retos que el mundo de hoy les presenta

Foto: Freepik

BRASIL

Vinicius Ferreira

La tecnología de huellas dactilares es un método consolidado y probado para autenticar usuarios en una gran variedad de industrias, aplicaciones y entornos.

La elección de la tecnología de huellas dactilares adecuada depende de varios factores cruciales, como el nivel de seguridad y precisión al momento del cotejo requerido, las funciones y características necesarias, así como la facilidad de uso para lograr la adopción de los usuarios y su productividad en el entorno de implementación.

La creciente aceptación de las tecnologías biométricas debido a su asequibilidad y fácil uso impulsa el crecimiento de este mercado en América Latina, donde se espera que crezca a una tasa anual compuesta de alrededor del 12.30 % entre los años 2023 y 2028. El aumento de las transacciones en línea, la preocupación por las actividades engañosas y el creciente gasto de los gobiernos en seguridad, son los factores que impulsan esta industria en la región.

¿POR QUÉ ELEGIR LAS HUELLAS DACTILARES?

La huella dactilar es uno de los métodos de autenticación biométrica más utilizados debido a su rapidez, facilidad de uso, alto nivel de precisión y excelente relación costo-beneficio.

Las huellas dactilares poseen cualidades únicas que las hacen valiosas para diversas aplicaciones.

En primer lugar, son universales, lo que significa que casi todas las personas las tienen. En segundo lugar, cada huella dactilar es única y distinta de las demás, lo que la convierte en un excelente identificador individual. Además, son bastante estables y permanentes y por lo general se mantienen consistentes a lo largo del tiempo. También son de fácil obtención, puesto que se pueden tomar, medir y procesar sin mayores complicaciones.

Adicionalmente, las huellas dactilares son resistentes, lo que significa que pueden protegerse contra abusos, uso indebido, robo, imitación y suplantación. En combinación con las técnicas de reconocimiento adecuadas, las huellas dactilares brindan un alto nivel de efectividad, precisión, rapidez, escalabilidad y facilidad de uso en diversas aplicaciones. Además, gozan de amplia aceptación entre los usuarios y cuentan con la tasa de adopción más alta en la industria de la autenticación biométrica, según un informe del sector.

LOS TRES COMPONENTES DE LOS SISTEMAS BIOMÉTRICOS DE HUELLAS DACTILARES

Un sistema biométrico de huellas dactilares se compone de varios elementos que trabajan en conjunto para brindar una solución efectiva.

El procedimiento comienza con el sensor de huellas dactilares diseñado específicamente para capturar y realizar un procesamiento preliminar de los datos. Posteriormente, se emplea un algoritmo biométrico para extraer detalles de las minucias de la huella, que comprenden características como puntos finales, bifurcaciones e islas de las crestas y otras medidas.

Además, durante la captura de la huella dactilar, es posible implementar una técnica de detección de intentos de suplantación (PAD, por sus siglas en inglés), para verificar la autenticidad, asegurando que provenga de un dedo vivo y no de imitaciones hechas con materiales como el látex o arcilla.

Si se cumplen las condiciones de autenticidad preestablecidas, los datos recopilados y procesados de la huella se almacenan de forma segura en un registro denominado "plantilla" dentro de un enclave de almacenamiento protegido con técnicas de cifrado.

Si es necesario llevar a cabo una operación de cotejo, la huella dactilar se somete a una nueva evaluación y la plantilla correspondiente se recupera del almacenamiento seguro para realizar este procedimiento.

A continuación, destacamos tres factores fundamentales que se deben tener en cuenta para diferenciar entre un sistema biométrico de autenticación óptimo y uno de bajo rendimiento:

- La efectividad de la captura con diversos tipos

de dedos, tonalidades de piel y condiciones de impresión en distintos entornos, incluyendo variaciones de temperatura, humedad, iluminación, presencia de aceites en la superficie, polvo o suciedad.
- La capacidad del sistema para identificar y rechazar intentos de suplantación con dedos falsos.
- La precisión del sistema al cotejar las huellas presentadas para identificar con certeza a los usuarios legítimos y rechazar a los que no lo son.

Tres componentes de los sistemas biométricos de huellas dactilares

CONSIDERACIONES FUNDAMENTALES PARA SELECCIONAR LA TECNOLOGÍA DE HUELLAS DACTILARES APROPIADA

Las consideraciones y requisitos que recomendamos tener en cuenta para seleccionar la tecnología de huellas dactilares se enfocan en encontrar un equilibrio entre el costo total de propiedad, la seguridad, la adecuación al entorno y las necesidades de la organización, así también como la funcionalidad y facilidad de uso.

Consideraciones de seguridad

- ¿La industria en la que se empleará la tecnología de huellas dactilares está sujeta a regulaciones estrictas, como sucede, por ejemplo, en los servicios financieros, la atención médica, las entidades gubernamentales o los organismos de seguridad?
- ¿Se requieren especificaciones avanzadas para la captura y autenticación biométrica?
- ¿Es necesario garantizar la inviolabilidad de las huellas dactilares y prevenir su suplantación?
- ¿Se deben implementar medidas de seguridad en los puntos finales para preservar la integridad de las redes, sistemas y datos protegidos con el cortafuegos en caso de que el dispositivo de huellas dactilares sea vulnerado?

Consideraciones sobre adecuación al entorno

- ¿La tecnología se integrará en dispositivos que requieren bajo consumo energético, funcionamiento con batería y portabilidad?
- ¿La tecnología debe adaptarse a espacios reducidos o ser utilizada en condiciones o entornos difíciles, ya sea en interiores o exteriores?
- ¿La capacidad de resistir condiciones climáticas y de iluminación impredecibles es un factor importante?
- ¿En dónde se utilizará la tecnología, en implementaciones donde su funcionamiento es esencial para el éxito de una operación, como el control fronterizo, o en usos comerciales más comunes?

Consideraciones sobre funcionalidad y facilidad de uso

- ¿La tecnología realiza de manera sencilla y consistente la captura y cotejo de huellas?
- ¿Es necesario que la tecnología procese grandes volúmenes de capturas y cotejos de huellas dactilares?
- ¿El cotejo es rápido y preciso, permitiendo a los usuarios ser productivos en lugar de causarles molestias debido a dificultades en la identificación biométrica?
- ¿El dispositivo será utilizado por diferentes personas en estaciones de trabajo compartidas?
- ¿El lector puede procesar todo tipo de huellas dactilares y adaptarse a las distintas características demográficas de la población en general?

En función de los criterios mencionados, las organizaciones pueden decidir qué tipo de tecnología de captura de huellas dactilares responde mejor a sus necesidades.

Por ejemplo, en entornos compartidos con espacio limitado —como terminales de profesionales de la salud—, una buena opción sería un sensor de huellas dactilares capacitivo delgado y resistente. En casos de uso más exigentes, en entornos con regulaciones muy estrictas y donde esta tecnología es fundamental para el desarrollo de las operaciones y en los que no se puede correr el riesgo de cometer un error en la identificación —como la banca o el control fronterizo—, se recomienda considerar tecnologías más avanzadas, como los lectores de imágenes multiespectrales (MSI).

Con sólo un toque de un dedo, la biometría permite una amplia gama de casos de uso en múltiples sectores industriales, desde la banca y el sector financiero, pasando por el comercio minorista y la atención médica, hasta el gobierno y las fuerzas de seguridad.

A medida que las industrias diseñan sus estrategias de identidad y acceso, se encuentran con amenazas y desafíos como el fraude, la apropiación de cuentas y la suplantación de identidad. La biometría de huellas dactilares ofrece una solución más precisa, eficiente y segura para que las organizaciones de América Latina enfrenten los retos que el mundo de hoy les presenta. Es por esto, que, de acuerdo con la CEPAL, los gobiernos en la región están adoptando la biometría para incrementar la seguridad y la eficiencia, mientras que las empresas la utilizan para mejorar, además de lo anterior, la experiencia del cliente. ■

Vinicius Ferreira, *Solutions Engineer* en HID Global. *Más sobre el autor:*

TIPOS DE SISTEMAS DE ALARMAS


Foto: - Freepik

COLOMBIA | Javier Nery Rojas Benjumea

Protección efectiva contra intrusiones

El sistema de alarmas es una parte del programa de seguridad física y está constituido por aquellos equipos de tecnología aplicada a la seguridad que permiten construir el segmento de detección (que es una de las tres dimensiones con las que se debe planificar este programa, las otras dos son el retardo y la respuesta), permitiendo controlar una determinada área, facilitando la tarea de los equipos de seguridad.

ELECTROMECÁNICAS:

1) Lámina metálica.
2) Interruptores magnéticos.
3) Detección de servicio de alambre (esterilla, listón, discos de presión).

VOLUMÉTRICAS:

4) En Exteriores: capacitancia, vibración, microondas.
5) En Interiores: (emisor y receptor) ultrasonido, infrarrojo pasivo, fotoeléctrico.


Foto: - Freepik

PARTES BÁSICAS DE UN SISTEMA DE SENSORES:

6) Sensor o dispositivo disparador (detecta: intruso, violación, anormalidad).
7) Circuito que transporta el mensaje al aparato señalador (tiene una alimentación o fuente de poder de 120 voltios, microprocesador PLC, módulo de control directo digital) todo sistema electrónico se debe solicitar con respaldo de batería.

FUNCIONES DE UN SISTEMA DE ALARMA:

8) Detección de fuego.
9) Detección de intrusión.
10) Notificaciones de emergencia.
11) Monitoreo de las condiciones del equipo o instalación.

PROPÓSITOS:

12) Economizar.
13) Sustituir a otras medidas de seguridad.
14) Suplementar mediante el suministro de controles adicionales.

PRINCIPIOS BÁSICOS DE LA OPERACIÓN DEL SISTEMA DE DETECCIÓN DE INTRUSIÓN:

15) Apertura de un circuito eléctrico.
16) Interrupción del haz de luz.
17) Detección del sonido.
18) Detección de vibración.
19) Detección de un cambio en la capacitancia debido a la penetración de un campo electrostático.
20) Falsas alarmas: el 98% de todas las alarmas emitidas son falsas de sistemas de alarma y son producidas por:

- Negligencia del usuario.
- Mala instalación.
- Mal servicio de mantenimiento.
- Equipo defectuoso.

Foto: - Freepik

TIPOS DE SISTEMAS DE DETENCIÓN CON ALARMA:

21) Sistema de alarma local (activan una señal visual o audio).
22) Ventajas: se detiene sociológicamente al intruso, de los costos de instalación y mantenimiento son baratos, el daño podría ser minimizado.
23) Desventajas: fácil de desactivar, el intruso probablemente no puede ser aprendido, el intruso podría no ponerle atención porque sabe que la respuesta podría tardar.
24) Sistema auxiliar (tiene una extensión directa con la policía y/o bomberos).
25) Sistema de estación central fuera de las instalaciones (se transmite desde allí a la policía y/bomberos).

MÉTODOS DE TRANSMISIÓN:

26) Cable directo anuncia los eventos de un sólo usuario.
27) Transmisión común varios suscriptores: incrementa los niveles de vulnerabilidad y podría dejar la señal fuera temporalmente.
28) Circuitos múltiples: transmite simultánea o secuencialmente las señales posibilidad de identificar cada señal.
29) Comunicación digital telefónica: las comunicaciones pueden ser usadas por otros.
30) Sistema de propiedad (es propiedad de la instalación La respuesta es inmediata).

Foto: - Freepik

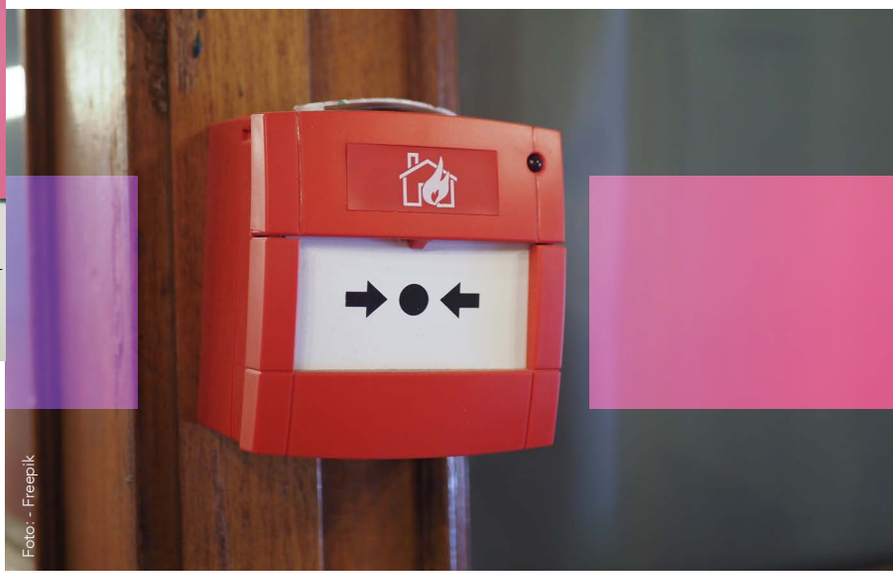


Foto: - Freepik

SISTEMAS BIOMÉTRICOS:

31) Miden una característica individual única en cada organismo vivo.
32) Características individuales únicas de las personas.
33) Voz.
34) Huella digital completa minucias.
35) Firma, dibujo, dinámica.
36) Ojos, iris, retina.
37) Mano y dedos, geometría o características vasculares.
38) Cara: termografía geometría diseño.
39) Usos principales.
40) Identificación personal.
41) Control de acceso.
42) Registro y control horario.
43) Acceso a sistemas transacciones restringidas.

BENEFICIOS DE LOS BIOMÉTRICOS EN CONTROL DE PROCESOS:

Los sistemas basados en credenciales permiten el acceso sólo a los plásticos autorizados y los PINs a quienes los conocen y recuerdan.

En cambio, la biometría no se olvida ni se pierde fácilmente, la biometría siempre se lleva consigo y no se presta, identificación automática. ■

Javier Nery Rojas Benjumea, MBA, CPP,
Board Certified in Security Management.
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.

Más sobre el autor:

Protección contra incendios durante la construcción

Existen, durante la construcción, muchas fuentes de ignición, como trabajos de soldadura, conexiones eléctricas temporales, y almacenamiento de líquidos combustibles

EUA

Las condiciones, sobre todo al final de la construcción de un edificio, son propicias para un incendio que puede suponer graves riesgos tanto para los trabajadores como para la propia estructura. Varios factores pueden contribuir a la ocurrencia de incendios en la obra, por lo que es esencial implementar medidas de seguridad para prevenir y manejar tales incidentes.

Por ejemplo, un hotel, en los últimos meses antes de su apertura, es un edificio bajo intensa actividad, comúnmente llamada como la "recta final". Esta fase se caracteriza por un mayor nivel de presión por parte del contratista general que resultan en esfuerzos de todos los subcontratistas, enfocados en completar las tareas restantes y llevar el proyecto a su conclusión. A medida que el proyecto se acerca a su finalización, se hace mucho hincapié en el cumplimiento de los plazos establecidos de entrega. Durante estos momentos, la prevención de incendios está lejos de las prioridades de los miembros del equipo de construcción.

Efectivamente, un tema que raramente se evalúa durante la construcción, son las medidas de seguridad contra incendios que se deberían tomar. La realidad es que los edificios en construcción, así como las edificaciones que están siendo renovadas o demolidas, tienen una más alta probabilidad de incendiarse que los edificios ya construidos. Existen, durante la construcción, muchas fuentes de ignición, como trabajos de soldadura, conexiones eléctricas temporales, y almacenamiento de líquidos combustibles.

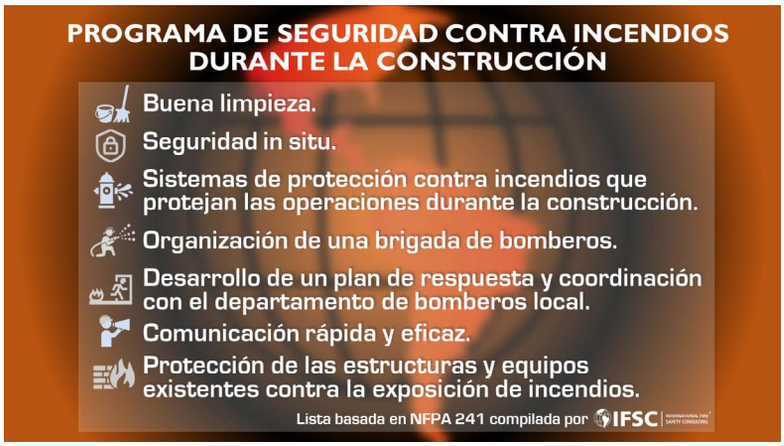
El incendio se puede extender fácilmente pues los sistemas de protección contra incendios del edificio están sin terminar y las protecciones pasivas están incompletas. La falta de cerramiento exterior hace que el viento pueda tener una incidencia importante en el rápido desarrollo de las llamas. Como mencioné anteriormente, durante esta intensa actividad, el edificio está repleto de trabajadores, mientras que las escaleras de evacuación están aún sin cerramientos adecuados y el sistema de alarma contra incendios está inoperable o todavía no instalado.

Foto Cortesía IFSC

El más reciente análisis estadístico de la NFPA, entre el 2017 y el 2021, indica que la fuente principal de los incendios son los equipos para cocinar, utilizados por los trabajadores de la construcción, para cocinar sus alimentos

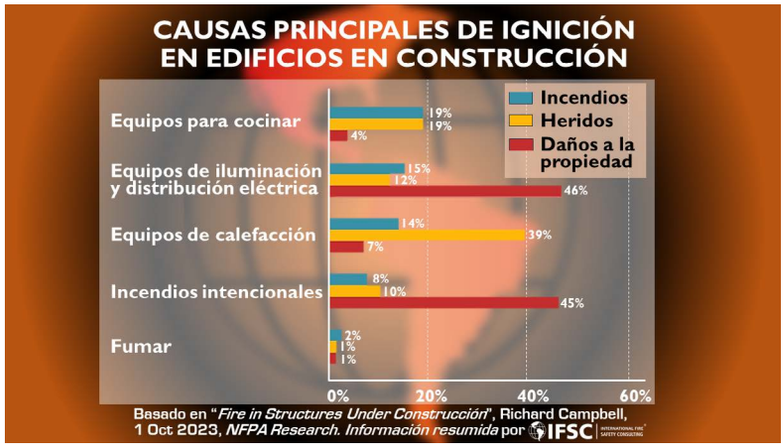
¿QUÉ DICEN LOS CÓDIGOS CONTRA INCENDIOS?

La NFPA 1, el Código de Prevención de Incendios establece las salvaguardas que deben existir en un edificio en construcción. Lo indicado en este código es un resumen de otra norma, la NFPA 241, Norma para la Salvaguarda Durante los Procesos de Construcción, Alteración y Demolición de Edificios. Estas normas requieren que se desarrolle un Plan de Seguridad Contra Incendios específico para el proceso de construcción del edificio.



FUENTES DE INCENDIOS

El más reciente análisis estadístico de la NFPA, entre el 2017 y el 2021, indica que la fuente principal de los incendios son los equipos para cocinar, utilizados por los trabajadores de la construcción, para cocinar sus alimentos. Sin embargo, incendios en los equipos de iluminación y distribución electrónica son los que causan la mayoría de los daños a la propiedad. Los incendios intencionales son también una importante causa de daños a la propiedad, lo cual apunta a tener protocolos de seguridad física en la obra.



LAS PRINCIPALES PRECAUCIONES CONTRA INCENDIOS

La NFPA 241 establece precauciones mínimas contra incendios que se deberían seguir durante la construcción, las cuales pudieran ser genéricamente resumidas así:

- **Columna de agua (*standpipe*):** A medida que la construcción va avanzando, la columna de agua debe extenderse paralelamente con la construcción del edificio. Cuando un nuevo piso se adiciona y la escalera se instale, la columna de agua debe extenderse al mismo tiempo.
- **Mangueras:** Aunque las mangueras ya no son requeridas en edificios altos, durante la construcción del edificio, se deben conectar mangueras con pitones, las cuales deben permanecer conectadas a la columna de agua en aquellas áreas donde la construcción esté en proceso. Estas conexiones pueden ser Tipo II o III.
- **Conexiones para Bomberos:** Las columnas de agua deben estar conectadas a conexiones para bomberos, las cuales deben estar estratégicamente marcadas y ser fácilmente accesibles a los bomberos locales.
- **Extintores:** Debe haber un extintor por lo menos por cada piso.
- **Hidrantes de calle:** La red contra incendios y los hidrantes deben ser instalados, completados y puestos en servicio antes de la que la construcción de la estructura pueda comenzar. Se permite que los trabajos de cimentación puedan comenzar antes de la finalización de los hidrantes.
- **Rociadores Automáticos:** Si se requiere en el edificio la instalación de rociadores automáticos, estos se deben poner en servicio lo más pronto posible.
- **Alarma de Incendios:** En edificios grandes o muy altos debe existir un equipo de alarma audible para iniciar una alarma de evacuación.
- **Escaleras:** En edificios de más de un piso, por lo menos una escalera debe estar disponible y utilizable en todo momento y que cumpla los requerimientos de la NFPA 101.
- **Fumar:** Se debe restringir a los trabajadores para que no fumen dentro de la obra.
- **Basura:** La basura se debe eliminar diariamente al final del día.
- **Pre-Planeamiento de Incendios:** Debe existir un plan que establezca como el equipo de construcción y los bomberos locales van a afrontar un incendio en el edificio durante su construcción.
- **Programa de Seguridad de Incendios:** Se debe desarrollar un programa de seguridad contra incendios que enfatice limpieza, seguridad, instalación de los sistemas de protección contra incendios, organización y entrenamiento de la brigada contra incendios, desarrollo del Pre-Planeamiento de Incendios con el departamento de bomberos local, comunicación, y consideraciones de los riesgos especiales, entre otros.

Foto: - Freepik

UN INCENDIO TÍPICO

En un viaje a la Ciudad de Panamá, tuve la oportunidad de corroborar lo antes mencionado de primera mano. Me encontraba en una reunión, cuando nos informaron sobre un incendio en progreso, en una de las torres más altas de esa ciudad, y salimos directamente hacia el edificio. El incendio se generó en el piso 52 de una torre de oficinas en sus fases finales de construcción. La Torre, llamada Costa del Este Financial Park, se encuentra en el sur de la ciudad, en una de sus zonas más modernas. El edificio tiene una altura de 205 metros, un área construida de aproximadamente 1000 m2 por piso, con fachadas tipo muro cortina. El incendio se generó en la torre de enfriamiento en la azotea del edificio.

El edificio estaba protegido con rociadores automáticos, pero estos no estaban operativos en el momento del incendio. Afortunadamente, el espectacular incendio no pasó a mayores, pero puso en relieve una vez más que la arquitectura que se está construyendo en esta ciudad, como en muchas otras capitales latinoamericanas, por su tamaño y altura, requiere de sistemas de seguridad contra incendios modernos, eficaces y eficientes.

Mientras estaba en el sitio del incendio, tuve la oportunidad de conversar con los bomberos responsables de la emergencia, quienes me informaron que no habían podido llegar con agua a la base del incendio, pues la columna de agua todavía no estaba operando. Les expliqué, luego de un par de cálculos simples, la logística necesaria para poder llegar con agua al incendio. Les sugerí conectar dos carros de bomberos en serie, suplidos desde los hidrantes de calle, inyectando agua por las conexiones para bomberos, para así, en la conexión para manguera en la columna de agua en el último piso, conectar finalmente mangueras para poder extinguir el incendio. Quedó claro para todos que un pre-planeamiento y subsecuente entrenamiento es esencial para poder operar efectivamente, durante una emergencia, en este tipo de edificios super altos.

La lección para mí de todo esto es que durante la construcción de cualquier edificio se debe tener una infraestructura mínima para poder controlar un incendio cuando este se declare. Por otro lado, debe existir, en los pliegos de diseño, una clara estrategia acerca de cómo mantener un nivel mínimo de seguridad contra incendios durante el proceso de construcción. ■

Incendio en la torre de enfriamiento en la azotea de esta torre de 52 pisos (Foto: Cortesía del Cuerpo de Bomberos de Panamá)

SISSA
Monitoring Integral

LA SEGURIDAD NO TIENE QUE SER UN JUEGO

Seguridad Electrónica Fábrica de Software Infraestructura de TI

SISSA MONITORING

www.sissamx.com

Foto: : Freepik

CONFLICTOS DE LA CIBERGUERRA

VENEZUELA | **Adolfo M. Gelder**

A medida que más grupos y actores se unan a la lucha, las amenazas a la seguridad cibernética no harán más que aumentar

Hace años que se considera el ciberespacio como un espacio más en el que puede desarrollarse el conflicto bélico más allá de los tradicionales tierra, mar y aire. Hay que tener en cuenta que Rusia es una de las potencias mundiales en ciberseguridad.

La situación de las guerras ha cambiado, o al menos, como la conocemos, cuando Rusia invadió Ucrania, arrancó una segunda y menos visible batalla en el ciberespacio, ellos buscaron o crearon una red voluntaria de hackeo con un grupo de Telegram de casi 200 mil usuarios, con esto lograron para secuestrar estaciones de radio rusas y transmitir el sonido de sirenas antiaéreas falsas que alertan a ciudadanos para que busquen refugio.

Muchos expertos predijeron que los *hackers* jugarían su papel en el conflicto de Ucrania, pero la escala está sorprendiendo. Ejércitos de *hackers* emergen en ambos bandos, por ejemplo, la pandilla de *hackers* rusos Killnet, con un grupo de Telegram de casi 100 mil suscriptores, trabaja directamente con los cibermilitares rusos.

Killnet ha llevado a cabo ataques perturbadores, aunque temporales, en sitios web de hospitales tanto en Ucrania como en países aliados, aunque no existe una Convención de Ginebra para la guerra cibernética, el Comité Internacional de la Cruz Roja argumenta que algunos códigos existentes podrían aplicarse. Atacar hospitales, por ejemplo, sería violar esos códigos.

Si países de la OTAN son atacados, esto también podría provocar una respuesta colectiva si se causan daños graves, el fin de semana de Pascua, el canal de Telegram de Killnet fue utilizado para crear un equipo llamado KillNATO Pshychos (mata a los psicópatas de la OTAN). En pocas horas tenía cientos de miembros y lanzó una ola de ataques que desconectaron temporalmente sitios web de la OTAN. El grupo también publicó una lista de correos electrónicos de trabajadores de la OTAN e incitó a la gente a acosarles.

Sin embargo, los hacktivistas ucranianos no sólo atacan la maquinaria de guerra rusa. Los hackeos están organizados para causar todos los problemas posibles al pueblo ruso. La ciberguerra en Ucrania es asistida por cibermilitares occidentales y compañías privadas de ciberseguridad, financiadas con millones de dólares donados por sus aliados.

Según la información publicada por UATV con referencia al Servicio de Seguridad de Ucrania, Rusia lleva a cabo una media de más de diez ciberataques diarios al país ucranio. De hecho, desde principios de año, la cifra de este tipo de ataques se ha disparado y se ha multiplicado incluso por tres con motivo de la guerra que se está librando en el norte de Europa.

Un detalle significativo, pues es lo que diferencia a las guerras modernas de las guerras del pasado. Básicamente, se trata de privar a la otra parte de obtener recursos. Además, es un acierto atacar los centros de datos. Un estudio de Venafi, una firma estadounidense especializada en protección cibernética, reveló a fines de agosto que el 77 por ciento de las organizaciones del planeta modificaron sus estrategias de ciberseguridad, como "respuesta directa al conflicto entre Rusia y Ucrania".

En los últimos meses se ha observado un creciente número de ataques dirigidos a altos cargos del gobierno de Ucrania y de su ejército, así como de diferentes países miembros de la OTAN. Este tipo de ataques suelen intentar recabar información sensible sobre movimientos de tropas, estrategia militar, aprovisionamiento de bienes de primera necesidad y armamento, etc.

Killnet ha llevado a cabo ataques perturbadores, aunque temporales, en sitios web de hospitales tanto en Ucrania como en países aliados, aunque no existe una Convención de Ginebra para la guerra cibernética, el Comité Internacional de la Cruz Roja argumenta que algunos códigos existentes podrían aplicarse

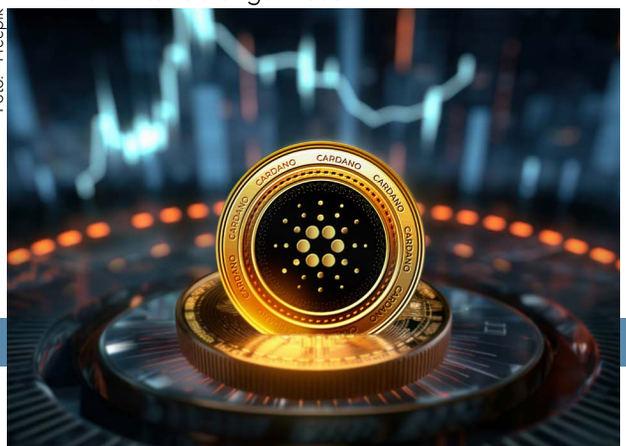
El primero fue el ataque a Viasat una hora antes de que comenzara la invasión. Se trata de una compañía estadounidense en la que confiaba el ejército ucraniano para disponer de enlaces de comunicación vía satélite.

El ejército ruso empleó un *malware* denominado AcidRain para inutilizar completamente millas de terminales de comunicaciones de la red KA-SAT, tanto *routers* como módems. Este ataque afectó también a otras infraestructuras europeas, por ejemplo, a turbinas de generación de energía eólica.

La guerra entre Rusia y Ucrania ocasionó una serie de ataques cibernéticos que afecta los servicios básicos de ambos países. La ciberseguridad y el conflicto entre Rusia y Ucrania tienen una relación estrecha porque, en un mundo cada vez más digitalizado, en el cual los procesos sociales y económicos dependen de tecnologías informáticas el planeta es testigo de enfrentamientos de tipo convencional, invasiones y tensiones diplomáticas en la frontera entre Rusia y Ucrania. Simultáneamente, se dan altercados cibernéticos entre sistemas de inteligencia y ciberactivistas (estos últimos congenian con una u otra nación). Por ejemplo:

- **Ataques a sistemas de entidades:** el 13 de enero de 2022, un *malware* destructivo atacó los equipos tecnológicos de entidades sin ánimo de lucro y empresas tecnológicas de Ucrania y dejó inutilizables los datos que contenían.
- ***Hacking* a estaciones de radio:** una estación rusa fue intervenida el 17 de enero de 2022 por un grupo cibernético, que inhabilitó la transmisión y publicó imágenes en sus señales.
- **Daños a sitios web gubernamentales:** setenta sitios web del gobierno ucraniano fueron atacados el 14 de enero de 2022; seis de ellos quedaron fuera de servicio y sin posibilidad de recuperación.
- **Secuestro de información de sistemas ferroviarios:** durante el trayecto del 24 de enero de 2022, en las vías de tren bielorrusas, un grupo de personas capturó la información del sistema ferroviario, lo que inhabilitó el transporte de tanques y maquinaria militar de origen ruso.

Foto: - Freepik



ISRAEL - PALESTINA

En la reciente guerra no parece que Israel vaya a necesitar mucha ayuda para mantener lo que ya es una clara superioridad cibernética. Si se han convertido en una de las grandes potencias militares, gran parte de culpa la tiene la inversión en desarrollo tecnológico del país, algo que no sólo incluye armamento, sino también herramientas de reconocimiento facial, las vallas inteligentes o el *software* de espionaje.

En el conflicto actual entre Israel y Hamás, se han visto a grupos hacktivistas intentar muchas de las mismas técnicas que se utilizaron con éxito contra Rusia. Sin embargo, ahora parecen ser menos eficaces. El factor principal que diferencia estas tácticas de guerra cibernética es el tiempo entre conflictos. En los 19 meses transcurridos desde que los hacktivistas declararon la ciberguerra contra Rusia, los expertos en ciberseguridad y los servicios de inteligencia de todo el mundo han tenido tiempo para analizar, prepararse y tratar de aislarse aprendiendo de las fallas de las ciberdefensas de Rusia. Después de todo, es un hecho que la guerra cibernética desempeñará un papel importante en cualquier conflicto actual y futuro. El ciberespacio actúa ahora como un segundo frente sin reglas de enfrentamiento definidas. Los hacktivistas y los grupos afiliados al gobierno pueden elegir un bando y lanzar numerosos ataques en función de sus habilidades específicas, inclinando la balanza del conflicto aparentemente con sólo unos pocos clics.

Entre los atacantes se encuentran grupos extranjeros: *hackers* rusos propalestinos y *hackers* indios proisraelíes, pero no hemos visto ataques de borrado de datos como los que sufrió Ucrania, aunque Irán está en condiciones de proporcionar tales herramientas. Es cierto que el nivel de ciberdefensa de Israel es muy alto, aún más que en Ucrania.

Por otro lado, grupos indios han atacado sitios web palestinos. Esto es una consecuencia de los lazos diplomáticos entre India e Israel. En el pasado, Hamás ha sido acusada de distribuir versiones maliciosas de la aplicación Red Alert, que la población de Israel usa para emplear notificaciones sobre bombardeos y saber cuándo tiene que dirigirse a un refugio. Estos últimos días el grupo AnonGhost parece haber atacado de nuevo a este sistema para provocar caos y confusión, pero todavía se deben analizar los detalles de este ataque y no se sabe qué tipo de vulnerabilidad, si de la aplicación o de la plataforma, se ha explotado. Los impactos producidos han sido falsos mensajes de alerta y *spam*.

En lo que se refiere a los ciberataques en el sentido contrario, no parece que Israel o su esfera de influencia los vayan a considerar esenciales en esta guerra, en la que se ha anunciado un cerco total a Gaza que bloqueará su suministro de combustible, electricidad y comunicaciones y que va a implicar un apagón total. El grado de destrucción física que están sufriendo las pocas infraestructuras tecnológicas que funcionan allí hace completamente innecesaria la utilización de ciberataques.

En cuanto al resto de la población, de momento no se ha observado un incremento en los ataques a infraestructuras críticas en otros países. Pero sí se está advirtiendo de la posibilidad de que en los próximos días Internet, y en concreto las redes sociales, se vea inundado de videos muy duros, con torturas o ejecuciones en tiempo real. Es especialmente importante saber esto, sobre todo, para proteger a los menores y a otras personas sensibles a estos contenidos que pueden afectar a su futuro desarrollo o a su salud mental. No es algo a lo que se hayan enfrentado en muchas ocasiones en el pasado y deben estar preparados.

Los hackers utilizan la región latinoamericana para entrenar a sus recursos antes de enviar un ataque destructivo contra una infraestructura mucho más madura, Latinoamérica es un cuarto de juegos para los ciberatacantes

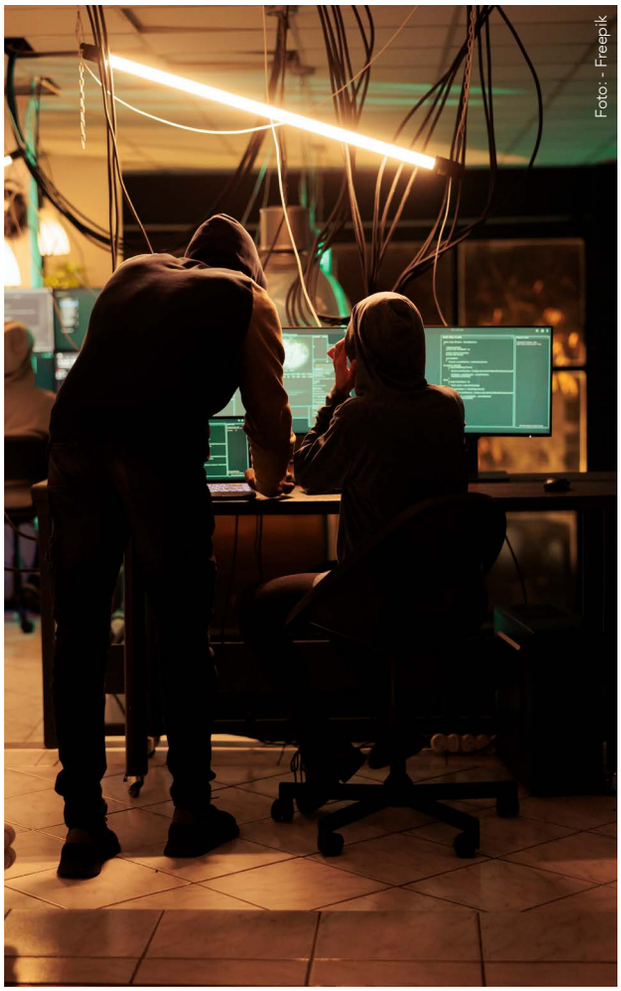


Foto: - Freepik

En el contexto del conflicto Israel-Hamas, el ciberespacio se ha convertido en un terreno fértil para la lucha encubierta, ya que se subraya la necesidad urgente de una mayor seguridad cibernética y cooperación internacional para abordar las amenazas cibernéticas en el contexto de conflictos políticos.

En última instancia, la escalada de ataques cibernéticos en el conflicto Israel-Palestina destaca la necesidad apremiante de un enfoque global y colaborativo para abordar los retos de seguridad cibernética en el mundo actual. La colaboración entre países, agencias de seguridad y sectores público y privado se vuelve esencial para identificar, rastrear y neutralizar las operaciones de estos grupos extremistas en línea.

