SEGURIDAD® EN AMÉRICA

M360

Reconoce a su fuerza de monitoreo

Año 24 / No.139
Julio - Agosto

www.seguridadenamerica.com.mx

@MultiprosegOficial

@MULTIPROSEGOFICIAL

MULTIPROSEG OFICIAL

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

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

ALGUNOS DE NUESTROS CLIENTES

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

AMESP

CDMX
CIUDAD DE MÉXICO

CNS

redconocer
de prestadores de servicios
Entidad de Certificación y Evaluación

ISO

BAC

ema
entidad mexicana
de acreditación, a.c.

ANERPV
Asociación Nacional de Empresas de Rastreo y Protección Vehicular

COPARMEX

REPSE
Registro de Prestadoras de Servicios Especializados u Obras Especializadas

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

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

(55)7959 9598
(55)3455 4375

INFO@MULTIPROSEG.COM.MX

WWW.MULTIPROSEG.COM.MX

SEGURIDAD EN AMÉRICA

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

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

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

Coordinación de Diseño
José Arturo Bobadilla Mulia

Arte & Creatividad
Diego Idu Julián Sánchez
arte@seguridadenamerica.com.mx

Administración
Oswaldo Roldán
oroldan@seguridadenamerica.com.mx

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

Reporteros
Mónica Ramos
redaccion1@seguridadenamerica.com.mx

Antonio Venegas
redaccion2@seguridadenamerica.com.mx

Medios Digitales
Dulce Anel Sánchez Mata
mdigital@seguridadenamerica.com.mx

Circulación
Alberto Camacho
acamacho@seguridadenamerica.com.mx

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

María Esther Gálvez Serrato
egalvez@seguridadenamerica.com.mx

Año 24 / No. 139 / Julio - Agosto / 2023

Portada:
M360

Síguenos por

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

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

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

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

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

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

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

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

Apoyando a:

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 Instituto 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.

EDITORIAL

La administración del presidente mexicano, Andrés Manuel López Obrador, impuso récord de 156 mil 136 asesinatos registrados en el periodo de diciembre de 2018 al 24 de mayo de 2023, de acuerdo con el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, por lo que es ya el sexenio más violento de la historia reciente de México.

En conferencia de prensa en las instalaciones de la Primera Región Naval, en Ciudad Madero, Tamaulipas, López Obrador reconoció que su gobierno es el más violento en la historia reciente del país, pero acusó que esto es debido a que la "mala herencia" que le dejaron los gobiernos anteriores. Responsabilizó a sus antecesores de haber creado estos grupos criminales, pues acusó que había un "Narco Estado", y aseguró que el delito de homicidio está bajando.

De nuevo, puso como ejemplo a Genaro García Luna, ex secretario de Seguridad durante el gobierno de Calderón, y quien fue declarado culpable por una corte en Estados Unidos por sus nexos con el narcotráfico.

Señaló que "el país estaba en bancarrota, inmerso en un decadencia, ni siquiera era una crisis, era una decadencia y por eso, frente a ella, lo único que debía hacerse era llevar a cabo un proceso de transformación, arrancar de raíz a la corrupción y eso no les ha gustado a los que antes se sentían los dueños de México y son los responsables de la tragedia nacional".

"Deberían estar ofreciendo disculpas aquí en Tamaulipas, cuántos gobernantes mediocres, ladrones, por eso celebro que después de años los tamaulipecos, mujeres y hombres hayan decidido tener un gobernador honesto, íntegro, decente, no malandrín, para decirlo con toda claridad", agregó.

Según el INEGI (Instituto Nacional de Estadística y Geografía), los estados con mayor número de asesinatos son: Guanajuato, Baja California, Estado de México, Ciudad de México, Jalisco, Chihuahua, Tamaulipas, Michoacán, Zacatecas y Guerrero. Un 65% de los expedientes de homicidios se concentran en dichas entidades.

Mientras que en todo el sexenio de Enrique Peña Nieto mataron a 156 mil 066 personas y con Felipe Calderón la cifra alcanzó los 120 mil 463 homicidios, el doble del sexenio de Vicente Fox Quesada, que dejó el gobierno con 60 mil 280 asesinatos. Esto significa, que cada día se impondrá un nuevo récord en materia de homicidios y no hay una solución a la crisis.

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 Mónica Rodríguez, *Coach* de Seguridad en Universidad de las Américas Puebla (UDLAP) y el Tecnológico de Monterrey, facilitadora del desarrollo del potencial humano a través de la congruencia, quien en generosas ocasiones ha presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

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

Si desea conocer más del experto, consulte su currículo:

ENTREVISTA EXPRÉS CON

Cap. José Carlos Sánchez Guzmán,

director general de GECSA

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

Hace 12 años, aproximadamente, no había militarización. La Seguridad Privada era coadyuvante de la Seguridad Pública, motivo por el cual hoy en día no podría contribuir para combatir la inseguridad en el país, partiendo del siguiente planteamiento: ¿Quién pagaría la contribución para combatir la inseguridad? La Seguridad Privada cobra por su trabajo en cualquiera de las seis modalidades, y no hay institución federal, estatal o municipal que pague sus servicios.

SISSA
Monitoring Integral

GARANTIZANDO LA SEGURIDAD

DE TUS INSTALACIONES CRÍTICAS

Asegura la continuidad de tu negocio mediante la integración de **sistemas de cómputo y telecomunicaciones** que protejan y optimicen tus procesos de conectividad:

Redes de datos

Inhibición de señales de comunicación

Hiperconvergencia

Radiocomunicación

Sonificación y voceo

Almacenamiento masivo

Tecnología informática e impresión

Contáctanos y descubre cómo podemos ayudarte a garantizar la seguridad y adecuado funcionamiento de tus instalaciones críticas.

www.sissamx.com

ÍNDICE

Julio - Agosto 2023

VIDEOVIGILANCIA

CONTRA INCENDIOS

CIBERSEGURIDAD Y TI

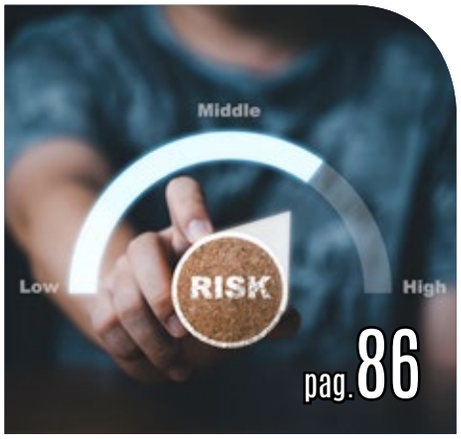
SEGURIDAD PRIVADA

ÍNDICE

Julio - Agosto 2023

ADMINISTRACIÓN DE LA SEGURIDAD

SEGURIDAD PÚBLICA



ESPECIAL

REPORTE

EL PROFESIONAL OPINA

CONOCE A TU ASOCIACIÓN

FOROS Y EVENTOS

ENTREVISTA CON EL EXPERTO

TIPS

FUNDAMENTOS BÁSICOS Y FINALIDAD DE UN SISTEMA DE CONTROL DE ACCESOS

MÉXICO | José Leonardo Gómez Ruiz

Foto: - Freepik

Cualquier empresa que ofrece los servicios de un sistema de control de accesos, debe contar con: personal especializado/certificado, pólizas de mantenimiento del fabricante, *software*, licenciamiento, actualizaciones, *firmware*, insumos, consumibles, refacciones e interfaces necesarias para intervenir cualquiera de los equipos

DEFINICIÓN

Un sistema de control de acceso se implementa derivado de la necesidad de vigilar las entradas y salidas en una instalación (sea estratégica, empresarial, educativa, etc.); así como monitorear la actuación del personal de manera que se pueda prevenir operaciones no autorizadas. Asimismo, facilita el registro, revisión y autentificación vehicular y del personal que tiene acceso a diferentes áreas y unidades funcionales; además de dar seguimiento a eventos, alarmas, apertura y cierre de accesos en tiempo real.

Los equipos tecnológicos instalados (torniquetes, pilonas, poncha llantas, plumas vehiculares, PLC/ Controlador Lógico Programable, DPS/Door Position Switches, intercomunicadores, biométricos, puertas y *software*) permitirán la verificación y automatización de accesos; sin la necesidad de contar con personal en sitio para dichas actividades, o en su caso, con el mínimo necesario. Es importante mencionar que ello dependerá de los procedimientos de operación de cada instalación en particular. Aunado a lo anterior, con los datos que recaban los equipos tecnológicos, se logra la gestión de los mismos, logrando bases para la generación de datos, que bien procesados, pueden generar desde información estadística hasta de inteligencia.

En otras palabras, un sistema de control de accesos bien implementado, permite a las diferentes áreas de ingreso y/o egreso, denegar o permitir el acceso a personal, además de controlar la apertura y cierre de puertas y portones, enrolamiento de personal e identificación de sucesos.

Foto: - Freepik

Foto: - Freepik

ESTRUCTURA Y FUNCIONAMIENTO DE UN SISTEMA DE CONTROL DE ACCESOS

De acuerdo a la Real academia de la Lengua Española, uno de los significados de la palabra “sistema” es: m. Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto.

Por ende, el sistema de control de acceso puede ser fragmentado en las siguientes etapas: Insumo – Proceso – Servicio.

Por insumo se entenderá a todo aquello que el equipo tecnológico tome como elemento para su base de datos, a quien le brindará, como ejemplo, el servicio de poder entrar a las instalaciones; pudiendo ser estas personas o vehículos.

Un sistema de control de accesos bien implementado, permite a las diferentes áreas de ingreso y/o egreso, denegar o permitir el acceso a personal, además de controlar la apertura y cierre de puertas y portones, enrolamiento de personal e identificación de sucesos

Ellos Aprenden.

NOSOTROS PROTEGEMOS.

Confía en los productos de seguridad para detección de metal y escaneo térmico Garrett.

GARRETT Multi Zone

GARRETT

Foto: - Freepik

El servicio se traducirá como tareas realizadas por el sistema de control de acceso, a fin de contar con indicadores de distintos tipos: cantidad de personas/vehículos que engrosan la base de datos, trazabilidad de las personas/vehículos que se encuentran o encontraban dentro de las instalaciones, etc.

Por proceso, se concebirá como la realización de diversas fases para la consecución óptima del servicio. Como muestra, se podrá decir que para agregar a una persona/vehículo a la base de datos que conformará el sistema, es necesario contar con los subsistemas de gestión de identidades biométricas y de control de acceso vehicular, que permitirán el agregado de las personas/vehículos a la base de datos.

El servicio se traducirá como tareas realizadas por el sistema de control de acceso, a fin de contar con indicadores de distintos tipos: cantidad de personas/vehículos que engrosan la base de datos, trazabilidad de las personas/vehículos que se encuentran o encontraban dentro de las instalaciones, etc.

También es importante destacar que el sistema de control de acceso debe estar respaldado por un *software* accesible en la operación con el personal que se encuentra de servicio frente a una estación de trabajo (usuario final); en los casos en que por reglas de operación de la instalación, éste sea el responsable de atender solicitudes de aperturas de puertas de manera remota; así como de la verificación de la persona/vehículo que solicita dicho acceso (complementándose a través de diversos sistemas tecnológicos, como puede ser un sistema de Circuito Cerrado de Televisión o de reconocimiento facial para procesos automatizados).

Foto: - Freepik

De manera enunciativa, los sistemas de control de accesos y sus componentes que ofrecen diversos proveedores son:

- Control de acceso de personal.
- Identidad biométrica.
- Acceso para puertas.
- Control acceso vehicular.

No se debe de olvidar que, cualquier empresa que ofrece los servicios de un sistema de control de accesos, debe contar con: personal especializado/certificado, pólizas de mantenimiento del fabricante, *software,* licenciamiento, actualizaciones, *firmware,* insumos, consumibles, refacciones e interfaces necesarias para intervenir cualquiera de los equipos; asimismo, realizar mantenimiento preventivo, predictivo y correctivo, que interrelacionados permiten la correcta operación del sistema.

Al final, el éxito de un sistema de control de accesos dependerá, como en toda relación hombre-máquina, en la calidad de la interacción de los equipos tecnológicos con los procesos y procedimientos de operación de la organización, así como la capacitación/experiencia del personal. ■

José Leonardo Gómez Ruiz, Mtro. en Seguridad Industrial y Protección Ambiental con experiencia como jefe-subjefe de Monitoreo en Departamentos de Centro de Control y Comunicaciones de diversos Centros Penitenciarios. Más sobre el autor:

Protectio
Seguridad Logística

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

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

ESR EMPRESA SOCIALMENTE RESPONSABLE

COPARMEX CIUDAD DE MÉXICO

AMESP

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

TELECOMUNICACIONES:
UN SERVICIO DE MISIÓN CRÍTICA QUE GARANTIZA LA CONTINUIDAD DE LOS SISTEMAS DE SEGURIDAD

En SISSA Monitoring Integral contamos con 12 años de experiencia en el diseño, implementación, migración y mantenimiento de grandes centros de datos y soluciones de redes de misión crítica, impulsando el cumplimiento de los objetivos de negocio y seguridad de nuestros clientes

MÉXICO | Jamín Castillo Ocampo

Como suele pasar con los servicios más esenciales, las telecomunicaciones, al funcionar correcta y adecuadamente, pasan completamente desapercibidas para la mayoría de las personas; en cambio, si llegasen a fallar por tan sólo un segundo, las consecuencias de este suceso podrían ser catastróficas para la operación y economía de las organizaciones.

¿QUÉ SON LAS TELECOMUNICACIONES?

Definamos en pocas palabras este concepto. Entendemos por telecomunicaciones al conjunto de procesos y dispositivos conectados a una red de datos para la transmisión y recepción de información a distancia. En este sentido, podemos decir que las telecomunicaciones fungen como una portadora de señales de audio y video, datos, documentos, y cualquier tipo de información digital para dar funcionamiento a múltiples dispositivos, como teléfonos, computadoras, cámaras de seguridad, sistemas de control biométrico, entre otros.

UN SERVICIO DE MISIÓN CRÍTICA

Las telecomunicaciones se destacan por brindar un servicio de misión crítica, el cual se encarga de asegurar la operación ininterrumpida de todos los sistemas de una organización —especialmente de los sistemas de seguridad—, garantizando así el funcionamiento continuo e ininterrumpido de todas las tecnologías que convergen en un centro de monitoreo y control, como cámaras de videovigilancia, sensores y teléfonos. En otras palabras, las telecomunicaciones ofrecen un servicio de misión crítica para instalaciones de alta criticidad.

¿CÓMO PROTEGER TUS TELECOMUNICACIONES?

Dado que las redes de telecomunicaciones transmiten información sensible y crítica para los negocios, es importante que este medio o servicio de comunicación crítica cuente con los esquemas de seguridad necesarios para cumplir su tarea eficazmente, como la autenticación de protocolos de infraestructura y mecanismos de encriptación de comunicaciones, los cuales se encargan de evitar interferencias que puedan vulnerar la información sensible de las organizaciones.

Es importante tener siempre presente que una red de telecomunicaciones no acepta degradaciones (afectación parcial) ni mucho menos interrupciones en su servicio.

Aunado a esto, los proveedores de servicios de telecomunicaciones deben implementar políticas y estándares de seguridad robustos a fin de garantizar la integridad, la confidencialidad y la disponibilidad de los datos transmitidos, así como prevenir cualquier tipo de ataque o vulnerabilidad que pueda comprometer la seguridad de un negocio u organización.

BENEFICIOS DE UNA CORRECTA IMPLEMENTACIÓN

La implementación y adecuado mantenimiento de un servicio de telecomunicaciones aporta numerosos beneficios para las organizaciones que dependen de la continuidad de sus sistemas y tecnologías de seguridad. A continuación, te presentamos los más destacables:

- **Alta disponibilidad y redundancia:** permite mantener la continuidad del negocio en caso de fallas. Esto se logra a través de la conmutación automática del tráfico hacia dispositivos de respaldo, lo que minimiza los tiempos de interrupción y asegura la continuidad de los servicios.
- **Reducción de costos:** evita pérdidas económicas significativas a causa de la interrupción de las operaciones o productividad, lo que también protege la reputación de las organizaciones. Además, las telecomunicaciones permiten compartir una infraestructura centralizada de telefonía, sistemas de gestión, bases de datos y otros tantos dispositivos ubicados en diversos sitios remotos de una manera segura y sin necesidad de utilizar enlaces e infraestructura dedicados que tienen un costo operativo muy elevado.
- **Experiencia del usuario:** garantiza una experiencia ágil y sin interrupciones, lo que mejora la eficiencia operativa y la satisfacción de las personas que lo utilizan.

¿CÓMO SE IMPLEMENTA UNA RED DE TELECOMUNICACIONES?

Para garantizar una implementación eficaz de una red de telecomunicaciones, es necesario atravesar por distintas etapas, las cuales se describen a continuación de manera general:

- **Evaluación:** los especialistas deben evaluar y analizar las expectativas del cliente y los requerimientos técnicos del proyecto para dimensionar los dispositivos por implementar.
- **Diseño:** posteriormente, los especialistas diseñan diagramas físicos y lógicos, flujos de datos, esquemas de seguridad, segmentaciones de redes y datos, a fin de garantizar el cumplimiento de los estándares de seguridad y el correcto funcionamiento de la red.
- **Pruebas de funcionamiento:** luego de concluir la etapa de diseño, es importante realizar pruebas a los equipos a fin de mitigar todo tipo de fallas en su funcionamiento, mismas que dependerán de la robustez y criticidad de las soluciones. En el caso de las soluciones de alta criticidad, las pruebas para verificar su alta disponibilidad suelen ser muy exhaustivas, ya que se busca eliminar cualquier riesgo de degradación en los servicios de comunicación.
- **Suministro:** una vez realizadas las pruebas y comprobar que no existe ningún error, es momento de suministrar la solución y hacer entrega del inventario.
- **Pruebas de comprobación:** en un ejercicio de transparencia y profesionalismo, los especialistas deben correr protocolos de pruebas en presencia del usuario final y auditores externos, a fin de corroborar el perfecto estado de la solución implementada.

MONITOREO CONTINUO PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO

Aunque dichas etapas son las mínimas necesarias para entregar una solución que ofrezca un servicio de misión crítica funcional, es importante monitorear de manera constante su infraestructura, incluyendo desde los CPU y memorias, hasta la capacidad de conmutación y el consumo en interfaces usadas.

Afortunadamente, hoy día existen herramientas especializadas para el correcto monitoreo de telecomunicaciones, las cuales, con ayuda de miles de sensores desplegados en la red, identifican fallas o cambios inesperados en la infraestructura y emiten diversos tipos de alertas (alarmas sonoras, mensajes de texto, llamadas de voz) para que los ingenieros o personal responsable sea capaz de actuar de manera oportuna y evitar interrupciones en el servicio.

Los proveedores de servicios de telecomunicaciones deben implementar políticas y estándares de seguridad robustos a fin de garantizar la integridad, la confidencialidad y la disponibilidad de los datos transmitidos

INTEGRAMOS SOLUCIONES, ENTREGAMOS RESULTADOS

En SISSA Monitoring Integral contamos con 12 años de experiencia en el diseño, implementación, migración y mantenimiento de grandes centros de datos y soluciones de redes de misión crítica, impulsando el cumplimiento de los objetivos de negocio y seguridad de nuestros clientes.

Tal es el caso del último proyecto que hemos desarrollado este 2023, en el cual gestionamos una red de datos de más de 200 equipos interconectados y miles de dispositivos cliente distribuidos en al menos 13 subsistemas de misión crítica, con todas las implicaciones técnicas que esto supone.

En SISSA Monitoring Integral buscamos brindar soluciones personalizadas que se adapten a las necesidades específicas de cada uno de nuestros clientes, sin estar limitados por marcas o fabricantes específicos, asegurando así la confiabilidad, la seguridad y la continuidad de las soluciones de telecomunicaciones suministradas. ■

Fotos: SISSA Monitoring Integral

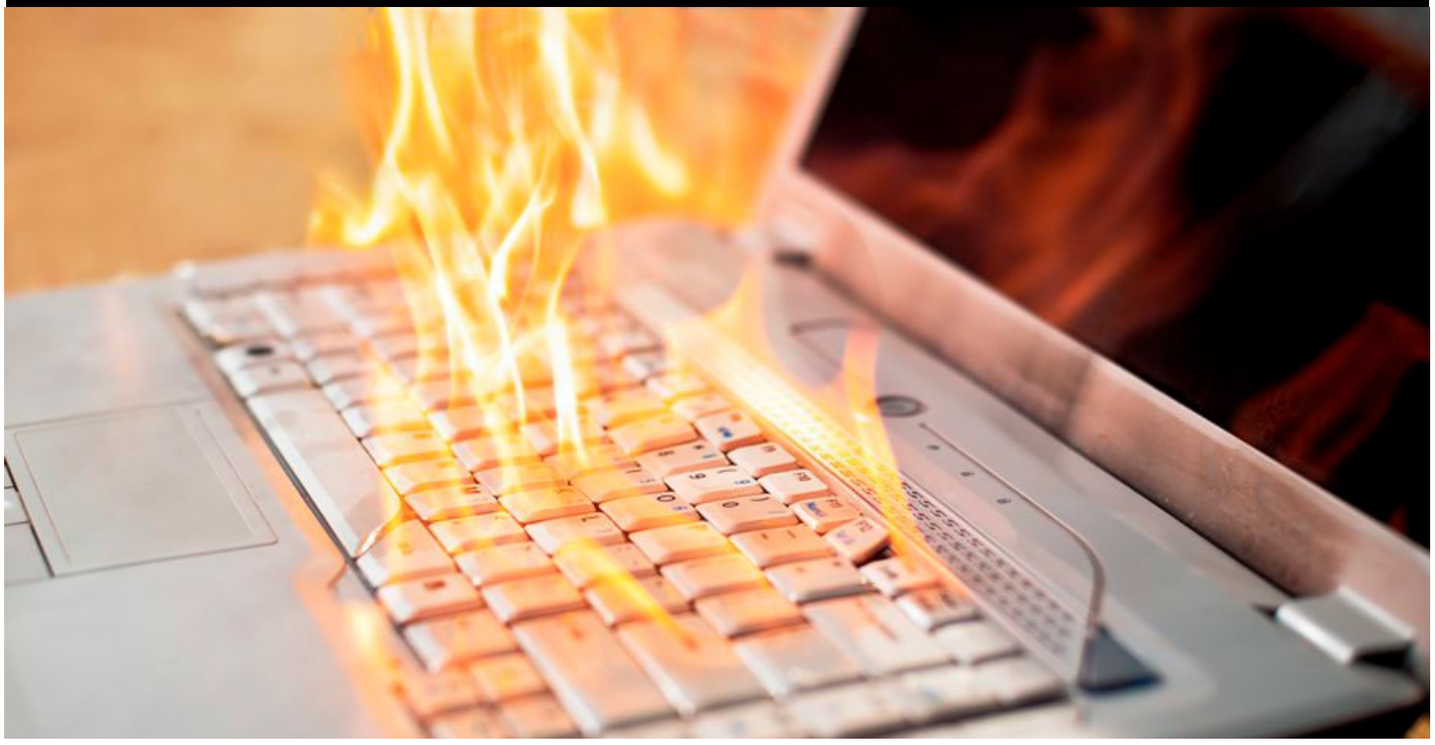
Jamín Castillo Ocampo, director de Operaciones en SISSA Monitoring Integral. Más sobre el autor:

Columna de
Jaime A. Moncada, PE
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:

LAS BATERÍAS DE LITIO *Y SU RIESGO DE INCENDIO*



Aproximadamente el 90% de los SAEBs hoy día utilizan baterías de iones de litio, porque estas proporcionan una alta densidad de energía en un paquete pequeño y liviano y requieren poco mantenimiento

EUA

Aunque la batería de litio es un avance tecnológico reciente, hoy día este tipo de batería se encuentra por todas partes, desde *laptops* y celulares, hasta bicicletas eléctricas (*eBikes*), automóviles eléctricos y grandes sistemas de almacenamiento de energía. Incendios recientes en aviones, automóviles, edificios y parques de generación eléctrica han puesto en relieve la necesidad de mejores métodos de seguridad y mayor entendimiento sobre su protección contra incendios. Por ejemplo, un tipo de incendio que recientemente ha empezado a ser reportado en los edificios en Estados Unidos es aquel iniciado por una *eBike* siendo recargada dentro de un edificio de apartamentos.