En resumen, la incorporación de Libyan Ghosts Hackers a la lista de actores cibernéticos en el conflicto Israel-Palestina subraya la necesidad apremiante de una acción global coordinada para abordar las amenazas cibernéticas en evolución, proteger las infraestructuras críticas y garantizar la seguridad de las personas en línea.

FINANCIAMIENTO POR CRIPTOMONEDAS

Una vez pasada la fiebre, las criptomonedas han vuelto a aparecer en Gaza, donde nadie las esperaba. Estas monedas digitales han sido la forma de evitar las restricciones de financiación de Hamás, la Yihad Islámica Palestina (YIP) y Hezbolá, que habrían recibido cantidades equivalentes a decenas de millones de dólares en los últimos meses a través de esta vía, según datos del Gobierno de Israel y firmas de la industria cripto, recogidos por The Wall Street Journal. Entre ellos, YIP habría sido quien habría recibido una suma mayor, con una cifra que ronda los 93 millones de dólares. Algunas de las cuentas ya estarían siendo cerradas por Tel Aviv, aunque la sospecha es que sólo podrán hacerlo con un pequeño porcentaje de ellas, ante la dificultad de seguir el rastro de las cadenas de bloques en las que circulan estas divisas.

LATINOAMÉRICA CUARTO DE JUEGO PARA LOS *HACKERS*

Los *hackers* utilizan la región latinoamericana para entrenar a sus recursos antes de enviar un ataque destructivo contra una infraestructura mucho más madura, Latinoamérica es un cuarto de juegos para los ciberatacantes; *hackers* internacionales vulneran los sistemas informáticos de instituciones y empresas como parte de su proceso de entrenamiento, para incluirlos en operaciones más complejas.

Ante la eventualidad de que la guerra de Ucrania y la crisis de Taiwán escalen, expertos en ciberseguridad latinoamericanos consideran que el Canal de Panamá, que es esencial para el comercio mundial, está en un "gravísimo riesgo", como en otras infraestructuras de pasos navales bloqueados por Rusia en medio de su guerra contra Ucrania.

Al igual que en el conflicto rusoucraniano, el número de ciberataques ha aumentado. Pero no podemos hablar de ciberguerra: son principalmente ataques de denegación de servicio, una congestión intencional sin gravedad que hace que un sitio web sea inaccesible durante algunas horas.

CONCLUSIONES

No hay duda de que se está produciendo una guerra cibernética en línea junto con la actual guerra física. Por ahora, el impacto de estos ataques cibernéticos parece ser mínimo y sólo causan interrupciones menores. A medida que más grupos y actores se unan a la lucha, las amenazas a la seguridad cibernética no harán más que aumentar. Agregaremos actualizaciones a este artículo a medida que se produzcan ataques cibernéticos importantes. ■

Referencias:

- *www.google.com*
- *www.defensa.com*
- *www.alainet.org*
- *www.theconversation.com*

Adolfo M. Gelder, gerente general en S&S Consultores Corporativos. *Más sobre el autor:*

LA TECNOLOGÍA
Y EL SOPORTE TÉCNICO
APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA




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

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD ALAS SOCIO ALAS

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

Achilles No. 329,814

COPARMEX

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

WWW.PEM-SA.COM

gerenciacomer@pem-sa.com 222 141 12 30

CARACTERÍSTICAS DE UN PROGRAMA DE SEGURIDAD INFORMÁTICA

Foto: - Freepik

COLOMBIA | Javier Nery Rojas Benjumea

El arte de reducir y administrar el riesgo requiere comunicación y cooperación entre todos los niveles de la organización

Toda vez que las medidas implementadas en un programa de seguridad, afectan de una u otra forma la productividad de las empresas en su campo de aplicación especifica, surge como un verdadero problema, la implementación de medidas en lo relacionado con la protección de los bienes informáticos o seguridad de la información, habida cuenta que hoy día la gran mayoría de la información de las empresas, está contenida en los medios de almacenamiento y transmisión electrónicos.

Dicho lo anterior es importante referir las características que debería tener todo programa de seguridad de los bienes informáticos, para que de una parte brinde los mínimos requerimientos de protección y a su vez no se convierta en un obstáculo en el desarrollo de las tareas diarias de los operadores de los sistemas.

CONFIDENCIALIDAD

La confidencialidad de la información asegura que sólo aquellos con suficientes privilegios y una demostrada necesidad pueden acceder a cierta información, es un concepto parecido al de la compartimentación, cada colaborador debe saber únicamente lo necesario para el efectivo cumplimiento de sus funciones. Para lograr este objetivo se deberían tener en cuenta, entre otras, las siguientes medidas:

- **Aplicación de políticas de seguridad:** Las políticas son los lineamientos generales, dictados desde la alta dirección, que formulan los parámetros que debe cumplir la organización para el logro de los objetivos formulados en la estrategia empresarial.
- **Clasificación de la Información:** Hace referencia a que todo documento realizado en la organización, debe tener asignado un parámetro de divulgación, en tanto su contenido sea más o menos sensible para la empresa.
- **Almacenamiento seguro de documentos:** Los lugares donde la información es almacenada, ya sea en medios físicos o electrónicos, deben ser protegidos físicamente, para evitar el acceso fraudulento, o sustracción deliberada, así como los daños producidos por riesgos naturales, accidentales o provocados.
- **Criptografía:** Es el arte de cifrar o codificar la información, en general la información más sensible debe estar protegida bajo este parámetro.

Por lo general el nivel de identificación es dado mediante un nombre de usuario o ID; su manejo confidencial, así como su permanente actualización son claves a la hora de la implementación

DISPONIBILIDAD

Consiste en tener acceso a la información sin interferencia y sin obstrucción. Disponibilidad no implica que la información sea accesible para cualquier usuario, lo que significa es que tenga disponibilidad sólo para usuarios autorizados.

PRIVACIDAD

La definición de privacidad no se enfoca sobre la libertad de observación o acceso a la información, se debería enfocar en el uso de la información en formas conocidas para la persona que la provee. Es ahora posible recolectar y combinar información desde diferentes fuentes, las cuales han producido detalladas bases de datos cuyos componentes podrían ser usados de manera incorrecta, o sin la debida autorización del dueño de la información. Existen varios métodos técnicos para proteger las bases de datos y documentos con información sensible, en este sentido, es también importante proteger la información durante su transmisión por las redes internas y externas.

IDENTIFICACIÓN

Un sistema de información posee las características de identificación cuando es capaz de reconocer usuarios individuales. La identificación es el primer paso en conseguir el acceso para el material seguro, y sirve como soporte para las subsiguientes autenticación y autorización. La autenticación e identificación son esenciales para estandarizar el nivel de acceso o autorización que se le concede a un individuo. Por lo general el nivel de identificación es dado mediante un nombre de usuario o ID; su manejo confidencial, así como su permanente actualización son claves a la hora de la implementación.

AUTENTICACIÓN

La autenticación ocurre cuando un control da pruebas de que el usuario posee la identidad que suministra. Existen algunos *hardware* en criptografía que facilitan este mecanismo.

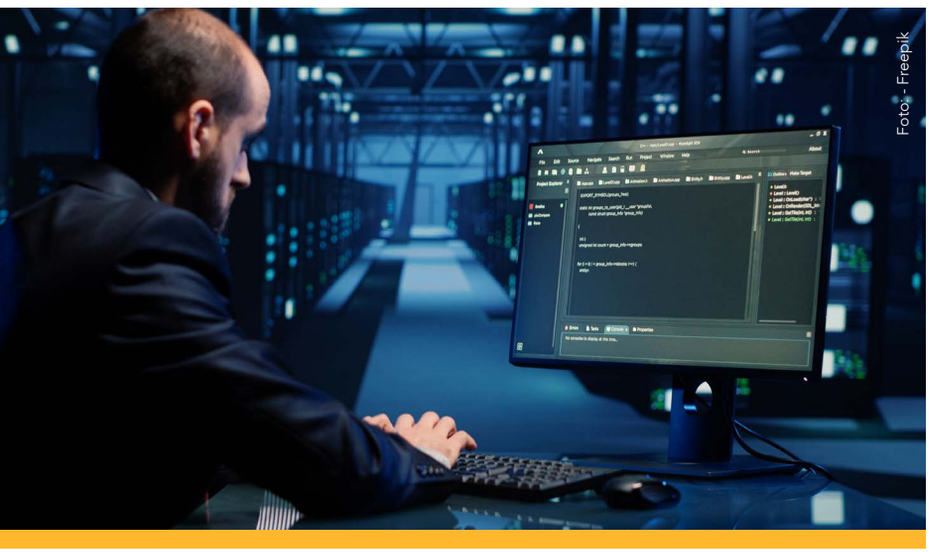


Foto: - Freepik

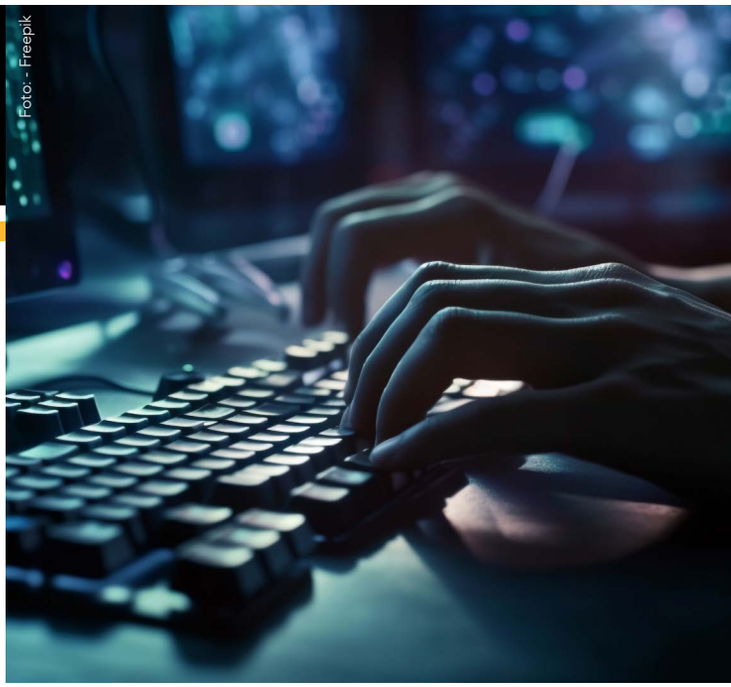


Foto: - Freepik

AUTORIZACIÓN

Después de que la identidad del usuario es autenticada, un proceso llamado autorización da la seguridad de que un usuario ha sido específicamente y explícitamente autorizado para acceder, actualizar o eliminar los contenidos de un archivo, un ejemplo de este control es la activación o uso de listas de control de acceso y grupos de autorización en un ambiente de trabajo en red. Es una característica muy importante cuando se utilizan varias terminales donde las personas pueden adicionar o cambiar datos a la información contenida en bases de datos.

Un programa de seguridad en información exitoso, combina estos y otros elementos. El arte de reducir y administrar el riesgo requiere comunicación y cooperación entre todos los niveles de la organización.

En otras palabras, el aseguramiento de los activos de información puede ser alcanzado sólo a través de la administración cuidadosa y la concientización de todos los colaboradores, lo cual genera cultura en torno al tema de la Seguridad. ■

Referencias:

- *Comentario del libro: Management of information security, Michael Whitman y Herbert Mattord.*

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

DECÁLOGO DE *BRANDING* PARA CREAR UNA IMAGEN SÓLIDA DE LAS EMPRESAS DE SEGURIDAD PRIVADA

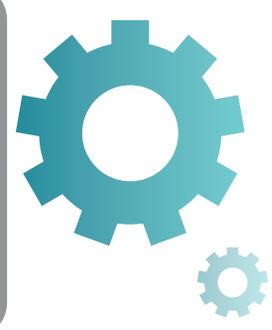
MÉXICO | **Julieta Alvarado Aldama**

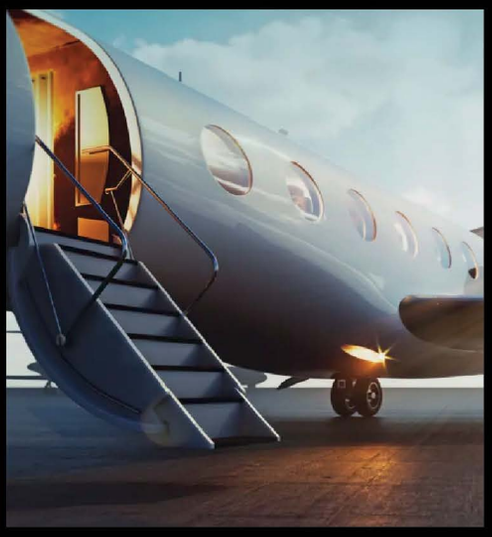
La mercadotecnia es una herramienta indispensable para todas las empresas, hoy quisiera hablar de un elemento muy importante llamado '*Branding*'. Philip Kotler, el padre de la mercadotecnia, define al *branding* como el "ejercicio estratégico y creativo que lleva a una compañía a estar en la mente de sus consumidores/clientes". Es por eso que es indispensable utilizarlo para darle identidad y sentido a lo que hacemos, a continuación, les comparto diez aspectos a considerar para crear y consolidar la imagen que quieren proyectar de su empresa de seguridad privada.

Foto: - Freepik

1. ¡Conoce tu marca! Plantéate cuál es su propósito y su diferenciador en el mercado.
2. Evalúa tu posicionamiento. ¿Qué te hace único?
3. Define tu identidad de marca. ¿Cómo van a poder diferenciarte del resto?
4. Construye una imagen corporativa que esté alineada a tus valores y principios.
5. Utiliza la autenticidad de tu marca para sobresalir ante tu competencia.
6. ¿Cuáles son los valores de tu marca? ¿Qué aportas a la sociedad, a tus clientes y a la competencia?
7. Evalúa el nivel de lealtad de tus clientes ¿Qué nivel de compromiso tienen?
8. Siempre busca innovar, sé trascendente en el sector.
9. Pregúntate si tu marca es perdurable. ¿Su esencia permanecerá?
10. No olvides tu eslogan, dale a tu marca ese sentido de expresar su propósito. ■

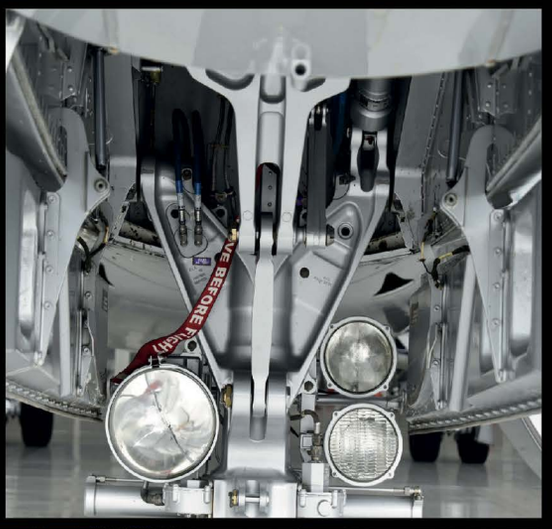
Julieta Alvarado Aldama, fundadora JUMI-MKT y líder de la Comunidad Nextgen ASIS Capítulo México 217, responsable de Mercadotecnia y Comunicación en Multiproseg, y miembro del Steering Commmitte de la Comunidad NextGen de ASIS Internacional. *Más sobre la autora:*





JVP

LOGÍSTICA



SEGURIDAD

Comprometidos con nuestros clientes excediendo sus espectativas, superándonos constantemente y adaptándonos a cada una de sus necesidades, ofrecemos:

. Servicio de protección para ejecutivos de alto perfil en todo el país.
. Entrenamiento de Seguridad Corporativa.
. Seguridad de integridad física y personal.
. Desarrollo de inteligencia y mapas de riesgo.
. GPS y monitoreo en tiempo real (COI).

/jvplogistica

@jvplogistica

55 81 08 05 87
55 67 02 34 79

https://www.jvplogistica.com/

Foto: - Freepik

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

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

MÉXICO | **Hermelindo Rodríguez Sánchez**

PROVEEDORES

1. El oficial de seguridad debe solicitar que el personal externo se registre en la "Bitácora de Proveedores".
2. El oficial de seguridad debe registrar en el formato correspondiente, el ingreso de unidades de carga y descarga, la descripción de la unidad, hora de llegada, producto o materiales, cantidad o piezas, número de factura o remisión, hora de salida y el nombre de quien autorizo el ingreso.
3. Si la espera excede diez minutos, reportar al gerente de Área o jefe de Operaciones, asentar los comentarios y observaciones con el motivo por el cual no se autorizó el ingreso.

Nota: La única persona autorizada para regresar a algún proveedor o contratista es el gerente de Planta.

VISITANTES

1. El oficial de seguridad, a través de un breve cuestionamiento, a manera de entrevista, deberá preguntar el nombre de la persona a quien visita, el motivo de su visita y de la empresa que representa.
2. Solicitar la autorización del huésped "Colaborador de la empresa" para su ingreso.
3. El oficial de seguridad debe entregar un gafete de visitante a cambio de una identificación oficial, la cual quedará a resguardo como recibo, hasta que el visitante se retire de las instalaciones.

El oficial de seguridad debe entregar un gafete de visitante a cambio de una identificación oficial, la cual quedará a resguardo como recibo, hasta que el visitante se retire de las instalaciones

4. Cuando la visita se retire, debe registrar la hora de su salida en la bitácora de registro de visitantes.
5. Solamente la Dirección General o la Gerencia de Contabilidad pueden autorizar el ingreso de los clientes o de personal VIP a las instalaciones.
6. El visitante anotará los siguientes datos en la bitácora de registro:
   - Fecha.
   - Hora de entrada y hora de salida.
   - Nombre completo.
   - Empresa que representa.
   - Persona que visita.
   - Asunto a tratar en la empresa.
   - Firma.
7. En caso de que la persona solicitada no se encuentre presente o no haya llegado, el visitante podrá permanecer en la sala de espera o en la recepción. Por ningún motivo se le permitirá el acceso a las instalaciones, evitando así que deambule por el interior.
8. El gafete forma parte del procedimiento de control de acceso y el personal que lo porta no lo excluye de cumplir con los procedimientos de seguridad, por lo que no se le permitirá el ingreso a áreas restringidas si no va acompañado por el huésped o si no cuenta con la debida autorización.
9. El portador del gafete, es responsable de la pérdida o mal uso que se le dé y le obliga a portarlo en el interior de las instalaciones. El visitante deberá devolverlo en el momento que se le requiera o al finalizar su visita a la empresa.
10. El oficial registrará cualquier muestra, obsequio, material o equipo que el visitante quiera ingresar, anotando su descripción, número de serie, modelo, color, marca, tipo, etc. que ayude a su plena identificación cuando se retire, si el articulo al ingresar se quedara por tiempo indefinido, al sacarlo, se requerirá que presente el vale de salida debidamente autorizado por el huésped o el coordinador del área.
11. Por motivos de seguridad en el trabajo, está prohibido el ingreso de visitantes en compañía de menores de edad, amigos o familiares, sin previa autorización. De igual forma, se negará el acceso a la visita si se presenta bajo el influjo de alguna droga, estimulante, con aliento alcohólico o en estado de ebriedad.

Tu tranquilidad nuestra pasión

TRASECO

Seguridad Privada

Personal Operativo cualificado
(Valores, Capacitación y Adiestramiento)

- **Protección ejecutiva**
- **Guardias intramuros**
- **Custodios a bordo**
- **Custodios de vehículos**
- **Capacitación**

Ventas: 56 18829950
ventas@traseco.com.mx

Porfirio Díaz #67 int. 3,
Barrio de San Juan, Tultitlán,
Estado de México, C.P. 54900

Somos una nueva opción en protección
equipo Directivo con 30 años de experiencia en el ramo

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

AMEXSI

Cualquier movimiento de entrada y salida de bienes o materiales que sean propiedad de la empresa serán inspeccionados y controlados por el personal de Seguridad y Vigilancia en el acceso principal, a través de un vale de salida

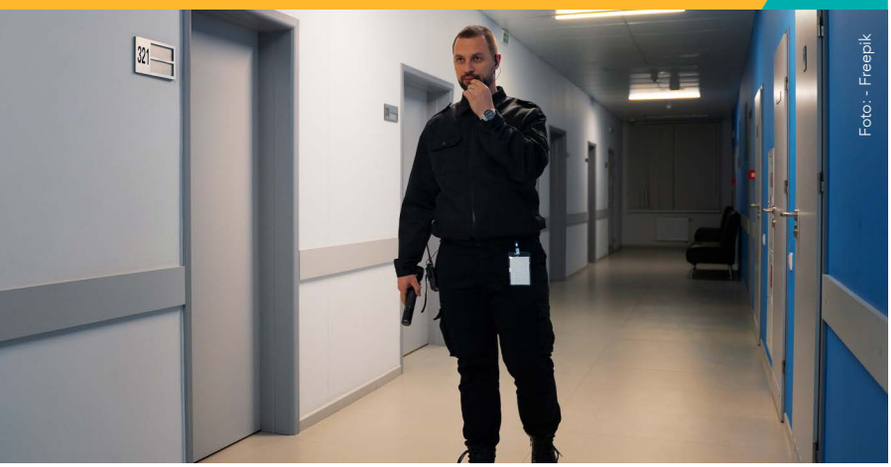


Foto: - Freepik

12. El oficial indicará a todo visitante que se disponga a salir, sobre la revisión de portafolios, bultos, cajas, bolsas, materiales o equipo. En los casos que a su salida lleve mercancía, materiales o equipo, sólo se permitirá la salida con el respectivo vale de salida autorizado, factura, remisión o carta porte, según sea el caso; si es equipo, muestra o materiales que traía al ingresar, el oficial debe verificar con el registro inicial de dicho material o equipo, para registrar en la bitácora que los artículos salieron de conformidad con lo ingresado.
13. Se prohíbe la entrada a la empresa de personas con bermudas, playeras sin mangas, tenis o huaraches.

ENTRADA Y SALIDA DE BIENES Y EQUIPOS

1. El oficial de seguridad vigilará que todos los bienes u objetos propiedad de la empresa, al salir deberán estar debidamente autorizados por escrito por el jefe o coordinador de cada área, verificando cada salida en la lista de firmas autorizadas. Sin este requisito, no se permitirá, bajo ningún concepto, la salida de bienes, objetos o materiales.
2. Cualquier movimiento de entrada y salida de bienes o materiales que sean propiedad de la empresa serán inspeccionados y controlados por el personal de Seguridad y Vigilancia en el acceso principal, a través de un vale de salida.
3. El vale de salida deberá especificar al menos:

    a) Cantidad y descripción del equipo o material.
    b) Motivo de la salida (reparación, devolución, venta, obsequio, etc.).
    c) Nombre y firma de quien autoriza.
    d) Nombre y firma de quien efectúa la salida, retira el material, equipo o mobiliario.
    e) Hora de salida y fecha.

4. Las salidas definitivas de desperdicio y basura serán autorizados por el jefe de almacén o coordinador del área, y revisados por Vigilancia para que no salgan ocultos otros productos, materiales y objetos de valor propiedad de la empresa.
5. Será responsabilidad del jefe de Área, documentar y autorizar la orden de salida de bienes, materiales o equipo propiedad de la empresa. El oficial de seguridad deberá reportar a la Dirección General o a la Gerencia de Contabilidad cualquier anomalía detectada en este procedimiento.
6. Para el retiro de basura, *scrap* o residuos peligrosos, el personal de la empresa recolectora podrá realizar el retiro entre los días lunes a viernes de cada semana. La empresa que retira la basura no puede sacar la chatarra ni manipular los residuos peligrosos.
7. El oficial de seguridad realizará el registro de los datos de la empresa recolectora, los cuales serán asentados en su reporte de novedades, siendo:
    - Fecha.
    - Nombre de la empresa recolectora.
    - Nombre del operador y de sus ayudantes.
    - Datos de la unidad de recolección.
    - Tipo de materiales que son recolectados. Hora de entrada y hora de salida.
    - Nombre de la persona que autoriza el ingreso y de quien verifica la salida.

Se deben realizar los recorridos por el perímetro interior de las instalaciones, verificando condiciones de seguridad en la misma, iluminación, defensas perimetrales y áreas de oportunidad, realizando el reporte describiendo detalladamente lo detectado en el recorrido

CRNOVA SECURITY

Custodia de Mercancía

Guardia Intramuros

Monitoreo y Rastreo

ISO 9001 · ISO 28000 · BASC Business Alliance for Secure Commerce · ISO 18788 · ISO 37001

AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C. · ESR · UN Global Compact · ASIS International

crnovaoficial

crnovasecurity

www.crnova.com.mx

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

CONTROL DE ACCESO A UNIDADES VEHICULARES

1. Verificar que el ingreso de las unidades vehiculares se realice de acuerdo al procedimiento establecido de identificación y control.
2. Los portones de acceso vehicular permanecen cerrados en todo momento y se abren sólo para el ingreso y salida de unidades de carga y particulares.
3. Antes abrir y/o cerrar el portón de acceso vehicular, el oficial de seguridad observa que no se encuentren personas y/o transportes sospechosos, en caso de detectarlo se reporta de manera inmediata a la Gerencia de Seguridad, teniendo a la mano los teléfonos de los servicios de emergencia de la zona.
4. El oficial de seguridad no debe permitir el acceso de personas que vengan acompañando al conductor (familiares o menores de edad.)
5. El oficial de seguridad no debe permitir el acceso a transportistas y empleados con aliento alcohólico, en estado de ebriedad o bajo la influencia de alguna otra droga o enervantes.
6. El oficial de seguridad permite el acceso a los transportistas que han sido identificados plenamente, a quienes se les pide registrarse en el formato correspondiente.
7. Si no se le detecta ningún objeto punzocortante, arma de fuego, artículo contundente a través de la observación, se le permitirá el acceso.
8. Se lleva una bitácora de registro de acceso para empleados y visitantes, donde se registra:
   a) Nombre de la persona.
   b) Puesto y Departamento.
   c) Nombre de la empresa que representa.
   d) Nombre de la persona con la que se entrevistará.
   e) Motivo de la visita.
   f) Hora de entrada y de salida.
9. Se le informará a la persona que ingrese a las instalaciones con unidad vehicular, que se realizará una revisión como medida de seguridad.
10. Los portones de acceso siempre deben tener colocados los candados de seguridad.
11. Si al realizarle la inspección manual se le detecta algún artículo punzocortante, arma de fuego, artículo contundente, "mantener la calma" de inmediato notificar al jefe inmediato o al área correspondiente sin perder de vista a la persona.
12. Cuando detecte que algún visitante o proveedor va a ingresar equipo personal (*laptop*, cámara fotográfica o herramientas), se le solicita que registre el ingreso de su equipo en bitácora.
13. El oficial de seguridad no debe permitir el ingreso y/o salida de personal o visitantes caminado por el acceso vehicular, que es exclusivo para unidades de uso particular y para transporte de carga y descarga.
14. El oficial de seguridad debe estar alerta para detectar personas o vehículos sospechosos ajenos a la empresa rondando por el exterior durante los horarios de entrada y salida del personal o de las unidades vehiculares, en caso de detectar alguna anomalía, se lo reportará al momento al jefe inmediato o al área correspondiente de la situación. El oficial de seguridad por ningún motivo abandonará su puesto para investigar el motivo de la presencia de estas personas.

ESTACIONAMIENTO INTERNO

1. Debe cumplir con el control de ingresos autorizados de autos, del personal Directivo, Administrativo y Operativo (utilitarios y de uso personal), así mismo se le asigna la función de vigilar el perímetro frontal de la empresa y reportar cualquier situación de riesgo.
2. El oficial de seguridad asignado a la vigilancia del estacionamiento, debe contar con un silbato, paletas de acrílico y lámpara con la finalidad de marcar el alto o el avance de las unidades que salen o ingresan, procurando que la maniobra se realice de manera segura.
3. Cualquier conducta de falta de respeto a la autoridad por parte del personal, se debe informar a la Dirección o a la Gerencia de Seguridad para tomar las medidas correspondientes, evitando entrar en controversias.
4. Debe permanecer atento a la llegada de los vehículos con el fin de constatar en lo posible el estado en que ingresan y notificar al conductor de la anomalía, evitando con esto reclamaciones posteriores.
5. Debe realizar un inventario general de las condiciones de los autos que presentan algún tipo de daño con la finalidad de evitar reclamaciones injustificadas.

Los autos que pernocten en el interior de las instalaciones deben ser reportados a la Gerencia de Operaciones para su conocimiento, en la bitácora de novedades.


Foto: - Freepik

SEGURIDAD E HIGIENE

El personal de seguridad deberá conocer el uso y manejo de los extintores e hidrantes, así como de la cantidad y ubicación de cada uno de ellos dentro de las instalaciones. Deberá verificar que los extintores no se encuentren bloqueados de manera temporal o permanente por mobiliario, tarimas, vehículos o botes de basura, reportando cuando así suceda al responsable del área de Higiene y Seguridad.

1. No está permitido el uso de cámaras fotográficas ni de video, sin la autorización correspondiente del director general de la empresa.
2. Se debe mantener la disciplina en la empresa (están prohibidas las bromas, juegos de azar y festividades fuera de orden dentro de las instalaciones).
3. Todo el personal, incluyendo el oficial de seguridad debe ajustarse al cumplimiento de todas las normas y políticas de seguridad de la empresa, siendo responsable de cualquier infracción a las mismas.
4. En caso de que se realicen trabajos de remodelación dentro de las instalaciones, se debe apegar a los procedimientos, normas y horarios establecidos por la empresa.
5. Queda prohibido el ingreso de bebidas embriagantes, enervantes, así como armas de fuego u objetos punzo cortantes (que no sean considerados dentro de las herramientas de trabajo).
6. Todo el personal, incluyendo al oficial de seguridad debe acatar las instrucciones de seguridad en el trabajo y, en su caso, detener cualquier actividad que pueda poner en riesgo la integridad física del personal, de las instalaciones o del medio ambiente.
7. Todo el personal, incluyendo el oficial de seguridad debe respetar el horario autorizado para laborar dentro de las instalaciones.

QUEDA PROHIBIDO EL INGRESO DE BEBIDAS EMBRIAGANTES, ENERVANTES, ASÍ COMO ARMAS DE FUEGO U OBJETOS PUNZOCORTANTES (QUE NO SEAN CONSIDERADOS DENTRO DE LAS HERRAMIENTAS DE TRABAJO)

Foto: - Freepik

RONDÍN DE SEGURIDAD

El personal de seguridad deberá realizar los recorridos de vigilancia durante su horario del servicio, el objetivo es salvaguardar las instalaciones y verificar que no haya ninguna anomalía. En caso de existir alguna condición de riesgo o situación irregular, se registrará en la bitácora del reporte de novedades y se mencionará a detalle, directamente a la Dirección General.

Se deben realizar los recorridos por el perímetro interior de las instalaciones, verificando condiciones de seguridad en la misma, iluminación, defensas perimetrales y áreas de oportunidad, realizando el reporte describiendo detalladamente lo detectado en el recorrido.

Al momento de realizar el recorrido, el oficial de seguridad deberá:

1. Comprobar las condiciones prevalecientes en pasillos, oficinas, puertas, techos, baños y observar que las salidas de emergencia no se encuentren bloqueadas.
2. Detectar las áreas donde el personal se reúne para platicar, fumar o disponer de tiempo libre, áreas comunes, depósitos de basura, estacionamiento, etc.
3. En el caso de detectar equipo de cómputo encendido, no se apaga, debido a que puede contener información importante por guardar. Sin embargo, esta situación se registra en la bitácora de novedades, la hora y el lugar de lo observado.
4. Mantener una estrecha vigilancia en los cristales y ventanales de la fachada exterior del inmueble.
5. Reportar el equipo contra incendio o cilindros de extintores que se encuentren caducados en su vigencia (recarga) de acuerdo a la etiqueta.
6. Reportar el mal funcionamiento de lámparas y luminarias interiores y exteriores para que sean reemplazadas a la brevedad.
7. Solicitar que se realice el mantenimiento preventivo y correctivo a los dispositivos de seguridad, alarmas y señalamientos de los que dispone la empresa como defensa perimetral. Conservar una copia del calendario de pruebas y simulacros realizados en la empresa.
8. Realizar recomendaciones al cliente para la implementación de dispositivos de seguridad física y electrónica, y aumentar los niveles de seguridad en la empresa. De ser necesario, recomendar el incremento de plantilla de oficiales de seguridad para lograr un efecto más disuasivo entre los empleados y visitantes.

El oficial de seguridad asignado a la vigilancia del estacionamiento, debe contar con un silbato, paletas de acrílico y lámpara con la finalidad de marcar el alto o el avance de las unidades que salen o ingresan, procurando que la maniobra se realice de manera segura

Foto: - Freepik

A través del rondín de vigilancia, los oficiales de seguridad tendrán perfectamente identificadas y reconocidas las instalaciones. Ante cualquier contingencia, los oficiales conocerán la ubicación de los extintores, de las salidas de emergencia, los hidrantes y los tableros de suministro de energía para cortar la energía eléctrica en caso de incendio o sismo, así como el procedimiento para la evacuación del personal.

Revisarán minuciosamente que las chapas, cerraduras y candados de puertas y cortinas, se encuentren en buen estado. Si existiera algún indicio de que fueron forzados para abrirlos, el oficial de seguridad dará parte a la Dirección de la empresa. Y así mismo a su jefe inmediato.

Durante el horario nocturno, el oficial de seguridad deberá realizar rondines de observación en todas las áreas autorizadas por la empresa, en periodos de no más de una hora y media de intervalo, registrando su recorrido por las estaciones con el puntero electrónico.

Reportará inmediatamente las condiciones en que se encuentren las instalaciones (interior y exterior) con el fin de que se detecten actos inseguros que sean producto del olvido; como puertas abiertas de las oficinas, objetos olvidados en áreas comunes, vehículos abiertos o con luces encendidas, unidades vehiculares que pernocten en el interior de las instalaciones, cafeteras, pantallas de televisión y aparatos eléctricos conectados, entre otros.

El oficial de seguridad realizará el rondín de vigilancia de acuerdo a sus consignas e indicaciones del cliente. Realizará el recorrido por el inmueble, en áreas de ingreso de personal, estacionamiento, portones de acceso, áreas perimetrales, sanitarios y vestidores de las instalaciones. En ningún momento el oficial de seguridad tendrá acceso en áreas restringidas de la empresa, a menos que sea con indicación directa y por escrito de la Dirección. De lo contrario, se realizarán los rondines solamente por su área de responsabilidad.

En el turno nocturno, el personal de Seguridad realizará los rondines de forma aleatoria por las instalaciones sin establecer rutinas ni horarios específicos; registrando en su bitácora las conductas que observe de los trabajadores, como es el caso de:

- Personal que se encuentre durmiendo en lugares obscuros y apartados.
- Participando en juegos de azar.
- Fumando, comiendo, descansando o en la comisión de acciones que pongan en peligro la seguridad de sus compañeros y de las instalaciones.
- Personal que se distrae por el uso de teléfonos celulares en áreas de maquinaria en funcionamiento, etc.
- Verificará que el personal que se encuentra en el área de producción continua, cuente con el equipo de seguridad correspondiente, de lo contrario deberá hacer la observación al supervisor en turno.

El control de encendido y apagado de las luces se realizará por parte de los elementos de seguridad, previa instrucción del personal de mantenimiento, teniendo cuidado de no apagar los interruptores del área de sistemas y de aquellas que se les indique no tocar.

El personal de Seguridad deberá verificar que el encendido y apagado de los reflectores se realice normalmente. En caso de detectar alguna falla o desperfecto, registrarlo en el reporte de novedades, indicando el lugar y el tipo de desperfecto. Al día siguiente, reportarlo de manera inmediata.

CONTROL DE ALMACÉN, CORTINAS Y RAMPAS DE CARGA

El oficial de seguridad asignado a esta área, deberá permanecer alerta mientras la unidad de transporte se encuentra cargando o descargando materiales, mercancía o producto; poniendo especial atención al personal que circula por el área y a que el acceso (rampa/cortina) no permanezca abierta al terminar las actividades.

Antes de salir las unidades de la rampa, el operador deberá presentar la salida correspondiente, el responsable de almacén habrá firmado la hoja de entrega o recepción y verificado que la cantidad de cajas o piezas son las mismas que presenta la hoja de salida, factura o remisión. El oficial de seguridad deberá coordinar la salida de la unidad asegurándose que no se encuentre otra unidad en posición de ser golpeada.

El oficial de seguridad debe registrar en la bitácora de la caseta los datos del proveedor, compañía transportista, datos del vehículo, fecha, hora de entrada / salida y el motivo del ingreso.

Los horarios designados para la recepción y entrega de materiales o producto terminado serán determinados por la Gerencia de Almacén de la empresa.

El oficial de seguridad de Patio deberá verificar que el personal ajeno al área de almacén, bodega o recibo no se encuentre en la zona de maniobras sin justificar su presencia y cuente con la autorización del personal a cargo. El oficial de seguridad debe verificar que el personal que se encuentre en el área, porte correctamente el gafete de identificación (gafete de proveedor, visitante o contratista).