Las baterías de litio más grandes se encuentran en un Sistema de Almacenamiento de Energía en Batería (SAEB). El SAEB es un medio para almacenar importantes cantidades de electricidad para su uso posterior. Un SAEB puede variar desde sistemas de tamaño residencial hasta grandes conjuntos de uso comercial. Tal vez el uso más popular es el almacenamiento del exceso de producción de energía a partir de fuentes renovables, como en una granja solar, la cual puede almacenar energía en periodos de alta producción, y durante los periodos de baja producción de energía, puede utilizar y poner en línea esta energía almacenada.

SISSA DIGITAL

www.sissadigital.com

SISSA DIGITAL

IXMAKI

SISTEMA DE GESTIÓN DE IDENTIDAD

SISTEMA DE **GESTIÓN DE IDENTIDAD**

Garantiza la seguridad física de tus estudiantes, y optimiza la gestión de los trámites y servicios académicos de tu centro educativo:

- **Control** de acceso
- **Registro** de personas autorizadas para la entrega de estudiantes
- **Identificación y seguimiento** de estudiantes en aulas, exámenes y excursiones
- **Administración y control** de servicios y equipo didáctico
- **Registro y control** de visitantes

CONTÁCTANOS

55 6651 0200

WWW.IXMAKI.COM.MX

Aunque se continúa investigando y aprendiendo sobre los incendios en las baterías de litio, sabemos que estas baterías son muy sensitivas a las altas temperaturas y son inherentemente combustibles

Aproximadamente el 90% de los SAEBs hoy día utilizan baterías de iones de litio, porque estas proporcionan una alta densidad de energía en un paquete pequeño y liviano y requieren poco mantenimiento. El mecanismo de la batería de iones de litio está inmerso en un electrolito conductor de iones. El electrolito es un disolvente líquido inflamable de baja viscosidad.

Las baterías de iones de litio juntas, en una carcasa o contenedor, se llaman "celdas". Un SAEB puede contener docenas a miles de celdas para almacenar energía. Las celdas generalmente se empaquetan en módulos sostenidos en bastidores, y los bastidores normalmente se almacenan en estructuras como puede ser un contenedor.

EL RIESGO DE INCENDIO

Cada vez que se comprime una gran cantidad de energía en un espacio reducido, existe el riesgo de que se escape esta energía de manera incontrolada. Cuando esto sucede, el fuego es un resultado común y las explosiones son también posibles. Varios incidentes recientes en grandes instalaciones de SAEB demuestran la magnitud de este tipo de incendios, su dificultad en extinguirlos y el riesgo para los bomberos que responden al incendio.

En julio de 2021, en Moorabool, Victoria, Australia ocurrió un incendio en un parque de baterías llamado "*Victorian Big Battery*". Este parque estaba compuesto de 212 "*Megapacks*", la manera como Tesla llama sus contenedores de SAEB, que conjuntamente tenían una capacidad instalada de 300 MW.

La investigación del incendio apuntó a una fuga de refrigerante líquido que causó arcos en las celdas de batería, escape térmico (*thermal runaway*) y una reacción en cadena. El incendio duró cuatro días y los bomberos tuvieron problemas importantes durante el ataque del incendio y sólo pudieron refrigerar los contenedores adyacentes no incendiados, para que no creciera el incendio.

Por ejemplo un incendio de un vehículo eléctrico con baterías de litio puede ser un incendio mucho más intenso que el de un vehículo con motor de combustión y puede durar mucho más. El *website* de Tesla dice que un incendio de baterías puede durar 24 horas en extinguirse.

LA CAUSA DE LOS INCENDIOS CON BATERÍAS DE LITIO

Aunque se continúa investigando y aprendiendo sobre los incendios en las baterías de litio, sabemos que estas baterías son muy sensitivas a las altas temperaturas y son inherentemente combustibles. Aunque las baterías han sido diseñadas con varias medidas de seguridad, los riesgos de incendios pueden ocurrir por defectos de manufactura; defectos en el diseño, como por ejemplo durante su uso compacto en un nuevo automóvil; uso inapropiado o anormal, como cuando están cerca a una fuente de calor; cuando hay problemas con los cargadores que permitan sobre recarga; o cuando tienen componentes de baja calidad.

En un incendio de una celda de batería de litio ocurre fuga térmica (*thermal runaway*), o sea una reacción en cadena en la que la reacción exotérmica de una celda de batería defectuosa sobrecalienta una celda de batería adyacente. Es decir, la celda libera rápidamente su energía almacenada, y cuanta más energía haya almacenada en una celda, más energética y fuera de control será la reacción térmica. La batería adyacente falla de manera similar y, a su vez, sobrecalienta otras baterías.

El fuego puede sobrevenir rápidamente después de evolución de humo, aunque el evento de fuga térmica puede continuar durante horas sin ninguna producción de llama. Durante este período, se producen grandes cantidades de vapores y gases inflamables que se contienen en el recinto creando una atmósfera explosiva. En muchos casos, sin embargo, se produce una ignición y se desarrolla un incendio dentro del contenedor. A medida que los componentes de la batería son consumidos por el fuego, los gases combustibles no quemados se acumulan en el recinto. El fuego dentro del recinto puede aumentar la velocidad de la fuga térmica, lo que lleva a un evento devastador y difícil de extinguir.

GSI
SEGURIDAD PRIVADA

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

Profesionales en Seguridad Privada

Oficiales de Seguridad

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

SOMOS GRUPO GSI,

Orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx

atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

ESR Empresa Socialmente Responsable

redconocer

DNV·GL

AMESP

EMPRESAS DE GSI GRUPO SEGURIDAD INTEGRAL

BASC

A nivel comercial existen hoy día miles de diferentes artefactos que contienen baterías de litio, siendo éstas la fuente de energía más común desde celulares hasta *laptops*. Por consecuencia, existen inmensas bodegas que almacenan las baterías que se usan para reemplazar estas baterías

CRITERIOS DE PROTECCIÓN

La NFPA recientemente desarrolló la norma NFPA 855, *Standard for the Installation of Stationary Energy Storage Systems*. Esta norma establece criterios mínimos para mitigar los riesgos asociados con sistemas de almacenamiento de baterías y se puede utilizar cuando las baterías de litio exceden una capacidad agregada de 20 kWh. Esta norma por ejemplo establece criterios de separación, y cuando se debe usar detección y sistemas de rociadores automáticos. Cuando se usen sistemas de extinción que no sean rociadores se deben analizar las posibilidades con gran cautela. La norma también establece recomendaciones durante el combate del incendio. Como ocurre con otras normas de la NFPA, esta norma debe ser utilizada con el apoyo de un consultor en ingeniería de incendios con experiencia en la utilización de esta norma.

ALMACENAMIENTO DE LAS BATERÍAS DE LITIO

A nivel comercial existen hoy día miles de diferentes artefactos que contienen baterías de litio, siendo estas la fuente de energía más común desde celulares hasta *laptops*. Por consecuencia existen inmensas bodegas que almacenan las baterías que se usan para reemplazar estas baterías. Por esa razón, el sector asegurador ha estado muy preocupado de cómo proteger el almacenamiento de baterías de litio en bodegas, pues no existe en la NFPA 13, la norma de diseño de rociadores automáticos, criterios de cómo proteger este riesgo.

A raíz de esto la *Fire Protection Research Foundation* (FPRF) de la NFPA evaluó este problema, con el apoyo de FM Global, y las conclusiones muestran, que bajo ciertas condiciones las baterías se pueden proteger con rociadores. FM Global por ejemplo recomienda el uso de rociadores dentro de las estanterías (*in-rack*). Sin embargo, estas investigaciones aún preliminares, no han producido un criterio consensuado de protección. La mejor manera de evaluar las opciones de protección para este riesgo es con el apoyo de una firma de ingeniería de protección contra incendios.

Debo mencionar que existe una idea errónea de que el agua aumenta el peligro en un incendio de batería de iones de litio. Esta idea equivocada posiblemente se deba a la confusión de las baterías de iones de litio (UN 3480) con las baterías de metal de litio (UN 3090), las cuales son normalmente no recargables.

Las baterías de metal de litio contienen metal de litio libre, y si se aplica agua durante la combustión del metal de litio, se liberarán cantidades considerables de hidrógeno. Este gas se quemará, intensificando el fuego, lo que resultará en un rápido aumento de calor y una reacción similar a una explosión. Sin embargo, a diferencia de las baterías de metal de litio, no hay metal de litio libre dentro de una batería de iones de litio, por lo que este fenómeno no puede ocurrir. ■

Fotos: Cortesía de Jaime A. Moncada, PE

EL MEJOR ALIADO EN
SEGURIDAD Y MONITOREO
PARA TU NEGOCIO Y OPERACIONES

RASTREO MONITOREO VISÍTANOS SOS ALARMAS CCTV

www.skyangel.com.mx

(55) 5687 9011 Ext. 400-405
info@skyangel.com.mx

+1 (956) 568 3611
info@skyangelguard.us

/SkyangelGPS /company/SkyangelMx /SkyangelGPS

MAK EXTINGUISHER
INAUGURA SUCURSAL DE MAK OCCIDENTE

MÉXICO

La empresa integradora más experimentada de México en sistemas contra incendio, inspección, videovigilancia y control de acceso, abrió una sucursal en Guadalajara, Jalisco

Con especial cariño por la zona de Occidente, como lo mencionó en su discurso de inauguración la Mtra. Perla Liliana Ortega Porcayo, Directora General de MAK Extinguisher de México, se dio el banderazo de arranque de operaciones a la Sucursal de MAK Occidente el pasado 12 de mayo en Guadalajara, Jalisco.

Fueron momentos emotivos al recordar por parte de la Directora General y el Ing. Javier Fernández Soto, quien con gusto asumió la dirección de esta sucursal, los que se vivieron en ambas participaciones, los dos coincidieron en que la confianza de los clientes y el apoyo de los colaboradores es sin duda la clave para la continuidad y expansión de las operaciones de MAK Extiguisher, una empresa que ya cuenta con más de 40 años de existencia y cuyo enfoque actual para lograr mayores y mejores resultados se centra en la cultura organizacional, el aprendizaje y la innovación.

"En ocasiones, se piensa que ya nos ha tocado vivir y aprender todo en la vida, sobre todo cuando uno pertenece a la actual generación con juventud acumulada, pero las sorpresas siempre están ahí para todos y no cabe duda que día con día se aprende cosas nuevas, sólo hay que estar abierto a seguir actualizándose y preparándose para ir hacia adelante", mencionó el Ing. Javier Fernández, cuando narraba la forma en la que está propuesta por parte del Lic. José Arturo Ortega Porcayo para ser el encargado de esta nueva aventura que MAK Extinguisher tenía en mente.

SIN PRETEXTOS

"Estoy convencida que en México con más de 90% de micro, pequeñas y medianas empresas, el sector empresarial es columna vertebral para un cambio estructural así sin pretexto", concluyó la Mtra. Perla Ortega Porcayo, como parte de una reflexión sobre los últimos años en donde no sólo México, sino el mundo entero se ha visto transformado para asumir retos como la pandemia, cierres de empresas, despidos masivos, inseguridad y economía.

Sin duda los intangibles como la pasión y servicio fueron los poderosos motores que motivaron los corazones de quienes materializaron esta expansión y fue en el marco de este gran evento que contó con la presencia de representantes de los aliados comerciales de MAK como SIEMENS, ADISES y amigos de asociaciones como Seguridad por México, ASUME (Asociaciones de Seguridad Unidas por México), UNESPA y ASIS Capítulo Occidente. ■

Fuente y fotos: Mak Extinguisher

CIBERSEGURIDAD Y TRANSPORTE EN LA INDUSTRIA FARMACÉUTICA

Las empresas farmacéuticas han comprendido las necesidades de seguridad y protección en todos los niveles de su organización: satisfacción al operario, consecución de los objetivos de gestión del centro y cumplimiento de los aspectos normativos y de gestión de costos

Foto: - Freepik

MÉXICO | José Luis Sánchez Gutiérrez

Estimados lectores, muy agradecido por su acostumbrada preferencia; y en esta ocasión tocaremos el tema de la Seguridad en la Industria Farmacéutica.

Siempre nos preguntamos: ¿Cómo debe ser la seguridad y protección en el servicio de farmacias? Y la básica respuesta es: que todas las áreas correspondientes al Servicio de Farmacia deben tener un área física exclusiva, alejada de áreas contaminadas, independiente y de circulación restringida, donde los pisos deben ser de materiales impermeables, resistentes y deben contar con sistema de drenaje que permita su fácil limpieza y sanitización. Y en seguridad, tener personal que atiende la unidad de negocio estando perfectamente capacitado y entrenado, que las instalaciones cuenten con CCTV, sistema de alarma, botón de pánico, área restringida de productos controlados, etc.

Y cuando nos referimos a los temas específicos de seguridad en las compañías farmacéuticas, identificamos cinco grandes riesgos por temas de ciberataques, con los montos millonarios que implican. En la industria farmacéutica se es consciente de las consecuencias catastróficas que puede suponer un ciberataque contra sus sistemas informáticos. Al trabajar con datos extremadamente sensibles, como información sobre pacientes, medicamentos y dispositivos médicos, es necesario implementar medidas fuertes y consistentes de ciberseguridad para garantizar la integridad y privacidad de dicha información. A pesar de la importancia de la ciberseguridad en todos sus procesos y tareas, la industria farmacéutica no avanza en este aspecto al mismo ritmo que otros sectores, lo que ha creado un nuevo sentido de urgencia.

Un ataque cibernético supondría, para una farmacéutica, grandes pérdidas en diferentes ámbitos (impacto en el precio de las acciones, pérdida de prestigio y confianza en la marca, por ejemplo), por lo que los consejos de administración deben comprender los grandes riesgos que suponen las vulnerabilidades, para poder así aplicar las medidas adecuadas para solventarlos.

Estos son los cinco hechos relacionados con la ciberseguridad, que son una realidad hoy en día para las empresas farmacéuticas:

Una de las grandes ventajas de la clasificación de información es que se puede automatizar, lo que aporta resultados inmediatos y no supone un gran impacto en los costos

Con medidas exigentes a la hora de otorgar privilegios de administrador o con los famosos superusuarios, se reduce el número de personas que tienen acceso a datos realmente importantes, siendo mucho más sencillo y eficiente realizar un seguimiento y vigilancia sobre quién, cuándo y cómo accede a esa información sensible

1. LA REALIDAD DE LOS CIBERATAQUES

Los ciberataques han dejado de ser algo puntual, o propio de la ficción. Hoy en día es habitual que los sistemas informáticos, de grandes y medianas empresas, sufren distintos ataques de manera periódica.

Para los ciberdelincuentes, las farmacéuticas se encuentran entre sus principales objetivos debido a los datos de gran valor que manejan (como la propiedad intelectual de los fármacos, por ejemplo). Incluso en la actualidad, las empresas del sector salud se sitúan como objetivo prioritario por delante de otros sectores, como el comercio minorista.

Las empresas de este sector que aún están esperando señales de advertencia para invertir en ciberseguridad se encuentran en una situación de alto riesgo, y necesitan una acción inmediata, pues están muy retrasadas respecto a la realidad en la que operan.

2. EL CIBERATAQUE INTERNO

La evolución de los ataques informáticos es evidente, pues los ciberdelincuentes se van adaptando a los avances tecnológicos y a las nuevas medidas de protección. En un entorno globalizado y digitalizado como el actual, las farmacéuticas son el blanco de muchos ciberataques realizados desde los países externos, que buscan extraer datos confidenciales de medicamentos o de los propios pacientes.

Una de las formas habituales de este tipo de ataques es la de infiltrar a un usuario en el organigrama de la farmacéutica para que identifique datos de valor. Los ciberdelincuentes también captan a empleados descontentos o que se enfrentan a procesos de despido, para que les puedan facilitar información valiosa, como direcciones IP a atacar o localización de bases de datos con datos clave.

3. LA IMPORTANCIA DE CLASIFICAR LA INFORMACIÓN

Para poder implementar un buen sistema de protección de la información de una farmacéutica se hace indispensable realizar una buena organización de los datos que maneja. De esta manera, es más sencillo monitorizar y controlar el acceso a información realmente valiosa y tener una trazabilidad precisa de la misma.


Foto: - Freepik

Una de las grandes ventajas de la clasificación de información es que se puede automatizar, lo que aporta resultados inmediatos y no supone un gran impacto en los costos. En este aspecto es muy importante destacar que las empresas del sector manejan gran cantidad de información, mucha de ella no estructurada. Esto quiere decir que no basta con etiquetar datos, y que es necesario la aplicación de nuevas tecnologías para identificar los datos de mayor valor y así poder protegerlos (inteligencia artificial).

4. MEDIDAS CONTRA LOS ATAQUES INTERNOS

Uno de los grandes riesgos de las farmacéuticas, como ya comentamos anteriormente, vienen de los ataques o filtraciones internas. Contar con una buena política de seguridad es indispensable para evitar o minimizar el impacto de este tipo de ataques, que vienen desde dentro de la organización.

La gestión de las credenciales de acceso a la información juega un papel fundamental en esta lucha contra los ataques internos. Con medidas exigentes a la hora de otorgar privilegios de administrador o con los famosos superusuarios, se reduce el número de personas que tienen acceso a datos realmente importantes, siendo mucho más sencillo y eficiente realizar un seguimiento y vigilancia sobre quién, cuándo y cómo accede a esa información sensible.

Las nuevas soluciones de ciberseguridad implementan cambios en este tipo de cuentas con accesos privilegiados, impidiendo que puedan borrar el rastro de sus acciones. Esto evitará muchas filtraciones que se realizaban en el pasado, y que eran indetectables para las empresas del sector, incrementando de forma notable el nivel de seguridad de la industria sobre sus datos y sistemas.

5. LA CIBERSEGURIDAD COMO FILOSOFÍA DE EMPRESA

La gran solución a los desafíos en seguridad de la industria farmacéutica tiene lugar en la implantación de una filosofía de empresa enfocada en la ciberseguridad. En todas las decisiones que se tomen, a cualquier nivel dentro de las empresas del sector, la ciberseguridad debe estar siempre presente para poder implementar las medidas adecuadas que eviten vulnerabilidades, así como mantener los datos y sistemas bien protegidos.

Se trata de concienciar a los trabajadores de las farmacéuticas, en todas las áreas y niveles, de la importancia y prioridad de la seguridad para la empresa. Conseguirlo, requiere un cambio de paradigma, descentralizando la ciberseguridad e implementando procesos de seguridad en las acciones habituales del día a día de la empresa.


Foto: - Freepik

El uso de herramientas modernas y automatizadas de ciberseguridad facilitan la implantación de esta filosofía en la empresa, adaptándose a sus necesidades, ayudando en la organización del personal, automatizando procesos de ciberseguridad, sin que suponga un gran impacto económico y en los procesos que se realizan de manera habitual en la actividad de la empresa.

El sector farmacéutico se está enfrentando a una situación de máxima alerta en relación con los ataques que reciben, con el fin de extraer su información más valiosa. La gran dependencia tecnológica y el uso de herramientas en la Nube hace necesario que las empresas del sector añadan el aspecto de la seguridad en cualquier decisión que tomen en su negocio. Se trata de abrazar la ciberseguridad como un elemento común a toda la empresa, abandonando la postura tradicional de centralizar todo lo que tenga que ver con la protección de información y sistemas.

Implementar un buen plan de respuesta ante incidentes de seguridad es una de las claves para prevenir ataques y minimizar su impacto. Además, enriquecer los controles de acceso a información sensible, tanto a nivel digital, como físico, se hace indispensable para evitar la fuga de datos.

Si las empresas del sector no entienden todos los vectores de amenaza a los que están expuestos, difícilmente podrán dar una respuesta en ciberseguridad adecuada. Las farmacéuticas necesitan un plan sólido y eficiente para poder defenderse de los ciberataques a los que son sometidas de forma habitual, tanto desde el exterior, como a nivel interno. Se tiene que crear y desarrollar estrategias y soluciones IT para estas compañías.

CADENA LOGÍSTICA EN FARMACÉUTICA

También debemos considerar que hay puntos que son clave para el transporte farmacéutico. Tengo que comentarles que el transporte farmacéutico es la parte más importante en una cadena logística, porque los productos que se están transportando son para el consumo humano. Por lo tanto, hay que tener un control increíblemente exhaustivo de toda la cadena de distribución para asegurar que los medicamentos lleguen al consumidor en perfectas condiciones.

El fabricante de productos farmacéuticos siempre le va a exigir al operador logístico que cuando manipule y transporte este tipo de mercancías se cumplan todos los requisitos exigidos. La seguridad, la trazabilidad o el mantenimiento de la temperatura en el transporte farmacéutico son elementos críticos y clave que todo operador logístico debe garantizar.

Como ejemplo, una normativa importante, que en la Unión Europea se exige a fabricantes y a empresas de transporte o proveedores de servicios logísticos, es la referida a las Buenas Prácticas de Distribución, GDP *(Good Distribution Practices)*. La normativa DGP obliga al operador de transporte farmacéutico a cumplir diversos requisitos relacionados con la trazabilidad de los productos y la seguridad en las instalaciones.

Se trata de una reglamentación, también denominada BPDs, para garantizar la seguridad y la calidad en la distribución de medicamentos, que son altamente sensibles. Por tanto, regula aspectos como los equipamientos e instalaciones, el seguimiento documental, el transporte, la limpieza de los vehículos, la monitorización de la temperatura o la logística inversa.

Es importante destacar que la cadena logística de un producto farmacéutico empieza en el momento en el que se fabrica en el laboratorio hasta que llega al consumidor final. En esta cadena hay actividades de almacenamiento, de traslado a los centros de distribución de los operadores y de transporte final desde estos centros hasta las farmacias u hospitales.

Para el caso de los profesionales cualificados (en la cadena logística del amplio abanico de productos farmacéuticos que existen), exige que los operadores estén altamente especializados de forma permanentemente.

El equipo humano siempre debe estar preparado para asegurar la trazabilidad de la temperatura, desde la carga hasta la entrega de la mercancía, y para solventar cualquier incidencia que pueda surgir.

Un entorno de trabajo saludable y seguro es una condición esencial e innegociable. Este principio se traslada a los empleados mediante una cultura de seguridad interdependiente que equilibre la proactividad y la disciplina, siempre con el fin de cumplir las políticas internas de Salud y Protección Medioambiental, así como las normas nacionales e internacionales.

Las empresas farmacéuticas han comprendido las necesidades de seguridad y protección en todos los niveles de su organización: satisfacción al operario, consecución de los objetivos de gestión del centro y cumplimiento de los aspectos normativos y de gestión de costos; además de la incorporación de medidas preventivas que eviten el robo de este tipo de mercancía durante su trayecto (incorporando todo lo que ustedes, como expertos en seguridad, ya conocen: cámaras de CCTV interiores y exteriores, bloqueo de quinta rueda, apertura remota de chapas electromecánicas, botones de pánico con audio a dos vías, velocidad ralentí para evitar accidentes al parar el motor, remotamente bajar la presión de aire de los neumáticos, geocercas con sistemas RFID y GPS para su trazabilidad, sensor en el asiento del copiloto para saber si hay alguien en ese lugar, sensor en el cinturón de seguridad para saber si está alguien al volante o conocer los movimientos del operador, sensor biométrico que dé arranque de inicio al motor del vehículo, etc.). ■

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

SOMOS LÍDERES EN SEGURIDAD

PROTEGE

Servicios de Seguridad Privada S.A. de C.V.
Seguridad Privada Armada

GUARDIAS INTRAMUROS

CUSTODIA ARMADA A TRASLADO DE VALORES

CUSTODIA ARMADA A TRANSPORTE DE CARGA

CONTACTO

Leona Vicario No. 6 Cuautitlán Izcalli

ventas@gcprotege.com

55 7931 6739

SÍGUENOS EN REDES SOCIALES

@protegeseguridadprivada

@protegeseguridadprivadasadecv

@protege_privada

ASIS INTERNATIONAL CAPÍTULO MÉXICO 217

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

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

LA GOBERNANZA DE LOS DATOS PERSONALES

La protección de los datos personales es un elemento clave en el actual contexto tecnológico y es responsabilidad de todos evitar su mal uso y cumplir la normativa sobre su protección

ESPAÑA | José Manuel Ballester Fernández

EMPRESAS Y PERSONAS, ¿QUIÉN CONTROLA?