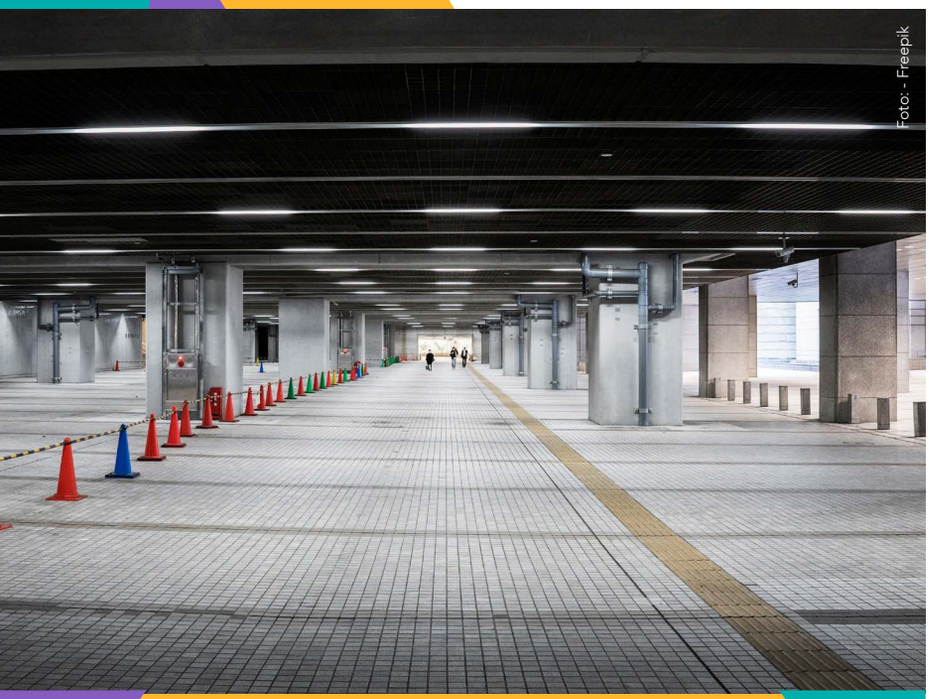


Foto: - Freepik

El oficial de seguridad no debe permitir el acceso a transportistas y empleados con aliento alcohólico, en estado de ebriedad o bajo la influencia de alguna otra droga o enervantes

El oficial de seguridad le indica la ubicación de la rampa y el número de cortina donde será atendido por personal del área.

El oficial de seguridad debe verificar que los proveedores sean atendidos de acuerdo al orden de ingreso y número de folio asignado, salvo en el caso que el supervisor del área de recibo le indique pasar a un proveedor por concepto de entrega o recepción urgente.

El oficial de seguridad debe verificar que el personal transportista y operador no raye el piso o los muros del almacén al momento de operar el montacargas o patines.

El responsable del área de recibo es el único que puede romper el sello y abrir la caja para verificar la mercancía, el oficial de seguridad hace acto de presencia para cerciorarse que se realicen los procedimientos. Se toma la numeración del sello roto y se deposita en el contenedor para recicle. El oficial de seguridad debe anotar la hora de llegada de la unidad, la hora de registro y la hora de enrampe, así como el número de tarimas, la hora de salida y el nombre de las personas que intervinieron en la operación y, si las hubiera, las observaciones correspondientes.

Una vez que la unidad fue cargada o descargada completamente, el oficial de seguridad indicará al operador de la compañía transportista que debe retirar materiales sobrantes, basura y tarimas del área de recibo de materiales.

Cuando el supervisor de recibo le informe al oficial de seguridad que será devuelto material a algún proveedor debe especificar el nombre del proveedor, la cantidad y el motivo de la devolución (material excedente, material mal facturado o material defectuoso).

El oficial de seguridad debe anotar en la bitácora de novedades los datos del proveedor, cantidad de material que será devuelto, el motivo de la devolución y la descripción de los equipos o materiales.

Si en el transcurso del turno, el oficial de seguridad detecta personal en actitud sospechosa, reporta el hecho al Centro de Monitoreo para su seguimiento y al gerente de Operaciones, de quien recibirá las acciones a seguir.

El oficial de seguridad debe verificar que el transportista porte ropa adecuada para el desempeño de sus labores, así como el calzado de seguridad, no se permite el acceso a personal con bermudas, *shorts*, tenis, zapato de vestir.

El oficial de seguridad debe registrar en la bitácora de reporte de novedades el número de la orden de salida / entrega, factura, pedido, remisión o carta porte y que cuente con la firma de autorización correspondiente, además de los siguientes datos:

- Hora de entrada.
- Hora de salida.
- Nombre de la empresa transportista o razón social del proveedor.
- Fecha.
- Nombre de quien recibe / entrega.
- Número de folio de factura.
- Vehículo, No. de placas, No. Eco.
- Cantidad de material, especificando el número de tarimas, contenedores, cinturones, *racks* y piezas (en unidades de poco volumen). ■

Foto: - Freepik

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

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

SOCIO DIRECTOR,
ALTAIR *SECURITY*
CONSULTING & TRAINING.

Más sobre el autor:

LA IMPORTANCIA DE LOS PROTOCOLOS DE SEGURIDAD *(SEGUNDA PARTE)*

LATINOAMÉRICA

Concientizar a las personas de que estamos trabajando en probabilidades y no hay ambientes 100% seguros, ayudará en gran medida a la implementación y adopción de los protocolos de seguridad. Mientras más protocolos se adopten, la probabilidad de riesgos será menor, aumentando así los niveles de seguridad

Foto: Freepik

Estamos navegando desde el mundo VUCA hasta el BANI, donde los delincuentes están aumentando, organizándose y sofisticándose, con una sociedad atemorizada y poco preparada en la prevención, así como autoridades prometiendo mucho, una sociedad y empresariado ávidos de soluciones mágicas e inmediatas y los empresarios gastando en modelos parciales y no eficaces para evitar ser víctimas.

Dando continuidad al artículo de la edición anterior, donde hablamos de la inminente necesidad de los protocolos de seguridad, qué son y cómo se componen. Se requiere de un compromiso con la gestión integral de riesgos, para identificar adecuadamente los riesgos en la empresa que están dentro del alcance definido del rol de seguridad, para hacer que esos riesgos sean transparentes y responder a los riesgos en conjunto con los líderes empresariales. Los protocolos de seguridad son una gran herramienta en la gestión de riesgos.

¿CÓMO ELABORAR PROTOCOLOS DE SEGURIDAD?

Estoy escribiendo a especialistas de seguridad y comprendo que entre ustedes hay muchísimos que saben ampliamente de ello y las metodologías son variadas; no obstante, acá pongo a su consideración uno de cuatro pasos sencillos que nos ha funcionado perfectamente y pudiera apoyarles.

Debe partirse desde una evaluación de riesgos, donde identifiquemos las amenazas y la probabilidad de que estas sucedan y su impacto consecuencial, para saber dónde estamos parados y hacia dónde debemor ir. Conocer el contexto y con lo que contamos actualmente es importante. Por supuesto, enfocarse en los tres riesgos principales ayudará en buena forma al avance del proyecto y sin el desgaste adicional de recursos.

Concientizar a las personas de que estamos trabajando en probabilidades y no hay ambientes 100% seguros, ayudará en gran medida a la implementación y adopción de los protocolos de seguridad. Mientras más protocolos se adopten, la probabilidad de riesgos será menor, aumentando así los niveles de seguridad.

Posterior al análisis viene la planeación y el diseño de las medidas, de manera que te permitan evitar agresiones (medidas preventivas), así como reaccionar eficientemente en caso que suceda, preservando la integridad y con el menor impacto a las personas o a la institución (reacción eficiente y efectiva).

La implementación de los protocolos de seguridad dará continuidad al proceso. El establecimiento de responsabilidades y tiempos de ejecución de las medidas acordadas son importantes

Esto no se establece a la ligera, incluye mesas de trabajo y discusiones, negociaciones y reflexiones colectivas para llegar a los mejores protocolos, que repercutan positivamente, pero que también eviten molestias o el entorpecimiento en las personas y/o las organizaciones. Protocolos sencillos, simples y realistas siempre serán lo mejor.

La implementación de los protocolos de seguridad dará continuidad al proceso. El establecimiento de responsabilidades y tiempos de ejecución de las medidas acordadas son importantes. Este proceso es tan importante como los otros, porque permite comenzar a permear en los colaboradores, para ir inculcando una cultura de seguridad.

Los esfuerzos de capacitación a través de seminarios y cursos, *coaching*, infografías, comunicados, procesos y otras herramientas en seguridad resultan fundamentales lograr un compromiso con el proyecto. Si bien los esfuerzos aislados sirven de alguna forma, debe aspirarse a una inmersión y capacitacion continua de todo el personal, sólo así lograremos mantener a los empleados informados sobre las amenazas presentes y los mejores protocolos de neutralización y prevención. Lograr que los métodos de entrenamiento sean más amigables, atractivos e inspiradores para fomentar la seguridad, la participación activa de los colaboradores y la retención de conocimientos, considerando escenarios y experiencias de la vida real.

Todo esfuerzo debe llevar una evaluación para una mejora continua. Los protocolos son dinámicos y pueden ir mutando constantemente, máxime después de algún contexto de riesgo o posterior a una agresión o ataque, adecuándose a las necesidades de cada persona, organización y/o contexto.

EL DUEÑO DEL PROYECTO, EL LÍDER DE SEGURIDAD

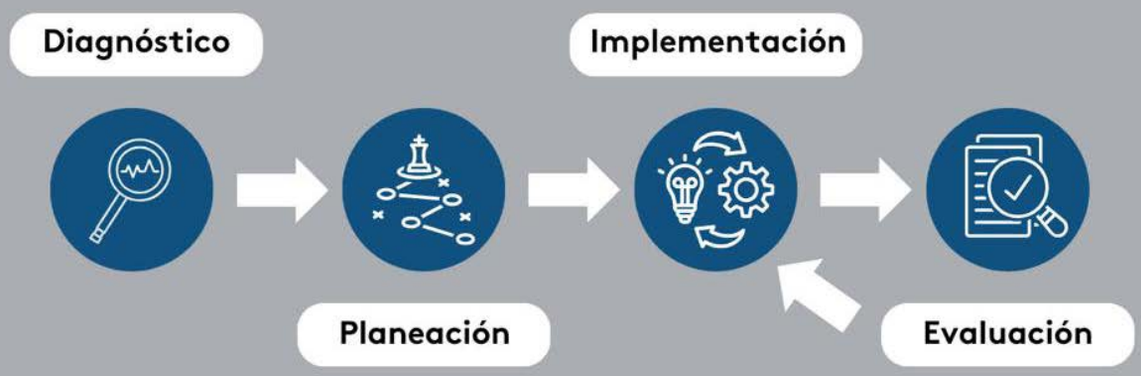
Los resultados de este proyecto dependerán de la capacidad del profesional de seguridad para alcanzar las metas. Un rasgo básico en el profesional de seguridad es la acción y estrategia. La acción está en la mente y en el corazón del profesional. El profesional de seguridad debe ser la luz que guía al desarrollo del trabajo en un ambiente humano. Es una gran oportunidad para los Profesionales de la Seguridad en ser una opción seria y viable de solución a los retos de inseguridad.

Diagnóstico de Vulnerabilidades

La finalidad del proceso de soporte y de los protocolos de seguridad, es que las personas, los activos y la continuidad de las operaciones de la compañía se encuentren debidamente protegidos, de manera que los negocios puedan desarrollar con normalidad y se salvaguarde y fortalezca la reputación de la empresa, colaborando así en el incremento de valor para la organización. Las mejores prácticas representarán el justo equilibrio entre hacer las Cosas Correctamente (eficacia y especialización) y hacer Cosas Correctas (Eficiencia y profesionalismo).

Bien decía el gran escritor y orador Zig Ziglar, en su valiosa iniciativa de ayudar a la gente "espera siempre lo mejor, pero prepárate para lo peor".

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



ESTRATEGIAS DE SEGURIDAD EN HOTELES

Este año México ingresó a la Guía Michelin, con Ciudad de México, Oaxaca, Baja California, Los Cabos, Nuevo León y Quintana Roo; como los primeros destinos; y se espera que este año incremente la derrama económica en el sector hotelero por turismo y nearshoring

Foto: Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Una de las industrias en México que promete continuar con su crecimiento para este año, es la industria hotelera, siguiendo con la tendencia que le antecedió en el año 2023 en el que se registró un Producto Interno Bruto (PIB) de 747 mil 927M pesos hasta el tercer trimestre, mostrando un alza de 3.07% con respecto al mismo periodo del año anterior[1]. En un informe emitido por Miguel Torruco, secretario de Turismo del gobierno de México, la ocupación hotelera en el país ascendió a 60.2% en los primeros siete meses de 2023; los centros turísticos con mayor ocupación hotelera fueron: Akumal (85.1 %); Playa del Carmen (84.1 %); Cabo San Lucas, (81.2 %); Nuevo Nayarit, (78.4 %); Cancún (76.4 %) y Puerto Vallarta, (76.3 %)[2].

Pero los destinos de playa no serán los únicos que requerirán para este año los servicios hoteleros, sino que con la llegada del *nearshoring* será indispensable contar con más habitaciones para los nuevos huéspedes; estados del norte como Durango, Nuevo León y Chihuahua se encuentran en los destinos industriales para este año, así como Quintana Roo.

Ejemplo de esta atracción internacional hacia el país, se ha mostrado con España, pues entre enero y noviembre del 2023, llegaron a México 333 mil 995 turistas españoles vía aérea los cuales dejaron una derrama económica de 376.3 millones de dólares, incrementando en un 3.7 por ciento mayor a lo registrado en 2019 (antes de la pandemia)[3].

Se espera que este año la industria de los hoteles continúe creciendo, tan sólo en el primer fin de semana largo del año, que fue del 03 al 05 de febrero, la estimación de la derrama económica fue de más de 46 mil millones de pesos (2 mil 680 millones 811 mil dólares) por consumo de servicios turísticos; con una ocupación hotelera a nivel nacionales de 62%, siendo cuatro puntos porcentuales más, comparado con el mismo fin de semana largo de 2023, el cual registró 58% de ocupación general, de acuerdo con información emitida por la Secretaría de Turismo previo al puente vacacional conmemorativo del Aniversario de la Constitución Política de los Estados Unidos Mexicanos.

Tanto el *nearshoring* como los atractivos turísticos del país, atraerán no sólo inversionistas, sino también a nuevos clientes potenciales del sector hotelero y de diferentes nacionalidades, cada uno con sus propias necesidades y retos de seguridad.

PRINCIPALES RIESGOS Y RETOS DE SEGURIDAD

El año 2024 es más que representativo para los mexicanos, ya que se esperan elecciones presidenciales, mismas que marcarán el camino a seguir en los próximos seis años de gobierno. La inseguridad ha invadido todo el territorio del país, las zonas turísticas no están exentas de confrontamientos entre los cárteles de droga. Uno de estos casos es Chiapas, donde el mismo gobierno del estado ha declarado que al menos dos sitios arqueológicos muy conocidos, se han vuelto inaccesibles para los turistas debido a la disputa de tierras de los cárteles.

Se le suman otros riesgos de seguridad mismos de la propia naturaleza, como ya se vio el año pasado con el Huracán Otis arrasando la costa de Guerrero, de ahí que los responsables de Seguridad se encuentren en constante actualización e implementación de estrategias para contrarrestar estas situaciones.

"Entre los principales riesgos de seguridad en la industria de los hoteles, está la falta de estrategias coordinadas y unificación de criterios para enfrentar los delitos relacionados con el crimen organizado y la posibilidad latente de involucramiento por omisión de normas de cumplimiento (*Compliance*) en delitos de impacto internacional como es el de la trata de personas y abuso. Sin olvidar los temas

"Entre los principales riesgos de seguridad en la industria de los hoteles, está la falta de estrategias coordinadas y unificación de criterios para enfrentar los delitos relacionados con el crimen organizado", **Juan Antonio Arámbula**

de la Gestión adecuada de los riesgos de origen geológico e hidrometeorológico y finalmente el impacto de las conductas fraudulentas y de suplantación que afectan desde el sistema de reservaciones hasta el acceso desautorizado a las redes", comentó en entrevista Juan Antonio Arámbula, titular de la Vocería de la Secretaría Municipal de Seguridad Pública y Tránsito de Cancún.

El especialista recomendó fortalecer los programas de desarrollo profesional del área de seguridad, así como el rediseño de los criterios para la selección y permanencia del personal y la reformulación de los esquemas de ayuda mutua, asociación sectorial y realizar una sinergia con las autoridades, para mitigar esos riesgos.

La coparticipación es un aspecto muy importante. El especialista destacó que en el caso de Benito Juárez, Quintana Roo, los índices de percepción de seguridad y la reducción efectiva de eventos delictivos se ha logrado gracias a una efectiva coordinación de la seguridad municipal con las fuerzas estatales y federales, así como una intensa participación del sector privado y muy especialmente del sector hotelero.

Y precisamente la capacitación al personal de los hoteles, no sólo de Seguridad, contribuirá con la disminución de los riesgos.

CREANDO UNA CULTURA DE LA SEGURIDAD

En enero del presente año (del 24 al 28), se llevó a cabo la Feria Internacional de Turismo (FITUR) 2024, en Madrid, España, encabezada por Miguel Torruco Marqués, secretario de Turismo del Gobierno de México, en donde el país ingresó a la Guía Michelin, con Ciudad de México, Oaxaca, Baja California, Los Cabos, Nuevo León y Quintana Roo; como los primeros destinos, y de la mano de Canirac (Cámara Nacional de la Industria de Restaurantes y Alimentos Condimentados); así como la noticia de que México será el País Socio de FITUR 2025 por su gran representatividad del turismo en América y España.

"El otorgamiento de la categoría de privilegio en la más reciente feria turística internacional FITUR en España y la inclusión de Cancún en la Guía Michelín, refleja que éste es uno de los sectores privilegiados que se destacarán por el gran posicionamiento de México en el entorno internacional para este año", comentó Juan Antonio Arámbula.

Pero para lograr este posicionamiento internacional, existen diferentes estrategias de seguridad que contribuirán con este objetivo, una de ellas es la creación de una cultura de la seguridad entre el personal, de todos los niveles, de los hoteles.

Es importante tomar en cuenta que existen antecedentes y diferentes factores internos y externos para el desarrollo de esta cultura, además de que cada región enfrenta sus propios retos de seguridad. Enrique Tapia Padilla, socio director de Altair Security Consulting & Training, explicó que para comenzar con el cambio de la visión de las personas, en este caso de la concientización de una cultura de prevención en el personal hotelero, lo primordial es enseñar a la sociedad a auto protegerse. ¿Y cómo se logra esto?

Para empezar, es importante desarrollar un plan, una estrategia que parta de los valores básicos de la familia: amistad, amor, honestidad, honradez, solidaridad, respeto, responsabilidad, paz, tolerancia, libertad, civismo, generosidad; mismos que a su vez serán reproducidos en casa para así contribuir no sólo a la seguridad de la corporación, sino también al desarrollo de cada una de las personas que integran la familia del personal hotelero.

"Los elementos esenciales para crear y fomentar una cultura de prevención son: confianza más disciplina, con esto se podrá tener éxito en la implementación de nuestro plan", comentó el especialista.

La resistencia al cambio es una actitud "normal", sobre todo en los adultos, y vivimos en un país donde la mayor parte de las situaciones se resuelven después de que sucede el incidente, por eso, Tapia compartió el siguiente esquema que utiliza en sus conferencias, en donde se explica cómo aprenden conceptos nuevos los adultos, es decir, con qué herramientas podemos hacer efectiva la comunicación con el personal hotelero para implementar el plan de la cultura de prevención.

Fuente: Programa Learnind Doing de www.ciebarcelona.com/ Por: William Glasser - Psicólogo USA

Si se aprende en un 95% gracias a diferentes elementos visuales, acompañamiento, capacitaciones y a través del ejemplo; lo que se requiere es toda una campaña de comunicación interna específica para la creación de la cultura de la prevención. De acuerdo con el especialista, podemos lograrlo a través de:

1) Definir un objetivo.
2) Conocer la organización.
3) Respetar las jerarquías.
4) Buscar el momento oportuno.
5) Uso de lenguaje sensible, ideas claras.
6) Con diversidad e inclusión.
7) La exposición–*lobbing* (estrategia de comunicación que tiene como finalidad la participación e integración).
8) Apoyo y compromiso.
9) Más que métricas, el apoyo y la confianza.

"Los elementos esenciales para crear y fomentar una cultura de prevención son: confianza más disciplina, con esto se podrá tener éxito en la implementación de nuestro plan", **Enrique Tapia Padilla**

Si bien el área de Seguridad debe trabajar en conjunto con otras áreas, específicamente en este plan, tanto el área de Recursos Humanos, *Marketing*, como de Comunicación Interna o Corporativa, serán pieza clave para lograr el objetivo.

En el siguiente esquema, Enrique Tapia compartió cinco vías para establecer la Cultura de Seguridad:

Además de una buena estrategia de comunicación, se requiere de un líder para que, ante la resistencia al cambio, éste genere la confianza necesaria en el personal y con el ejemplo logre que los demás adopten esta cultura.

"¿Qué características tiene un líder? Piensa y busca el beneficio de todos, antes que el tuyo, está disponible y provee un apoyo cordial, aplica su liderazgo dependiendo de cada una de las personas con las que interactúa. Es ético y coherente, toma tiempo para escuchar y entender el fondo; mantiene una comunicación abierta/auténtica, con claridad. Fomenta el respeto y obtiene credibilidad, empuje, disciplina, empatía. Acepta retroalimentación y sugerencias, resuelve retos y conflictos, enfoque en soluciones, es estratégico y crea alianzas. Tiene control e inteligencia emocional, es resiliente, y tiene un enfoque en las relaciones de largo plazo".

Foto: Freepik

Retomando la estrategia que propone Enrique Tapia, el primer paso es analizar la situación de seguridad global, ubicar los riesgos y retos de la región donde se ubican los complejos hoteleros, definir un plan estratégico acompañado de otras áreas, y lo más importante: aterrizarlo como una inversión benéfica para la corporación apoyados del cálculo del Retorno sobre la Inversión en Seguridad (ROSI), que es igual a: mitigación del riesgo monetario – costo del control. "Se determina que una inversión en seguridad es rentable si el efecto de mitigación del riesgo es mayor que los costos estimados". (Fuente: Christian Locher, Methodologies for evaluating information security investments, 2005).

También se puede apoyar del ROI (por sus siglas en inglés para Retorno Sobre la Inversión), y se calcula mediante la división de las ganancias obtenidas entre los gastos (o la inversión). El resultado de esta operación se multiplica por 100 para saber cuál es el porcentaje de retorno.

"Lo que se espera de la implementación de una cultura de prevención, además de los beneficios sociales, es la reducción de los niveles de riesgo, así como de las reclamaciones y costos de compensación, de los incidentes y accidentes; una mejoría en las condiciones y comportamiento de seguridad de las personas. Pero también el abaratamiento de pólizas de seguro y cumplimiento de normatividad, y la mejoría del nivel de compromiso de las personas y su productividad", finalizó el especialista.

La cultura de la seguridad, de la prevención, es algo que se debe adoptar desde casa, en las familias, las escuelas, para que, al llegar a una corporación, las personas sean menos renuentes y por el contrario, adopten esta cultura con familiaridad. "Cualquier cambio en un elemento de la cultura provoca desajustes. Las sociedades receptoras, al ver comprobado su éxito, aceptan los cambios".

Referencias:

[1] *"Hoteles, moteles y similares" Data México. Ene-sep. 2023 https://www.economia.gob.mx/datamexico/es/profile/industry/traveler-accommodation*

[2] *"La ocupación hotelera en México asciende a 60.2% en primeros siete meses de 2023", Forbes Staff. Sep. 17 2023 https://forbes.com.mx/la-ocupacion-hotelera-en-mexico-asciende-a-60-2-en-primeros-siete-meses-de-2023/*

[3] *"Derrama económica en México crece 3.7% por turismo español: Sectur", Milenio Digital. 28/01/2024 https://www.milenio.com/politica/derrama-economica-en-mexico-crece-por-turismo-espanol-sectur*

ISIS SEGURIDAD INTEGRAL

Creamos entornos seguros

Servicios:

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

AFAC AGENCIA FEDERAL DE AVIACIÓN CIVIL

BASC BUSINESS ALLIANCE FOR SECURE COMMERCE CERTIFICATION /CERTIFICACION Nº MEXGDL00175-1

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

ASIS INTERNATIONAL

amesis

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

MUJERES EN LA SEGURIDAD:

Cuestión de habilidades y profesionalismo, no de género

En conmemoración del "Día Internacional de la Mujer", SEA realizó entrevistas a diferentes especialistas del sector, que han destacado por su trabajo, profesionalismo y compromiso con la seguridad

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Por cuarto año consecutivo, y en conmemoración del "Día Internacional de la Mujer", **Seguridad en América** reunió a algunas especialistas del sector que han destacado por su trabajo, dedicación y conocimientos de la industria, que contribuyen no sólo al desarrollo y continuidad de una corporación, sino que también han influido en el desarrollo de sus colaboradores y en que el sector sea innovador y rentable.

Las siguientes ocho especialistas en seguridad confirman que, a pesar de que aún haya un porcentaje más alto de hombres en este sector, la seguridad es cuestión de perfiles, no de género, y ellas son el vivo ejemplo de esto. A continuación, nos compartieron su trayectoria y experiencias en esta industria.

MÓNICA MOLINA, DIRECTORA COMERCIAL Y SOCIA DE SEPSISA

Egresada de la Licenciatura en Derecho, por la Universidad La Salle, Mónica Molina inició su camino en la seguridad hace 19 años cuando se constituyó SEPSISA Seguridad Privada; y en palabras propias, la entrevistada agradece haber llegado al sector, ya que se ha "enamorado en el alma" de la seguridad; ya sea porque cada día se presentan nuevos retos, nuevas expectativas, o porque siempre hay algo nuevo qué aprender, algo qué analizar, retos por cumplir y sueños que lograr. "Como muchos de esta industria llegamos a la Seguridad por diferentes motivos y nos quedamos por vocación".

"Como muchos de esta industria llegamos a la Seguridad por diferentes motivos y nos quedamos por vocación"

Seguridad en América (SEA): ¿Cuáles son los desafíos que enfrentan las mujeres en la Seguridad?

Mónica Molina (MM): Me atrevo a decir que los desafíos que enfrentamos son iguales a otras industrias. Hace 19 años era muy diferente, casi todas las personas con quien uno trataba eran hombres; hoy esto ha cambiado de manera significativa. Hoy muchas mujeres estamos en esta industria con diversas posiciones, mujeres muy preparadas y con gran conocimiento a las que respeto y admiro.

La primera barrera que debemos quitar es de nosotras mismas, el ser mujer no me impide crecer de manera profesional, pueden presentarse muchos obstáculos, más no necesariamente por género.

Desde que inicié en seguridad me han tratado con mucho respeto y de igual a igual; no me he sentido menospreciada o limitada por ser mujer, por el contrario, tengo grandes amigos dentro del medio a los que les he aprendido muchísimo, a los que los admiro y respeto.

SEA: ¿Cuál es su percepción sobre las mujeres que ocupan puestos de liderazgo en esta industria?

MM: Me siento muy orgullosa, definitivamente las mujeres estamos ocupando día a día más lugares en la industria, estamos demostrando a nosotras mismas la capacidad que tenemos y lo preparadas que estamos. Veo con mucha alegría cada vez más mujeres en foros de seguridad, aportando conocimiento y gran experiencia. Líderes de empresas de seguridad que hoy marcamos una diferencia y que se nos reconoce por los resultados. Definitivamente no es fácil, pero para nadie lo es, el éxito es el premio a la constancia y como cualquier persona que sea constante en su día a día, logrará lo que desea.

SEA: ¿Cómo ha sido su experiencia como mujer dentro del sector de la Seguridad?

MM: He tenido grandes experiencias de mucho aprendizaje, con momentos de incertidumbre y también maravillosos. En SEPSISA he podido apoyar de manera directa el crecimiento y desarrollo de diversas áreas y hoy como directora comercial me ha permitido llevar esta área a un crecimiento exponencial lo cual me causa gran orgullo. El poder desarrollarme e interactuar con los socios comerciales es verdaderamente gratificante, cada día busco elevar los estándares de la empresa, siempre con fines de éxito, y no importa si soy mujer o soy hombre esto es por resultados.

Como todo he tenido experiencias difíciles que intentan tratarte diferente por el hecho de ser mujer, pero ahí sale lo que somos y se toma como experiencia.

En este camino he conocido tanto hombres como mujeres excepcionales que me han apoyado a ser mejor, debo decir que dentro de SEPSISA siempre he contado con el respeto y apoyo de mis socios que confían en mí y con el respaldo de todo el equipo que conforma la empresa. ■

FERNANDA ARMENTA, *SUPPLY CHAIN SECURITY REGIONAL MANAGER* EN FLEX

Hace 13 años, Fernanda Armenta, Administradora de Empresas egresada de la Universidad Nacional Autónoma de México, con especialidad en Estrategias de Recursos Humanos, comenzó su carrera en la Seguridad. Y aunque ella "nunca" se visualizó en esta industria, en el momento que se dio cuenta de la importancia que tiene "hacer seguridad" a través de convertirse en un "aliado del negocio" y trabajar mano a mano con la gente, su perspectiva cambió.

"Me considero una líder incluyente, enfocada en potencializar el talento, en la eficiencia y en los resultados"

SEA: ¿Has notado a lo largo de tu carrera, diferencias en las oportunidades de formación y desarrollo entre hombres y mujeres en este sector?

Fernanda Armenta (FA): Sí. Durante estos años he tenido la oportunidad de conocer diferentes sectores, tales como: la industria textil, farmacéutica y de manufactura, lo que sin duda me ha dado la oportunidad de ver diferentes maneras de trabajo y distintas perspectivas de lo que significa la equidad de género y la seguridad.

Sin duda, el estereotipo social nos ha enseñado que hay ciertas carreras/profesiones que no son para mujeres, y mucho tiempo tuve comprada esta idea. Hoy, creo firmemente que tanto mujeres como hombres tenemos una gran responsabilidad de trabajar por nosotros mismos y nuestros ideales personales y profesionales, levantar la mano, buscar oportunidades y desarrollarnos y convertirnos en personas que sean vistas por el talento y aportaciones, no por "role-models" impuestos por el género al que pertenecemos.

SEA: ¿Cuáles considera que son las habilidades o aptitudes que las mujeres aportan al sector?

FA: Está científicamente comprobado que las mujeres destacamos en algunas habilidades cognitivas y los hombres en otras. Basado en diversos estudios realizados por los expertos, en promedio las mujeres obtenemos puntajes más altos en campos como: información fonológica y semántica (indicativas de más memoria a largo plazo); comprensión de prosa compleja (explica sus mayores competencias lingüísticas); velocidad de percepción y procesamiento de la información (mayor intuición y velocidad tomando decisiones); así como habilidades motoras finas.

Tomando en cuenta lo anteriormente mencionado, desde mi punto de vista, ser mujer significa ser "agente de cambio". Tenemos la capacidad de adaptarnos, de responder en momentos de crisis y trabajar bajo presión en momentos en los que se requieren más flexibilidad y capacidad de aprendizaje. Somos apasionadas, reconocemos y promovemos el trabajo en equipo sin perder de vista el objetivo del negocio.

SEA: ¿Cómo contribuye a la equidad de género en su trabajo?

FA: El secreto para mí, es aprovechar y explotar (en el buen sentido) las fortalezas de cada persona, dedicarnos a trabajar y enfocarnos en resultados. Solamente a través de esos dos componentes se puede empezar a ganar reputación y a ser reconocidos. Me considero una líder incluyente, enfocada en potencializar el talento, en la eficiencia y en los resultados; pienso en el equipo como una unidad y le dedico mucho tiempo y recursos al desarrollo de mi equipo de trabajo. Otro punto importante es apoyar la diversidad de perspectivas, estilos, culturas. Promover la escucha y participación activa en mi equipo de trabajo, para desarrollar un ambiente de respeto, tolerancia e inclusión.

Como mujeres, el pensamiento de auto superación debe ser pieza clave, dependerá del enfoque y la determinación propia que se logren o no los objetivos de cada una de nosotras. ■

MARIBEL CERVANTES, DIRECTORA DE SEGURIDAD EN HSBC

Una de las mujeres más imponentes de la Seguridad y quien inició su carrera en la industria como analista del CISEN (Centro Nacional de Inteligencia) en 1993, es Maribel Cervantes. Egresada de la Licenciatura en Ciencias de la Comunicación, a los pocos meses de entrar al CISEN, fue enviada a tomar un curso en Manejo de Fuentes con el Mossad y "literal" su vida cambió. Cuenta con una Maestría en Administración para la Seguridad y Defensa Nacionales por el Colegio de Defensa Nacional, en donde también completó el curso con su respectiva certificación de Poligrafía y Grafología.

También cuenta con los cursos de Análisis Operativo de la Criminalidad, en el Cuerpo Nacional de Policía de España; Análisis contra el Terrorismo, en el Departamento de Estado de US, y el de Líderes para Latinoamérica en el la Academia de Quántico, del FBI.

En abril de 1999, del CISEN, pasó a formar parte de la Policía Federal Preventiva, donde fue secretaria técnica del Coordinador General de Inteligencia. Posteriormente en el 2000, con el cambio de gobierno, ingresó a la entonces Policía Judicial Federal, siendo parte del equipo encargado de la transformación de Policía Judicial Federal a Agencia Federal de Investigación. En 2003 regresó al CISEN, esta vez como responsable del área de Análisis contra la Delincuencia y posteriormente le asignaron la responsabilidad del programa contra el terrorismo y contra inteligencia, donde estuvo hasta 2006, año en el que la mandaron a estudiar la maestría.

En 2007, al concluir la maestría del CISEN, la mandaron a la Secretaría de Seguridad, donde estuvo unos meses como Jefa de la Unidad de Desarrollo, para después ser nombrada Jefa de la División de Inteligencia y en febrero de 2102 fue nombrada, por el presidente de la república, comisionada general de la Policía Federal. En 2013 salió del servicio público e ingresó al Banco HSBC, donde se desempeñó como directora de la Unidad de Inteligencia Financiera. En 2017, el gobernador del Estado de México, la nombró secretaria de Seguridad, puesto que desempeñó hasta septiembre de 2020. El haber pertenecido al sector de la seguridad pública y ahora de la seguridad privada, le da a Maribel una visión más amplia de los desafíos tanto internos como externos, y al mismo tiempo, el poder comparar y actuar con ambas visiones.

"El reconocimiento y respeto de la gente cuando se hacen las cosas bien, es la mejor sensación que puedes experimentar"

SEA: ¿Cuáles considera que son los principales desafíos de las mujeres en el sector de la seguridad?

Maribel Cervantes (MC): El principal desafío es lograr que las mujeres tengan las mismas oportunidades de desarrollo, profesionalización, crecimiento y retiro, que los hombres; además que las condiciones de trabajo, en particular de las mujeres operativas, sean dignas y bien pagadas.

Actualmente la mayoría de las mujeres que realizan tareas operativas, como patrullaje, investigación, anti motines, etc., no tienen un espacio especialmente diseñado para ellas; es decir, comparten con los hombres áreas de descanso o para cambiarse, esto históricamente ha generado un sinnúmero de abusos hacia ellas. También es urgente diseñar esquemas de apoyo para las mujeres con hijos o familias, ya que hay evidencia que al tener que trabajar en turnos de más de 12 horas o esquemas de 24 x 24, los hijos quedan en el abandono expuestos a las drogas y el alcohol; lo cual eventualmente se convierte en un problema para la propia familia y hasta de delincuencia en algunos casos.

SEA: ¿Cuál ha sido su experiencia personal en el sector y qué es lo que más le apasiona de la seguridad?

MC: Siempre me tocó ser la única mujer al nivel de mando medio y superior en las instituciones en las que estuve, con un poco de vergüenza, o mucha, tengo que decir que hasta normalice la "violencia de género" hacia mí; fui consciente de esto cuando en el Edomex siendo Secretaria de Seguridad, me involucré mucho en este tema. Creo que a las mujeres se nos ha exigido el doble que a los hombres

y nos han llevado a un tema de "demostrar" por qué estamos o llegamos a ciertos puestos. Esto es algo que tenemos que cambiar.

De la seguridad me apasiona todo; la información, cómo se obtiene, cómo se procesa, cómo se convierte en inteligencia y en acciones específicas; obviamente cuando los resultados son buenos, la satisfacción es algo que no puedo describir. Parece demagogia, pero el reconocimiento y respeto de la gente cuando se hacen las cosas bien, es la mejor sensación que puedes experimentar.

SEA: ¿Qué cambios o mejoras le gustaría ver para que este sector sea más inclusivo o haya más mujeres en puestos de liderazgo?

MC: Tiene que estar cercano el día en que veamos más Secretarias de Seguridad, mujeres que vengan de la Academia, que pasado por las áreas de sustantivas de las Policías, mujeres que hayan encabecen las áreas de Inteligencia, Investigación y Reacción. Este país ya está listo para ver en acción a las mujeres, hay muchas ya en las instituciones, hay que ir por ellas e impulsarlas. Tendremos una comandante suprema de las Fuerzas Armadas y espero tengamos también pronto una jefa del Centro Nacional de Inteligencia, y una secretaria de Seguridad, surgida de la Academia de Formación. ■

MARCELA GARCÍA, DIRECTORA GENERAL DE BASC CAPÍTULO MÉXICO OCCIDENTE

Otra de las mujeres que cuenta con una larga trayectoria en el sector, es Marcela García. Primero en una agencia aduanal, conformando su sistema de gestión de seguridad, para después trabajar durante 17 años para BASC (Business Alliance for Secure Commerce) en México. Cuenta con una formación académica en Comercio Internacional, especializándose después en el campo de la seguridad orientada al comercio internacional y gestión de riesgos en la cadena logística.

La especialista ha dado capacitaciones y conferencias para eventos privados y de gobierno en México y otros países, conociendo y conviviendo con diferentes especialistas de otras certificaciones, como lo son OEA y C-TPAT, enriqueciendo sus conocimientos. A lo largo de estos años, ha sido testigo de la diversificación y evolución de muchos de los riesgos presentes en el comercio entre países y, asimismo, ha sido partícipe del desarrollo de medidas preventivas para que los riesgos no se vean materializados. Es testigo de seis versiones de la Norma BASC, la creación de la norma de C-TPAT, y el nacimiento y evolución del Operador Económico Autorizado en el mundo.

"Las mujeres que son madres cuidan cada día, no sólo el equilibrio en su familia, sino también el desempeñar con profesionalismo su trabajo"

SEA: ¿Cuáles considera que son los principales desafíos que enfrentan las mujeres en el sector de la seguridad?

Marcela García (MG): Como mujeres siempre la exigencia es más alta. Creo que existe un patrón inconsciente en la sociedad que nos exige que las mujeres en el ámbito de la Seguridad demostremos que tenemos la misma experiencia, capacidad, objetividad y disponibilidad que los hombres en el manejo de situaciones del trabajo diario y sobre todo en casos de emergencia. Las mujeres que son madres cuidan cada día, no sólo el equilibrio en su familia, sino también el desempeñar con profesionalismo su trabajo. Cada día deben administrar su tiempo, atención y energía en sus prioridades personales y en las necesidades de la empresa y el entorno en el que ésta opera. Esto obviamente es común en todos los sectores, pero creo que se puede resaltar mucho más en nuestra área.

SEA: ¿Cuál ha sido su experiencia como mujer dentro del sector de la seguridad?

MG: Cuando inicié en esta área a inicios de la década del 2000, el índice de mujeres trabajando en la seguridad era demasiado bajo. Poco a poco se han ido sumando más mujeres a la seguridad y a puestos de gran responsabilidad y liderazgo, sin embargo, aún son pocas en comparación a los hombres.

Puedo decir que mi experiencia ha sido muy buena, no sin dejar de lado que ha habido ocasiones en donde se ha puesto en duda mi desempeño por ser mujer o porque en algún momento mi edad era corta en comparación con la edad promedio de los demás profesionales de la seguridad.

Las mismas condiciones externas nos han llevado a adaptarnos a trabajar en un entorno de hombres, en su mayoría, pero creo también que cada vez más los hombres se han abierto a comunicarse y trabajar en un entorno mixto.

SEA: ¿Considera que actualmente continúan existiendo diferencias salariales, de liderazgo, de género en esta industria? Si es así, qué recomienda para eliminar las malas prácticas hacia el género.

Definitivamente. Los sueldos para mujeres en puestos de seguridad continúan siendo bajos. Los puestos deberían ser pagados de acuerdo con el cumplimiento del perfil y objetivos según las necesidades de cada puesto y empresa, no de acuerdo con el género, estado civil o número de hijos de una persona. Recomendaría a las empresas en que más que basarse en una cuota de género, sus contrataciones se encuentren al mejor candidato o candidata para el puesto según su formación y experiencia, siendo los sueldos y prestaciones, las mismas para mujeres y hombres. ■

MARGUERITE DESMICHELLE, *CLUSTER SECURITY MANAGER* EN ALSTOM

Gracias a un intercambio universitario en Madrid, España, Marguerite Desmichelle, de nacionalidad francesa y quien pasó de Historia y Geografía, a Geopolítica, actualmente lleva nueve años desarrollándose en el sector de la seguridad; los primeros en Francia, y desde finales del 2019, en México.

Buscando carrera para dedicarse al acabar la maestría, llegó a conocer la función de Seguridad Corporativa (o Patrimonial) en las empresas internacionales, lo cual le llamó mucho la atención. Después de una posición corporativa en París por varios años, hoy está a cargo de la Seguridad Patrimonial a nivel subregional, abarcando al menos diez países de América Latina, desde Ciudad de México.

SEA: ¿Por qué cree que haya menos participación de las mujeres en puestos de liderazgo en el sector de la seguridad en México?

Marguerit Desmichelle (MD): Creo que hay que considerar varios elementos. Primero, el rol que le fue asignado a la mujer en la sociedad por mucho tiempo y, por consiguiente, el espacio restringido que tenía en el ámbito laboral. Este desequilibrio se va ecualizando poco a poco y las mentalidades evolucionando, pero requiere tiempo. Además, se explica tanto por un tema de formación académica que de experiencia laboral previa como por los clichés que caracterizan al mundo de la seguridad corporativa.

Al fin de cuentas, el sector de la seguridad sigue siendo uno bastante joven a nivel global, unos 30-40 años según el sector de actividad y el país. Inicialmente, no había formación académica por lo que fueron a buscar los perfiles disponibles en el mercado que podían cumplir con los requisitos corporativos. Ello llevó al reclutamiento de profesionales proviniendo del servicio público, en particular de las fuerzas de seguridad y pocas mujeres por decirlo. Luego, se crearon carreras universitarias dedicadas, pero ya correspondía a la generación siguiente quien ha tenido que hacerse un espacio legítimo en el sector. Además, se explica tanto por un tema de formación académica que de experiencia laboral previa.

"Los actores maliciosos tienen eso de bueno que se reinventan siempre, obligándonos, nosotros profesionales de la seguridad, a adaptarnos de manera continua"

SEA: ¿Cuáles han sido los retos a los que se ha enfrentado en el sector de la seguridad? ¿Han sido por género?

MD: Dejé de contar cuántas veces escuché que era una "mujer muy joven para ocupar esta posición". Prefiero no prestarle atención

a ello y que me consideren como la profesional que soy y no por otras características.

SEA: ¿Cómo contribuye en la equidad de género en la industria?

MD: Trato de seguir dos vías: primero dar a conocer a las siguientes generaciones los logros de la mía, para que se sientan motivadas. Eso va a la par con el hecho de dar visibilidad a la posición que tengo. Segundo, en caso de que tenga que contratar, solicito siempre una diversidad de perfiles que refleja nuestra sociedad para dar oportunidad a todas y todos, incluso si eso hace que demore más el proceso.

SEA: ¿Qué es lo que más le apasiona de la seguridad?

MD: ¡Ni un día le parece al otro!

Los actores maliciosos tienen eso de bueno que se reinventan siempre, obligándonos, nosotros profesionales de la seguridad, a adaptarnos de manera continua. Además, de un sector de actividad a otro, las problemáticas cambian mucho por lo que es un aprendizaje permanente. ■

"Es esencial desafiar los estereotipos de género en los roles laborales y promover la evaluación basada en habilidades y mérito en lugar de género"

NATALIA MAHECHA, *BUSINESS DEVELOPMENT AND MARKETING DIRECTOR* EN ALLIED UNIVERSAL SECURITY (AUS)

Licenciada en Administración de Negocios por la Universidad EAFIT en Medellín, Colombia, Natalia Mahecha cuenta con más de 10 años de experiencia en el sector de la seguridad. Tiene una Maestría en Administración y Dirección de Empresas (MBA), por la Universidad de las Islas Baleares y un Master en Dirección de Marketing y Comunicación Empresarial por la Universidad de Valencia en España.

Comenzó su carrera en G4S, hoy Allied Universal, desempeñando varios roles, entre esos, directora comercial regional de la zona Noroccidente para las cuatro líneas de negocio. Posteriormente, asumió la responsabilidad de gestionar las cuentas regionales de Latinoamérica, tales como: Shell, GSK, Nike, Syngenta, entre otros.

En los últimos cuatro años, ha tenido el privilegio de trabajar en México como *Business Development and Marketing Director*, donde ha liderado estratégicamente las operaciones comerciales de la empresa. "Esta experiencia me ha proporcionado una perspectiva invaluable sobre la gestión de negocios en un entorno internacional y me ha permitido fortalecer mis habilidades en el desarrollo de estrategias comerciales y la gestión de relaciones con los clientes en diversos entornos culturales y geográficos".

Seguridad en América (SEA): ¿Ha notado, a lo largo de su carrera, diferencias en las oportunidades de formación y desarrollo entre hombres y mujeres en este sector?

Natalia Mahecha (NM): He observado disparidades en las oportunidades de formación y desarrollo entre hombres y mujeres. Aunque la industria ha progresado en términos de equidad de género, persisten ciertas diferencias que merecen una consideración más profunda. En algunos entornos laborales, los hombres suelen tener un acceso más amplio a programas de formación y desarrollo, especialmente en roles técnicos o de liderazgo, posiblemente debido a prejuicios arraigados en la cultura organizacional o estereotipos de género. Sin embargo, se está reconociendo cada vez más el valor y las habilidades que aportan las mujeres al sector, y muchas empresas están adoptando medidas para promover la diversidad de género y ofrecer oportunidades equitativas para todos los empleados.

Personalmente, he experimentado el impacto positivo de programas de formación y desarrollo en mi carrera en seguridad, que han enriquecido mis habilidades profesionales y fortalecido mi confianza en roles de liderazgo.

SEA: ¿Qué cambios o mejoras se pueden implementar en el sector para que exista mayor representatividad del género femenino?

NM: Es crucial implementar políticas de inclusión y diversidad, estableciendo oportunidades equitativas de reclutamiento y desarrollo profesional. Esto implica la creación de programas de mentoría, redes de apoyo y promoción de modelos femeninos a seguir, junto con la sensibilización sobre los sesgos de género y la promoción de una cultura laboral inclusiva. Además, ofrecer flexibilidad laboral y realizar evaluaciones periódicas para monitorear el progreso hacia la igualdad de género, son medidas esenciales para crear un entorno de trabajo más equitativo y representativo para todas las personas.

De igual forma, es esencial desafiar los estereotipos de género en los roles laborales y promover la evaluación basada en habilidades y mérito en lugar de género. Esto implica implementar medidas afirmativas que brinden oportunidades equitativas para las mujeres, al tiempo que se mantienen sistemas de selección y promoción de objetivos. Además, es crucial abordar las percepciones culturales y los sesgos dentro de la industria, involucrando a los clientes para promover una cultura inclusiva que valore las contribuciones de todos los empleados independientemente de su género, y superar las barreras que puedan estar obstaculizando la representación femenina en posiciones de liderazgo.

SEA: ¿Cómo contribuye a la equidad de género en su trabajo?

NM: Siendo un modelo a seguir y abogando activamente por la igualdad en todas las áreas. Me aseguro de alzar la voz cuando veo situaciones de discriminación o desigualdad de género, tanto en las políticas de la empresa como en las interacciones diarias. Además, ofrezco mi apoyo y mentoría a otras mujeres en la organización, compartiendo mi experiencia y brindándoles las herramientas necesarias para alcanzar sus metas profesionales.

Así como siendo exigente con todos los empleados y proporcionar oportunidades equitativas para hombres y mujeres, asegurando de que estén capacitados para cumplir con su rol y no tengan un estándar diferente debido a su género. ■

GLORIA MELÉNDEZ PAREDES, DIRECTORA DE PREVENCIÓN DE PÉRDIDAS EN GRUPO CHEDRAUI

Con más de 25 años de trayectoria en la industria de la Seguridad, Gloria Meléndez es Licenciada en Relaciones Comerciales, y cuenta con una Maestría en Dirección de Capital Humano (UP Universidad Panamericana), así como el Diplomado en Alta Dirección de Empresas impartido por IPADE Business School, y diversos diplomados relacionados con el *retail*, Prevención de Pérdidas y Seguridad, cursados en la Universidad Pontificia Comillas y otras instituciones.

"A lo largo de los años fui adquiriendo experiencia y me especialicé en la Prevención de Pérdidasen el sector del *retail*; actualmente desarrollo todo ese aprendizaje que he ido acumulando, en una compañía que me abrió sus puertas, me arropó y, que acompañada de un gran equipo de trabajo, buscamos todos los días superar los retos que se nos presentan, con lealtad y responsabilidad, cumpliendo con la nuestra misión, que es la de 'llevar a todos los lugares posibles lo productos que los clientes prefieren, a mejor precio'".

La especialista, además de los retos que se presentan en el sector, tiene como objetivo continuar desarrollando un Modelo de Seguridad, que les permita estar a la vanguardia en temas de Tecnología, Seguridad, Inteligencia, Prevención y Protección, contribuyendo a que sus clientes tengan la mejor experiencia de compra desde el primer contacto que lo recibe en nuestras Unidades de Negocio.

SEA: ¿Cuáles considera que son los principales desafíos de las mujeres en el sector de la seguridad?

Gloria Meléndez (GM): Considero que los principales desafíos son los estereotipos de género, porque al asumir ideas excluyentes reafirmando un modelo de feminidad y masculinidad, en donde decimos: "este perfil es para hombres no para una mujer", ahí está el primer punto de enfoque, porque en realidad trabajar por perfiles hace que busques las competencias más adecuadas y no definas que el género es el que hace la diferencia.

"Se trata de avanzar en cambios transformadores desde la Cultura de una Organización hasta generar foros donde la mujer se sume con una participación proactiva"

SEA: En su opinión, ¿por qué considera que hay menos mujeres en esta industria y cómo podría lograrse mayor participación de este género en el sector?

GM: Se requiere una mayor exposición y visibilidad de la mujer, pero no me refiero a ser un número más en la estadística y la medición obligada para aumentar participación de la mujer; se trata de avanzar en cambios transformadores desde la Cultura de una Organización hasta generar foros donde la mujer se sume con una participación proactiva, dudas, participación a través de Círculos de Mentoría, generando redes de apoyo que debemos llamar ejemplos de SORORIDAD.

SEA: ¿Cuál ha sido su experiencia personal en el sector y qué es lo que más le apasiona de la seguridad?

GM: A título personal comparto que ha sido una experiencia llena de retos, aprendizajes, sacar de mi mente que el ser mujer limita el desarrollo y crecimiento, creer en mí, aprender de los hombres, pero no imitarlos o buscar ser como ellos. Me apasiona buscar el problema de raíz para armar un caso de negocio, enfocándome en solucionar el 80/20 del problema; me apasiona la combinación de la tecnología y la Inteligencia Artificial como herramienta para estructurar el mejor modelo de Seguridad acorde a la necesidad, me apasiona sumar en los resultados de un negocio con la perspectiva de seguridad sin afectar la venta.

SEA: ¿Qué cambios o mejoras le gustaría ver para que este sector sea más inclusivo o haya más mujeres en puestos de liderazgo?

GM: Centrarnos en las competencias de cada individuo y no en el género. Elaborar políticas de inclusión y diversidad, compartirlas, promover y vivir la pluralidad de género para poder integrar a más mujeres en puestos de liderazgo; debemos dejar de trabajar en silos, ser agentes de cambio en los distintos procesos en los que podamos intervenir en un negocio, generar un entorno de confianza, exceder las expectativas de resultados, aprender a ser productivas, buscar redes de apoyo, y realizar Networking, sin dejar de aprender cada día. ■

Fotos: Mónica Ramos / SEA

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 de prestadores de servicios Centro de Evaluación

Certificación del Sistema de Calidad DNV ISO 9001

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

Empresas de GSI Grupo Seguridad Integral

BASC

SEGURIDAD CORPORATIVA EN CASINOS Y CENTROS DE ENTRETENIMIENTO

En el 2023 entró en vigor el decreto que modifica el Reglamento de la Ley Federal de Juegos y Sorteos, en el que se establece que no se otorgarán nuevos permisos para operar máquinas tragamonedas en casinos y salas de juego; por lo que nuestros especialistas nos indican cómo continuar con el negocio a pesar de éste y otros retos que enfrenta ese sector

Foto: Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Los centros de entretenimiento están hechos para cumplir un solo objetivo: generar en sus asistentes alegría, emoción, entusiasmo, satisfacción, felicidad, asombro; todas esas experiencias que se viven en el momento y se quedan para siempre; pero los asistentes no están, en su totalidad, conscientes de los riesgos que en estas edificaciones pueden existir, para ello están cada una de las áreas de la corporación que administra los recintos y la que los organiza. En los casinos, sucede algo similar, con la diferencia de que, en vez de recibir a mil, diez mil, sesenta mil personas, recibe a cada cliente de forma personalizada. Ambos establecimientos requieren estrategias de seguridad específicas y generales, de la mano de otras áreas.

En un casino, de acuerdo con el análisis de José Luis Coria Arreguín, gerente nacional de Protección Civil de Codere, los incidentes de seguridad más comunes que suceden son: inconformidad de clientes, generada por la falta de atención a peticiones o servicios; y algunos otros menores como: tropiezos y/o caídas, en adultos mayores, ocasionados por la falta de movilidad.

Los incidentes pueden resolverse en ese momento, pero implican toda una capacitación previa por parte del personal, protocolos establecidos y un líder en Seguridad que atienda y redireccione las acciones a tomar en caso de que sucedan situaciones de riesgo más críticas.

"De los puntos de riesgo a considerar y a lo que nos vemos obligados a reforzar en nuestros protocolos de actuación, todos los que estamos involucrados en este amplio ramo de *Security* y *Safety*, son los fenómenos socio organizativos, naturales y sanitario ecológicos, citando como principales ejemplos, las afectaciones a la infraestructura, ocasionadas por el Huracán Otis, sumando el comportamiento que presentó la sociedad civil en la entidad; la pandemia por COVID-19, la cual genero pérdidas de vidas humanas, afectación a la economía global, teniendo como resultado afectación a la continuidad de operaciones en general", comentó José Luis Coria.

Y aquellos riesgos que superan ser sólo incidentes como cuando los clientes "conflictivos", los cuales al no ver reflejada una ganancia a su favor, ocasionan daños a las terminales de juego. "El contar con el soporte de personal externo de seguridad con los perfiles requeridos y altamente capacitados en materia de Seguridad Patrimonial y Prevención, es fundamental para no dañar la continuidad del negocio ante estas situaciones", añadió el especialista.

Una de las áreas que se encarga, no sólo del cumplimiento de sus objetivos, sino que constantemente realiza sinergias y coadyuva con las otras áreas, es Seguridad Corporativa.

OBJETIVOS DE LA SEGURIDAD CORPORATIVA EN EL SECTOR DEL ENTRETENIMIENTO

La seguridad en general tiene como prioridad el salvaguardar vidas y bienes materiales, en el caso específico del sector del entretenimiento, incluyendo casinos, existen diferentes aspectos que se deben tomar en cuenta para analizar, definir e implementar las diferentes estrategias de seguridad, incluyendo tecnología, que resultarán efectivas en el desarrollo de los eventos; por ejemplo: la capacidad de las personas que alojan los centros donde se desarrollan los espectáculos varían, pueden existir concentraciones desde 50 personas hasta las 70 mil o más, como es el caso del Foro Sol o el Estadio Azteca.

También es importante considerar quién se presentará, qué tipo de espectáculo dará, quiénes son sus seguidores, las vías de acceso, el tiempo del show, las salidas de emergencia, la colaboración con las autoridades, etc. El átrea de Seguridad Corporativa atiende ésta y otras situaciones de estos recintos, pero de acuerdo a Antonio Gaona, director de Seguridad Corporativa en Grupo Codere, primero es importante identificar el "*branding*" de la propia área, es decir, la imagen que queremos dar y lo que queremos lograr con las estrategias a implementar, para que así se pueda colocar el apoyo y atención necesaria al área y lograr que la seguridad siempre esté dentro de la planeación de los eventos.

El especialista comentó que existen premisas de la Seguridad Corporativa para lograr el objetivo antes mencionado, las cuales son:

- **Tener siempre presente el salvaguardar vidas.** El ofertar espacios y experiencias seguras, tanto a clientes, como personal y proveedores.
- **Continuidad del Negocio.** Entender el impacto que tiene la seguridad en el negocio, en una empresa donde el margen es crítico, esto resulta muy importante.
- **Protección de activos.** La importancia de la imagen de la empresa y qué aporta la Seguridad Corporativa para que se conserve esta imagen.

Además de tener en cuenta que la seguridad en el sector del entretenimiento es la primera puerta que se abre a los clientes, de ahí la importancia de dar un buen servicio desde que el guardia de seguridad apertura los accesos y recibe a los visitantes, da soporte al desarrollo del evento a través de los diferentes mandos de la seguridad para lograr así el control que permita conservar la imagen de quien desarrolla el evento. Sumando el servicio, el soporte y el control, junto con una buena comunicación, la Seguridad logra que las otras áreas de negocio de la empresa que emite el espectáculo, invierta y comprenda el beneficio del área en la corporación.

NATURALEZA DEL NEGOCIO: CASINO

Uno de los integrantes de la industria del entretenimiento, son los casinos, considerados también como parte del *retail,* ya que todo lo que en él suceda impacta directamente en el margen negocio, lo que obliga a lograr una experiencia particular en cada uno de los clientes, por ende la inversión económica de cada cliente impacta en las ganancias del negocio, si se pierde un cliente, se pierden esas ganancias, por eso la experiencia que cada uno de los clientes se lleve del casino, es tan relevante para el desarrollo del negocio.

"De los puntos de riesgo a considerar en un casino y a lo que nos vemos obligados a reforzar en nuestros protocolos de seguridad son: fenómenos socio organizativos, naturales y sanitario ecológicos", ***José Luis Coria***

"En el sector del entretenimiento, y sobre todo en los casinos, el trato con cada cliente es crítico. Aunque el contacto con éste es similar al que se tiene en las tiendas departamentales o de retail, en un casino se cuida la experiencia del cliente desde que éste es recibido por el elemento de seguridad, hasta que se retira, y todo lo que haya sucedido en ese periodo de tiempo, influirá si el cliente regresa o no al casino".

La Seguridad Corporativa ayuda a mantener, contener y retener a los clientes a través de la forma hábil, inteligente y humana en cómo se tratan a los clientes, y siendo casinos, las personalidades de cada cliente son diferentes en cada zona, lugar y horarios, de ahí que el área debe comprender y capacitar para su personal sepa converger con este contacto directo con el cliente, el desarrollo de recursos y habilidades humanas es fundamental.

Otro de los aspectos que se deben tener en cuenta respecto a la naturaleza del negocio, es la normatividad. La regulación es crítica para el desarrollo del negocio, por eso se debe tener contacto con otras áreas como el área de *Compliance*, ya que la regulación es constante y estricta, y estar actualizados en el tema.

Por ejemplo, en noviembre del año pasado (2023), entró en vigor el decreto que modifica el Reglamento

de la Ley Federal de Juegos y Sorteos, en el que se establece que no se otorgarán nuevos permisos para operar máquinas tragamonedas en casinos y salas de juego, de acuerdo con Miguel Ángel Ochoa, presidente de la Asociación de Permisionarios, Operadores y Proveedores de la Industria del Entretenimiento y Juego en México (AIEJA), las máquinas tragamonedas representan el 85% del negocio[1], por lo que esta acción puede tener repercusiones graves a largo plazo, desde la salida de inversionistas en México de máquinas tragamonedas, hasta el juego ilegal a causa de permisos vencidos y sin posibilidad de renovación.

FACTORES EXTERNOS E INTERNOS EN LOS CASINOS

Dado que cada cliente es representativo para el casino, se debe tener en cuenta el trato personalizado a éstos, para lograr una experiencia satisfactoria y así, lograr su permanencia en el establecimiento; sin embargo, existen múltiples factores que determinan el cómo tratar a cada cliente, de acuerdo a Antonio Gaona, existen principalmente dos factores de cada cliente:

- **Externo.** Cada entorno trae clientes y situaciones diferentes. En el caso específico de Codere, compañía a la que representa el experto, tiene salas en estados donde la seguridad es crítica, por ejemplo, en el norte y occidente del país, en donde se deben tomar medidas preventivas tanto para el exterior del casino, como de los usuarios de éste. "La Seguridad tiene un papel muy importante y de mucha responsabilidad en un casino, ya que debes responder por la vida de las personas que asisten a éste, y además de las vidas de tus colaboradores quienes deben contener situaciones violentas en aquellos lugares donde la situación de seguridad externa es crítica. El responsable de la Seguridad Corporativa de un casino, debe tener talento fino para decidir cómo hacer las cosas y la responsabilidad de tomar la decisión para hacerlas, siempre acompañado de un equipo capacitado, eficiente, como el que tengo yo, y que además debemos tomar decisiones a larga distancia", expresó el especialista.
- **Internas.** La experiencia del cliente es vital para el negocio, así como el trato con los empleados, el manejo de los protocolos, los procedimientos, la normatividad, y el trabajo y coordinación con los diferentes equipos de seguridad.

"En un casino la seguridad es parte de la experiencia del cliente, es parte de la imagen, y además de la contención de situaciones críticas. Somos parte del cómo atraer al cliente al juego, de ahí la importancia del trabajo en equipo con las diferentes áreas de seguridad, y la profesionalización de todo el personal de seguridad. Los casinos tienen centros de monitoreo muy complejos, en donde los monitoristas no sólo están leyendo el lenguaje corporal de los clientes, sino también la conducta, las posibles alertas, si hay que realizar investigaciones, se requiere realmente de un talento en particular para trabajar en estos centros de monitoreo. El trabajo en conjunto con otras áreas operativas y de seguridad dará el soporte necesario que requiere un establecimiento de juego, que cumpla con la normatividad y la experiencia que necesita cada cliente de ese lugar", destacó Antonio Gaona.

"La Seguridad tiene un papel muy importante y de mucha responsabilidad en un casino, ya que debes responder por la vida de las personas que asisten a éste, y además de las vidas de tus colaboradores", ***Antonio Gaona Rosete***

"El mundo de la seguridad en el sector del entretenimiento es extraordinario, cada área tiene su tema, no es lo mismo llevar la seguridad de un estadio de futbol, que de un concierto o un casino. Hay que entender la naturaleza del negocio para lograr los objetivos del mismo", finalizó. ■

Referencias:

"Qué significa el nuevo decreto de juegos y sorteos para el panorama del juego en México", Redacción. Milenio, 05/12/2023 https://www.milenio.com/content/juegos-y-sorteos-en-mexico-que-pasa-con-la-nueva-ley

5 ASPECTOS BÁSICOS Y NECESARIOS QUE SE DEBEN IMPLEMENTAR EN UN CASINO, REFERENTE A PROTECCIÓN CIVIL, DE ACUERDO CON JOSÉ LUIS CORIA

1) Contar con la documentación vigente de acuerdo a los lineamientos establecidos y requerida por autoridades de los tres niveles de Gobierno, para la Gestión del Programa Interno de Protección Civil.
2) Capacitación.
3) Mantenimiento a sistemas de alertamiento y equipos, contenido en la Unidad de Negocio.
4) Establecer programas adecuados de revisión.
5) Contar con Dictámenes vigentes en materia de electricidad, gas y estructural, que la autoridad solicita, con el propósito de prevenir riesgos, ya que la operación de las Unidades de Negocio están en operación continua.

MEXSEPRO

SEGURIDAD Y PROTECCIÓN DE MÉXICO

[SEGURIDAD | inteligente]

[ANIVERSARIO]

La nueva generación en
seguridad privada

mexsepro.com
(55) 6585 4448
(55) 4141 8573
facebook.com/MEXSEPRO
instagram.com/mexsepro
twitter.com/spmexsepro

TÉCNICAS EN PRUEBAS DE CONFIANZA E INVESTIGACIONES: LOS RIESGOS ASOCIADOS A LA INEXPERIENCIA

Foto: Freepik

"Ataque que no se previene, difícilmente se detiene"

MÉXICO

Antonio Venegas / *Staff* Seguridad en América

Durante el primer *Roadshow* del año, organizado por **Seguridad en América**, el Lic. Víctor Hugo Martínez Enciso, DSI, DAS, socio director de iMetis Consulting Group y coordinador de la Comunidad de Investigaciones e Inteligencia de ASIS Internacional Capítulo México 217, se presentó con la charla magistral titulada "Las investigaciones corporativas y los riesgos asociados a la inexperiencia", en la que habló sobre las Técnicas en Pruebas de Confianza e Investigaciones.

Cuando un incidente ocurre existen cuatro verdades relevantes: la verdad personal, la verdad social, la verdad histórica, la verdad real o material y la verdad legal. Posteriormente, el Lic. Víctor Hugo Martínez, DSI, DAS mostró una gráfica de PwC (Pricewarerhouse-Coopers) de los tipos de delitos financieros más comunes en las empresas en el Mundo y en México, perpetrados por empleados, son: en primer lugar: la apropiación indebida de activos y en segundo lugar el soborno y la corrupción. Los principales riesgos en los negocios corporativos son: el fraude general, la vulnerabilidad al ciberataque y la falta de normatividad antisoborno y corrupción, el cumplimiento a las regulaciones especificas por industria, la falta de medidas anticompetencia, la PLD Prevención de Lavado de Dinero, entre otros, son las que vulneran los activos de la empresas, que impacta a los costos, en la operación y en la armónica Continuidad en los Negocios.

Dentro de los riesgos que impacta en el patrimonio de las empresas en México se encuentran los delitos e incidentes como: el robo, robo hormiga, abuso de confianza, competencia desleal, sabotaje, asaltos, extorsiones, robo de mercancía en tránsito, espionaje, secuestros, fraudes, entre otros.

El Lic. Víctor Hugo Martínez, DSI, DAS, destacó que en los riesgos cibernéticos, el usuario (empleado) puede vulnerar los protocolos de seguridad lógica o cibernética al darle clic a vínculos, al instalar *apps* en sus dispositivos o al descargar archivos o contenido infectado por *malware*, y en ocasiones pueden verse expuestos a los delitos como robo de base de datos, compromiso de credenciales de usuarios privilegiados, pérdida de datos, secuestro de información, sabotaje a través de un insider o delacement (alteración en un sitio web).

Posteriormente compartió una relación de controles antifraude: como la auditoria externa de los Estados Financieros, el Código de conducta y un fuerte Departamento de auditoría interna, según lo refiere KPMG en sus informes. En la esfera corporativa, el perfil del defraudador más frecuente, tiene una antigüedad de 3 a 5 años, va desde los 25 hasta los 40 años de edad, su nivel educativo es de secundaria o menor, los fraudes que comete están entre los 10 mil dólares a los 50 mil dólares anuales; por otro lado, el defraudador más costoso, posee una antigüedad de más de 10 años, su edad va de entre los 41 y los 55 años, y su educación puede llegar al nivel universitario, los fraudes cometidos están entre los 100 mil y los 500 mil dólares anuales.

El Lic. Víctor Hugo Martínez compartió el perfil del defraudador, de una gráfica basada en datos de la empresa KPMG, en dónde describió: Hay dos tipos de personas que hicieron fraude: el personal interno (empleados) y el externo (proveedores). El personal interno que defraudó constituye un 59%, que se divide en 35% *Staff*, 9% Supervisor, 9% Gerente y 6% Alta Gerencia / Dirección. Por otro lado el personal externo (proveedores) equivale al 10% de los fraudes; ahora, la colusión entre el personal interno (empleados) y el externo (proveedores) constituyó un 31%. Los motivos personales principales que incentivan al perpetrador incluyen son: la oportunidad (40%), la ambición o codicia (34%), los problemas económicos (13%), la presión por alcanzar los objetivos (6%), resentimiento hacia la compañía (4%).

ELEMENTOS CLAVE PARA PROTEGER A LAS EMPRESA

De esta manera, el Lic. Víctor Hugo Martínez, DSI, DAS, también compartió cinco elementos clave para proteger a las empresas del crimen financiero, principalmente hacer uso de una política de integridad empresarial para mejorar la estructura de control interno para prevenir el fraude, corrupción y lavado de dinero, que son los crímenes financieros más comunes para las organizaciones; estos cinco elementos incluyen: la línea ética, los programas de prevención,

estrategias contra fraude, programas anticorrupción y estándares anticorrupción. A lo largo de su presentación, compartió casos de estudio donde se realizaron las investigaciones correspondientes para definir las situaciones del delito.

De igual forma, destacó el papel de Recursos Humanos como una medida preventiva al incrementar los filtros antes de su contratación con un *Backgroud Check* o *Vetting*, es decir la verificación profunda de sus antecedentes jurídicos, laborales, profesionales y de su entorno social, con una perspectiva de inclusión y de género, considerando el *Ethical Compliance* o Cumplimento Ético de los empleados y de los proveedores o clientes. Considerando un monitoreo y evaluación anual en puestos claves, para su permanencia en el puesto o para una promoción profesional, que es una buena práctica que se emplea en diversas industrias.

En los estudios que emite KPMG a por región, para México, encontraron los siguientes hallazgos, según lo indicó el Lic. Víctor Hugo Martínez, DSI, DAS, que el que el 75% de las empresas más importantes en México han sufrido algún tipo de fraude en el último año, y 46% han sido por personal interno. En el 60% de los casos, el fraude fue detectado por medio de controles y auditorías internas; sin embargo, en el 86% de los casos, el fraude se descubrió hasta seis meses después de haberse cometido el ilícito. Es decir, hay muchas empresas que están sufriendo un fraude, aún no lo saben debido a que aún no lo han detectado oportunamente.

Ante este entorno tan crítico, el Lic. Víctor Hugo Martínez, DSI, DAS, mencionó la importancia de realizar investigaciones preventivas, para detectar oportunamente comportamientos no éticos o que puedan atentar en contra de los empleados o de los activos de la empresa, considerando que se puedan estar beneficiándose indebidamente al recibir dinero o beneficios indebidos, los cuales se deben de identificar objetivamente y trasparentemente a través de un Análisis de Responsabilidades (investigación interna) de forma encubierta o totalmente abierta, con el fin de detectar y tratar apropiadamente los hallazgos, debido que el empleado, puede reaccionar y sabotear la operación y las relaciones de negocios.

El nuevo paradigma de la Convergencia, consiste en la mejor alineación en la estrategia de seguridad corporativa, mejorando la comunicación y cooperación, las prácticas compartidas, que tiene tres ejes que se están consolidando, su seguridad física, la ciberseguridad, la Prevención del fraude y el cumplimiento regulatorio.

El *Ethical Compliance* es un eje hacia donde las empresas globales están guiándose derivado del Informa de los Riesgos Globales del Foro Económico Mundial en Davos, Suiza, ingrediente indispensable para la cultura en los negocios y la estabilidad y continuidad en los negocios; por lo que se está fortaleciendo el comportamiento tanto de empleados y directivos, así como la alineación de integridad, en proveedores, clientes o socios de negocio, fortaleciendo el tejido de normatividad y legalidad como práctica cotidiana. Es importante replantear las políticas relacionadas al código de conducta y de conformidad, que incluyan incidentes como el acoso laboral y/o sexual, igualdad en oportunidades de empleo, prevención de la discriminación, seguridad en el trabajo, *copyright*, conflictos de interés, relaciones regulatorias, entre otros, como la Prevención del Lavado de Dinero.

Los propósitos de una investigación van desde documentar incidentes, identificar las causas de situaciones no deseadas, documentar hechos e identificar sospechosos involucrados, compilando información para aprobar o desaprobar un alegado y permitir una decisión. Para esto, compartió las capacitaciones de un investigador que incluyen: investigaciones computacionales, manejo de evidencia, crímenes de cuello blanco, acoso sexual, violencia en el lugar de trabajo, fraude en seguros, por mencionar algunos.

Como punto de origen, para comprender un incidente ocurrido en una empresa, es muy impórtate considerar una planeación, una recolección de datos, indicios, es "unir los puntos", unir los datos, los indicios, mediante el procesamiento y análisis de la información que te permita la trazabilidad histórica, que te permita generar inferencias de los hechos de manera lógica (deductiva o inductiva), metódica y legal, hasta generar hipótesis a verificar, que te permita construir escenarios y aterrizarlo en un Reporte Ejecutivo Final para la toma de decisiones al C-Suit o a la mesa directiva.

El Lic. Víctor Hugo Martínez, DSI, DAS, señaló que hay casos altamente sensibles y complejos, que pueden complicarse por manejarlo inapropiadamente, y generar riesgos altamente dañinos al filtrarse la información o al alertar a los probables responsables, quienes pueden sabotear la continuidad operativa; por lo que sugiere se deben de atender por expertos, con experiencia profesional probada en estos temas, certificados, con metodología y la aplicación de las *Best Practices*, también de tratarlo basado en Protocolos Internacionales como los de ASIS International, que tiene libros como el POA (Protection of Assets), sobre Investigaciones y el Manual del Investigador entre otros y protocoles de la ACFE (Association of Certified Fraud Examiners) y considerando atenderlo con absoluta pulcritud, confidencialidad y legalidad.

Lic. Víctor Hugo Martínez Enciso, *socio director de iMetis Consulting Group y coordinador de la Comunidad de Investigaciones e Inteligencia de ASIS Capítulo México 217*

Compartió su experiencia el Lic. Víctor Hugo Martínez, DSI, DAS, en las distintas áreas de investigación corporativa en las que ha participado, la variedad de las servicios que han realizado, *Background Check*, *Due Diligence*, Detección y Tratamiento del Fraude, Atención a extorsiones, Operaciones encubiertas, sustracción de mercancía en tránsito, sustracción hormiga, sustracción en CEDI´s, propiedad Intelectual y de Marcas, recuperación de información afectada por *Ransomware* entre otras actividades. ■

Si desea contactar al entrevistado, favor de escribirle a:
victor.m@imetis.mx

CLAVES PARA FACILITAR LA GESTIÓN EXITOSA DE SEGURIDAD EN AMÉRICA LATINA

Foto: - Freepik

Cuando sus clientes han sabido a ciencia cierta quién es usted y cómo responde en situaciones normales o de emergencia y ve que su comportamiento es congruente, sereno y firme en el manejo de crisis, su credibilidad y aprecio crecerán como nadie puede imaginarlo

MÉXICO **Diego Arévalo**

De mis largos años de experiencia en el manejo y la administración de la Seguridad en 10 países de Latinoamérica, son muchas las vivencias, aprendizajes, éxitos y fracasos, que al final han contribuido sustancialmente para enriquecerme como persona, como ciudadano y como profesional de la Seguridad.