El pasado 28 de enero se celebró el Día Europeo de la Protección de Datos, fecha que conmemora la firma del Convenio 108 adoptado por el Consejo de Europa en 1981. Este acuerdo internacional, jurídicamente vinculante en su ámbito de actuación, fue el primer instrumento adoptado con el fin de garantizar el adecuado tratamiento de la información de carácter personal de sus ciudadanos.

Muchos han sido los aspectos que cambiaron durante estas décadas en cuanto a la recopilación, el almacenamiento y el uso de los datos personales, especialmente los relativos a las empresas de servicios de identificación y autenticación destinados al acceso a productos y servicios. Incluso el reconocimiento biométrico ha sido incluido en estas regulaciones, en tanto que su uso ha dejado de ser esporádico y se ha incorporado progresivamente a la vida cotidiana, abriéndose un debate en torno a la efectividad de su uso y a la garantía del mantenimiento de la privacidad de las personas.

La responsabilidad de los usuarios en la protección de sus datos es esencial, y un aspecto a considerar es la creación y la gestión de contraseñas y para ello la adecuada selección de las plataformas que utilicen para su identificación. Este aspecto afecta tanto a las empresas como en particular a la gente corriente, en tanto que la gestión doméstica de los datos personales en *apps* y *webs* afecta a colectivos vulnerables, sean nativos digitales como no digitales.

La aparición de los gestores de contraseñas especializados ha sido una de las respuestas tecnológicas al reto de crear contraseñas adecuadas, aun cuando no son infalibles. Son numerosos los ejemplos de *hackers* que aprovechan las brechas de seguridad de los gestores a fin de secuestrar datos personales que facilitan el acceso a aplicaciones y servicios en la red. La oferta de las empresas generalistas que funcionan como proveedores de identidades, como Google, Facebook o Apple, aun cuando ofrecen un plus de comodidad eso no implica la falta de riesgos para asegurar la privacidad en los accesos de los usuarios.

Otra controversia procede del uso de imágenes sin el consentimiento de los involucrados, asumiendo que la ingente masa de información procedente de Internet y de las redes sociales sirve de base para la creación de *software* con diferentes fines. El reciente caso del Clearview AI la empresa que aportó al Gobierno ucraniano la herramienta de reconocimiento facial para reconocer a víctimas de los ataques rusos, es paradigmático, ya que su base de datos global incluye más de 20 mil millones de imágenes utilizadas sin conocimiento y autorización de los involucrados.

LOS DERECHOS DIGITALES

La creciente digitalización de la sociedad demanda normativas y acuerdos éticos que garanticen los derechos de los ciudadanos en este ámbito. Los escenarios generados por el avance tecnológico han dado lugar a la emergencia de riesgos sociales que obligaron a adaptar los ordenamientos jurídicos vigentes a las nuevas circunstancias. Esta salvaguarda es especialmente necesaria ante los efectos aún no determinados de la aplicación de la Inteligencia Artificial en los distintos ámbitos de la realidad.

Con ese ánimo, España adoptó en 2021 la Carta de Derechos Digitales que aplican al espacio digital los derechos recogidos en la Declaración Universal de los Derechos Humanos aprobados por la ONU en 1948. El derecho a la vida, a la libertad y a la seguridad de la persona contemplado en el punto 3 de esta Carta de Derechos Digitales, considerando en los derechos humanos fundamentales el derecho digital. En este contexto, se entiende como derechos digitales aquellos vinculados a la privacidad y a la libertad de expresión y al acceso universal y el uso adecuado de Internet, de las redes de comunicación y de cualquier dispositivo electrónico, evitando la brecha digital entre personas y empresas.

Los riesgos inherentes al desarrollo de la sociedad tecnológica son globales y sus desafíos demandan la adopción de mecanismos que disminuyan los efectos no deseados inherentes a su uso. Mitigar estos efectos implica asumir una ética digital aplicada a los espacios reales y virtuales que prevenga la transgresión de derechos de los ciudadanos y de las organizaciones.

TRASECO

Training Security Company

PERSONAL OPERATIVO CUALIFICADO

(Valores, Capacitación y Adiestramiento)

Guardias intramuros

Custodia y vigilancia

Tu tranquilidad nuestra pasión

Seguridad TRASECO Privada

Protección ejecutiva

Consultoría y capacitación

SOMOS UNA NUEVA OPCIÓN EN PROTECCIÓN

Equipo Directivo con 30 años de experiencia en el Ramo

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

5524493906

5618829950

CONTRATACIONES:
ventas@traseco.com

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

AMEXSI

LA CARTA DE DERECHOS DIGITALES EN ESPAÑA, ¿QUÉ ES Y PARA QUÉ SIRVE?

La protección de los derechos individuales y colectivos de las personas, recogidos en la Constitución, y el reconocimiento de los derechos digitales se encuentran regulados por varias normativas, tales como el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, y, especialmente, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, en particular, su Título X, que adapta el derecho interno español a la regulación europea según el Reglamento General de Protección de Datos aprobado el 24 de mayo de 2016.

A fin de adaptar el marco jurídico existente a los vertiginosos cambios de la realidad digital y virtual, y de adoptar una ética digital que evite la vulneración y la puesta en riesgo de los derechos humanos, España aprobó la Carta de Derechos Digitales el 14 de julio de 2021. La Carta da respuesta a uno de los mandatos de la Agenda España Digital 2025, presentada en 2020 en el marco de la Estrategia Nacional de Inteligencia Artificial y del Plan de Recuperación, Transformación y Resiliencia, aprobado por la Comisión Europea el 16 de junio de 2021.

La Carta es un texto de referencia que aspira a situarse en la vanguardia internacional en la protección de derechos de la ciudadanía. De carácter descriptivo, prospectivo y asertivo, la Carta carece de carácter normativo y queda sujeta a las disposiciones vigentes en el ordenamiento jurídico español, por lo tanto, no crea nuevos derechos fundamentales, sino que adapta al entorno digital derechos existentes y reconocidos.

Los objetivos de la Carta son tres: ser una guía para futuras propuestas legislativas, constituirse como marco de referencia para la acción de todos los poderes públicos, y servir de inspiración para el desarrollo de políticas públicas más justas que protejan a la ciudadanía. Asimismo, la Carta define diez derechos digitales: acceso universal e igualitario, libertad de expresión, información y comunicación, privacidad y protección de datos, derecho al anonimato, derecho al olvido, protección del menor y propiedad intelectual. Algunos considerandos tienen carácter pionero, como el derecho a la no discriminación algorítmica y el derecho a solicitar intervención humana. La Carta incluye un apartado de garantías y eficacias.

LA DECLARACIÓN EUROPEA SOBRE LOS DERECHOS Y PRINCIPIOS DIGITALES

En respuesta a las dinámicas derivadas de la transición tecnológica, el 26 de enero de 2022 la Comisión Europea presentó el proyecto de Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital con el que pretende crear un marco de referencia común en la UE. Se espera su aprobación por el Parlamento y el Consejo en el verano de 2023.

El texto tiene carácter declarativo y su principal objetivo es "promover una vía europea para la transición digital que sitúe a las personas en el centro". Su objetivo redunda en la aplicación de los valores de la transformación digital y en los derechos fundamentales de la ciudadanía en el mundo digital y virtual. En este contexto, la contribución de la Carta de Derechos Digitales española ha sido inspiradora.

LA IMPORTANCIA DE PROTEGER LOS DATOS PERSONALES

La protección de los datos personales es un elemento clave en el actual contexto tecnológico y es responsabilidad de todos evitar su mal uso y cumplir la normativa sobre su protección. Varios son los mecanismos que aseguran este cometido, entre los que destacan:

- **Responsabilidad proactiva:** las organizaciones deben tanto cumplir con la normativa como tomar la iniciativa y demostrar que lo hacen, empleando auditorías o certificaciones de sus procesos.
- **Delegado de Protección de Datos:** figura relevante dentro de las organizaciones dedicado a orientar su compañía asegurando el cumplimiento de la normativa. Además de tener conocimientos de privacidad, riesgos, controles y estar al día en materia de protección de datos, el delegado ejerce de nexo de contacto con la Agencia de Protección de Datos, los titulares de datos personales y las asociaciones de profesionales en la materia.
- **Principio de transparencia:** implica que los titulares de datos personales deben ser informados de manera clara, concisa, precisa y entendible sobre sus derechos y el tratamiento esperado de sus datos.
- **Respetar y aplicar** los derechos de los afectados: necesario especificar y respetar los derechos de los titulares de datos personales. No obstante, en caso de que sean vulnerados, estos últimos han de informar a los titulares, a la Agencia de Protección de Datos, y ejecutar un plan de acción que mitigue el riesgo producido.
- **No enviar comunicaciones sin el consentimiento del interesado.**
- **Medidas organizativas y técnicas necesarias para evitar brechas de seguridad:** la normativa incluye entre sus medidas la obligatoriedad de mejorar la capacidad de prevenir y minimizar los riesgos derivados del tratamiento de la información.
- **Respetar los derechos digitales de los trabajadores:** se refiere a la no obligación de los trabajadores a utilizar dispositivos electrónicos con motivos profesionales fuera de su horario laboral.

Aplicar estas medidas en el entorno empresarial será cada vez más relevante, considerando los efectos esperados en las organizaciones y entornos de los nuevos avances tecnológicos, especialmente los relacionados con el desarrollo de la Inteligencia Artificial, los sistemas de identificación biométrica y la gestión federada de identidades. ■

José Manuel Ballester Fernández,
socio director del Área de Consultoría de TEMANOVA. Más sobre el autor:

TIMUR
Latinoamérica

GALEAM

NUESTRO VALOR, SU SEGURIDAD

SERVICIOS

GUARDIAS INTRAMUROS

PROTECCIÓN EJECUTIVA

CONSULTORÍA

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

info@galeam.mx | info@timurlatinoamerica.com

55 6840 1036 / 56 3048 9610 / 56 3700 0133

CERTIFICACIONES

CPP Certified Protection Professional

American Heart Association.

ALiCE

AVATAR 2 Y LA SEGURIDAD

COLOMBIA | Jeimy Cano

Reflexiones y recomendaciones para los profesionales de seguridad y control

INTRODUCCIÓN

Dicen los militares que en los conflictos todo es distracción y engaño. Recientemente luego de haber visto la última producción de James Cameron ("Avatar. El camino del agua") se advierten algunas estrategias y lecciones que los ejecutivos de seguridad/ciberseguridad deben recordar con el fin de tratar de mantenerse un paso delante de los retos de sus adversarios.

Sin pretender hacer un "*spoiler*" de la cinta cinematográfica, se presentan a continuación algunas reflexiones tomadas de diferentes momentos de esta película, como elementos claves a tener en cuenta por los profesionales de seguridad/ciberseguridad para avanzar en la comprensión del adversario y sus estrategias.

1. EL ADVERSARIO TIENE MOTIVACIÓN Y UNA MISIÓN, POR LO TANTO PERSISTIRÁ DE DIFERENTES MANERAS PARA LOGRAR SU OBJETIVO

Esta primera consideración habla de las amenazas que son persistentes (avanzadas o no avanzadas) que se generan por cuenta de una misión, que leído en lenguaje militar se trata de la razón de ser de una operación (que lleva en sí misma una orden) y por lo tanto todo los implicados saben que deberán utilizar todos los medios disponibles para lograr la encomienda. No hacerlo es desobedecer una orden, y comprometer la esencia misma del orgullo de los participantes, que termina con deshonra y afectando la autoestima de los operadores.