He querido compartir estás líneas con tan respetable audiencia de expertos en Seguridad, sobre cinco aspectos que considero claves para lograr liderar con acierto operaciones tan dinámicas y complejas como las que se enfrentan en una empresa responsable por la fabricación, distribución y venta de sus productos y la cual que opera en tan diversos y exigentes entornos del continente americano.

Esta operación incansable y exigente obliga al funcionamiento las 24 horas del día, los 365 días del año, que maneja más de 80 mil colaboradores directos, 56 plantas manufactureras, 240 centros de distribución y más de 10 mil camiones de reparto desplegados en territorios, zonas, barrios, comunas y colonias, muchas de ellas de alta complejidad y riesgo.

Las amenazas que afectan las operaciones son de diversa magnitud y presionan en cada país con distinta intensidad. Los actores delincuenciales van desde las guerrillas de izquierda como las Fuerzas Armadas Revolucionadas Comunistas (FARC) y el Ejército de Liberación Nacional (ELN), en Colombia, pasan por delincuencia organizada como el Tren de Aragua en Venezuela y siguen con las pandillas como las Maras (Mara 18 y Salvatrucha) en Guatemala, hasta llegar a la influencia devastadora de los cárteles y grupos de delincuencia común y organizada que en México sobrepasan la centena.

Con todo este panorama en mente, además del conocimiento, la preparación física, moral y psicológica y dotado de una inquebrantable voluntad de servicio, lealtad y honradez; considero que se deben reforzar los siguientes aspectos de la gestión para conducir los esfuerzos del equipo de seguridad y protección hacia el cumplimiento de la tarea encomendada por la organización y personas a las que representa.

Foto: - Freepik

Se debe defender y proteger al guardia, porque, por lo general, se trata de personas altamente vulnerables que no han tenido mucha oportunidad de educarse y buscar mejores destinos, constituyéndose en últimas, en la persona que en la organización queda al cuidado de bienes, instalaciones y servicios cuando días y horas hábiles terminan para el resto del personal de la organización

Las normas de seguridad deben ser ampliamente conocidas por los niveles establecidos, de modo que todos en la organización sepan qué hacer, en determinadas circunstancias; pero, ese nivel de conocimiento no debe traspasar los límites de confiabilidad y confidencialidad que vuelvan vulnerables los planes de seguridad de la empresa

BLINDAR LOS PROCESOS *"CORE"* DEL NEGOCIO

Una vez concebida y definida la estrategia de seguridad y enfocada a los objetivos del negocio se deben identificar en toda la operación, las áreas claves y los procesos que "mueven" la organización, para construir con los responsables de las mismas, una agenda de trabajo que permita la identificación de amenazas, riesgos, vulnerabilidades y falencias, desechando todos aquellos pasos innecesarios (metodología LEAN) o que generan re trabajos; y proceder bajo la dirección del área de Seguridad a la elaboración de planes y procesos para enfrentarlos, definiendo metas y objetivos mensurables a corto, mediano y largo plazo que tengan como fin último el mejoramiento de los índices de Seguridad y eficacia de sus áreas.

CUIDAR A TU GENTE

A pesar de los desarrollos tecnológicos que en muchas empresas están suplantando máquinas por hombres; a pesar de la facilidad que hoy en día ofrece la tecnología para supervisar a distancia muchos procesos; el hombre continúa teniendo un valor incalculable e insustituible en muchos de los procesos de Seguridad en nuestros países latinoamericanos.

Se debe defender y proteger al guardia, celador, vigilante o guardián, como se conoce en varios países del continente, porque, por lo general se trata de personas altamente vulnerables que no han tenido mucha oportunidad de educarse y buscar mejores destinos, constituyéndose en últimas, en la persona que en la organización queda al cuidado de bienes, instalaciones y servicios cuando días y horas hábiles terminan para el resto del personal de la organización.

También se constituye en el eslabón más débil de la cadena cuando algún proceso falla y surgen problemas que pueden afectar la seguridad. En esa instancia lo determinarán, pero, de manera inquisidora, buscándolo para responsabilizarlo sin conocimiento de causa y sin ninguna consideración del infortunado suceso acaecido.

SER FIEL A LA "PROMESA DE VENTA"

Creo que muchos de los que trabajamos en esta bella profesión, hemos querido influir sustancialmente en todas las áreas, secciones y departamentos de operaciones de la organización buscando alinearlos, disciplinarlos y en fin hasta ordenarlos con el propósito último de hacer cumplir las normas y procedimientos de seguridad que le brinden a la organización la certeza de que está protegida contra riesgos y amenazas y pueda dedicar totalmente sus esfuerzos al cumplimiento de los objetivos estratégicos del negocio.

Para que esto funcione tranquila y racionalmente hay que ampliar la visión a una más holística, que permita en un principio escuchar a todos los responsables de las diferentes áreas para estructurar los procesos, tiempos y movimientos; escuchar sus recomendaciones y finalmente plasmar todo en el plan de acción y acuerdo de servicio de la organización.

La imposición de medidas sólo debe darse en caso de que el cliente interno no quiera llegar a acuerdos o simplemente, una vez acordados los incumpla generando situaciones de riesgo para las demás secciones.

En caso de enfrentar situaciones imprevistas de riesgo mayor, habrá que aplicar medidas no negociadas o inconsultas, que sean las más convenientes, oportunas y favorables para el funcionamiento seguro del negocio.

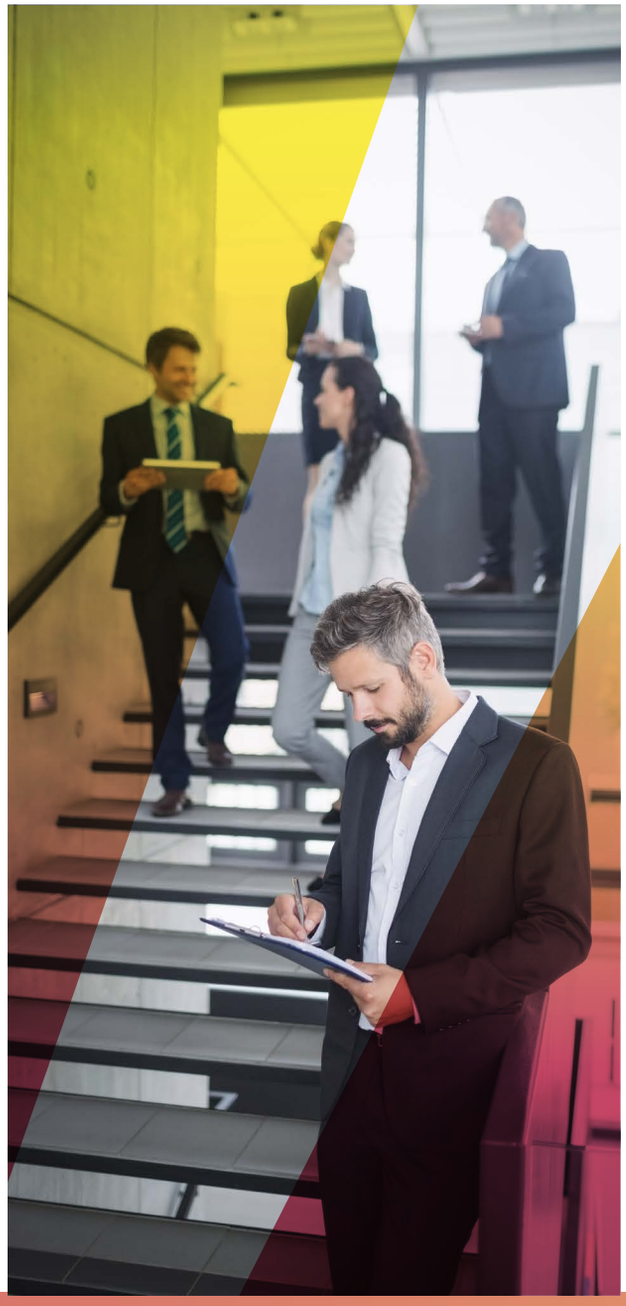


Foto: - Freepik

Las normas de seguridad deben ser ampliamente conocidas por los niveles establecidos, de modo que todos en la organización sepan qué hacer, en determinadas circunstancias; pero, ese nivel de conocimiento no debe traspasar los límites de confiabilidad y confidencialidad que vuelvan vulnerables los planes de seguridad y protección de la empresa.

LIDERAR CON EL EJEMPLO

Creo firmemente que liderar no es sólo el conjunto de habilidades que un individuo tiene para influir en la forma de actuar de las personas; sino también es encontrar al final de la faena la satisfacción del deber cumplido y tener la certeza de que los compañeros de labor no sólo crecieron como personas y como profesionales, sino también que encontraron la felicidad en lo que hacían.

Las excepciones siempre las habrá y de las "ovejas negras" existentes en todo rebaño también se sacan experiencias valiosas. En general, cuando el líder guía a su gente enseñando y compartiendo sus conocimientos, corrigiendo en el momento y sitio oportunos, es cuando el equipo aprende y valora el esfuerzo realizado, lo cual indudablemente se traduce en sentido de pertenencia, compromiso inigualable, satisfacción del deber cumplido y felicidad en el trabajo.

Así se logra sacar lo mejor de cada uno de los compañeros y se les demuestra que ellos son capaces de lograr metas que nunca se imaginaron podrían alcanzar.

De los múltiples casos de superación personal que se presentaron durante tantos años de gestión, recuerdo con especial satisfacción el de un compañero que se inició como guardia de seguridad y hoy lidera las operaciones de seguridad en uno de los países más importantes para la compañía. En segundo lugar, también merece especial mención otro caso similar de un compañero que se inició como coordinador de Seguridad en Colombia, un país que en esa época estaba sometido a múltiples amenazas y demandaba una labor especialmente dedicada y profesional. Hoy en día es él, quien lidera esa operación donde las condiciones continúan siendo críticas y exigentes.

Las anteriores son solamente pequeñas muestras de logros alcanzados y satisfacción que se siente cuando se tiene la certeza del deber cumplido.

Foto: - Freepik

Foto: - Freepik

SER AUTÉNTICO

Si al término de la misión los diferentes actores, colaboradores, subalternos y compañeros de la organización reconocen la autenticidad y valor de la persona que maneja los retos de seguridad de la compañía, la recompensa estará dada.

Cuando sus clientes han sabido a ciencia cierta quién es usted y cómo responde en situaciones normales o de emergencia y ve que su comportamiento es congruente, sereno y firme en el manejo de crisis, su credibilidad y aprecio crecerán como nadie puede imaginarlo.

Ser auténtico y ser genuino de modo que nunca los logros, premios o reconocimientos opaquen la humildad, la gentileza y la suprema excelencia, que es la sencillez.

Son en últimas, la autenticidad y la sencillez el toque de verdad que por fortuna Dios nos ha concedido a quienes lideramos personas en organizaciones tan complejas en el mundo, igualmente complejo y difícil en el que nos ha tocado vivir. ■

CUANDO EL LÍDER GUÍA A SU GENTE ENSEÑANDO Y COMPARTIENDO SUS CONOCIMIENTOS, CORRIGIENDO EN EL MOMENTO Y SITIO OPORTUNOS, ES CUANDO EL EQUIPO APRENDE Y VALORA EL ESFUERZO REALIZADO, LO CUAL INDUDABLEMENTE SE TRADUCE EN SENTIDO DE PERTENENCIA, COMPROMISO INIGUALABLE, SATISFACCIÓN DEL DEBER CUMPLIDO Y FELICIDAD EN EL TRABAJO

Diego Arévalo, profesional independiente en seguridad. *Más sobre el autor:*

LÍDERES EN SOLUCIONES DE

RASTREO SATELITAL

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

+ de 50,000 equipos instalados

25 AÑOS DE EXPERIENCIA

Recuperación 98.5% Aviso en menos de 30 minutos*

24/365 DÍAS Monitoreo de equipos

WEB APP

Desarrollo de WEB y APP

amazon web services

Azure

Infraestructura sustentada por AWS y Azure

Tecnología 3G/4G/Satelital

Contamos con puntos estratégicos en todo el país

- Cadena de suministro
- Prevención y seguridad
- Safty
- Logística
- Tráfico
- Reparto

Más Información:

Socio Amesis amesis.org.mx

AMESP ANTP ASIS INTERNATIONAL CAPÍTULO MÉXICO 217 CANACAR CÁMARA NACIONAL DEL AUTOTRANSPORTE DE CARGA CNSP EMPRESAS DE CALIDAD COPARMEX ConaLog Consejo Nacional de Ejecutivos en Logística y Cadena de Suministro, A.C.

Contáctanos 55·5374·9320

Columna
EL TIGRE TIENE RAYAS

ballesteros.barrera@hotmail.com

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

Más sobre el autor:

¿CÓMO ES EL LIDERAZGO DEL SIGLO XXI?

Foto: - Freepik

Los accesos no autorizados pueden resultar en situaciones peligrosas o incluso en la pérdida de información confidencial

MÉXICO

La gestión de grupos se ha convertido en uno de los aspectos más importantes dentro de cualquier organización. Si bien es cierto que **las empresas han tenido que adaptarse al nuevo escenario provocado por la transformación digital,** hay algunos de sus líderes que no se han actualizado en aspectos como el liderazgo. El **componente humano** ha adquirido mucha importancia y cualidades como la inteligencia emocional han pasado al primer plano a la hora del valorar el liderazgo del siglo XXI.

El mayor desafío del liderazgo es **escuchar las opiniones de todos y llegar a una solución que sea beneficiosa para el conjunto.** En estos casos, a la hora de escuchar todo tipo de opiniones, es importante ser imparcial y no tener ningún tipo de favoritismo. Este aspecto es clave para ganarte la confianza del resto, lo cual es fundamental para ser un buen líder.

Es importante **comprender el perfil psicológico de los miembros del equipo** para saber cómo les afecta una decisión y cómo puede ser su comportamiento entre ellos. Hacer que las personas trabajen juntas es un gran desafío en sí mismo. Por ello, si hay cualquier problema en el equipo tienes que hacerte responsable, por lo que tienes que intervenir inmediatamente en caso de malentendidos. Por otra parte, ten en cuenta que eres la cara visible del equipo, por lo que tienes que actuar como puente entre los empleados y la gerencia. Esto es relevante por los diferentes tipos de liderazgo empresariales que existen actualmente.

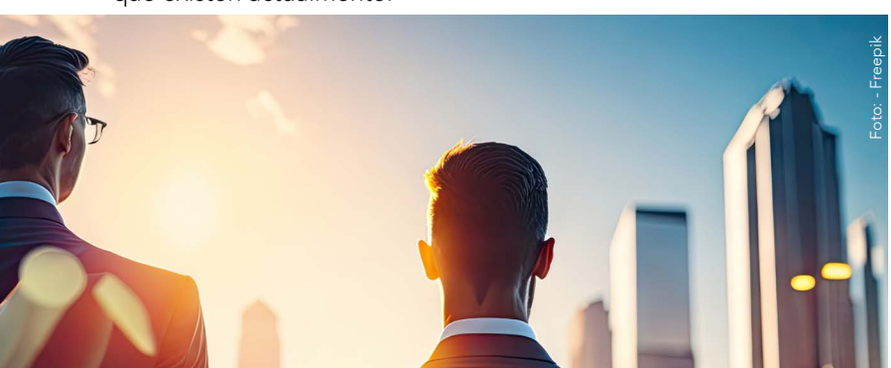


Foto: - Freepik

¿CÓMO HA CAMBIADO EL LIDERAZGO EN EL SIGLO XXI?

A la hora de analizar cualquier cambio en una figura individual, hay que tener en cuenta el contexto en el que se produce. El panorama empresarial de nuestros tiempos es muy competitivo a todos los niveles, además de que aspectos como la conectividad y la inmediatez son factores que destacan sobre el resto. Esto significa que los líderes de las organizaciones tienen unas exigencias altas. A esto se le suma la toma de conciencia de la sociedad sobre temas sociales, por lo que los líderes tienen que saber incorporar estos valores a la organización y darles la importancia que merecen.

Por ello, un liderazgo del siglo XXI no sólo busca ser transformador y obtener el mayor beneficio económico posible, sino que también debe darle importancia a cuestiones éticas. Por ello, la responsabilidad social corporativa tiene cada vez más importancia. De esta forma, los líderes de los negocios se presentarán como ejemplos a los que seguir bajo un enfoque holístico que no coloque por delante constantemente el beneficio económico a la resolución de los problemas sociales.

"Los empleados de hoy están rechazando los modelos tradicionales de liderazgo. Los líderes que ejercen control sobre sus equipos no sólo alienan a los empleados de hoy, sino que también tienen un impacto negativo en todos los aspectos del negocio, desde la rotación del personal y la productividad hasta el crecimiento de los ingresos", declara Robert Ordever, MD de cultura laboral de OC Tanner Europe.

Además, a todos estos factores hay que sumarle los nuevos modelos laborales surgidos a partir de la pandemia. Por ello, es vital conocer las claves del liderazgo en el trabajo remoto.

¿CUÁL ES EL ESTADO DE LA FIGURA DEL LÍDER?

Según el Informe de Cultura Global 2020 del Instituto OC Tanner, sólo el 26% de los empleados sienten que su líder fomenta la colaboración, dato que dice mucho del estado actual del liderazgo.

"Los mejores líderes muestran su aprecio, dan reconocimiento regularmente y brindan apoyo, aliento y consejos continuamente. Y los empleados con grandes líderes comprenderán su valor para el negocio y cómo contribuyen al 'panorama general'. Se les animará a llegar más alto y soñar en grande. En última instancia, los grandes líderes dejarán un legado inspirador y un negocio próspero".

"La investigación muestra que las empresas que mantienen enfoques de liderazgo tradicionales tienen puntajes de experiencia y compromiso de los empleados deficientes. Son deficientes en todas las áreas de la cultura del lugar de trabajo, incluido el propósito de la empresa, las oportunidades, el éxito organizacional, la apreciación, el bienestar y, por supuesto, el liderazgo", declara Ordever.

En este contexto, la ética a la hora de resolver asuntos ha pasado a un primer plano. Según el estudio de Deloitte "Liderazgo para el siglo XX", destacaron que el rasgo más significativo de un líder actual es "la capacidad de liderar a través del cambio y de la ambigüedad", seguido de "la capacidad de liderar a través de la influencia". Esto demuestra que liderar no es sinónimo de ordenar o imponer, sino actuar como ejemplo para los empleados y tengan un referente.

"Desarrollar líderes con nuevas competencias requiere más que una evolución propia. Igualmente, primordial es que la organización tenga la cultura, la estructura y los procesos de gestión para cultivar estos líderes", dijo un portavoz de Deloitte en referencia al informe.

Las competencias para ser un líder eficiente y adaptado al contexto actual son las siguientes:

- **Transparencia:** en un contexto actual en el que la incertidumbre y la diversidad son tan relevantes, un líder debe comprender las necesidades de sus empleados y ser claro con los objetivos y el estado de la organización.
- **Colaboración interna:** para saber qué necesitan los empleados, un líder debe ser atento y buscar formas de comunicarse y colaborar con ellos.
- **Gestión de desempeño:** medir el éxito es un factor importante a la hora de comprender el impacto de un líder empresarial. Si lo haces, ayudará a una empresa a decidir cuáles son los rasgos más importantes.

Según el Informe de Cultura Global 2020 del Instituto OC Tanner, sólo el 26% de los empleados sienten que su líder fomenta la colaboración, dato que dice mucho del estado actual del liderazgo

SER INSPIRADOR

Los líderes deben alentar e inspirar a los miembros de su equipo. Poder ayudar a tu equipo a mantener la moral alta y la esperanza en tiempos difíciles los ayudará a prosperar. Las propias acciones e historias personales de un líder pueden inspirar a otros a trabajar de manera más inteligente, a cuidarse mejor, a ver su objetivo colectivo desde una nueva perspectiva y mucho más.

SER INCLUSIVO

También es importante que los líderes sean inclusivos en su liderazgo. Los líderes deben considerar y empoderar a quienes los rodean al tomar decisiones y planes para el futuro. El objetivo de un líder es cultivar un equipo que tenga un sentido de pertenencia y puedan trabajar juntos con éxito. Esto requiere tratar a todos los empleados y compañeros de trabajo de manera justa; recibir aportes de todos (mientras se ciñe a la visión y misión de la empresa) y proporcionar los recursos y el apoyo que los miembros del equipo necesitan para alcanzar su máximo potencial, tanto individual como colectivamente. La diversidad y la inclusión son fundamentales en toda empresa.

Además deberán afrontar cambios demográficos —como el envejecimiento de la población laboral, teniendo que conjugar armónicamente la experiencia con el empuje de la juventud—, el creciente y necesario papel de la mujer en las estructuras, la globalización, la protección del medio ambiente y la responsabilidad social, la diversidad y la multiculturalidad, la incorporación masiva de los robots, la inteligencia artificial y otros extraordinarios avances que generan las nuevas tecnologías en beneficio colectivo. Hacer lo que es necesario es trabajar ante todo para construir el bien común, respondiendo a las necesidades de las personas y de la organización en vistas a su sostenibilidad.

Un líder del siglo XXI debe ser un visionario inspirador para el futuro. Deben proporcionar una meta e inspirar a otros con su sentido de propósito. Los líderes necesitan empatía y creatividad para inspirar, apoyar y alentar a los miembros de su equipo. También necesitan buenas habilidades de toma de decisiones para realizar movimientos inteligentes que sean prácticos tanto para el equipo como un todo y como individuo.

Los mejores líderes de hoy tienen una visión y marcan la pauta para su equipo. Los verdaderos líderes van más allá del papel de "jefe" y animan a otros a liderar, creando a su vez más líderes. ¿Eres un jefe o un líder?

Por último, las capacidades tecnológicas y el conocimiento digital son aspectos que deben incluirse en el liderazgo del siglo XXI. "La tecnología es un lenguaje importante que los líderes de todas las industrias deben comprender y adoptar. Los líderes efectivos necesitan saber a detalle los cambios tecnológicos que están ocurriendo, o si no, deben tener un gran control sobre las personas que los manejan", explicó Ben Hunt-Davis, cofundador de Will it Make the Boat Go Faster. ■

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

Columna de GEMARC

LIDERAZGO EN SEGURIDAD

CONSTRUIDO SOBRE LA CONFIANZA, RESPETO E INTEGRIDAD

Una entrevista con Lourdes Morales Aguilar, directora *Senior* de Seguridad Global de Walmart Internacional

MÉXICO

Lourdes Morales Aguilar, directora *Senior* de Seguridad Global de Walmart Internacional

"En el ámbito corporativo, el liderazgo impregnado de confianza, respeto e integridad juega un papel crucial. Es de suma importancia alinear los valores personales con los corporativos y crear espacios respetuosos para fomentar la diversidad e inclusión en el entorno laboral", según Lourdes Morales Aguilar.

TRAYECTORIA PROFESIONAL Y DESAFÍOS SUPERADOS

Lourdes comparte su experiencia como criminóloga con 18 años de trayectoria, especializada en seguridad corporativa, investigaciones y seguridad de la cadena de suministro. Con una destacada carrera en Walmart que abarca 15 años, ha desafiado paradigmas al ingresar a una industria tradicionalmente masculina.

En su rol actual se convirtió en la primera mujer latina en ocupar dicha posición, durante su trayectoria se ha convertido en la primera mujer en ocupar varios de sus roles, sin embargo, su misión con ello es allanar el camino para futuras generaciones de mujeres en seguridad.

LIDERAZGO EN ACCIÓN

Los grandes líderes son reconocidos por su capacidad para inspirar, motivar, retar y dar soporte a sus equipos para alcanzar el éxito y el crecimiento. Siempre hay que tomar en cuenta que liderazgo no significa únicamente estar a cargo, sino, por el contrario, se trata de tomar la responsabilidad y cuidar a quienes están a tu cargo. Con la mentalidad y enfoque correctos, puedes convertirte en un líder confiable y efectivo que impacta de manera positiva a quienes te rodean.

LA REGLA DE ORO Y PRINCIPIOS CLAVE DEL LIDERAZGO DE SERVICIO

El liderazgo de servicio es un enfoque de liderazgo que se centra en servir y satisfacer las necesidades de los demás. En lugar de simplemente dirigir o supervisar, los líderes de servicio buscan entender y abordar las necesidades de su equipo. Este estilo de liderazgo implica empatía, colaboración y orientación hacia el bienestar de los demás, con el objetivo de contribuir al crecimiento y éxito conjunto.

La regla de oro y los valores del liderazgo de servicio están fundamentados en el principio de tratar a los demás como te gustaría ser tratado. Algunos valores clave asociados con el liderazgo de servicio incluyen:

1) **Empatía:** Comprender y compartir los sentimientos de los demás, mostrando preocupación genuina por su bienestar.
2) **Humildad:** Reconocer y apreciar las contribuciones de los demás, sin jactarse ni buscar reconocimiento excesivo.
3) **Colaboración:** Fomentar un entorno donde el trabajo en equipo y la cooperación son valorados para lograr objetivos comunes.
4) **Integridad:** Actuar con honestidad y ética, manteniendo coherencia entre lo que se dice y se hace.
5) **Compromiso con el desarrollo:** Apoyar el crecimiento y desarrollo personal y profesional de los demás, proporcionando oportunidades de aprendizaje.
6) **Enfoque en el servicio:** Priorizar las necesidades y bienestar de los demás sobre el interés personal, buscando maneras de contribuir positivamente.

Estos valores y la regla de oro forman la base del liderazgo de servicio, promoviendo relaciones positivas y un ambiente de trabajo colaborativo. ■

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

COMEXA 30 años

ALAS Asociación Latinoamericana de Seguridad · ASIS International · AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C. · CPP Certified Protection Professional, Board Certified in Security Management · NFPA International

Universidad Pontificia ICAI ICADE Comillas Madrid · COPARMEX · IMEI Asociación Mexicana del Edificio Inteligente y Sustentable A.C. · Consejo Nacional de Seguridad Privada CNSP Empresas de Calidad · 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

Laura Barrera
A LA CABEZA DE EXPO SEGURIDAD MÉXICO Y EXPO SEGURIDAD INDUSTRIAL 2024

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

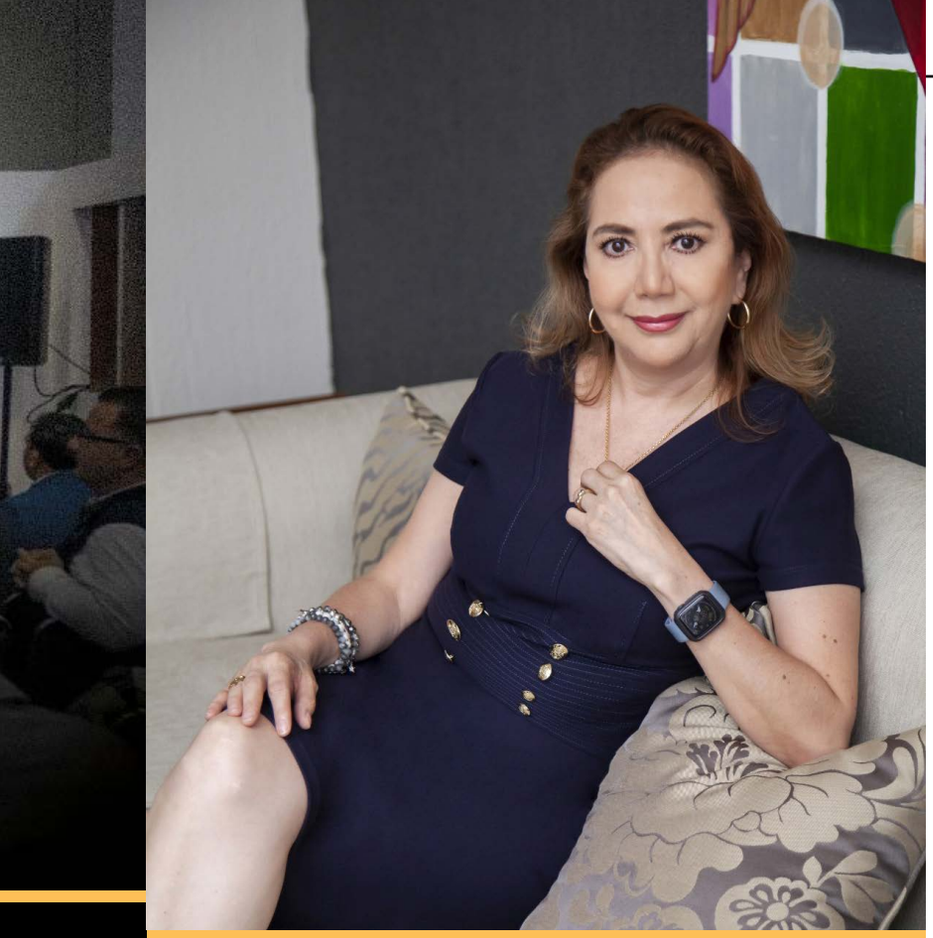
Con más de 26 años de experiencia en organización, desarrollo y comercialización de eventos, este año Laura Barrera espera recibir a más de 17 mil visitantes en la Expo de Seguridad más importante de Latinoamérica

Con un área total de 24 mil metros cuadrados, de los cuales 10 mil (m^2) estarán destinados a los más de 350 expositores nacionales e internacionales que participarán en la vigésima primera edición de Expo Seguridad México, así como Expo Seguridad Industrial, se espera la asistencia de más de 17 mil visitantes. Este año, la expo de seguridad más importante de Latinoamérica próxima a realizarse del 16 al 18 de abril en el Centro Citibanamex (Ciudad de México), está encabezada por Laura Barrera, quien a finales del año pasado (2023), se integró a las filas de RX México (antes Reed Exhibitions) como directora general de este magno evento.

"Estoy emocionada por la realización de Expo Seguridad, por mi llegada a RX México (antes Reed Exhibitions), y sobre todo por ir abriendo cada vez más, posiciones de liderazgo para las mujeres, algo que he venido trabajando junto con colegas mías en este tipo de exposiciones. Tengo más de 25 años trabajando en la industria de exhibiciones de talla nacional e internacional, y considero que es gracias a toda esa experiencia que RX México (antes Reed Exhibitions) , que Héctor Morfín, director de Portafolio, me dieron la oportunidad de sumarme a este equipo; así como Luiz Bellini, director general de RX México (antes Reed Exhibitions); Claudio Della Nina, responsable en Brasil, y por supuesto Fernando Fischer, CEO de Norteamérica. Parte de este esfuerzo es ir sumando áreas de contenido, ya que la capacitación es muy importante, y lo que buscamos es que tanto expositores como visitantes cumplan con sus expectativas y cada año las vayamos superando", comentó Laura Barrera en entrevista.

TRAYECTORIA

Egresada de la licenciatura en Administración por la Universidad del Valle de México, Campus San Ángel, Laura Barrera también realizó estudios de Mercadotecnia y Desarrollo de Negocios en el Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Ciudad de México. Tiene la certificación en Organización de Exposiciones (2017) que otorga AMPROFEC junto con ESDAI de la Universidad Panamericana. Ha dirigido varios de los eventos más grandes del país, entre los que destacan: EXPO COMM, Salón Internacional del Automóvil, IV Foro Mundial del Agua, Plasti-



"Estoy emocionada por participar de alguna manera en incentivar la seguridad de mi país a través de un foro de negocio de gran nivel"

magen, Expo Pack, Expo Manufactura, Cumbre Mundial de la Leche, adicionalmente ha dirigido más de 43 exposiciones internacionales con dimensiones desde 9 mil m^2, hasta más de 40 mil m^2 de exhibición con crecimientos anuales de alrededor del 20%. Fue profesora del Diplomado "Organización de Eventos, Congresos y Convenciones" para la Universidad Iberoamericana y para el Tecnológico de Monterrey.

Toda esa trayectoria la ha posicionado dentro de la expo más importante de seguridad pública y privada en Latinoamérica, sin dejar de lado, que además de su experiencia, es una realidad que esta industria se enfoca en el cumplimiento de los perfiles que requiere una industria tan importante como es la seguridad, y que abre cada vez más oportunidades de liderazgo para las mujeres.

"Este año hemos preparado un fuerte programa académico para nuestros visitantes, buscamos fortalecer la capacitación a través de las diferentes conferencias impartidas por reconocidos especialistas en seguridad; también integramos la sustentabilidad al programa académico; y seremos perseverantes para asegurar que cada sala de conferencias, de paneles, tenga la audiencia esperada por nuestros expositores, con los perfiles requeridos. Contemplamos tanto las fuerzas del orden, como la seguridad privada, todos los niveles de tecnología, blindaje, etcétera".

SIA EDUCATION

En esta edición, además de Laura, Security Industry Association (SIA) se incorpora al programa académico de Expo Seguridad México con el programa "SIA Education", el cual se enfocará en la ciberseguridad pública y corporativa, en estrategias de seguridad nacional y pública, en mejores prácticas en seguridad privada, manejo de crisis, prevención del crimen, infraestructura de tecnología de la información, esquemas de protección corporativa, y seguridad física y operativa, entre otros temas.

"Uno de los objetivos como directora de estas exposiciones, es que se sigan fortaleciendo, que la parte de capacitación, de educación que ofreceremos, ayude a profesionalizar al sector. A manera personal, estoy emocionada por participar de alguna manera en incentivar la seguridad de mi país a través de un foro de negocio de gran nivel, fortaleciendo a las empresas nacionales con alianzas estratégicas internacionales, a los asistentes con todo el acervo que brindan los expositores, con el acercamiento a las tecnologías más innovadoras, y que todo contribuye en mejorar la vida de los colaboradores de esta industria".

"SIA Education" es un programa internacional de capacitación con un alto nivel educativo, en el que especialistas de gran talla internacional brindarán su experiencia y aprendizajes, una gran oportunidad para las pymes del país. Los temas de este programa estarán enfocados a la región, con los problemas y retos de seguridad de Latinoamérica. Expo Seguridad México y Expo Seguridad Industrial están direccionadas por una mujer con experiencia en el desarrollo de eventos grandes y reconocidos en el mundo, con fuerte tendencia en la promoción a la capacitación, a la profesionalización del personal y quien espera sea una edición que cumpla y supere las expectativas de los asistentes.

"He estado en muchas industrias y siempre busco el beneficiar al ser humano de alguna manera. Este año, me toca estar al frente de un evento de seguridad que contribuye no sólo al desarrollo de esta industria, sino a la seguridad de mi país; me apasiona el cómo proteger a quienes nos están fortaleciendo, y creo que la educación contribuye, en cualquier nivel, a que se fomente la seguridad de todos. Y bueno, las mujeres tendremos una participación activa en este evento, tanto hombres como mujeres profesionales de la seguridad; de esta manera puedo continuar motivando a más mujeres y abriendo oportunidades en puestos de liderazgo", finalizó Laura Barrera. ■

Fotos: Cortesía RX México (antes Reed Exhibitions)

MEJORES PRÁCTICAS PARA LA SEGURIDAD EN CASINOS Y CENTROS DE ENTRETENIMIENTO

Foto: - Freepik

Todas las técnicas que implementemos para la seguridad y protección para casinos y centros de entretenimiento deben tener el potencial de ser innovadoras, viables y específicas para cubrir todas las necesidades, con un impacto significativo, y una aplicabilidad favorable

MÉXICO | **José Luis Sánchez Gutiérrez**

Nuevamente estimados lectores, realmente muy agradecido por su acostumbrada preferencia; y en esta ocasión tocaremos el tema de la seguridad en casinos y centros de entretenimiento.

Para todo profesional de Seguridad Patrimonial, Seguridad Corporativa y Seguridad Física de una empresa en México; proteger casinos y centros de entretenimiento implica abordar desafíos específicos en seguridad. Aquí hay algunas de las mejores técnicas para proteger estos lugares:

- **Vigilancia y sistemas de CCTV avanzados:** Instalar y mantener sistemas de cámaras de vigilancia de alta calidad en áreas clave, como pisos de juego, entradas y salidas, para monitorear actividades y prevenir incidentes.
- **Control de acceso:** Implementar controles de acceso rigurosos para restringir la entrada sólo a personal autorizado y clientes. Esto puede incluir sistemas de tarjetas de acceso, verificación de identificación y personal de seguridad en puntos clave.
- **Personal de seguridad capacitado:** Contratar y capacitar a un equipo de seguridad altamente calificado para manejar situaciones delicadas, patrullar áreas críticas y responder rápidamente a emergencias.
- **Tecnología de reconocimiento facial y biométrica:** Utilizar tecnología avanzada para identificar posibles amenazas o personas no autorizadas que puedan ingresar al casino o centro de entretenimiento.
- **Iluminación y diseño ambiental:** Mantener áreas bien iluminadas para disuadir la actividad delictiva. Además, el diseño arquitectónico del lugar puede ayudar a crear un entorno seguro.
- **Sistemas de detección de intrusos:** Instalar sistemas de detección de intrusos para proteger áreas sensibles y restringir el acceso no autorizado a ciertas zonas.
- **Capacitación del personal:** Proporcionar capacitación regular al personal sobre seguridad, procedimientos de emergencia y manejo de situaciones delicadas para fortalecer la preparación y respuesta.
- **Colaboración con las fuerzas del orden:** Establecer relaciones con las autoridades locales y trabajar en estrecha colaboración con ellas para compartir información y mejorar la seguridad en general.

VIDEOVIGILANCIA

Desarrollar un sistema de vigilancia avanzado con CCTV (Circuito Cerrado de Televisión) implica una planificación cuidadosa y la implementación de tecnología de vanguardia. Un sistema de vigilancia avanzado con CCTV no sólo ofrece una disuasión visual contra actividades delictivas, sino que también proporciona evidencia crucial en caso de incidentes, contribuyendo a la seguridad general del casino o centro de entretenimiento. Aquí hay algunos pasos y elementos clave para establecer un sistema avanzado de CCTV:

- **Evaluación de necesidades y riesgos**: Comprender las áreas críticas y vulnerables del casino o centro de entretenimiento es fundamental. Realizar una evaluación de riesgos para determinar las zonas que necesitan una cobertura especial.
- **Diseño del sistema:** Trabajar con expertos en seguridad y proveedores de sistemas de CCTV para diseñar un sistema adaptado a las necesidades específicas del lugar. Esto incluye la selección de cámaras, ubicación estratégica, cobertura óptima y consideraciones de iluminación.

Un sistema de vigilancia avanzado con CCTV no sólo ofrece una disuasión visual contra actividades delictivas, sino que también proporciona evidencia crucial en caso de incidentes, contribuyendo a la seguridad general del casino o centro de entretenimiento


Foto: - Freepik

- **Elección de equipos de alta calidad:** Optar por cámaras de alta resolución con capacidades de visión nocturna, zoom óptico, panorámicas e inclinaciones, y características de detección de movimiento avanzadas. También es crucial elegir sistemas de almacenamiento confiables para grabaciones.
- **Instalación profesional:** Contar con instaladores capacitados y experimentados para colocar estratégicamente las cámaras en lugares clave. Asegurarse de que la instalación cumpla con estándares de seguridad y privacidad.
- **Integración y conectividad:** Integrar el sistema de CCTV con otros sistemas de seguridad (como alarmas, sistemas de acceso, etc.) para una gestión centralizada. También, asegurar la conectividad a una red segura para la transmisión y almacenamiento de datos.
- **Monitoreo en tiempo real:** Establecer un centro de monitoreo que permita a los operadores supervisar continuamente las cámaras. Implementar *software* avanzado de gestión de video para análisis de datos y búsqueda eficiente de grabaciones.
- **Capacitación del personal:** Proporcionar capacitación al personal encargado de operar y mantener el sistema, incluyendo la interpretación de imágenes, gestión de alarmas y procedimientos de respuesta a emergencias.
- **Actualizaciones regulares y mantenimiento:** Programar mantenimiento periódico y actualizaciones tecnológicas para asegurar un funcionamiento óptimo y mantener la eficacia del sistema a lo largo del tiempo.

CONTROL DE ACCESO

El control de acceso es esencial para garantizar la seguridad en casinos y centros de entretenimiento. Un sistema de control de acceso robusto y bien gestionado es fundamental para la seguridad general de un casino o centro de entretenimiento, garantizando que sólo el personal autorizado tenga acceso a áreas críticas y contribuyendo a la prevención de actividades delictivas. Aquí se detallan los aspectos clave para desarrollar un sólido sistema de control de acceso:

- **Identificación de puntos críticos:** Identificar y categorizar áreas sensibles, como áreas de juego, cajas, áreas de almacenamiento, etc., para determinar niveles de acceso y restricciones adecuadas.
- **Tecnologías de acceso seguras:** Implementar sistemas de identificación avanzados, como tarjetas de acceso con tecnología RFID o biometría (huellas dactilares, reconocimiento facial), para garantizar la autenticación precisa del personal autorizado y restringir la entrada a áreas restringidas.
- **Puertas y barreras físicas:** Instalar puertas de seguridad y barreras físicas en puntos de acceso críticos, controladas por el sistema de acceso, para permitir o denegar la entrada según los permisos de cada individuo.
- **Zonas de segregación:** Utilizar zonas de segregación para dividir áreas de acceso público y áreas restringidas. Estas áreas permiten un control más preciso del movimiento de personal autorizado.
- **Gestión centralizada del acceso:** Implementar un sistema de gestión de acceso centralizado que permita la administración y monitorización remota de autorizaciones de acceso, así como la revocación inmediata de privilegios en caso de emergencia.
- **Auditoría y registro:** Registrar y auditar todas las actividades de acceso para realizar un seguimiento de las entradas y salidas, identificar anomalías y detectar posibles problemas de seguridad.
- **Capacitación y procedimientos:** Proporcionar capacitación adecuada al personal sobre el uso del sistema de control de acceso, y establecer procedimientos claros para situaciones de emergencia o cambios en los niveles de acceso.
- **Mantenimiento y actualización:** Realizar mantenimiento regular y actualizaciones tecnológicas para garantizar la eficacia continua del sistema y protegerlo contra vulnerabilidades.

PERSONAL DE SEGURIDAD CAPACITADO

Desarrollar un equipo de seguridad altamente capacitado es esencial para garantizar la protección efectiva en casinos y centros de entretenimiento. Un personal de seguridad altamente capacitado no sólo protege el lugar, sino que también contribuye a una experiencia positiva para los visitantes, al garantizar un entorno seguro y confiable. Aquí están los pasos clave para lograrlo:

- **Selección cuidadosa:** Realizar un proceso de selección riguroso para contratar a personal de seguridad idóneo. Buscar habilidades específicas como experiencia previa en seguridad, capacitación en primeros auxilios, capacidad de manejo de situaciones delicadas y habilidades de comunicación.
- **Entrenamiento integral:** Proporcionar una formación integral que incluya procedimientos de seguridad, manejo de conflictos, protocolos de emergencia, técnicas de observación y reporte, así como conocimientos legales relevantes.
- **Capacitación continua:** Ofrecer programas de capacitación periódicos para mantener al personal actualizado sobre nuevas amenazas, tecnologías emergentes, cambios en políticas de seguridad y prácticas recomendadas en el campo de la seguridad.
- **Simulacros y ejercicios prácticos:** Realizar simu-

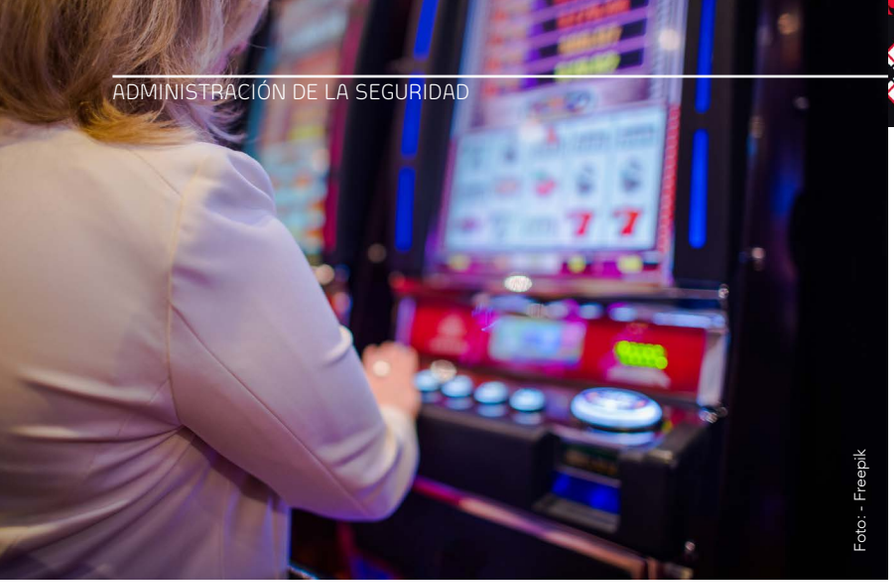


Foto: - Freepik

lacros de emergencia y ejercicios prácticos para poner a prueba la preparación del personal frente a escenarios reales. Estos ejercicios mejoran la capacidad de respuesta del equipo ante situaciones críticas.

- **Énfasis en la conducta:** Enfatizar la importancia de la integridad, la ética profesional y la conducta apropiada en todas las interacciones con los clientes y entre el personal. Esto incluye la capacitación en habilidades de comunicación y trato con el público.
- **Liderazgo y supervisión efectivos:** Garantizar que los líderes y supervisores del equipo de seguridad estén capacitados para guiar al personal, tomar decisiones rápidas y mantener altos estándares de desempeño.
- **Fomentar el trabajo en equipo:** Promover un ambiente de trabajo colaborativo y de apoyo mutuo entre el personal de seguridad. Esto fortalece la cohesión del equipo y mejora la capacidad de respuesta en situaciones de emergencia.
- **Evaluación de desempeño:** Realizar evaluaciones regulares para medir el desempeño del personal de seguridad. Estas evaluaciones pueden ayudar a identificar áreas de mejora y reconocer el buen desempeño.

TECNOLOGÍA DE RECONOCIMIENTO FACIAL Y BIOMÉTRICA

Desarrollar y aplicar tecnología de reconocimiento facial y biométrica es un enfoque avanzado para fortalecer la seguridad en casinos y centros de entretenimiento. La tecnología de reconocimiento facial y biométrica brinda una capa adicional de seguridad al identificar de manera precisa y eficiente a individuos autorizados, controlar el acceso a áreas sensibles y detectar cualquier actividad sospechosa. Aquí se detallan los aspectos clave:

- **Sistemas de reconocimiento facial:** Utilizar sistemas avanzados de cámaras y *software* que puedan identificar y autenticar personas mediante el análisis de características faciales únicas. Esto ayuda a monitorear la presencia de individuos en áreas específicas y puede detectar personas no autorizadas.
- **Implementación de escaneo biométrico:** Incorporar sistemas de escaneo biométrico, como lectores de huellas dactilares, reconocimiento de iris o venas, para autenticar la identidad de empleados autorizados y visitantes de alta seguridad. Esto garantiza un acceso altamente seguro a áreas restringidas.

La implementación de sistemas de detección de intrusos efectivos proporciona una capa adicional de seguridad, detectando y alertando sobre intrusiones no autorizadas para prevenir incidentes y proteger la seguridad

- **Integración con bases de datos:** Integrar los sistemas de reconocimiento facial y biométrico con bases de datos de seguridad para identificar automáticamente a individuos registrados o de interés, como aquellos con prohibiciones de entrada o búsquedas específicas.
- **Análisis de comportamiento:** Utilizar tecnologías de reconocimiento facial que incluyan análisis de comportamiento, como la detección de emociones o comportamientos inusuales, para prevenir y responder a situaciones de riesgo.
- **Conformidad con la privacidad:** Asegurar que la implementación de estas tecnologías cumpla con las leyes de privacidad y protección de datos. Garantizar la transparencia en la recopilación y uso de datos biométricos, obteniendo el consentimiento cuando sea necesario.
- **Capacitación y mantenimiento:** Proporcionar capacitación al personal sobre el uso correcto de esta tecnología y realizar mantenimiento regular para asegurar su funcionamiento óptimo.
- **Actualización continua:** Mantenerse al día con las últimas innovaciones en reconocimiento facial y biométrico para aprovechar mejoras tecnológicas y garantizar la efectividad de los sistemas de seguridad.

ILUMINACIÓN Y DISEÑO AMBIENTAL

El diseño ambiental y la iluminación adecuada son componentes vitales para fortalecer la seguridad en casinos y centros de entretenimiento. Un diseño ambiental adecuado y una iluminación estratégica contribuyen significativamente a la seguridad general del entorno, proporcionando visibilidad, disuadiendo la actividad delictiva y mejorando la sensación de seguridad para empleados y visitantes. Aquí se detallan los aspectos clave:

a) **Iluminación estratégica:** Implementar una iluminación adecuada en todo el establecimiento, especialmente en áreas clave como entradas, pasillos, estacionamientos, zonas de juego y alrededores. La iluminación brillante disuade la actividad delictiva al reducir los lugares donde los delincuentes pueden ocultarse.

b) **Luces direccionales:** Utilizar luces direccionales para resaltar áreas específicas y evitar sombras que puedan servir como escondites. Esto aumenta la visibilidad y la percepción de seguridad.

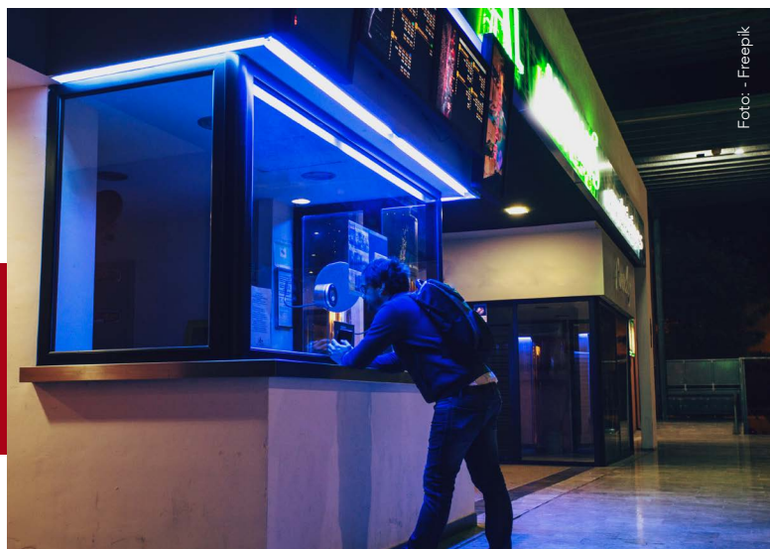


Foto: - Freepik


Foto: - Freepik

c) **Iluminación de emergencia:** Instalar sistemas de iluminación de emergencia que se activen en caso de cortes de energía para garantizar que las áreas críticas permanezcan iluminadas y los procedimientos de evacuación sean seguros.
d) **Diseño de entorno seguro:** Considerar el diseño arquitectónico y paisajístico para crear un entorno seguro. Esto incluye minimizar áreas de acceso oscuro, mantener líneas de visión claras y eliminar posibles escondites.
e) **Tecnología de iluminación inteligente:** Emplear sistemas de iluminación inteligente que puedan ajustarse automáticamente según la luz natural y las condiciones ambientales para mantener un entorno bien iluminado en todo momento.
f) **Diseño de interiores y señalización:** Utilizar colores y diseños que faciliten la orientación y la seguridad de los visitantes. Señalizar claramente las salidas, áreas de seguridad y rutas de evacuación.
g) **Sistemas de control de iluminación:** Implementar sistemas de control de iluminación centralizados que permitan la programación y el monitoreo remoto de las luces en todo el establecimiento.
h) **Mantenimiento regular:** Realizar un mantenimiento periódico de las instalaciones de iluminación para garantizar que todas las luces estén en funcionamiento y proporcionen la iluminación adecuada en áreas críticas.

SISTEMAS DE DETECCIÓN DE INTRUSOS

Desarrollar sistemas de detección de intrusos efectivos es esencial para reforzar la seguridad en casinos y centros de entretenimiento. La implementación de sistemas de detección de intrusos efectivos proporciona una capa adicional de seguridad, detectando y alertando sobre intrusiones no autorizadas para prevenir incidentes y proteger la seguridad. Aquí se detallan los aspectos clave:

- **Sensores y dispositivos de detección:** Instalar una variedad de sensores, como sensores de movimiento, rotura de vidrio, magnéticos en puertas y ventanas, y otros dispositivos de detección que alerten sobre intrusiones no autorizadas.
- **Sistemas de alarma**: Implementar sistemas de alarma que se activen inmediatamente al detectar intrusiones, alertando al personal de seguridad y activando protocolos de respuesta.
- **Integración con sistemas de vigilancia:** Integrar los sistemas de detección de intrusos con el sistema de CCTV y otros sistemas de seguridad para proporcionar una respuesta rápida y una visualización inmediata de la intrusión.
- **Control de acceso inteligente:** Utilizar tecnología de control de acceso que no sólo permita el acceso autorizado, sino que también detecte intentos no autorizados y active alertas.
- **Monitoreo remoto:** Establecer un centro de monitoreo que supervise continuamente los sistemas de detección de intrusos y responda rápidamente a cualquier alerta.
- **Capacitación y procedimientos:** Capacitar al personal de seguridad para manejar y responder efectivamente a las alarmas de intrusión, incluyendo la coordinación con las autoridades locales en caso de emergencias.
- **Pruebas y mantenimiento:** Realizar pruebas regulares y mantenimiento de los sistemas de detección para garantizar su funcionamiento óptimo en todo momento.
- **Actualización tecnológica:** Mantenerse al día con las últimas tecnologías de detección de intrusos para asegurar que los sistemas sean efectivos y puedan adaptarse a las amenazas emergentes.

CAPACITACIÓN DEL PERSONAL

La capacitación del personal es un pilar fundamental en la gestión de la seguridad en casinos y centros de entretenimiento. La capacitación del personal no sólo mejora la seguridad física del establecimiento, sino que también fortalece la conciencia y la capacidad de respuesta de los empleados, contribuyendo a un ambiente más seguro y protegido. Aquí se detallan los puntos clave para un programa de capacitación efectivo:

- **Concienciación de seguridad:** Iniciar la capacitación con sesiones de concientización sobre la importancia de la seguridad, los riesgos potenciales y el impacto de las acciones del personal en la seguridad general del lugar.
- **Procedimientos y políticas:** Educar al personal sobre los procedimientos operativos estándar (SOP, por sus siglas en inglés) y las políticas de seguridad específicas del establecimiento. Esto incluye procedimientos de emergencia, manejo de incidentes y respuesta a situaciones críticas.

La capacitación del personal no sólo mejora la seguridad física del establecimiento, sino que también fortalece la conciencia y la capacidad de respuesta de los empleados, contribuyendo a un ambiente más seguro y protegido

La tecnología de reconocimiento facial y biométrica brinda una capa adicional de seguridad al identificar de manera precisa y eficiente a individuos autorizados, controlar el acceso a áreas sensibles y detectar cualquier actividad sospechosa

- **Tecnología y equipos:** Capacitar al personal en el uso adecuado de la tecnología de seguridad, como sistemas de CCTV, alarmas, control de acceso, sistemas de detección de intrusos, entre otros equipos de seguridad específicos del lugar.
- **Prevención de delitos:** Enseñar técnicas para identificar y prevenir posibles delitos, incluyendo la detección de comportamientos sospechosos, gestión de multitudes, y manejo de situaciones conflictivas.
- **Manejo de conflictos:** Proporcionar capacitación en habilidades de comunicación y resolución de conflictos para lidiar con situaciones desafiantes y clientes difíciles de manera efectiva y no violenta.
- **Primeros auxilios y respuesta a emergencias:** Ofrecer entrenamiento en primeros auxilios y técnicas de respuesta a emergencias, incluyendo evacuaciones, manejo de incendios, y asistencia en situaciones médicas de urgencia.
- **Simulacros y ejercicios prácticos:** Realizar ejercicios de simulacro para poner a prueba la preparación del personal y mejorar su respuesta a situaciones reales de emergencia.
- **Evaluación y retroalimentación:** Realizar evaluaciones periódicas para medir la efectividad de la capacitación y proporcionar retroalimentación para mejorar continuamente el programa de seguridad.

COLABORACIÓN CON LAS FUERZAS DEL ORDEN

Colaborar con las fuerzas del orden es crucial para fortalecer la seguridad en casinos y centros de entretenimiento. Aquí están los aspectos esenciales para establecer una colaboración efectiva:

- **Relaciones establecidas:** Establecer y mantener relaciones sólidas con las agencias policiales locales, así como con otras fuerzas del orden relevantes, para facilitar la comunicación y la colaboración en situaciones de emergencia.
- **Compartir información:** Colaborar activamente compartiendo información relevante sobre amenazas potenciales, delitos previos o actividades sospechosas en o alrededor del establecimiento.
- **Protocolos de comunicación:** Establecer protocolos claros de comunicación y procedimientos de contacto para emergencias, asegurando canales de comunicación directa y rápida en caso de incidentes.
- **Entrenamiento conjunto:** Realizar ejercicios y entrenamientos conjuntos con las fuerzas del orden para mejorar la coordinación y la respuesta en situaciones de crisis.
- **Asistencia mutua:** Establecer un protocolo para solicitar y brindar asistencia en operaciones de seguridad, tales como patrullajes conjuntos, vigilancia en áreas comunes o coordinación en eventos masivos.
- **Participación en reuniones de seguridad:** Asistir a reuniones regulares de seguridad en la comunidad donde las fuerzas del orden y otros actores de seguridad discuten estrategias y comparten información sobre la prevención del delito.
- **Respeto a las leyes y regulaciones:** Cumplir con todas las leyes y regulaciones pertinentes en la colaboración con las fuerzas del orden, asegurando una cooperación legal y ética.
- **Evaluación y mejora continua:** Realizar revisiones periódicas de la colaboración y los protocolos establecidos para identificar áreas de mejora y fortalecer la asociación con las autoridades.

Todas estas técnicas, cuando se aplican de manera integral y coordinada, pueden ayudar a mantener la seguridad en casinos y centros de entretenimiento, protegiendo tanto a empleados como a visitantes, y minimizando riesgos asociados con actividades delictivas o situaciones de emergencia.

PROS Y CONTRAS

Ahora, desde mi observador les comparto los Pros y Contras para la protección y seguridad, para casinos y centros de entretenimiento:

Vigilancia por CCTV (Circuito Cerrado de Televisión)
Pros:
* **Detección y Prevención:** Proporciona un amplio alcance de monitoreo para detectar actividades sospechosas y prevenir delitos.
* **Registro de Evidencia:** Sirve como una valiosa herramienta de registro visual para eventos pasados, y ayuda en la investigación de incidentes.
* **Disuasión:** La presencia visible de cámaras de seguridad, puede disuadir a posibles delincuentes.
Contras:
* **Costos:** La instalación, mantenimiento y actualización de sistemas de CCTV puede ser costosa.
* **Áreas ciegas:** A pesar de su cobertura, pueden existir áreas no monitoreadas o con visión limitada.
* **Privacidad:** Existen preocupaciones sobre la invasión de la privacidad de los empleados y clientes.

Control de Acceso Biométrico
Pros:
* **Seguridad:** Proporciona un nivel de seguridad avanzado al requerir verificación biométrica, como huellas dactilares o reconocimiento facial.
* **Acceso personalizado:** Permite un control preciso sobre quién puede acceder a áreas restringidas.
* **Registro preciso:** Registra y rastrea la entrada y salida de individuos de manera precisa.
Contras:
* **Costos iniciales:** La implementación inicial, puede ser costosa debido a la compra de equipos y la instalación.
* **Falsos positivos/negativos:** En algunas circunstancias, los sistemas biométricos pueden fallar, al identificar correctamente a las personas.
* **Privacidad y preocupaciones éticas:** Similar al CCTV, hay preocupaciones sobre la privacidad y la ética en el uso de datos biométricos.

Foto: - Freepik

Personal de Seguridad Capacitado
Pros:
* **Respuesta rápida:** El personal capacitado puede responder efectivamente a emergencias y situaciones críticas.
* **Prevención:** Su presencia puede disuadir a posibles delincuentes, y prevenir incidentes.
* **Conocimiento especializado:** Puede manejar adecuadamente el equipo de seguridad y los protocolos de respuesta a emergencias.
Contras:
* **Costos continuos:** Mantener personal altamente capacitado, implica gastos constantes en entrenamiento y desarrollo.
* **Posible error humano:** A pesar de la capacitación, el personal puede cometer errores en situaciones de alto estrés.
* **Disponibilidad:** La cantidad y la disponibilidad del personal de seguridad puede ser limitada en ciertos momentos.

NOVELTY, FEASIBILITY, SPECIFICITY, IMPACT Y *WORKABILITY*

Ahora te presento un análisis utilizando los criterios de: *novelty, feasibility, specificity, impact y workability* aplicado a la Protección de Casinos y Centros de Entretenimiento:

- ***NOVELTY* (NOVEDAD):**
  - Ventajas: La introducción de tecnologías de vanguardia como reconocimiento facial, sistemas de detección avanzada y seguridad biométrica pueden ser consideradas como novedosas y de vanguardia.
  - Desafíos: Algunas tecnologías pueden estar en etapas incipientes, lo que podría presentar desafíos de implementación y adopción completa.

- ***FEASIBILITY* (VIABILIDAD):**
  - Ventajas: La viabilidad financiera de implementar estas técnicas puede ser alta, ya que la protección de activos valiosos, es esencial para la rentabilidad de los casinos y centros de entretenimiento.
  - Desafíos: Algunas tecnologías de alta gama, pueden requerir inversiones considerables en instalación, mantenimiento y capacitación.

- ***SPECIFICITY* (ESPECIFICIDAD):**
  - Ventajas: Las técnicas de protección pueden ser altamente específicas para las necesidades de seguridad de estos lugares, como la detección de fraude, el control de acceso a áreas restringidas y la vigilancia intensiva.
  - Desafíos: La adaptabilidad de estas técnicas a diferentes configuraciones y necesidades específicas de cada casino, puede requerir una personalización significativa.

UN DISEÑO AMBIENTAL ADECUADO Y UNA ILUMINACIÓN ESTRATÉGICA CONTRIBUYEN SIGNIFICATIVAMENTE A LA SEGURIDAD GENERAL DEL ENTORNO, PROPORCIONANDO VISIBILIDAD, DISUADIENDO LA ACTIVIDAD DELICTIVA Y MEJORANDO LA SENSACIÓN DE SEGURIDAD PARA EMPLEADOS Y VISITANTES

- ***IMPACT* (IMPACTO):**
  - Ventajas: La implementación exitosa de estas técnicas puede tener un impacto significativo en la reducción de robos, fraudes, y en la creación de entornos más seguros y confiables para los visitantes.
  - Desafíos: El impacto puede variar dependiendo de la capacidad de integrar estas técnicas con otros sistemas de seguridad existentes y la capacidad de adaptarse a las amenazas emergentes.

- ***WORKABILITY* (TRABAJABILIDAD):**
  - Ventajas: La aplicabilidad y la capacidad de estas técnicas para funcionar en el entorno dinámico de un casino o centro de entretenimiento pueden ser altas.
  - Desafíos: Se debe tener en cuenta la coordinación y la interoperabilidad entre diferentes sistemas de seguridad, para garantizar su funcionamiento eficaz y sin inconvenientes.

Todas las técnicas que implementemos para la seguridad y protección para casinos y centros de entretenimiento deben tener el potencial de ser innovadoras, viables y específicas para cubrir todas las necesidades, con un impacto significativo, y una aplicabilidad favorable; sin embargo, el desafío radica en su implementación integral, la adaptabilidad a diferentes entornos y la coordinación real y efectiva entre las diversas tecnologías y estrategias de seguridad.

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

Foto: - Freepik

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

Foto: - Freepik

APARICIÓN DE LA CRIMINOLOGÍA

CORPORATIVA Y LA PARTICIPACIÓN DEL CRIMINÓLOGO

En una empresa pueden cometerse muchos tipos de delitos, como, por ejemplo, delitos de cuello blanco, delitos de crimen organizado o ciberdelincuencia. Es por ello la vital importancia de un criminólogo para poder prevenirlo y también para saber cómo actuar cuando esto ocurra

MÉXICO **Wael Sarwat Hikal Carreón y Raquel Hernández López**

DESARROLLO DE LA CRIMINOLOGÍA CORPORATIVA

El término y concepto aparece por primera vez en 1984 de la mano de Jay Abanese, profesor de la Universidad de Virginia. Alude la importancia del estudio de los factores que influyen en la desviación de conductas en entidades organizacionales para plantear estrategias de control y de prevención de la criminalidad.

En México en 2008, Wael Hikal en su libro "Introducción al Estudio de la Criminología y su Metodología" desarrolla el término y concepto "Criminología Laboral" como estudio de las conductas antisociales que pueda presentar alguna persona en el desarrollo, o desde antes de realizar cierto tipo de trabajo; aspectos a observar: acoso, hostigamiento sexual, rechazo, discriminación salarial y contractual.

En 2017, Pedro Alejandro Zapata Reyna populariza el término "Criminología Empresarial" como área de la Criminología encargada de intervenir en empresas o instituciones de la iniciativa privada a través de la identificación, medición, control y prevención de los eventos delictivos.

En 2019, José Luis Prieto, difunde a la "Criminología Corporativa", refiriéndose a la especialización que tiene como propósito gestionar la seguridad integral de las organizaciones y sus integrantes a través de la identificación, medición, control y prevención de los eventos delictivos o nocivos que tiene lugar en el contexto socio-laboral.

FUNCIONES DE LA CRIMINOLOGÍA LABORAL O CORPORATIVA

La Criminología Laboral desarrollada en 2008, es la rama de la Criminología General dedicada al estudio de las conductas antisociales que pueda presentar alguna persona en el desarrollo o desde antes de realizar cierto tipo de trabajo. Importante aspecto a observar es también el de la violencia, en el medio laboral tiene expresiones diversas: acoso, hostigamiento sexual, rechazo, discriminación salarial y contractual, así como relegación a tareas subordinadas y de servicio, entre otras.

Esta Criminología se apoyará de la entrevista laboral, en ella podemos apreciar la sociabilidad, la facilidad de palabra, correcta vestimenta e higiene, educación, adaptación, autoconcepto y claridad de ideas de los aspirantes a un determinado puesto. Tiene por objetivo estudiar a la persona e identificar ciertos problemas internos (por medio de observar su conducta se conocerá si tiene tendencias antisociales) y de su ambiente que puedan llevarlo a cometer alguna conducta antisocial (habrá que vigilar al trabajador).

No sólo se estudiarán a los que tengan condiciones pobres en sus hogares, sino que también se estu-

diarán a los sujetos inteligentes y con buenas posibilidades, ya que existe una gran variedad de conductas que pueden realizar en contra de la institución, desde fraudes, robos, acosos, etcétera; aunque cualquiera de estos delitos se presentan en todo tipo de circunstancias económicas.

La Criminología Laboral deberá utilizar distintas técnicas para detectar problemas:

- **Detector de mentiras.** Se ha determinado que los individuos tienen cambios fisiológicos al momento de estar ante una situación que los pone al descubierto sobre algo. Aquí el criminólogo hará uso de sus conocimientos para aplicar la prueba de polígrafo, la entrevista y el interrogatorio.
- **Exámenes médicos.** Permiten conocer con exactitud si un empleado puede ser susceptible o no a uno o más tipos de enfermedades o sustancias tóxicas.
- **Historia personal.** Se refiere al ámbito familiar, económico, de salud, educación, sociocultural, condiciones de la colonia, de la vivienda, etcétera.

Además se estudian las condiciones de estrés laboral, ya que el individuo se enfrenta a problemas como: temperatura, humedad, ruido y vibraciones, iluminación y fuerzas de aceleración y desequilibrio, etcétera.

El criminólogo tendrá que estudiar cómo estos factores influyen en el comportamiento de los trabajadores: si los estresa, si los pone violentos y el efecto que éstos tienen para dar lugar a las conductas antisociales.

Esto es fácil de observar en distintos trabajos; por ejemplo: basta con subirse a un camión a las 07:00 a.m. o a las 06:00 p.m., para poder ver cómo los conductores de diferentes vehículos están estresados y se genera violencia que da lugar a colisiones, riñas, etcétera.

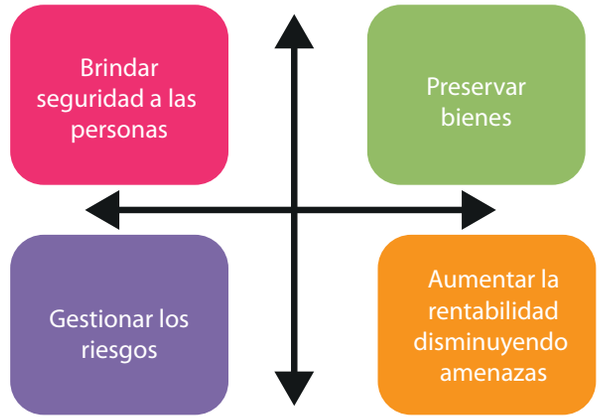
ENFOQUES DE LA CRIMINOLOGÍA EN EL ÁMBITO LABORAL Y ACTIVIDADES DEL CRIMINÓLOGO

Tiene como enfoque aquellas acciones o comportamientos manifestados que tengan como fin, causar un daño psicológico, físico, económico o sexual en el entorno laboral. Para lo anterior, el criminólogo tendrá como medios de trabajo:

- Reclutamiento y selección de personal, clima laboral.
- Mediación de conflictos (el criminólogo como mediador).
- Seguridad: establecimiento de medidas preventivas que reduzcan las posibilidades de un acto delictivo para proteger a la empresa.
- Análisis y evaluación de riesgos externos e internos.

Se pretende prevenir los delitos corporativos, que son cometidos por la propia organización o por una persona (colaboradores, directivos, administrativos, entre otros) que trabaje en dicha entidad. Las actividades básicas se concretan en la investigación de: robo interno/externo, fraudes, servicios financieros, robo a caja de seguridad, a valores, bienes, acciones preventivas de secuestro, riesgo a personal, a instalaciones, detección de vulnerabilidades, etcétera.

Figura 1. Objetivos de la Criminología Corporativa.



Nota: Elaboración propia

El criminólogo diseñará el plan de trabajo el cual consiste en la elaboración de las políticas preventivas, capacitación preventiva al equipo de trabajo, gestión con las autoridades de justicia y seguridad pública, protección civil, y las investigaciones criminológicas.

CONCLUSIONES

El ámbito empresarial, laboral o corporativo se ha convertido en un área de desarrollo profesional para los egresados de Criminología y Criminalística. Por lo anterior, la importancia de conocer algunos detalles de la aparición histórica de esta Criminología especializada en lo laboral, y principalmente las funciones, enfoques, rutas de trabajo, acciones y demás actividades. Las empresas tienen necesidad de prevenir sus riesgos para aminorar pérdidas, y el criminólogo-criminalista es el profesional idóneo para atender las vulnerabilidades en la infraestructura de la empresa, así como en el personal y las dinámicas que en esta ocurren. ■

Referencias:

- *Hikal Carreón, W.S. (2023). La mediación de conflictos como área de oportunidad laboral para el criminólogo desde la Criminología de la Consejería Social. Revista de Derecho de la Universidad Nacional del Altiplano de Puno, 8 (1), 13-22. http://revistas.unap.edu.pe/rd/index.php/rd/article/view/221*
- *Hikal, W. (2009). Introducción al Estudio de la Criminología y a su Metodología. Porrúa.*

Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León y doctor en Educación por la Universidad Autónoma de Nuevo León, México. *Más sobre el autor:*

Raquel Hernández López, Centro de Control y Protección Patrimonial de Oxxo FEMSA y Licenciada en Criminología por la Universidad Autónoma de Tlaxcala. *Más sobre la autora:*

Foto: - Freepik

RIESGOS CORPORATIVOS

Para lograr que toda la organización y stake holders tengan clara la idea de la conciencia operacional, se debe trabajar arduamente con todos, de forma de que estén todos involucrados en un proceso continuo y responsable, con la sencilla razón de que el resultado debe ser óptimo, continuo, competitivo y sostenible

PERÚ

Herbert Calderón

Todos las empresas privadas, estatales, se encuentran expuestas a dos tipos de riesgos, el primero de ellos es el relacionado a la operación misma y como consecuencia del tipo de operación, ubicación geográfica, entorno social, delincuencia, entorno de desastres naturales, tipo de personas o empleados, entorno político, etc. Sin embargo existe adicionalmente el riesgo denominado funcional, que es el relacionado propiamente con el aspecto de la función en cuanto al alcance gerencial con la organización, conciencia operacional e involucramiento de la organización misma.

Muy comúnmente evaluamos los riesgos tan solamente operativos, pero muchas veces la ausencia de apoyo, el involucramiento o conciencia, ocasionan que los riesgos operativos se incrementen, agraven o tal vez se mitiguen.

Particularmente pienso que el 90% de los riesgos provienen del riesgo funcional.

RIESGO CORPORATIVO = (RIESGO OPERACIONAL) (RIESGO FUNCIONAL) (VALOR DEL ACTIVO)

RIESGOS OPERATIVOS

El riesgo operativo es el riesgo existente en toda organización como consecuencia de su actividad en el día a día. Esta motivado por factores externos e internos, y se traduce en pérdidas económicas.

En el ámbito económico, se denomina riesgo operativo a la posibilidad que exista de tener pérdidas financieras motivadas por el entorno de una organización.

En ese sentido, este tipo de riesgo se relaciona tanto con el comportamiento de los procesos propios de la empresa como con la coyuntura en la que se desenvuelva.

Este tipo de riesgo cuenta con la condición de inevitable, ya que es muy frecuente su aparición en todas las empresas. Esto responde a la propia condición humana, que precisa de periodos de adaptación y aprendizaje.

Factores causantes de riesgo operativo:

Existen distintas causas principales a la hora de estudiar el origen del riesgo operativo. Estas pueden clasificarse del siguiente modo:

- **Origen interno:** Motivado por los riesgos inherentes a la misma organización que se estudie.
- **Origen externo:** Toda organización es susceptible de ser afectada por los comportamientos propios del contexto socioeconómico en el que opere.
- **Recursos humanos:** Al contar con la participación y el trabajo de personas, las empresas están condicionadas por las acciones y el desempeño de las mismas.
- **Relevancia tecnológica:** En prácticamente la totalidad de negocios, existe una acentuada relevancia de la mecánica o la tecnología. Especialmente en la era digital y el mundo globalizado.

A raíz de estos grupos, es posible estudiar, en la cotidianidad económica y empresarial, la aparición de multitud de casos de riesgo operativo.