Estudiar al adversario, sus motivaciones y misiones permite al profesional de seguridad establecer el marco de trabajo y operación que se requiere para enfrentar al atacante y reconocer sus modos de acción para movilizarse, y así pactar con el incierto que se genera, sus estrategia de disuasión, defensa, contención y respuesta requeridas, más allá de una posición de víctima que sólo se prepara para atender un incidentes y dar cuenta de su nivel de aseguramiento del proceso de gestión de eventos adversos de seguridad, y mostrar su cumplimiento normativo.

2. EL ADVERSARIO USARÁ UN TERCERO PARA PROVOCARTE Y QUE MUESTRES LO QUE TIENES, PARA TOMAR SUS POSICIONES

Los atacantes no sólo son pacientes y estudiosos de sus futuras víctimas, terminan perfilando sus estrategias de defensa y respuesta con el fin de cerrar posibles formas de acción frente a eventos que estén más allá de su preparación. Por tanto, las organizaciones que están ajustadas y enmarcadas exclusivamente en sus buenas prácticas terminarán posiblemente "acorraladas" en sus propios procesos, pues el agresor conoce claramente el siguiente movimiento que hará y por tanto, se adelantará y creará una situación aún más retadora que deje sin oxígeno al equipo de atención de incidentes, y con más dudas que certezas a los ejecutivos corporativos y de seguridad de la información.

En este sentido, el equipo ejecutivo y táctico de seguridad deberá desarrollar escenarios retadores y exigentes que pongan a prueba la capacidad de respuesta de la organización, como una forma de experimentar en primera persona el mismo incierto que se puede generar por cuenta de un ataque desconocido y crear la zona de volatibilidad, que implica sacar a la organización de la zona cómoda de los estándares, y superar la falsa sensación de seguridad que pueden generar las tecnologías de seguridad y control actualmente instaladas.

3. EL ADVERSARIO CONOCE Y EXPLORA SU TERRITORIO, USA LA TECNOLOGÍA DISPONIBLE Y SE APOYA CON TERCEROS PARA LOGRARLO

El agresor por lo general, aparte de la motivación que ya trae, cuenta con los recursos necesarios para avanzar y contar con la información que requiere para identificar y sondear de la mejor forma el perímetro de defensa y establecer los tiempos de respuesta de la organización con el fin de conocer el espacio de tiempo que tiene para actuar y no ser detectado. El reto está en tener los suficientes radares e inteligencia avanzada para descifrar y descubrir la estrategia de defensa que se ha planteado en la víctima y desde allí establecer la forma de operación que se mimetice con la dinámica de la operación de su objetivo.

Frente a esta realidad, se plantea un juego de inteligencia y contrainteligencia que lleva a la organización a un nuevo nivel el ejercicio de protección, pues en la medida que pueda deteriorar y comprometer los intentos de recolección de información de su adversario, podrá manejar y ajustar sus estrategia de disuasión, confusión y distracción, para crear tanto incierto como el que el atacante quiere lograr cuando ejecute de forma exitosa su posible ataque. De esta forma la corporación podrá avanzar y posicionar una ventaja estratégica mientras puede observar y contener posibles efectos de las agresiones que tenga preparadas el adversario.

4. EL ADVERSARIO SABE DÓNDE TE DUELE Y SABRÁ CÓMO HACERTE DAÑO, NO SUBESTIME EL VALOR DE TUS ACTIVOS

El agresor sabe y conoce muchas veces mejor que la misma organización, cuáles son los activos más importantes y sensibles que ella tiene. En este sentido, hace la exploración en el entorno de la valoración de dichos activos, sabiendo cuáles son los de mayor facilidad de monetización y cuáles los de mayor valor para otros, con lo cual establece con claridad prioridades y mercados donde estos activos será más apreciados y por lo tanto, mejor recibidos y comprados por terceros de quiénes se desconoce su agenda o motivación. La información es un activo estratégico que tiene muchos usos ilegítimos que terminen afectando los derechos de otros.


Foto: - IMDB

La organización frente a este escenario deberá contar no sólo con el "famoso inventario" de activos críticos, sino con la referencia concreta de cuál es ese dato, ese activo digital, que si queda en manos de terceros no autorizados puede convertirse en un activo tóxico que comprometa la reputación y la imagen de la empresa frente a sus diferentes grupos de interés y termine enmedio de un fuego cruzado, donde no tenga margen de maniobra para responder ni a sus clientes, ni a sus autoridades, dado que el incendio mediático mantendrá ocupado y distraído al equipo de respuesta, así como a los especialistas de comunicaciones que harán su mejor esfuerzo para contener la ola de desinformación e inestabilidad que se genere por la brecha de datos que se ha generado.


Foto: - IMDB

Estudiar al adversario, sus motivaciones y misiones permite al profesional de seguridad establecer el marco de trabajo y operación que se requiere para enfrentar al atacante y reconocer sus modos de acción para movilizarse, y así pactar con el incierto que se genera, sus estrategia de disuasión, defensa, contención y respuesta requeridas

Los atacantes no sólo son pacientes y estudiosos de sus futuras víctimas, terminan perfilando sus estrategias de defensa y respuesta con el fin de cerrar posibles formas de acción frente a eventos que estén más allá de su preparación

Foto: - IMDB

5. EL ADVERSARIO NO TEME EQUIVOCARSE PARA LOGRAR SU OBJETIVO, SACRIFICA A SUS ALIADOS PARA ASEGURAR SU MISIÓN

El agresor puede terminar cegado por su motivación y llevar hasta el extremo sus operaciones aún sabiendo que podrá ser identificado, más no capturado. El atacante no actúa sin plan y sin conocer los riesgos que va a asumir con sus acciones, es un ejercicio de operaciones definidas que muchas veces termina cambiando enmedio de la zona de conflicto. En este sentido, el adversario "no tiene reglas", por lo que puede quebrar las alianzas y comprometer a sus propios aliados para lograr el cumplimiento de la misión. Esto crea mayor escenario de inestabilidad que podrá ser contraproducente para sus planes e inesperado para su posible víctima.

Las organizaciones deberán estar preparadas para asumir escenarios asimétricos de operaciones cibernéticas, las cuales podrán venir de diferentes lados y puntos de acción, de frentes amigos (posiblemente troyanizados vía la cadena de suministro), basados en desinformación creíble de terceros de confianza o posiblemente de acciones de personal interno debidamente distraído y engañado para generar mayor ruido y confusión que lleve a la organización a la inestabilidad, incierto y caos, escenario ideal para el adversario para concretar su agenda y pasar desapercibido enmedio del descontrol y las acciones erráticas de la organización.

El atacante no actúa sin plan y sin conocer los riesgos que va a asumir con sus acciones, es un ejercicio de operaciones definidas que muchas veces termina cambiando enmedio de la zona de conflicto

REFLEXIONES FINALES

Estas cincos declaraciones tomadas de la dinámica de la reciente producción de James Cameron, sólo son una excusa para explorar y profundizar en el estudio del adversario, una forma pedagógica para expandir una ventana de aprendizaje que permita a la función de seguridad y control mantenerse alerta, vigilante y entrenada para encontrarse con la incertidumbre y la volatilidad que representa el contexto actual para las organizaciones modernas.

Un adversario cada vez más entrenado, motivado y con aliados establece una amenaza cada vez más compleja y poco visible, dada su capacidad de mimetización con la realidad circundante que termina creando en las áreas de seguridad y control un superávit de futuro y paranoia, que muchas veces termina funcionando en contra de su propia misión: defender la promesa de valor de las empresas ajustada al apetito de riesgo de la compañía.

El reto más que contar con mayores y mejores tecnologías de seguridad y control, es establecer un equilibrio dinámico con la inevitabilidad de la falla, un pacto con el incierto de la materialización de una vulnerabilidad, con el fin de crear espacios de respuesta resilientes que preparen a la empresa como un todo, para mantenerse operando y viable en el mediano y largo plazo a pesar de la materialización exitosa de eventos cibernéticos inesperados. ■

Referencias

- Cameron, J. (2022). AVATAR. El camino del agua. Película. https://es.wikipedia.org/wiki/Avatar:_The_Way_of_Water

Jeimy Cano, CFE, CICA, miembro fundador del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes.
Más sobre el autor:

Cursos de Manejo Evasivo y Defensivo

La capacitación más avanzada del mundo

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

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

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

Programas de Capacitación

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

Contáctanos

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

Email
contacto@as3.mx

Web
as3.mx

Teléfono
+52 1 55 4181 8373

EL ESTADO DEL ENTORNO DE AMENAZAS EN EL INTERNET

Los usuarios de Internet están expuestos a un entorno de amenazas con una diversidad de tipos de ataque y modalidades de los atacantes de acuerdo con su motivación

Foto: - Freepik

MÉXICO | Carlos Alberto Gordillo Z.

INTRODUCCIÓN

Existe una relación directa entre vulnerabilidades y amenazas en el entorno de Internet; dado que las vulnerabilidades son las debilidades que explotan los atacantes, es necesario poder identificarlas, saber que existen en las redes informáticas y poder mitigar los riesgos de ataques para tener un entorno seguro dentro de la red conectada a Internet.

Existen diversas herramientas que pueden utilizarse para poder detectar las vulnerabilidades; que en la mayoría de los casos son cuestiones técnicas relacionadas al diseño, la implementación o la administración de un sistema de información, algún dispositivo conectado a la red o servicio; que permiten el acceso a un atacante para realizar un siniestro. Esto también involucra técnicas que utilizan los agresores para cometer su explotación de la vulnerabilidad identificada, para lo cual utilizan redes sociales, ingeniería social y lo conocido como Amenaza Persistente Avanzada (APT) tratando de recopilar datos y detalles de la red o equipo objetivo.

Debido a este concepto es necesario conocer los tipos de amenazas existentes y mantener un monitoreo constante, realizando pruebas rutinarias de identificación de vulnerabilidades, lo cual nos hará tener un diagnóstico de los posibles ataques a los que podríamos estar expuestos por un agresor que tenga la motivación necesaria para realizarlo.

ENTORNO DE AMENAZAS EN EL INTERNET

El Entorno de Amenazas en el Internet es el conjunto de atacantes y siniestros con los que se enfrentan los profesionales de seguridad informática; y para que las organizaciones tengan la habilidad de defenderse por ellas mismas, es necesario que se conozca y se entienda este entorno de amenazas, es decir, conocer cómo operan los tipos de agresores, así como los tipos de ataques que existen, sus características principales, las herramientas que utilizan y qué se busca lograr con dicho ataque; por decirlo así, "conocer a su enemigo y su táctica de ataque", dado que si se desconoce cómo puedo ser perjudicado, no puedo tener un plan para defenderme, por lo que en esta investigación se describirán los atacantes, los tipos de atentados que existen, y que son estudiados en el ámbito de la Seguridad Informática.

Una vez conozcamos esta información, podremos implementar contramedidas preventivas, en primer lugar, y posteriormente implementar contramedidas detectivas y correctivas, con el objetivo principal de defender la confidencialidad, integridad y disponibilidad de los sistemas, así como la información que contienen éstos, buscando en todo momento alcanzarlos o en cierta medida reducir los daños. Si ocurriera un incidente, o se detectara alguna brecha de seguridad, se debe definir un plan correctivo, medidas a imple-

mentar y un procedimiento a seguir para cada tipo de incidente, con la respectiva identificación de la vulnerabilidad en el sistema de información.

"Una vulnerabilidad es una debilidad en un sistema, ya sea un procedimiento de seguridad del sistema, los controles internos o la implementación de éstos, que podría ser explotada por una fuente de amenaza. Las vulnerabilidades dejan a los sistemas susceptibles a una multitud de actividades que pueden resultar en pérdidas significativas, y a veces irreversibles, para un individuo, grupo u organización. Estas pérdidas pueden ir desde un solo archivo dañado en una computadora portátil o dispositivo móvil, hasta bases de datos completas en un centro de operaciones comprometido. Con las herramientas y el conocimiento adecuados, un adversario puede explotar las vulnerabilidades del sistema y obtener acceso a la información almacenada en ellas. El daño infligido a los sistemas comprometidos puede variar dependiendo de la fuente de la amenaza"[1].