Principales ejemplos de riesgo operativo:

En el día a día de las sociedades mercantiles, existen ejemplos explicativos sobre este concepto. De este modo, es posible visualizar riesgos con carácter operativo en casos como los siguientes:

- **Errores de naturaleza humana:** La mala conducta de los trabajadores, o la acometida de errores en su desempeño laboral, producen, a la larga, pérdidas para su compañía.
- **Fallas tecnológicas y mecánicas:** El mal funcionamiento, la rotura o la llegada de la obsolescencia de dicha tecnología supone importantes problemas de riesgo operativo.
- **Diseño productivo ineficiente:** El diseño de malas estrategias empresariales, la aplicación ineficiente de los recursos, lleva a una situación de riesgo operacional.
- **Efectos externos:** Los vaivenes motivados por los ciclos económicos, o fenómenos como la inflación, así como la propia aparición de nuevos competidores pueden agravar los problemas financieros de una sociedad.

Foto: - Freepik

RIESGOS FUNCIONALES

Son los riesgos referidos a la gestión, el apoyo de la organización hacia los responsables de seguridad, así como de la percepción, el grado de responsabilidad percibida por todos los colaboradores.

Este viene a ser uno de los aspectos mas relevantes en el proceso, dado que de no tener resultados positivos en las varibales de análisis, es muy probable que impacte a los riesgos operacionales, en la forma de:

a) Eludir responsabilidades.
b) Culpar y no asumir faltas propias.
c) No liderar en su proceso sobre la protección de su patrimonio.
d) No reaccionar correctamente ante crisis operacionales como: incendios, desastres naturales, fraudes, sabotajes, extorsiones, acoso, huelgas, etc.
e) Ser cómplice o autor de un ilícito.
f) No apoyar y obstaculizar la gestión del proceso de protección.
g) Maltratar y genera un clima laboral inadecuado.
h) Seleccionar a personas inadecuadas para desarrollar gestión en el proceso.
i) No tomar acciones concretas y de acuerdo a recomendaciones para la protección del patrimonio.
j) Ausencia de apoyo y presupuestos para el proceso de poteccion.
k) Inversiones y gastos del proceso de protección no sale de las áreas de operación.
l) Ocultar, no informar, participar en ilícitos.
m) Desestimar, obstaculizar proyectos relacionados con la mejora de la protección, equipos de respuesta a contigencias, planes de continuidad del negocio.
n) Obstaculizar, postergar, aminorar, maquillar, los hallazgos o el proceso de las auditorías internas.

Variables para medir los riesgos funcionales:

a) Apoyo gerencial.
b) Conciencia operacional.
c) Involucramiento dueños de los procesos.

a. Apoyo gerencial

La supervivencia de la organización está basado en el proceso de continuidad del negocio, en el cual participa activamente toda la organización en cuanto al involucramiento y acción en este proceso.

En ello es importante el grado de madurez que tiene a organización con los riesgos, así como su respeto a los bienes valiosos para la operación relacionado con la información, personas, estructuras.

La protección de los bienes patrimoniales está en el campo de la prevención de pérdidas y su entorno seguro. Para el éxito de esta consideración es vital el apoyo incondicional de los niveles directivos y/o gerenciales de una organización. Es la Gerencia la que aporta los recursos y establece las directrices (aspecto tan importante como el anterior) para la ejecución e implementación de la gestión.

b. La conciencia y el liderazgo operacionales

El día de hoy las organizaciones operan de forma que tienen sumamente clara la necesidad de adoptar normas generales para impulsar su crecimiento, reducir el desperdicio, protegerse contra el riesgo, ser más sustentables, así como desarrollar una producción debidamente preparada para la su continuidad.

Estas normas les permiten a las empresas ahorrar tiempo y esfuerzo, así como el obtener el mejor conocimiento de empresas del mundo. Esto significa que no necesitan desperdiciar sus esfuerzos en lugares incorrectos.

En forma práctica estos estándares, le permitirán a las organizaciones la libertad de concentrar sus esfuerzos sobre lo que hacen mejor, fabricar brillantes productos nuevos, generando poderosas ideas creativas, proporcionando un gran servicio así como operar ante adversidades.

Sobre todo, con aquellas organizaciones que tienen representatividad internacional, los productos o servicios demuestran calidad, compatibilidad, consistencia, sostenibilidad y ayuda a crear un lenguaje común sobre el cual comercializar.

Las normas son particularmente importantes para las empresas que están a la vista del público, donde la reputación puede sufrir un daño catastrófico como resultado de un asunto ambiental o un problema que dañe a los clientes, así como nos ayudan a reducir la burocracia y las barreras al comercio. Así es como podemos estar seguros de que las normas de hecho ayuden a las organizaciones, más que frenarlas.

Las organizaciones cuentan normalmente con sistemas de control de Gestión de Calidad ISO 9001, Gestión ambiental ISO 14001,


Foto: - Freepik

ISO 45001 Gestión de Seguridad y Salud Ocupacional, Seguridad de la Información ISO/IEC 27001, Gestión de Energía ISO 50001, Gestión de la Continuidad del Negocio ISO 22301, todas ellas están sujetas a una serie de regulaciones internacionales tipo normas ISO.

Sin embargo al llevarse a cabo todas las actividades productivas, con las consideraciones anteriores se requiere que se lleven con responsabilidad con una buena conducción del equipo debidamente orientado hacia los valores y los objetivos trazados, pero erróneamente aún prevalece el concepto des integrado de los principios anteriores, lo correcto debe ser que todos los trabajadores deben caminar hacia esos principios que la organización está estableciendo: calidad, seguridad, medio ambiente, continuidad del negocio, etc.

Para lograr que toda la organización y *stake holders* tengan clara la idea de la conciencia operacional, se debe trabajar arduamente con todos, de forma de que estén todos involucrados en un proceso continuo y responsable, con la sencilla razón de que el resultado debe ser óptimo, continuo, competitivo y sostenible.

El éxito de incorporar a toda la organización a la práctica de los principios anteriores es con un sentido de profesar el ejemplo, la responsabilidad por imitación, ello es denominado comúnmente como el liderazgo operacional.

Finalmente, el concepto operacional es el máximo valor a la sostenibilidad de nuestra operación, y para mantener esta operación debemos actuar con todos estos principios de responsabilidad y liderazgo comentados líneas arriba.

c. Involucramiento de dueños en los procesos

Todas las empresas, compañías y organizaciones cuentan con el valioso elemento que son las personas que constituyen el equipo humano y profesional. Los medios técnicos, informáticos y las infraestructuras son importantes, lo cierto es que son las personas las que llevan a cabo los avances, los logros y los errores de las empresas para las que trabajan.

Son ellas las que, en última instancia, tienen que tomar las decisiones, lo que las convierte en responsables de la buena o mala marcha de la empresa. Por lo tanto, no es exagerado afirmar que el bien más apreciado de las empresas es el talento de las personas. Y el contexto actual, globalizado a nivel de economía, finanzas, mercado y tremendamente competitivo no ha hecho más que reforzar el valor de las personas, convirtiéndolas en el elemento que, a la hora de la verdad, marca las diferencias.

Más aún las personas son parte del equipo que enfrenta las contingencias y son participantes activos de la prevención de pérdidas. Sin embargo el aspecto personal o psicosocial como tener frustraciones, resentimientos, presión, acoso, ausencia de motivación, inteligencia emocional, motivación, etc.

Cuando, construimos un sistema de gestión en prevención de pérdidas, riesgos, continuidad del negocio, seguridad física, necesitamos diseñar un plan conjuntamente con toda la organización, dado que las personas de todas las áreas deben participar activamente en cuanto al conocimiento de los procesos, activos críticos, recursos apropiado, respuesta a eventos críticos, en general todo lo relacionado con la prevención y respuestas de eventos no deseados.

RIESGO FUNCIONAL = 1- (APOYO GERENCIAL) (CONCIENCIA OPERACIONAL) (INVOLUCRAMIENTO ORGANIZACIONAL)

La madurez de la organización la vamos a observar por las siguientes consideraciones como:

a) El grado de cultura a los riesgos, que posee la organización.

b) Los resultados obtenidos en el control de pérdidas y las tendencias del riesgo.

c) Capacidad de continuidad del negocio ante crisis.

Lograr los indicadores a un nivel aceptable, definitivamente definen la madurez de la organización. El no lograrlos arrastra a toda la empresa a grandes pérdidas y responsabilidades de acuerdo a los niveles funcionales. Nuestra gestión es preservar el patrimonio y sobre todo la operación productiva. En ese sentido los resultados dependen grandemente del apoyo e involucramiento gerencial respecto de la madurez, específicamente con la cultura operacional sobre el manejo de riesgos y su mitigación. ■

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

Ética Integral

Lo que dicen **nuestros clientes:**

*"Gracias a una denuncia **desmantelamos una red de robo** de material por más de **USD$26,000** en unas cuantas semanas."*

*"**Descubrimos casos de manipulación** de turnos y tiempos extras."*

*"Mejoró el clima laboral, **disminuyó la rotación** y ya **cumplimos con la NOM035** que exige tener una línea de denuncia."*

NUESTROS SERVICIOS

CANALES DE DENUNCIA

COMPLIANCE

THIRD PARTY RISK

¡DETRÁS DE CADA DENUNCIA,
UNA OPORTUNIDAD DE MEJORAR!

55 2855 5121
contacto@eticaintegral.com
www.eticaintegral.com

NUESTROS LOGROS

+350

Denuncias procesadas

+12

Clientes

3

Países en que operamos

CUMPLIMOS NUESTRO PRIMER AÑO DE OPERACIONES

Foto: - Freepik

PANORAMA DE SEGURIDAD PARA MÉXICO EN 2024

MÉXICO

Antonio Venegas / *Staff* Seguridad en América

"Este es el sexenio más violento de la historia contemporánea de México", Carlos Seoane

Durante la primera Reunión Mensual de este año de ASIS Capítulo México, se presentó Carlos Seoane Noroña, socio director de Seoane Consulting Group, con la conferencia titulada "Panorama de Seguridad para México en 2024", en la que habló de la estructura de control establecida por el unipartidismo en México antes del año 2000, lo cual presentó una estructura donde hubo diferentes mandos, diferentes partidos políticos y grupos de interés, donde las estructuras se reacomodaron en un nuevo esquema de violencia.

A finales del siglo pasado y principios del siglo presente, múltiples cárteles comenzaron un proceso de expansión que se vio reflejado en actos extremos de violencia, en respuesta, otras organizaciones criminales actuaron de la misma manera, lo que estableció un nuevo código genético en dichas organizaciones.

Carlos explicó que cuando una organización delictiva se divide da inicio a nuevas organizaciones como las que se formaron en el periodo de 2007 a 2011, a estos grupos se les denominan pandillas o mafias, las cuales tienen un código de violencia implementando de los cárteles de los que se derivan, ejerciendo violencia en sectores en los cuales no se había visto. Estas pandillas no poseen el poder de realizar grandes actividades como los cárteles mayores, sin embargo, desempeñan actividades delictivas haciendo uso de violencia en otras áreas.

Foto: - Freepik

Según datos de la Iniciativa Global en contra del Crimen Organizado Trasnacional, la cual evalúa 15 categorías, México se encuentra en los primeros lugares en varios crímenes

Foto: - Freepik

Las Fuerzas Armadas como la Guardia Nacional no cubren ni cubrirán las tareas que son de la policía civil, entrenamientos diferentes dan funciones diferentes

HABLEMOS DE CIFRAS

Los cárteles, o la delincuencia organizada, tienen una capacidad ociosa instalada, no sólo dirigida al tráfico de drogas, sino que ocupan sus recursos en otras actividades como el robo de mercancías. De acuerdo con datos actualizados al 16 de enero de este año, Carlos presentó estadísticas de homicidios por año en cada sexenio, ejemplificando con el sexenio de Felipe Calderón, que desde entonces ha presentado una tendencia al alta, misma que se ha reflejado en el sexenio actual de Andrés Manuel López Obrador. El peor año en el que se sufrió de homicidios fue en 2020 donde, en promedio, cada 14.3 minutos, alguien perdió la vida de manera violenta. En 2023 se presentó una diferencia de en promedio tres minutos, en comparación, en el periodo de Vicente Fox, el promedio era de 52 minutos.

Asimismo, presentó una gráfica con los datos de cada estado en este tema, teniendo a Yucatán en el último puesto, y al Estado de México como uno de los principales, esto derivado al punto geográfico que representa al colindar con ocho estados y su enorme población. Cada estado representa actividades diferentes. Se establece que para el final del sexenio se terminará con un total de más de 200 mil homicidios.

Con una gráfica presentada por el gobierno, Carlos analizó la cantidad de homicidios por día y mes, la cual no presenta tendencias observables. Las mejorías no son tan perceptibles, pero existen. Al paso del tiempo sí ha habido reducciones pequeñas pero la situación del país sigue complicada.

Compartió datos de la Iniciativa Global en contra del Crimen Organizado Trasnacional, la cual evalúa 15 categorías y distintos países, México esta en el primer lugar cuando se suman las 15 categorías. De igual forma señaló los cambios en la estructura del control y del poder en múltiples estados derivado del cambio de administración en los estados. Se puede observar el escalamiento en violencia homicida cuando hay un cambio en la estructura política.

Para junio de 2024, más de 20 mil puestos políticos serán renovados, entre gobernaturas estatales, senadoras, entre otros, y ya hay cinco precandidatos asesinados. Carlos ve estas acciones como el crimen votando, desechando a candidatos que no convengan con las intenciones de los grupos. Este sexenio ya es conocido como el más violento de la historia contemporánea; si se logra mantener una tasa anual de descenso del 10% en el delito de homicidio doloso, para 2030 se alcanzarán niveles de violencia como los establecidos en el sexenio de Felipe Calderón.

Carlos consideró que se pueden hacer mejor las cosas, sin embargo, desafortunadamente no existe la estructura para lograrlo. Las Fuerzas Armadas como la Guardia Nacional no cubren ni cubrirán las tareas que son de la policía civil, entrenamientos diferentes dan funciones diferentes. No se ha desmantelado ni una sola organización criminal de gran envergadura en esta administración, ya que, de acuerdo con el actual presidente, "los cárteles le fueron heredados". No va haber ajustes en temas de seguridad pública en lo que resta del sexenio.

Se estima que para las próximas elecciones, quien reciba la presidencia recibirá tendencias similares a las establecidas. Carlos compartió de manera breve su columna de predicciones para el 2024. Algo que destacó es que el sector de la seguridad privada tendrá mucho trabajo, algo que no necesariamente sea visto de manera positiva, pero que brindará la oportunidad de implementar el sector y ver de qué manera puede evolucionar para adaptarse a estos cambios. ■

Carlos Seoane Noroña, socio director de Seoane Consulting Group Risk Management

Foto: - Freepik

LA SEGURIDAD: TEMA CENTRAL DE LAS CAMPAÑAS POLÍTICAS DEL 2024 EN MÉXICO

Foto: - Freepik

"La seguridad real se encuentra sólo en la legislación y en la justicia", Harry Truman

MÉXICO | **Mercedes Escudero Carmona**

En el 2024, votaremos en México por 20 mil 375 candidatos a cargos de elección popular, 629 cargos de elección federal y 19,746 de elecciones locales, con un gasto autorizado en el Presupuesto de Egresos de la Federación (PEF) de 3 mil 370 millones 991 mil 486 (tres mil trescientos setenta millones novecientos noventa y mil cuatrocientos ochenta y seis pesos).

Las crisis en materia de seguridad y prevención del delito son los retos más importantes para los candidatos a estos puestos de elección popular que van desde la Presidencia, gobernadores, legisladores federales y diputados locales; así como presidentes municipales y regidores.

De no cambiar las estrategias se seguirá fortaleciendo la cultura de violencia y el incremento de impunidad en la procuración de justicia. ¿Qué se necesita? un plan de Seguridad Humana que instaure una Cultura de Paz que promueva valores, actitudes y comportamientos que rechacen la violencia, ayuden a prevenir y transformen de manera pacífica los conflictos. Asimismo, los candidatos ganadores al convertirse en gobierno deberán desarrollar y optimizar las políticas públicas para que provean el bienestar de las personas con igualdad y se determinen presupuestos equitativos que aseguren la instauración de: la seguridad educativa, social y laboral, así como el fortalecimiento de las instituciones que brindan atención social, psicosocial y jurídica.

Lo anterior será posible, mediante el desarrollo de empatía, reconocimiento de las diferencias, el diálogo, la escucha activa, la cooperación y la comunicación, para hacer frente a la realidad social, violenta e insegura que se vive en México y para ello, se necesita de los partidos políticos.

PARTICIPACIÓN ACTIVA

Los partidos políticos, sus candidatos y candidatas, se han olvidado que son organismos sociales y deben promover una educación cívica, política y de participación, independientemente de las épocas de campaña para elecciones. Con ello, estarían apoyando a la crea-

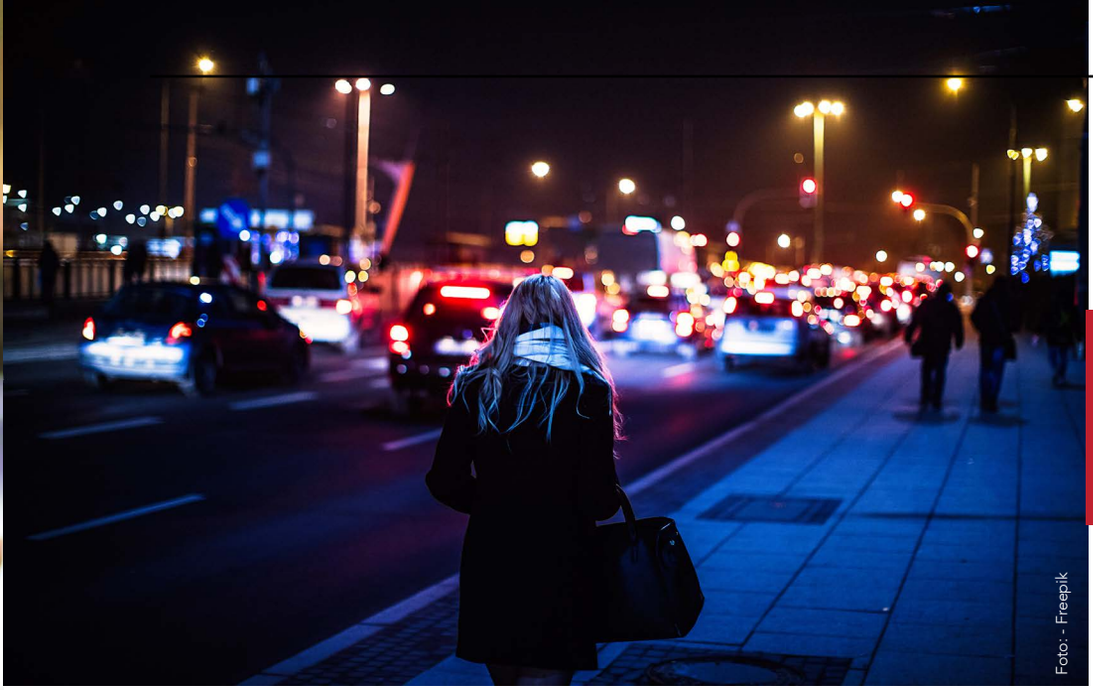


Foto: - Freepik

De no cambiar las estrategias se seguirá fortaleciendo la cultura de violencia y el incremento de impunidad en la procuración de justicia

ción de espacios de paz: donde el encuentro de la comunidad genere un sentido de identidad y pertenencia; que la producción de seguridad tenga una visión holística que garantice los derechos de las personas en sus dimensiones humanas: ambiental, política, económica, personal, salud, comunitaria y alimentaria.

Se necesita de la formación de capacidades y competencias ciudadanas para la paz: con la finalidad de promover la participación activa de las personas para su construcción colectiva. Sólo lo lograremos mediante un modelo de educación social, comunitaria con equidad y respeto a las leyes, que nos permita la toma consciente de decisiones y una convivencia pacífica. En resumen, debemos desarrollar e instaurar un modelo de Educación para la paz, mediante el cual se encaucen las actividades para lograr la consecución de resultados útiles a la sociedad.

Las propuestas y estrategias para la Seguridad de cada colonia, barrio, municipio, ciudad y entidad federativa de México deben tener como eje central la construcción de paz. Esto ayudará a promover el respeto, defender la vida y la dignidad humana. Asimismo, apoyará para la formación de ciudadanos críticos, con criterio, poder de decisión y capaces de participar en la construcción de una convivencia democrática, basada en el respeto de los Derechos Humanos.

¿Por qué empezar desde la oferta política de campaña y consolidar nuevas estrategias en las políticas públicas gubernamentales? Porque entonces se estará estableciendo un modelo de seguridad humana que se centra en la protección y el empoderamiento de los grupos sociales más vulnerables. Lo que significa, creación de políticas públicas, compromisos sociales y económicos con esfuerzos coordinados de los tres niveles de gobierno y metas concretas, que sean evaluadas con base en acciones que limiten las amenazas y mejoren el bienestar de la sociedad. ■

Se necesita de la formación de capacidades y competencias ciudadanas para la paz: con la finalidad de promover la participación activa de las personas para su construcción colectiva


Foto: - Freepik

Mercedes Escudero Carmona,
presidente de CPTED México
ICA Chapter. *Más sobre la autora:*

¿QUÉ SE PUEDE HACER PARA LOCALIZAR A PERSONAS DESAPARECIDAS?

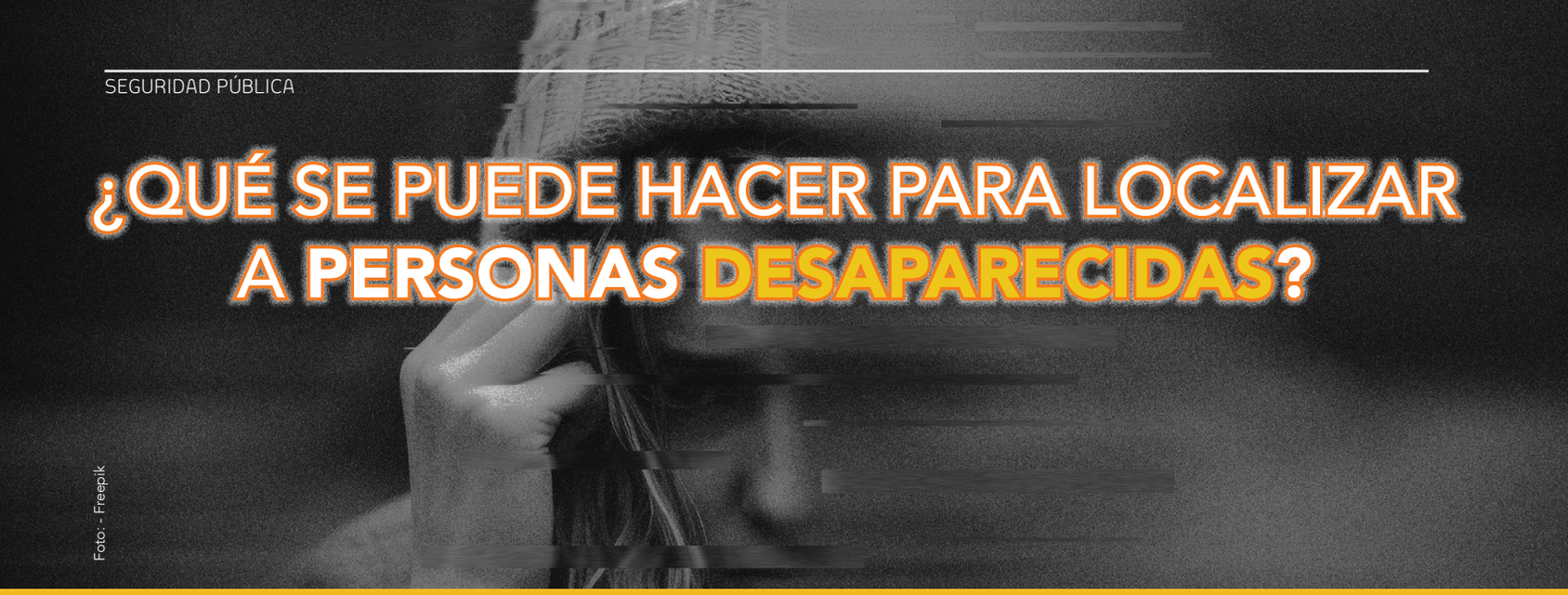


Foto: - Freepik

Desde el minuto uno empieza la búsqueda y a partir de las 72 horas la persona pasa de un estatus de desaparecida a no localizada

MÉXICO

Ricardo Nava Rueda

Hace 21 años presenté ante la Procuraduría General de la República (PGR) un proyecto de banco de datos para localizar a personas desaparecidas, hoy en día considero que se pueden retomar algunos puntos. Creo que se puede hacer un censo a través del INEGI (Instituto Nacional de Estadística y Geografía), para retomar caso por caso en toda la república mexicana, hasta lograr una exactitud y entregar este censo a la Comisión Nacional de Búsqueda (CNB).

Se deben separar los casos: robos, ausencias, voluntarias, coaccionadas e involuntarias y "levantones", migrantes, entre otros. Crear grupos especiales para cada tipo de búsqueda, como ejemplo, un médico general se puede especializar como geriatra, pediatra, gastroenterólogo, etcétera, así quienes harían la labor de investigación y búsqueda.

Regresando al ejemplo, un abogado puede apoyar e investigar en la búsqueda de menores sustraídos por el padre o la madre, así cada grupo se deberá enfocar a cada tipo de búsqueda y localización.

EL PAPEL DE LA BIOMETRÍA

También se puede hoy en día a través de la biometría y buscar en la calle a personas desaparecidas se presuma que ahí se encuentran, se calcula que en la Ciudad de México hay más de siete mil personas en esa situación y de esas muchas están como indigentes, ¿cuántas habrá en toda la república mexicana?

Buscar y regular a los grupos de Alcohólicos Anónimos, ya hay personas que son ingresadas, la mayoría contra su voluntad "anexado" como se dice coloquialmente, así como otros "centros de rehabilitación", estos grupos no reportan a alguna autoridad quienes llegaron ni quienes salen, menos en las condiciones entraron, que normalmente es contra su voluntad.

De igual manera se debe buscar en reclusorios, ahí puede haber personas con otra identidad, ya sea que no dan su nombre real para no crear antecedentes penales u otras circunstancias.

También la búsqueda en hospitales psiquiátricos, albergues y otros lugares donde se presuma que pueden estar. Con un nuevo censo puede llegar a tener mejor una cifra aproximada o exacta y aprovechar para saber el lugar, circunstancias y algunos datos más precisos, en pocas palabras, hacer un mapa y esto puede llegar a ser importante para prevenir.

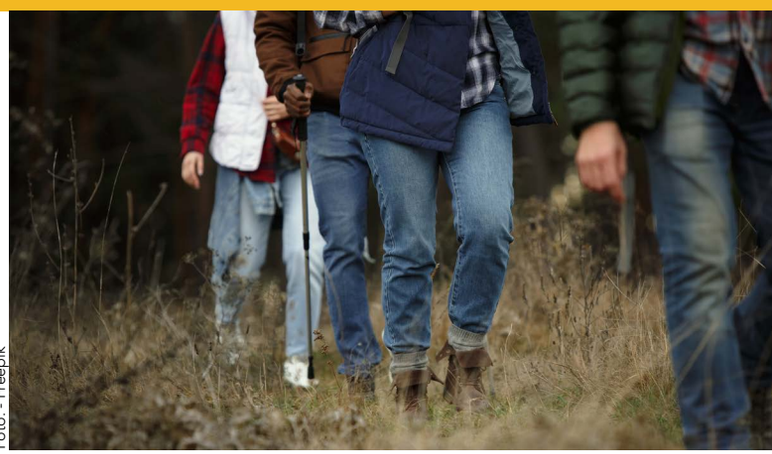


Foto: - Freepik

De esta manera a través del censo se puede saber si una persona desaparecida está reportada en varios lados y se puede pensar que son varias personas y es la misma, como ejemplo, puede tener una ficha de búsqueda local (municipio), otra estatal por la Fiscalías Especializadas en Búsqueda de Personas Desaparecidas, las Comisiones de Búsqueda Locales, la Comisión Nacional de Búsqueda, asociaciones de búsqueda, televisoras, es decir que se puede pensar que son cinco personas y es la misma; así en la temporalidad , el año que fue, como ejemplo: 1965, 1968, 1971 o reciente, también reitero que deberán ser grupos específicos para cada tipo de búsqueda, "sin minimizar o desestimar un sólo caso", mucho menos "revictimizar" sea como haya sido el caso. ■

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:*

AS3 DRIVER TRAINING

PRÓXIMOS CURSOS 2024

LOS CURSOS DE MANEJO EVASIVO Y DEFENSIVO MÁS AVANZADOS DEL MUNDO

HABILIDADES AVANZADAS DE MANEJO Y PREVENCIÓN DE EMBOSCADAS

MARZO 29 Y 30 / MAYO 24 Y 25 / JULIO 19 Y 20

MANEJO EVASIVO PARA EJECUTIVOS Y FAMILIAS

ABRIL 6 / JUNIO 15

MANEJO BÁSICO Y SEGURIDAD

FEBRERO 3 / ABRIL 5 / JUNIO 14

MANEJO BLINDADOS

FEBRERO 3 / ABRIL 5 / JUNIO 14

ÚNICO CURSO CUYOS RESULTADOS SON MEDIDOS POR COMPUTADORA EN TIEMPO REAL.

t +52-55-1085-7264 wa +52-55-4181-8373 contacto@as3.mx https://as3.mx

Privada de Av. México I PA, Col. San Pedro, Cuajimalpa, CDMX 05030

LA SEGURIDAD GLOBAL Y LAS INFRAESTRUCTURAS CRÍTICAS

Nuevos retos y desafíos a los que se ha de enfrentar la Seguridad Global. La globalización viene marcando el ritmo sobre las capacidades de los Estados y de la comunidad y sus infraestructuras, que viven este proceso con un aumento de la inseguridad

Foto: - Freepik

ESPAÑA

Manuel Sánchez Gómez-Merelo

Actualmente, los riesgos, las amenazas y las vulnerabilidades se presentan con muchas dimensiones y formas, derivadas de la inestabilidad geopolítica, la delincuencia y terrorismo, las catástrofes naturales y, más recientemente, las pandemias mundiales y la guerra en Ucrania y el conflicto entre Israel y la Franja de Gaza.

Hemos de estudiar los grandes cambios y tendencias que vivimos, diferenciando los riesgos económicos, políticos y de seguridad que nos acechan, para diseñar un nuevo escenario de presente y futuro en el que un modelo de gobernanza global de seguridad sea capaz de responder a los nuevos retos y exigencias de prevención y protección.

La seguridad se ha de entender, portanto, como un proceso global, integral e integrado, constituido por todos los elementos técnicos, materiales, humanos y organizativos relacionados con el sistema y su funcionamiento.

INFRAESTRUCTURAS CRÍTICAS Y ESTRATÉGICAS

Como definición general previa, se entienden como Infraestructuras críticas y estratégicas: "Aquellas instalaciones, redes, servicios y equipos físicos y de tecnologías sobre las que descansa el funcionamiento de los servicios esenciales y cuya interrupción o destrucción produciría un impacto mayor en la salud, la seguridad o el bienestar económico y social de los ciudadanos o en el eficaz funcionamiento de la Administración del Estado".

Al objeto de alcanzar un adecuado grado de protección en las instalaciones estratégicas clasificadas como infraestructuras críticas, frente a los riesgos o amenazas de sucesos o actos ilícitos deliberados que afecten a la protección del sistema, la Secretaría de Seguridad debe aprobar las revisiones de los Planes de Protección, competencia atribuida al Estado de la Nación.

SEGURIDAD GLOBAL

La seguridad global es uno de los pilares fundamentales sobre los que se deben apoyar las organizaciones, y ha de entenderse como un objetivo integral e integrado que tiene como finalidad la protección de personas y bienes o activos, además de servir para proteger intereses y objetivos estratégicos o de funcionamiento esencial.

El contexto en el que se está operando, y la importancia que está asumiendo y asumirá la seguridad global, demandan nuevos tipos de análisis y conocimiento multidisciplinar de las soluciones a aplicar.

Hay que tener en cuenta que el concepto de seguridad global es especialmente importante en el ámbito de la Protección de las Infraestructuras Críticas (PIC). Para ello, se ha de establecer una Política General de Seguridad Global donde han de tenerse en cuenta los aspectos fundamentales, como: la protección de los servicios esenciales; la gestión estratégica de la seguridad alineada con la política de riesgos; la estructura organizativa y de responsabilidades en materia de seguridad integral; la responsabilidad, compromiso y participación de todo el personal; la formación especializada y concienciación de los recursos humanos adscritos a la prevención y protección; el desarrollo y gestión de capacidades para la prevención, detección, protección, respuesta, resiliencia y recuperación; la colaboración con las Fuerzas y Cuerpos de Seguridad (Policías y Ejército); el cumplimiento normativo y aplicación de buenas prácticas; y la mejora continua de los procesos de seguridad implementados.

La prevención en el sistema PIC ante ataques deliberados es la columna vertebral sobre la que se sustenta el entramado de los distintos planes de los que podemos denominar Operadores Críticos que de-

ben elaborar para garantizar la seguridad de las infraestructuras. Así, se priorizará el impacto sobre la probabilidad, asegurando que cualquier infraestructura se encuentre prevenida ante un ataque deliberado, independientemente de la probabilidad que tenga de sufrirlo.

Por ello, los Planes de Seguridad del Operador (PSO) y los Planes de Protección Específicos (PPE), coordinados por la Secretaría de Seguridad e inspeccionados por las Fuerzas y Cuerpos de Seguridad, que igualmente cooperan en la elaboración y valoración de Planes Estratégicos Sectoriales y Planes de Apoyo Operativo, constituyen el elemento esencial de prevención sobre los riesgos y amenazas.

INFRAESTRUCTURAS CRÍTICAS Y SEGURIDAD GLOBAL

Sólo una seguridad global, integral e integrada, garantiza una protección eficiente frente a amenazas globales y, para ello, hemos de redefinir las políticas de seguridad, crear una nueva cultura de seguridad integral, establecer los mecanismos de control y gestión de la seguridad física y lógica, monitorear el sistema de seguridad y evaluar la resiliencia.

Una nueva redefinición y una nueva oportunidad para avanzar en la Seguridad Global en un mundo de retos y exigencias colectivas y futuro incierto, con necesidad de entender las nuevas dinámicas sociales, económicas, energéticas y tecnológicas para propiciar el desarrollo de ese amplio concepto de la nueva cultura de seguridad que va estando cada vez más presente.

Los desafíos que sugiere el nuevo contexto global de riesgos y amenazas requieren soluciones de seguridad innovadoras, tanto en el ámbito público como en el privado, que incorporen a la inteligencia y la tecnología como bases de una estrategia de seguridad necesaria para operar en las organizaciones y la sociedad en su conjunto, pero sin olvidar que el valor social contribuye a crear valor económico, y viceversa, siendo inexcusable el contemplar como un todo ambos tipos de valores.

Con ello, podemos ofrecer soluciones holísticas a la Gestión del Riesgo de las Infraestructuras Críticas y Estratégicas que, sin duda, requieren productos y servicios de seguridad adecuados a sus específicos riesgos, amenazas y vulnerabilidades.

Hemos de ser capaces de entender el ecosistema actual de la seguridad global y realizar un análisis profundo de sus fallos y de los retos más importantes a los que se enfrenta. Para ello, se ha de estudiar a fondo el impacto de la globalización y de los cambios sociales y económicos que vivimos, en la seguridad y sus organizaciones. Es preciso identificar las grandes tendencias de la seguridad, además de algunos de los riesgos en infraestructuras críticas, para evaluar su posible impacto y poder analizar las complejidades en la toma de decisiones, sin olvidar la importancia del liderazgo de la seguridad a nivel internacional, calculando sus capacidades y resiliencia.

Nuevos retos y nuevas respuestas globales que hacen precisa también una visión compartida, junto a la preparación adecuada de cada vez más profesionales, ejecutivos y operativos, que han de acreditar una formación y capacitación especializada, no lineal, basada en estrategias y pensamientos exponenciales, abiertos y flexibles, que les convierta en los lideres de la seguridad que venimos precisando.

Los directores de Seguridad, marcados por diversas situaciones acontecidas como la reciente pandemia, la aceleración de la transformación digital, la globalización de los riesgos y amenazas, etc., se encuentran motivados para un mayor desarrollo de sus carreras de cara a los nuevos retos, para abordar problemas transversales y globales con un mayor horizonte y una visión cooperativa.

La implementación y gestión de la seguridad Integral e Integrada exige una nueva figura con una visión holística y ejecutiva, un nuevo Director de Seguridad Global.

Por todo ello, se impone la revisión de las políticas de seguridad, creando una nueva cultura de seguridad global, integral e integrada, estableciendo los mecanismos de control y gestión de la seguridad física y lógica, y teniendo especialmente en cuenta la implementación de los nuevos sistemas y el potenciamiento de la resiliencia.

El objetivo es plantear la nueva cultura de la seguridad como un bien público, propiciando la evolución y desarrollo de un paradigma de seguridad de valor compartido, que abarque de lo global a lo local.

Estamos ante un nuevo cambio de paradigma en la Seguridad Global, (integral e integrada, pública y privada) como respuesta a los nuevos y grandes retos y exigencias derivadas del avance de la globalización.

Queremos progreso y bienestar para todos, pero no podemos olvidar su precio. Todo nuevo desarrollo implica el coste de su implementación, más el de sus estudios de impacto y consecuencias, su cuidado, su buen uso, su mantenimiento y la permanente formación de las personas que garanticen el perfecto funcionamiento y protección de las vidas y bienes implicados.

Crezcamos, pero no en vertical ni horizontal, sino de forma esférica y neuronal, integradora y consciente, de manera que se contemple de antemano el bien del conjunto y la detección de los riesgos y amenazas que toda desarmonía puede llegar a producir. Sólo así la seguridad adquiere su más importante dimensión, que, como en medicina, es la preventiva. ■

Manuel Sánchez Gómez-Merelo,
consultor internacional de Seguridad
y ex-coordinador de Seguridad
en Instituciones Penitenciarias.

LUEGO DE LA PANDEMIA DE COVID-19,
LA CULTURA PREVENTIVA INTEGRAL ES UNA PRIORIDAD

PERÚ | **César Ortiz Anderson**

Lo que ha dejado la inseguridad ciudadana

En la Asociación Pro Seguridad Ciudadana (APROSEC) cumplimos 25 años trabajando temas de seguridad preventiva enfocada a la problemática de inseguridad ciudadana, sin embargo desde nuestro punto de vista, la prevención debe estar presente en todos los ámbitos, acabo de leer el último informe global sobre la crisis alimentaria del año 2023, elaborado por el Banco Mundial.

Las cifras son desalentadoras, en el año 2021 la inseguridad alimentaria afectó a 192 millones de personas en el mundo, en el año 2022 la cifra aumentó a cerca de 258 millones de personas. Esta cifra incluye a 56.8 millones de personas que fueron afectadas por los diversos fenómenos de la naturaleza extremos, 83.9 millones de personas afectadas por las conmociones económicas producto de la pandemia del COVID-19 y la guerra; así como a 117 millones de víctimas de los conflictos y la inseguridad.

Foto: - Freepik

DESASTRES NATURALES Y CORRUPCIÓN

En el caso del Perú, el informe indica que los datos no cumplían con los requisitos GRFC, por lo que no pudieron registrar el número de personas afectadas por las crisis. Sin embargo, el Banco Mundial, en otro informe elaborado, denominado "Actualización sobre la seguridad alimentaria", correspondiente a este mes, advierte que en el mes de marzo del 2023, Perú se encontró con el inicio del fenómeno de El Niño Costero, lo que, junto con el ciclón Yaku, produjeron fuertes lluvias e inmundaciones, que provocó que aproximadamente 517 mil personas necesitaran asistencia, ello según la Red Humanitaria Nacional.

Foto: - Freepik

En tal sentido, se estima que los desastres naturales habrían afectado aproximadamente a 92 mil viviendas y dañado las principales infraestructuras y vías de comunicación. No obstante, el estudio considera como "la necesidad más apremiante", la seguridad alimentaria, en particular en zonas rurales y periféricas urbanas. Otra cifra a tomar en cuenta en este informe, es que las lluvias e inundaciones han afectado gravemente a las familias campesinas de las zonas rurales de Perú, con mas de 38 mil hectáreas de cultivo dadas y 22 mil hectáreas pérdidas.

El informe alerta, puntualizando, que incluso antes de la emergencia climática, un 55% de las poblaciones en los Departamentos de Lambayeque, Piura y Tumbes, estaban viviendo una situación de inseguridad alimentaria de moderada a severa. Hay que señalar que la inseguridad alimentaria en Perú siempre ha existido.

Finalmente es importante que los tres niveles de Gobierno esten trabajando prevención de acuerdo con los importantes datos de este informe, donde no señala los estragos que adicionalmente venimos sufriendo por la pandemia del dengue, por ello me indigno al estudio de la Contraloría General de la República, que determinan pérdidas por mas de 24 mil millones de soles, producto de la corrupción. Basta ya. ■

César Ortiz Anderson, presidente de Aprosec (Asociación Pro Seguridad Ciudadana del Perú). *Más sobre el autor:*

amesis MR

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

24/365 DÍAS
Atención personalizada de nuestro centro de monitoreo

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

TOTAL ACCESO
Consulta a reportes de estadísticas de robos

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

SOCIOS ACTIVOS

Tracking Systems de México S.A. de C.V. · sitel Seguridad Satelital · Holkan Rastreo Satelital · skyguardian · skymeduza · ADS LOGIC Telematics · SECUREWITNESS · INFO TRAX · TECNO LOGISTIK · RAINDE · SEGURIDAD 360 .com · ATLANTIDA · TTC · AISIS Seguridad Integral · GEOTRUCKS · GRUPO ALFIL · SEC SOLUCIONES · GPSMonitor Rastreo Satelital · GRUPO PRYSE · DUMAX Smart Tracking

SOCIOS ADHERENTES

GPS TRACKER MX Vamos contigo® · SATECH Rastreo Satelital · TSNISION Technology Security Vision · RCU Sistemas · GEOTRACKING Rastreo Satelital · Tecno GPS

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

COMUNÍCATE
55 3334 4707

Leopoldo Rodríguez Mendoza,

director general de Traseco

1. Actualmente, ¿cuáles considera que son los mayores desafíos de la protección ejecutiva?
Un estado fallido y por consiguiente una delincuencia organizada que ha rebasado al gobierno.

2. ¿Cómo puede una empresa conocer las tendencias y tecnologías en seguridad para asegurar la eficacia de la protección ejecutiva?
Asistiendo a eventos específicos sobre el tema e inscribiéndose a revistas especializadas, siguiendo empresas de renombre y especialistas en redes sociales.

3. ¿Cuáles son los aspectos más importantes a considerar para desarrollar un plan estratégico de seguridad para un principal?
- Conocer a quién voy a cuidar.
- Saber de qué lo voy a cuidar.
- Tener con qué cuidarlo.
- En qué momento voy a cuidarlo.

4. ¿Cómo equilibra la seguridad con la privacidad y comodidad de los clientes durante las operaciones de protección ejecutiva?
Eso es un mito, para brindar seguridad, privacidad y comodidad al mismo tiempo, sólo se puede hacer con un exceso de recursos.

5. ¿Cuál considera que es la innovación más significativa que ha implementado en la empresa en términos de protección ejecutiva?
Comunicación satelital.

6. ¿Cómo evalúa y mejora constantemente la calidad y eficacia de los servicios de protección ejecutiva que ofrece su empresa?
La mejor evaluación es la plena satisfacción de un cliente, y la mejora continua se logra atendiendo la formación, capacitación y desarrollo del personal.

7. ¿Qué se debe considerar para contratar un servicio de protección ejecutiva?
Primero, que sea necesario; segundo que no sea un lujo, y tercero, que tiene un costo significativo.

Leopoldo Rodríguez Mendoza es especialista en protección ejecutiva y dirección de empresas con portación de armas; egresado de la Licenciatura en Administración de Empresas, es Diplomado en Dirección de Empresas por la Universidad José Camilo Cela, de Madrid, España. También cursó el Diplomado en Dirección de Seguridad en Empresas por la Universidad Pontificia Comillas, en Madrid, España. A lo largo de su experiencia ha sido acreedor de las certificaciones CPO por la International Foundation for Proteccion Officers, y EPS por la International Bodyguard Security Services Association.

Su trayectoria de más de 30 años, lo ha llevado a estar en el cargo de director de varias empresas de Seguridad Privada, incluyendo seis años en España, y como Consultor Externo especializado en empresas con licencias colectivas de portación de armas de fuego. Actualmente dirige Traseco, empresa mexicana que ofrece los servicios de: guardias intramuros, protección ejecutiva, custodia y vigilancia, asesoría y consultoría, y capacitación profesional. ■

Asistencia Legal

ALES

Gestoría Jurídica
en materia de
Seguridad Privada

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

Asumimos la responsiva de su empresa en los siguientes rubros:

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

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

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

· Representación, atención y respuesta a visitas de verificación, supervisión o de inspección.

· Atención a multas y sanciones mediante recursos legales idóneos.

· Juicios de nulidad y amparo administrativo.

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

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

· Elaboración de manuales operativos o de capacitación.

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

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

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

licdantegarciamtz@outlook.com

Whats: 477 828 1291

ASOCIACIÓN MEXICANA DE PROFESIONALES EN PREVENCIÓN DE PÉRDIDAS, A.C.

En 1982 un grupo de profesionales en seguridad del estado de Nuevo León conformaron la Asociación Mexicana de Profesionales en Prevención de Pérdidas, A.C. (AMPPPAC), con el objetivo de intercambiar experiencias y aprendizajes sobre el sector y consolidar estrategias efectivas para el desarrollo de sus negocios y sobre todo contribuir con la seguridad del país.

El 02 de diciembre de 2023, tomó protesta la nueva Mesa Directiva, encabezada por el C.P. Ignacio Goytortúa del Ángel, director de Seguridad Corporativa en Grupo Gonher, y quien nos compartió los objetivos por cumplir de este periodo en la asociación.

¿Cuáles son los objetivos generales de la AMPPPAC?

- Profesionalizar la función de protección y seguridad.
- Brindar apoyo en estos campos a la Comunidad.

¿Cuáles son las metas de la Mesa Directiva para este 2024?

1. Ejecutar su labor profesional con apego a la ley y a los más altos principios morales, observando los principios de veracidad, honestidad e integridad.
2. Realizar eventos de capacitación, así como talleres sobre temas de seguridad; y el congreso anual, todo ello para continuar actualizándonos en el ramo de la seguridad.
3. Tener relaciones con los tres niveles de autoridades de seguridad para cualquier apoyo que requieran los socios y así poder contactarlos y realizar una sinergia.
4. Organizar eventos para socializar con los socios, en un ambiente familiar, de armonía y cordialidad.

¿Cuáles son los beneficios de pertenecer a la AMPPPAC?

- Pertenecer a la asociación de Seguridad con más prestigio y trayectoria en la región norte del país, con presencia en Monterrey por más de 42 años.
- Tener fuerza y representatividad de grupo ante las autoridades y demás instituciones públicas y privadas.
- El poder relacionarse con profesionales reconocidos en nuestro campo de acción.
- Tener acceso gratuito a conferencias especialmente dirigidas a socios.
- Tener un valor curricular adicional, para nuestro perfil profesional.
- Participar en el Congreso Internacional de Seguridad "La Seguridad y Protección Hoy", con interesantes conferencias.
- Beneficiarse con buenos precios, condiciones preferentes y becas del 100%, en nuestro Congreso Internacional anual.
- Convivencias con profesionales en las conferencias mensuales sin costo para los socios.
- Convivencia en la Posada Navideña anual, con regalos y sorpresas.

¿Cómo contribuye la AMPPPAC con la seguridad del país?
Al intercambiar experiencias y conocimientos profesionales relativos a la Seguridad y Protección; aunado a mantener relaciones con los tres niveles de autoridades en materia de seguridad; así como el fomentar la cultura de legalidad, con bases firmes, objetivos concretos y compromisos fuertes; además de la profesionalización de los integrantes de la asociación a través de capacitación continua.

¿Cuáles considera que son los principales aspectos que debe considerar un Profesional en Prevención de Pérdidas para aplicar en la seguridad de alguna organización o institución?
Se deben de elaborar planes de trabajo para salvaguardar la seguridad de miembros y bienes de la organización, garantizando la continuidad de negocio, dichos planes no pueden interferir o ser contrarios a los objetivos generales de la empresa sino al contrario, deben ayudar a la rentabilidad de la misma, dichos planes deben de ser prácticos y pragmáticos, cargados de altos niveles éticos y morales.

¿Cuál es el Plan de Trabajo de la nueva Mesa Directiva?

1. Realizar sinergias para dar a conocer la asociación a la sociedad a fin de consolidarla.
2. Promover una mayor difusión a las Conferencias-Desayunos, como plataforma de Capacitación y actualización.
3. Buscar una comunidad de seguridad participativa y más incluyente en todos los sectores.
4. Efectuar capacitaciones, cursos, seminarios y el Congreso Anual, con la intención de que los miembros estén actualizados en materia de seguridad.
5. Mantener relaciones permanentes con autoridades de todo orden de Gobierno (Federal, Estatal y Municipal).
6. Coordinar visitas de campo con diversos organismos en el ámbito Educativo, Gubernamental e Iniciativa Privada.

¿Cuáles son los requisitos para pertenecer a la AMPPPAC?

- Contar con una experiencia de por lo menos tres años en áreas de Seguridad y Protección.
- Haber cursado estudios de Licenciatura o posgrado en Seguridad y Protección.
- Llenar la solicitud de ingreso.
- La solicitud debe de contener la firma de dos socios activos.
- Enviar su información curricular.
- Cubrir el costo vigente de la membresía. ■

Fotos: AMPPPAC

Ignacio Goytortúa del Ángel es Contador Público y Auditor egresado de la Universidad Autónoma de Tamaulipas; es especialista en Dirección de Seguridad en Empresas (DSE) por parte de la Universidad Pontificia de Comillas; cursó el Diplomado de Dirección de Seguridad en Home Land Security Laboratory Tel Aviv Israel. Cuenta con más de 25 años de experiencia en seguridad y prevención de pérdidas, en el ramo del *retail* y en el sector industrial donde actualmente es director de Seguridad Corporativa en Grupo Gonher.

ASIS CAPÍTULO MÉXICO

Hace 23 años comencé en Seguridad con gran expectativa, ya que provenía de la industria logística y aunque tenía gran relación con este gran gremio como cliente, colocarme del otro lado del escritorio fue realmente fascinante y totalmente nuevo para mí.

Hace 14 años estuve en el emblemático podium de ASIS, como parte de una presentación como patrocinador, experimentando sensaciones mágicas y realmente el día de mi toma de protesta así me sentí, cumpliendo un sueño.

Ese día observando cada mesa, me congratulé de ver una parte de mi historia en cada una de ellas, ya sea como socios de negocio, cliente, proveedor, como compañero de actividades, director de empresa o simplemente amigos y colegas.

Debo reconocer y garantizar la continuidad de lo bien hecho con gratitud y humildad, se cierran círculos, pero se abren otros y estoy seguro que lo vamos a lograr.

Todo esto por medio de círculos de mejora continua que tienden a ser infinitos y que son la base para llevar a cabo las cosas con calidad y trascendencia.

Se presentan tiempos de agradecer a nuestros maestros y mentores, a nuestra querida familia aquí, a nuestras autoridades de ASIS Internacional que nos visitaron, a nuestras asociaciones hermanas que siempre son bienvenidas a esta su casa ASIS Capítulo México 217, a nuestras importantes empresas que son el bastión de nuestra vida cotidiana, pero sobre todo a nuestros amigos.

Hoy nuestro CD 2024 está conformado por personas que aman la seguridad y que tienen gran vocación de servicio, es un CD plural, profesional e inclusivo, cuya misión será en este año continuar con lo bien hecho el año pasado, pero dándole su mística y originalidad, así como lo marca la filosofía de mejora continua, siempre en pro de lo ofrecido a nuestros socios que conforman esta gran membresía de nuestro querido Capítulo México, considerado como uno de los más importantes e influyentes del mundo. ■

José Luis Alvarado Martínez, MBA, DSI, DSE, DAS, director comercial de Grupo Consultores y presidente de ASIS Capítulo México

AGRUPACIONES DE SEGURIDAD UNIDAS POR MÉXICO **(ASUME)**

ASUME
AGRUPACIONES DE SEGURIDAD UNIDAS POR UN MEXICO ESTABLE

LA INDUSTRIA DE LA SEGURIDAD PRIVADA EN EL 2024, RETOS VS. OPORTUNIDADES

Armando Zúñiga Salinas, presidente de ASUME

Estimados lectores:

ASUME (Agrupaciones de Seguridad Unidad por México) y las 33 asociaciones de Seguridad Privada que representa en todas las modalidades hemos llegado al 2024 convencidos en que este será un año lleno de retos y oportunidades para los empresarios y colaboradores que trabajan en nuestra industria. ¿Sabían que, de acuerdo a cifras oficiales, tenemos poco más de 450 mil guardias de seguridad registrados ante el IMSS (Instituto Mexicano del Seguro Social) y 950 mil personas de acuerdo con las cifras de la Secretaría de Economía en poco más de 7 mil 470 empresas registradas como unidades económicas de Seguridad Privada?

Esta fuerza laboral nos coloca en el número 11 de "Servicios de protección y custodia" del ranking de industrias en el país con más personas trabajando con un mismo fin, proteger y salvaguardar la operación, inversión, patrimonio y las personas de los clientes para quienes trabajamos.

Dentro de los temas importantes que consideramos serán grandes retos y oportunidades para nuestra industria, les compartimos los siguientes comentarios:

- **Entorno Político, Elecciones Presidenciales, gobernadores, senadores y diputados:** La historia de México nos ha enseñado que siempre en estos periodos el incremento de la violencia se hace presente, acciones de la delincuencia organizada y autoridades hace que nuestros productos y servicios tengan mayor demanda.
- ***Nearshoring*, relocalización de empresas globales y sus proveedurías de bienes y servicios:** Se calcula que se necesitan 11 millones de metros cuadrados para naves industriales y 50 parques industriales nuevos para satisfacer la demanda que generará este proceso. ¿Imaginan cuantas cámaras, guardias de seguridad, sistemas contra incendio, controles de acceso, entre otros sistemas y servicios de seguridad privada serán necesarios, sólo en éste, de los varios componentes que detonará la relocalización en nuestro país?
- **Inseguridad y violencia en zonas urbanas, industriales, comerciales y habitacionales:** Lamentablemente hemos sido testigos como cada día hay más eventos de violencia por grupos delictivos en espacios que son protegidos por las empresas que se dedican a la seguridad privada. Recordemos que todas las industrias en nuestro país, espacios públicos y privados de esparcimiento y recreo, así como unidades económicas y productivas son clientes de la Seguridad Privada en México.
- **Incremento de ataques cibernéticos y extorsiones:** Nuestro mundo cambia constantemente y la delincuencia también lo hace, adaptándose a su entorno y condiciones que tiene para materializar acciones en contra de las empresas y las personas. El uso de la tecnología por parte de la delincuencia para "profesionalizar" sus actividades nos obligan a también actualizarnos e innovar para neutralizar estas acciones. La ciberseguridad hoy es una materia obligada para todos los que nos dedicamos a la seguridad privada en todas las modalidades y el estudiar los diferentes mecanismos de extorsión que en los últimos meses han incrementado nos permitirán proteger de mejor forma a nuestros clientes y a la sociedad.
- **Nueva cultura laboral y salarial en beneficio de los trabajadores:** La llegada del REPSE, Ley Silla, reglas sindicales, incrementos salariales, vacaciones, días no laborales, una reforma laboral integral, acuerdos con Estados Unidos y CANADA por el T-MEC, etc., nos obliga a replantear modelos de servicio junto con nuestros clientes en beneficio de nuestros empelados sin poner en riesgo la seguridad y cumplimiento a los procesos establecidos.

Todo lo anterior refrenda nuestro compromiso y los principios de ASUME:

- Profesionalización de todos los que formamos parte de nuestra industria; empresarios, directivos y trabajadores.
- Dignificación del personal operativo y administrativo de seguridad privada.
- Desarrollo de la Industria en su conjunto para beneficio de nuestros socios y de México.
- Impulsar la Ley General de Seguridad Privada, Ciberseguridad y Extorsiones.

Por último, como parte del proceso legal de ASUME, para configurarnos como Cámara Industrial, les compartimos que nuestro nombre tendrá el siguiente ajuste: Sociedad Nacional de Industriales en Seguridad Privada (ASUME) y seguiremos comprometidos con México. ■

GRUPO DE EJECUTIVOS EN MANEJO DE CRISIS **(GEMARC)**

Queridos lectores de "**Seguridad en América**":

Es un honor dirigirme a ustedes como presidente de GEMARC (Grupo de Ejecutivos en Manejo de Crisis) para expresar mis más sinceros deseos de que hayan tenido unas festividades decembrinas llenas de alegría y amor. En esta temporada de reflexión y unión, es un placer extender mis mejores deseos a cada uno de ustedes y a sus seres queridos.

Al mirar hacia atrás en el año que terminó, me llena de gratitud ver el continuo crecimiento y compromiso de nuestra comunidad en el ámbito de la seguridad corporativa. GEMARC ha sido un faro de excelencia y colaboración, y estoy agradecido por el arduo trabajo y la dedicación de todos nuestros miembros. Ha sido un año desafiante, pero juntos hemos superado obstáculos y hemos fortalecido nuestra posición como líderes en la gestión de crisis y seguridad.

En nombre de todos los miembros de GEMARC, quiero expresar nuestro más profundo agradecimiento por su apoyo continuo. Ha sido un año en el que hemos aprendido, crecido y, sobre todo, colaborado para enfrentar los desafíos en constante evolución en el ámbito de la seguridad. Cada uno de ustedes ha contribuido de manera significativa al éxito colectivo de nuestra asociación, y les animo a seguir comprometidos en esta importante labor.

Mirando hacia el futuro, anticipamos con entusiasmo un año que se perfila como un periodo de consolidación para GEMARC. Nuestra asociación se encuentra en el camino de convertirse en la entidad más importante en el ámbito de la seguridad corporativa. Estamos comprometidos a fortalecer aún más nuestros lazos, compartir conocimientos y seguir siendo pioneros en la implementación de prácticas innovadoras en Seguridad Corporativa.

Este año, nuestras metas incluyen la expansión de nuestras actividades de formación, el desarrollo de nuevas alianzas estratégicas y la participación activa en debates que influyan positivamente en la seguridad a nivel corporativo. Al consolidar nuestra posición, estamos seguros de que podremos brindar un mayor valor a nuestros miembros y a la comunidad en general.

En el contexto actual, donde la seguridad es esencial para el bienestar de las organizaciones y sus colaboradores, GEMARC se compromete a liderar con integridad, experiencia y resiliencia. Nuestro compromiso con la excelencia en la gestión de crisis y seguridad nos impulsa a buscar constantemente formas de mejorar y adaptarnos a un entorno empresarial en constante cambio.

En conclusión, deseo a cada uno de ustedes un año lleno de éxitos, logros y prosperidad. Que nuestras acciones colectivas en GEMARC sigan siendo un faro de inspiración para la industria de la seguridad corporativa. Juntos, enfrentaremos los desafíos y abrazaremos las oportunidades que el futuro nos depara.

Gracias por su compromiso continuo y confianza en GEMARC. ¡Que este año sea testigo de un crecimiento continuo y de éxitos sin precedentes para todos nosotros! ■

Atentamente,

Héctor Coronado Navarro, CPP, DSE, presidente de GEMARC

ASOCIACIÓN MEXICANA DE ESPECIALISTAS DE SEGURIDAD INTEGRAL **(AMEXSI)**

Estimados amigos de la comunidad **SEA**:

Es con gran satisfacción y entusiasmo que me dirijo a ustedes en calidad de presidenta de AMEXSI, compartiendo los logros y compromisos excepcionales que hemos experimentado a lo largo de este último año. En nuestra firme dedicación a la excelencia profesional, hemos dedicado más de 1,500 horas hombre a actividades formativas y de desarrollo, tales como capacitaciones, talleres, cursos, desayunos, *webinars* y reuniones mensuales. Nuestro debut en la Expo Seguridad fue un hito trascendental, marcando un crecimiento significativo y fortaleciendo nuestra presencia en el sector. Esta experiencia no sólo amplió nuestro horizonte, sino que también nos permitió intercambiar ideas innovadoras y establecer conexiones valiosas con colegas destacados. Además, nuestra colaboración activa con asociaciones hermanas ha sido esencial para el crecimiento y la consolidación de nuestra área de acción.

La unidad ha sido y seguirá siendo nuestra mayor fortaleza. Hoy, con orgullo, contamos con 170 miembros comprometidos, a quienes agradecemos sinceramente por su confianza y participación en cada iniciativa. Bajo el lema "Donde vayamos, un amexiano encontramos", cada paso que damos cobra vida gracias a la dedicación y compromiso de nuestros miembros, permitiéndonos destacar en eventos y revistas especializadas, consolidándonos como referentes en el sector.

Nuestra base continúa siendo DSI, y celebramos con entusiasmo la incorporación de nuevos miembros. La diversidad de pensamientos y experiencias se ha convertido en nuestro mayor activo, enriqueciendo nuestras perspectivas y contribuyendo significativamente al sector. Estamos demostrando, con cada acción, que nuestra unión nos hace más fuertes.

En este año 2024, renovamos nuestro firme compromiso con la excelencia, la innovación y la colaboración en AMEXSI. Mantendremos la constancia en nuestras actividades programadas, las cuales desempeñan un papel fundamental en nuestro continuo crecimiento y desarrollo en el sector de la seguridad. Nuestros *webinars* seguirán siendo espacios de aprendizaje dinámicos, donde expertos destacados compartirán conocimientos vanguardistas y tendencias actuales. Las reuniones mensuales serán momentos cruciales para la interacción y el intercambio de ideas entre nuestros miembros, fortaleciendo así la red de colaboración que nos caracteriza. Los cursos especializados continuarán siendo una piedra angular de nuestra oferta formativa, proporcionando a nuestros miembros las herramientas necesarias para destacar en un entorno en constante evolución. Asimismo, mantendremos una búsqueda activa de expositores y oportunidades de capacitación, asegurándonos de ofrecer contenido de calidad que responda a las demandas del sector.

LRI. Ana Luisa Guzmán Contreras, presidente 2023-2024

Con miras al futuro, anticipamos con expectación y determinación las oportunidades y desafíos que se presentarán en el ámbito de la seguridad. Estamos preparados para seguir marcando la pauta y liderando iniciativas que impulsen la excelencia en nuestro campo.

Agradecemos sinceramente a cada uno de ustedes por ser parte esencial de la familia AMEXSI. Su compromiso y contribución son pilares fundamentales para nuestro éxito continuo. Que la amistad, profesionalización y amor por nuestro sector sigan siendo nuestros estandartes. ■

Orgullosos de ser AMEXSI.

Con gratitud y entusiasmo.

ASIS CAPÍTULO OCCIDENTE

Este año 2024 el Capítulo 247 ASIS Occidente contará en su mesa directiva con profesionales de seguridad que han colaborado en diversos campos de la seguridad, los cuales estarán enfocados en los valores y misión del capítulo; apoyar a quienes hacen de este país un lugar más seguro, conectar a las mujeres en la seguridad e involucrar a la próxima generación de profesionales de la seguridad.

¡Saludamos a nuestros nuevos miembros en la mesa directiva!

VICEPRESIDENCIA: PAULINA BUSTOS, CPP

Mensaje de Paulina:

Me siento muy orgullosa y comprometida con este nombramiento, estoy segura de que seguiremos haciendo grandes cosas en el Capítulo, esperen noticias de nosotros, continuaremos con grandes expositores y trabajo en conjunto con todos los comités.

COMISARIO: JAVIER RAMOS, CPP

Mensaje de Javier:

He visto nacer y crecer nuestro Capítulo por más de 20 años, agradezco la confianza de ejercer esta posición y apoyar la gestión de nuestro presidente.

TESORERO: ROBERTO ROMERO, CPP

Mensaje de Roberto:

Agradezco la confianza en su servidor para administrar el capítulo, reitero mi compromiso con esta mesa y con cada uno de los miembros del capítulo el cumplir y hacer cumplir los preceptos de ASIS de los cuales he brindado juramento.

SECRETARIO: ORLANDO PONCELIS, DSE

Mensaje de Orlando:

Agradezco la oportunidad de formar parte de este talentoso grupo de profesionales, que tendremos la misión de colaborar en el capítulo de ASIS Occidente. Estamos conscientes que enfrentamos desafíos críticos en materia de seguridad en México; pero estoy convencido que trabajaremos juntos para superar estos retos y promover un entorno más seguro para todos.

Paulina Bustos, CPP, vicepresidenta

Javier Ramos, CPP, comisario

Roberto Romero, CPP, tesorero

Orlando Poncelis, DSE, secretario

Nuestro mayor compromiso es hacer que cada uno de nuestros esfuerzos forme parte de una sola voz en la búsqueda de un bien común como gremio y sociedad. ■

¡Bienvenidos a esta maravillosa iniciativa!

BUSINESS ALLIANCE FOR SECURE COMMERCE
OCCIDENTE DE MÉXICO

JABIL CIRCUIT
EMPRESA COMPROMETIDA
por más de 18 años certificada en BASC

LSC. MBA, LUIS E. VALENCIA
Sr. Security Manager, LATAM

"NO EXAGERO CUANDO DIGO QUE EL ÉXITO DE LA SEGURIDAD ... TOCANDO TODOS LOS DIFERENTES GRUPOS FUNCIONALES DE LA COMPAÑÍA VIENE DE LA MANO DEL TRABAJO COMPARTIDO Y REALIZADO CODO A CODO CON EL CAPÍTULO BASC..."

Aunque parezca cliché, la vida profesional como todos los demás aspectos de la misma, no se detienen; hoy me toca escribir este artículo desde la mesa de un hotel en Santo Domingo, justamente mientras planeamos con el equipo de esta bella ciudad la siguiente auditoría del Capítulo del Caribe.

Y es que muchas veces cuando escuchamos BASC, pensamos en auditoría, en nervios, estrés y alta velocidad en la respuesta a aquellas preguntas que el auditor nos hace; nos volvemos por unos días personas inmersas en los procesos y procedimientos; o por lo menos, así fue alguna vez.

Sin embargo y sin duda alguna, los últimos años, y me refiero a los últimos 4 años no me equivoco al aseverar que ha sido una experiencia de vida el trabajar con el Capítulo BASC en México, en el Occidente específicamente, y créanme no exagero cuando digo que el éxito de la seguridad en la cadena de suministro, el cumplimiento a cabalidad del perfil de seguridad, así como el crear una cultura de seguridad y de gestión de riesgos de forma transversal, y tocando todos los diferentes grupos funcionales de la compañía viene de la mano del trabajo compartido y realizado codo a codo con el Capítulo BASC, desde los líderes globales en la WBO hasta los auditores que de forma profesional auditan los diferentes sistemas sin dejar de pasar por alto a todos los capacitadores, auditores internos y todos aquellos que viven comprometidamente en los valores que nos llevan a cumplir la misión de mantener sanas y seguras las operaciones en la industria manufacturera.

Se que todos aún recordamos, pues no se ve nada lejos los tiempos de pandemia, donde las auditorías tuvieron que tomar un giro hasta ante conocido en el ámbito de lo virtual. Así todos aprendimos de una u otra forma y tuvo que ser rápido. Pusimos claro el objetivo de la mano de BASC Capítulo Occidente el no dejar de lado la gestión del sistema de seguridad, en conjunto se evaluaron los riesgos, sumándole a este análisis realmente todos los riesgos que surgieron con ese desafortunado evento vivido por la humanidad.

Ahora en retrospectiva, de no haber sido por ese trabajo en equipo que involucró a tantos profesionales de la seguridad, de la gestión y del análisis de riesgos no estuviéramos aquí ahora escribiendo estas líneas mientras planeamos como seguir manteniendo seguras las operaciones de la cadena de suministro, y desde luego a toda la hermosa gente que trabaja alrededor de todo el sistema.

No puedo terminar esta columna sin dejar abierta la pregunta, ¿Qué nos viene en el futuro?, ¿Cuantos retos más tendremos que afrontar?, supongo que varios, los riesgos siempre mutan, evolucionan, y es un hecho que la única manera de no quedar atrás y vulnerables es mantener sanos nuestros sistemas, y sin duda, buscar cumplir con los estándares y la norma BASC será siendo una herramienta de punta que nos mantendrá en ventaja siempre.

¡Hasta la próxima!

LSC. MBA, Luis E. Valencia
Sr. Security Manager, LATAM

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

5 tips de seguridad para su perro

Hoy en día, las mascotas de la casa juegan un papel más importante en la familia, ya no son sólo animales de compañía, sino que se han adoptado como un integrante más del hogar, y quienes desde hace varios años han sido objeto de la delincuencia, desde robo por maldad hasta secuestros y chantajes. Es por ello que en esta edición compartimos algunos tips de seguridad para los amigos perrunos, extraídos del Blog del Manual de Seguridad de David Lee.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Adquisición.** Evite fomentar el comercio ilícito y el maltrato a los animales, adquiera o adopte a sus mascotas con personas o establecimientos comerciales formales, donde se le expida una factura oficial, así como los registros de calidad y certificados de vacunación y salud correspondientes.
2) **Identificación.** Coloque a su perro un collar y placa de identificación que incluya un correo electrónico, y de preferencia con un microchip para identificarlo en caso de que lo lleven a algún veterinario quien podrá establecer, con un escáner, su identidad y derecho de propiedad. Es importante tomarse fotos continuas con él mostrando señas particulares.
3) **Prevención.** Al pasear al perro, utilice una correa adecuada que le permita mantener su control. No lo deje suelto. De preferencia realice los paseos en lugares cercados y vigílelo en todo momento. Evite dejarlo atado o dentro de vehículos, así como en patios que permitan acceso desde la calle. Al salir, procure ir acompañado y manténgase alerta ante la presencia de personas o vehículos sospechosos. Si contrata los servicios de adiestradores o cuidadores profesionales, verifique su calidad y honorabilidad.
4) **Disuasión.** En la placa de identificación indique que está "esterilizado" (aunque no lo esté) a efecto de disuadir a personas que consideren robarlo y utilizarlo para crianza. Evite a las personas extrañas que le hagan preguntas sobre su perro, considere que lo pueden estar prospectando como su próxima víctima; disuádalos afirmando que el perro no es de raza, que es latoso y sucio.
5) **Reacción.** Si su perro es robado, denuncie a las autoridades. Si desapareció y coloca anuncios de recompensa, considere la posibilidad de ser extorsionado. Si recibe la llamada de alguien que dice haber encontrado a su perro, no acudas solo y acuerde la entrega en un lugar público, idealmente asistido por la policía. Ante cualquier dato del posible secuestrador, informe a las autoridades.

Foto: Free Pick

FOMENTE LA CULTURA DE LA SEGURIDAD

Consulte la revista digital en www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

ÍNDICE DE ANUNCIANTES

¡AFÍLIATE AHORA!

Conoce y disfruta nuestros **BENEFICIOS**

30 AÑOS
PROFESIONALIZANDO

#ProfesionalizateConInspiracion

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

- 12 Reuniones mensuales presenciales sin costo, con conferencistas de primer nivel que suman a tu proceso de profesionalización.
- Webinars sin costo.
- Instructores Certificados.
- Cursos especializados en los diversos campos de la seguridad, los cuales otorgan CPE'S para tu Recertificación.
- Estaremos presentes como Capítulo en los mejores eventos de seguridad de México.
- Convenios de descuento para diversos productos y servicios.
- Bolsa de trabajo.
- Comunidades temáticas.
- Newsletter semanal.
- Chat privado de socios activos.
- Acceso a las guías & estándares de ASIS Internacional.
- Acceso a la base de datos de más de 34 mil profesionales de seguridad alrededor del mundo.

AFILIACIÓN

ASIS MÉXICO 217
$5,650 MX

ASIS INTERNACIONAL
$125 UDS

* Vigencia de membresía del 1 de enero al 31 de diciembre 2024

MAYOR INFORMACIÓN
(55 1321 1289
socios@asis.org.mx

#InnovandoEnASIS

incluye gastos de envío

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. **(Marque así X)**

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en Banco Barnorte, SEA MEDIA GROUP, S. de R. L. de C. V. Cuenta: 1095 5437 37

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe: 0721 8001 0955 4373 78

_____
Firma

DATOS DEL CLIENTE (para el envío de la revista):

Nombre: _____

Compañía: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envío de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato vía: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2024

ALLIED UNIVERSAL®
SECURITY SERVICES

There for you.

COMPROMETIDOS CON LA SEGURIDAD DE NUESTROS CLIENTES Y LA CALIDAD EN EL SERVICIO

Allied Universal® es la empresa líder global en servicios de seguridad e instalaciones. Ofrecemos servicios de seguridad proactivos, tecnología de vanguardia y soluciones a medida para permitir a los clientes centrarse en su negocio principal.

Nuestros servicios:

- **Profesionales de Seguridad altamente capacitados y experimentados**
  - Investigaciones Corporativas
  - Respuesta a Emergencias
  - Protección Ejecutiva y Servicios de Inteligencia
  - Monitoreo
- **Servicios de Tecnología**
  - Videovigilancia
  - Controles de acceso
  - Diseño, Ingeniería e implementación de Servicios
- **Asesoría y consultoría de Riesgos**
  - Investigaciones e Inteligencia
  - Respuesta a Emergencias
  - Monitoreo y Centro de control

Contáctanos **www.ausecurity.mx/esp** **(+52) 55 5337 0444**

Allied Universal® ha encargado y publicado el primer **Informe Mundial sobre Seguridad.** Esta investigación innovadora documenta las opiniones y preocupaciones de 1,775 jefes de seguridad de 30 países. El informe completo, las principales conclusiones, las opiniones de los expertos en seguridad y los videos están disponibles en **https://www.worldsecurityreport.com/**

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.®

Guardias, guardias armados, custodias, custodias blindadas y custodias armadas.

Cobertura a nivel nacional.

www.sepsisa.com.mx comercial@sepsisa.com.mx 55 5351 0402

AMERICAN CHAMBER MEXICO · ESR EMPRESA SOCIALMENTE RESPONSABLE · ISO 9001:2015 CERTIFIED COMPANY · ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD · REPSE Registro de Prestadoras de Servicios Especializados u Obras Especializadas · CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C. EMPRESAS DE CALIDAD · ASIS CAPÍTULO MÉXICO 217 · AMESP Asociación Mexicana de Empresas de Seguridad Privada A.C. · BAC · COPARMEX®