MOTIVADORES Y TIPO DE ATACANTES

Debido a que existen diferentes motivadores, resulta en diferentes tipos de atacantes basados en dichos motivadores; describiremos a algunos de los grupos conocidos, y quienes han realizado diferentes tipos de ataques exitosos, los cuales han servido como casos de estudio para categorizarlos de acuerdo con su motivación primaria y al grado de sofisticación de sus ataques.

Tipo de atacante	Motivación
Naciones o Estados	Geopolítica
Hacker-criminal	Financiera
Hacker-activista	Ideológica
Hacker-vieja escuela	Satisfacción
Grupo Terrorista	Violencia ideológica
Atacante Interno	Descontento

Fig. 1 – Tipos de atacantes y Motivación[2]

Todos estos atacantes buscarán debilidades en las redes, o en los equipos terminales, tratando de encontrar las vulnerabilidades para poder violentar, dichas vulnerabilidades técnicas son debilidades en el sistema que permiten, por ejemplo, que el atacante instale *software* malicioso, llamado *malware*, o aprovechar las fallas existentes para explotar el sistema.

También hay que considerar las vulnerabilidades humanas, como el descuido y la confianza, para lo que se utiliza lo denominado como ingeniería social para engañar a una persona y así conseguir información que permita accesar al sistema, en su mayoría utilizan las redes sociales para obtener información de los usuarios, hacerse pasar por otras personas y logrando así, ampliarla cobertura de personas con un bajo costo. Pueden también simular ser proveedores de información legítima utilizando cuentas de otras personas, creando sitios web y cuentas nuevas.

Mediante la identificación de un ataque, determinando con precisión al responsable del conjunto particular de actividades maliciosas, se puede obtener información importante para que se puedan proteger las redes que fueron víctima del ataque, la disuasión de un nuevo ataque, la aplicación de la ley según sea el caso e incluso las relaciones exteriores para su persecución.

Normalmente los atacantes utilizan herramientas y técnicas para ocultar sus identidades, sus objetivos, e incluso a las mismas víctimas, enviado información encubierta a través de su conexión a Internet, evitando dejar pistas que se puedan utilizar para atribuir el ataque. El nivel para ocultar su identidad depende del nivel de sofisticación que esté usando para el siniestro y su motivación, por lo que en general, los estados o naciones y los delincuentes cibernéticos competentes, serán capaces de evitar la atribución y con muchas más razones, que los actores menos sofisticados.

El NIST[3](National Institute of Standard and Technology) también clasifica las fuentes de amenazas como Adversarias y No-Adversarias; siendo definidas como Adversarias las personas, grupos, organizaciones o entidades que buscan explotar los recursos cibernéticos de una organización, incluso dentro de éstos se consideran a los empleados, ex empleados y los usuarios confiables que han defraudado a una organización. Las fuentes de amenazas No-Adversarias se refieren a desastres naturales, o errores en un sistema, tomado por individuos en el curso de la ejecución de sus tareas diarias, identificando esta debilidad y explotándola para obtener algún beneficio. ■

Referencias:

[1] *An Introduction to Information Security - NIST Special Publication 800-12 Revision 1.*
[2] *Fuente: An Introduction to the Cyber Threat Environment - Canadian Centre for Cyber Security.*
[3] *NIST – National Institute of Standards and Technology – NIST Special Publication 800-12 Rev.1 4 X.800 forma parte de la Unión Internacional de Telecomunicaciones, aprobada el 22 de marzo de 1991 en Ginebra y el RFC 449 describe el Internet Security Glossary, Versión 2.*

Carlos Alberto Gordillo Z., Ingeniero en Electrónica y MSc Tecnologías de la Información con especialidad en Seguridad Informática. Más sobre el autor:

EL IMPACTO SOCIAL DE LA INTELIGENCIA ARTIFICIAL: *MÁS ALLÁ DE LOS MITOS*

Es esencial que tomemos las medidas necesarias; aplicando estándares internacionales y procesos debidos para proteger nuestra información, nuestros datos y la privacidad al usar cualquiera de estas herramientas tecnológicas

Foto: - Freepik

MÉXICO | Gigi Agassini

Últimamente se ha escuchado mucho sobre inteligencia artificial, y pareciera una tecnología reciente, pero esto no es un concepto tan nuevo, ni siquiera de los últimos diez años, ni tampoco de los últimos veinte años; es tecnología que data desde mediados de 1950 y fue Alan Turning quien comenzó con la idea de que había posibilidad de que las máquinas comenzarán a pensar, en esos años no se le conocía con el término que se le conoce hoy, pero desde aquel entonces se han tomado aquellos modelos desarrollados que se han mejorado en la línea del tiempo hasta su actualidad y continúan.

Uno de los *chatbots* más ilustrativos a mediados de los años 60 fue ELIZA, creado en el laboratorio del MIT por varios científicos informáticos, entre ellos el alemán Joseph Weizenbaum, para demostrar cuán superficiales eran las comunicaciones entre humanos y computadoras en ese momento. Lo hacía reconociendo palabras clave y preguntando sobre ellas como si fuera un psicólogo. Mediante el uso de la metodología de "conciencia de patrones" y sustitución, el programa brindaba respuestas enlatadas que hicieron que los primeros usuarios sintieran que estaban hablando con otra persona. ELIZA se escribió originalmente en MAD-Slip. Se hicieron muchas variaciones de los guiones originales mientras los codificadores aficionados jugaban con el código, que era bastante simple.

El concepto que definía la inteligencia artificial ha cambiado con el tiempo, pero la idea principal siempre ha sido la misma; la capacidad de los sistemas informáticos para realizar tareas que normalmente requieren inteligencia humana, como la percepción, el razonamiento, la toma de decisión y la traducción de idiomas.

El término "inteligencia artificial" se utiliza para describir el campo de la informática que se ocupa del desarrollo de sistemas informáticos que puedan realizar dichas tareas, por lo que es correcto concluir que la inteligencia artificial abarca una variedad de técnicas y enfoques, incluido el aprendizaje automático, los sistemas basados en reglas, los sistemas expertos y algoritmos evolutivos, entre otros.

IMITACIÓN DE LA INTELIGENCIA HUMANA

Todas estas técnicas se utilizan para desarrollar sistemas informáticos que pueden aprender de los datos, razonar sobre problemas complejos e interactuar con el mundo de formas que "imitan" la inteligencia humana. En resumen, es un campo amplio que se ocupa del desarrollo de sistemas informáticos, de la variedad de técnicas y enfoques, y la elección de éstas dependerán del problema específico que se esté abordando así como de los datos disponibles.

Lo anterior da cabida al pensamiento que la inteligencia artificial es capaz de simular el pensamiento abstracto, creativo y deductivo, particularmente la capacidad de aprender utilizando la lógica binaria digital de las computadoras.

La inteligencia artificial tiene el potencial de revolucionar muchas industrias; desde la médica, transporte, finanzas, entretenimiento y *marketing*, sin duda podría cambiar la forma en la que trabajamos y actualmente vivimos haciendo varias tareas más eficientes, rápidas y personalizadas, pero en todo esto es imperativo considerar las implicaciones éticas y asegurarse de que se utilice de manera responsable, precisamente para beneficiar y tener un impacto positivo a la sociedad como un todo.

Foto: - Freepik

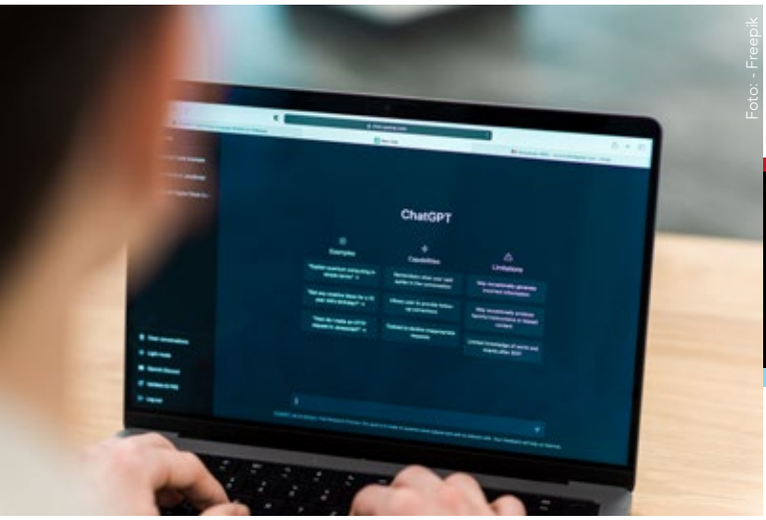


Foto: - Freepik

Uno de los *chatbots* más ilustrativos a mediados de los años 60 fue ELIZA, creado en el laboratorio del MIT por varios científicos informáticos, para demostrar cuán superficiales eran las comunicaciones entre humanos y computadoras en ese momento

Sin duda, ética y responsabilidad pueden ser subjetivos y dependen de los valores, así como de la perspectiva de cada individuo. Sin embargo, hay varios esfuerzos por establecer estos "principios éticos", guías para el desarrollo y uso de la inteligencia artificial. Es importante para los desarrolladores, los encargados de formular políticas y los usuarios que conozcan estos principios y pautas, para que trabajen en garantizar el buen uso de la inteligencia artificial y hacerlo parte de la política de ciberseguridad, privacidad y protección de datos. Además de entrenamiento constante y creación de cultura, también consciencia para fomentar la comprensión de los riesgos y beneficios de la inteligencia artificial.

La inteligencia artificial tiene muchas capacidades que la convierten en una herramienta poderosa para resolver problemas complejos y realizar tareas que serían difíciles o imposibles de hacer para los humanos, algunas de estas capacidades son: aprender de los datos, reconocimiento de patrones, procesamiento del lenguaje natural, optimización, robótica.

A pesar de las impresionantes capacidades también tiene limitaciones y desafíos que siempre deben mejorarse, algunas de estas son: sesgo, explicabilidad, limitaciones de datos, ciberseguridad y, por supuesto, preocupaciones éticas, como lo mencione anteriormente.

EL AUGE DE LOS CHATBOTS

Seguramente cuando piensas en inteligencia artificial lo primero que viene a tu mente es el ChatGPT (por mencionar alguno,) este tipo de inteligencia artificial es generativa, combina tecnologías como el procesamiento del lenguaje natural (PLN) y aprendizaje automático incluyendo aprendizaje profundo para generar texto de lenguaje natural. Las capacidades de procesamiento de lenguaje natural del *chatbot* le permite entender y generar texto en lenguaje humano, por lo que puedes sentir la impresión que estás verdaderamente charlando con otra persona.

Debes tener en mente que como es un algoritmo de aprendizaje tiene acceso a gran cantidad de fuentes e información, por lo que, si la información tiene sesgos o es incompleta, entonces los resultados serán poco acertados y con sesgos también; algunas de las muchas cosas a considerar cuando usas este tipo de inteligencia artificial, ya que ChatGPT no es el único *chatbot*, existen otros como Google Bard, Youchat, ChatSonic, por mencionar algunos.

Existen años de investigación y desarrollo con relación a la inteligencia artificial y podríamos decir que tiene dos ramas: "inteligencia artificial aplicada" e "inteligencia artificial generalizada". La primera usa principios de simulación del pensamiento humano para llevar a cabo una tarea específica, mientras que la segunda busca desarrollar inteligencias mecánicas que puedan dedicarse a cualquier tarea, como lo haría un ser humano.

La inteligencia artificial especializada y aplicada está proporcionando avances en campos de estudio; desde la física cuántica, donde se usa para modelar y predecir el comportamiento de sistemas compuestos por miles de millones de partículas subatómicas, hasta la medicina donde es usada para diagnosticar pacientes en función de datos genómicos; es usada también en la industria, en el mundo financiero para diferentes usos, desde la detección de fraudes hasta mejora de servicio al cliente. Se usa en procesos de producción, para predecir fallas antes de que ocurra algún accidente.

Existen varios enfoques de la inteligencia artificial, cada uno con sus propias técnicas y algoritmos como, por ejemplo: sistemas expertos, que utilizan reglas y bases de conocimiento para simular las habilidades de toma de decisiones, estos fueron algunos de los primeros desarrollados en las décadas de los 80 y 90. Sistemas basados en reglas, que son similares a los sistemas expertos, pero usan reglas -si-entonces- para tomar decisiones. Algoritmos evolutivos, que imitan el proceso de selección natural para encontrar la mejor solución a un problema. Lógica difusa, que permite la imprecisión y la incertidumbre en la toma de decisiones. Aprendizaje por refuerzo, que consiste en entrenar a un agente para que interactúe con un entorno y aprenda de recompensas o castigos. Redes neuronales, que se inspira en la estructura y función del cerebro humano.

Son sólo algunos ejemplos de los muchos enfoques de la inteligencia artificial que se utilizan en la actualidad, cada enfoque tiene sus propias fortalezas y debilidades; la elección del enfoque dependerá de lo que se esté abordando y obviamente de los datos disponibles, como ha sido mencionado a lo largo del artículo.

Lo cierto es que, diariamente usamos inteligencia artificial en nuestro día a día, cuando hablamos con Siri de Apple o con alguna asistente virtual como Alexa de Amazon o Cortana de Microsoft, incluso cuando usamos aplicaciones para saber el clima, entre muchas otras más.

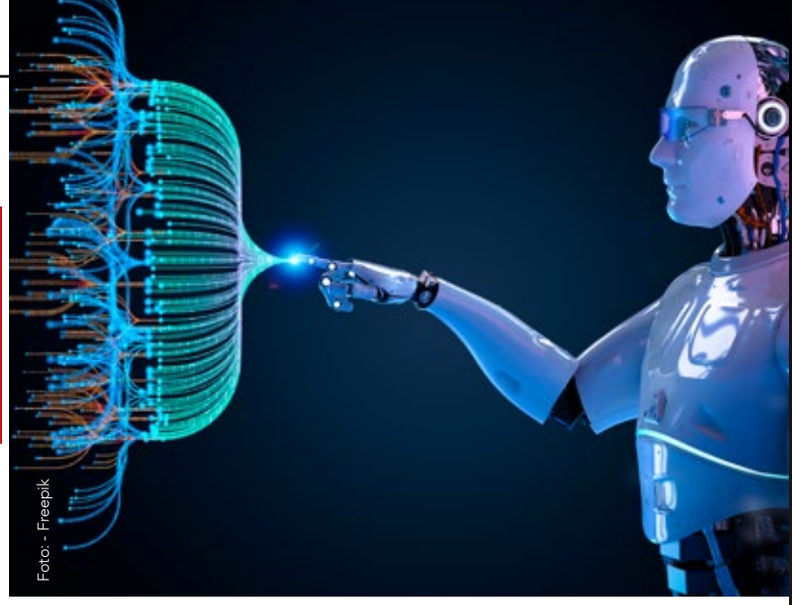


Foto: - Freepik

Es importante ser conscientes de los riesgos potenciales de la inteligencia artificial, ya que ésta puede ser utilizada para automatizar tareas peligrosas y repetitivas, mejorar la eficiencia en la producción y en la toma de decisiones, pero también puede ser utilizada para el mal si se usa en el campo de la ciberseguridad

La aplicación, desde la neurociencia a la arquitectura, de los sistemas ha llevado al desarrollo de redes neuronales artificiales, y aunque el trabajo en este campo ha evolucionado durante el último siglo, sólo recientemente se han puesto a disposición computadoras con la potencia adecuada para hacer la tarea una realidad cotidiana para cualquier persona, excepto para aquellos con acceso a las herramientas más caras y especializadas.

Definitivamente el principal factor de la activación de estas tecnologías ha sido la explosión de datos que se ha acelerado desde que la sociedad, en el mundo físico, se fusionó con el mundo digital. Esta disponibilidad de datos se genera desde las cosas que compartimos en las redes sociales, hasta los datos de máquina generados por otra maquinaria industrial conectada; significa que las computadoras tienen un universo de información disponible para ellos, para ayudarles a aprender de manera más eficiente a tomar mejores decisiones y entre más dispositivos interconectados existan, más información se genera.

Vivimos en un mundo hiperconectado y la realidad es que sólo seguirá en aumento, lo vemos con la creación de nuevas tecnologías y la adopción de éstas en la sociedad. Pero es verdad que toda evolución tecnológica trae consigo riesgos y peligros de los que debemos estar conscientes y conocer como poder mitigarlos de manera efectiva.

RIESGOS DE LA INTELIGENCIA ARTIFICIAL

Es importante ser conscientes de los riesgos potenciales de la inteligencia artificial, ya que ésta puede ser utilizada para automatizar tareas peligrosas y repetitivas, mejorar la eficiencia en la producción y en la toma de decisiones, pero también puede ser utilizada para el mal si se usa en el campo de la ciberseguridad o para crear *deepfakes* ataques de *phishing* u otros delitos cibernéticos.

Lo anterior es algo que hemos visto que aumenta considerablemente cuando ocurre alguna situación de impacto, desde la pandemia, la guerra en Europa, reuniones globales de jefes de estado, hasta campañas de *marketing* o temporadas de mucho movimiento como la navideña entre varios otros; son momentos que los delincuentes toman la oportunidad para crear más "caos" a través de desinformación, como imágenes o noticias falsas, con el uso de vectores de ataque como *smishing, phishing, vishing* por mencionar algunos, y por supuesto la ingeniería social como uno de los principales aliados para delinquir.

Adicional a estos riesgos, están los de privacidad y protección de datos, es decir, como lo mencione anteriormente, todo lo nuevo viene con sus propios riesgos y es nuestra responsabilidad conocerlo y lo que conlleva. Sin embargo, esta situación no es exclusiva de tecnologías de inteligencia artificial, la cual fue creada originalmente para ayudar a los seres humanos en su vida diaria, no para fines malintencionados como el *hacking*.

Aunque hay riesgos y preocupaciones asociados con la inteligencia artificial, es importante recordar que es una herramienta poderosa que puede ser utilizada para mejorar nuestras vidas si se usa adecuadamente, por lo que es importante que si la usas o es una herramienta en tu organización, desarrolles medidas para proteger la privacidad y la seguridad de los datos, al igual que tomar las medidas debidas para mitigar los riesgos asociados a ésta.

Es completamente entendible que todas las preocupaciones asociadas al mal uso de la inteligencia artificial no se limitan sólo a ésta, ya que cada vez que usamos cualquier herramienta para facilitar nuestras tareas diarias, sea de tecnología, automatización o cualquier otra, existirá siempre el potencial que se use para fines malintencionados o para violar la privacidad y seguridad de los usuarios y/o corporaciones.

Por lo tanto, es esencial que tomemos las medidas necesarias; aplicando estándares internacionales y procesos debidos para proteger nuestra información, nuestros datos y la privacidad al usar cualquiera de estas herramientas tecnológicas, y sobre todo asegurarnos de que dichas medidas, políticas y procesos sean implementados y monitoreados constantemente. Adicional a generar una cultura de seguridad, consciencia de los riesgos y las mejores prácticas, para evitar el uso indebido.

Si ya eres usuario de éstas herramientas no olvides estar alerta, y sí aún están pensando en usarlas o no, anímate; es importante conocer lo nuevo y apoyarnos de herramientas poderosas para hacer eficiente nuestras tareas, pero siempre considera que los procesos, el entrenamiento y los estándares vienen de la mano con esta tecnología y con todas las otras herramientas.

¡Hasta la próxima!

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

México – Jordania – Serbia – Israel – Italia – Rusia – Colombia - Venezuela

La capacitación que marca la diferencia

CURSOS:

GRUPO CIPI®

- Protección a funcionarios 360°
- Medicina táctica
- Manejo táctico antisecuestro
- Manejo de armas y defensa personal
- High level protection
- Inteligencia contra inteligencia antisecuestro
- Protección ejecutiva antisecuestro
- Blindajes / seguridad privada

DIPLOMADOS:

- Gestión integral de riesgos (protección civil)
- Protección Ejecutiva
- Seguridad Privada
- Seguridad Pública

56 1181 7875 771 284 0869

cipi@consultoresenproteccion.com

ISO 17024:2012 ISO 9001:2015 ISO 18788:2015 redconocer

DISCERNIR EL FUTURO DE LAS INVERSIONES EN TECNOLOGÍA EN EL *RETAIL*

El futuro de las inversiones en tecnología deben alinearse a la protección de información como la columna vertebral de los planes de seguridad corporativa

Foto: - Freepik

MÉXICO | **Iván Gustavo Islas Castillo**

El tiempo y la evolución de la tecnología es una dinámica imposible de detener o mantener estática. Si bien el tiempo es un valor de referencia para medir o separar acontecimientos, la tecnología es un instrumento creado para satisfacer necesidades y en algunos otros para crear otras.

Así como se detalla esta dinámica de cambio constante, el comportamiento y desplazamiento de los clientes a los que se dirige el comercio detallista, constantemente evoluciona, se balancea, se transforma y en algunos otros se reinicia a niveles rústicos en un afán de prevalecer con lo que se llama "la experiencia de compra" en tiendas tradicionales. Sin embargo, la tecnología ha diversificado en enorme medida su aplicativo en las tiendas (ya sea de grandes o medianas cadenas comerciales) la necesidad de monitorear los pisos de venta, los flujos de caja, el tráfico de transacciones en PoS, el volumen de visitantes, las zonas de alto tráfico, la falta de servicio, los procesos logísticos de atención a clientes, etc.

Y todo ello inclina la balanza a la seductora oferta de diferentes soluciones tecnológicas que prometen resolver nuestras necesidades básicas y atender otras tantas ocultas o creadas por la innovación y el ímpetu de mantenernos siempre actualizados y a la vanguardia, pero… ¿realmente tenemos identificado el rumbo y la solución en niveles escalables para saber discernir de todo un universo de soluciones? ¿Cuál es la indicada o la más certera para atender nuestro plan de inversión para soluciones en tecnología?

RIESGOS EN EL MUNDO DIGITAL

Si bien sabemos que el mundo con su transformación digital, sumado a la pandemia (que aceleró una evolución de los hábitos de consumo), han provocado que la dimensión matricial de los riesgos organizacionales cambie sus vectores a escenarios y modalidades jamás vistas. Hoy en día los canales virtuales crecen a pasos agigantados y cual caldo de cultivo, las amenazas y modalidades de escenarios por pérdida van vinculados principalmente a ilícitos en un submundo casi desconocido para muchos.

El mundo digital, un universo intangible donde la información, como eje principal del comercio, abunda en recovecos legales con infinidad de lagunas para poder cometer fraudes, robos de identidad, abuso de confianza y a ello agregado el ingrediente final, que es una cadena de suministro endeble; se cierra el círculo del cultivo idóneo para que nuevas organizaciones delincuenciales, literalmente, generen ganancias cuantiosas ante el empacho de las pérdidas que para las empresas minoristas representan en una nueva era pospandemia.

Por ello, el futuro de las inversiones en tecnología deben alinearse a la protección de información como la columna vertebral de los planes de seguridad corporativa. En muchas ocasiones hacer un *back to basic* es quizá la primera solución en la mesa. Y entiéndase que no debe focalizar únicamente en la información sensible de las bases de datos. Es incluso la información de mercancías, promociones, contenidos de embarques, paqueterías, etc.

La seguridad de las instalaciones y la gestión del modelo de información crítica debe estar tan perfectamente alineada a este principio incluso para poder rentabilizar todas las inversiones de seguridad tecnológica en nuestros modelos de gestión. Así pues, con la tecnología también entiéndase que debe integrarse a los modelos de gestión para la administración de personal y máxime para temas de reclutamiento (punto crítico y el más delicado para la gestión de información), pero de este tema, platicaremos en otra oportunidad. ■

Iván Gustavo Islas Castillo, subdirector de Prevención de Pérdidas en la cadena de suministro del Puerto de Liverpool.

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

PEQUEÑAS IDEAS PARA EVITAR GRANDES PROBLEMAS

Foto: Freepik

Recomendaciones para desempeñarse como personal de Seguridad Privada

ARGENTINA | Óscar Mario Díaz

Una característica del trabajo del personal de Seguridad Privada, es que generalmente, se ubica en medio de intereses y responsabilidades cruzadas con otros sectores de la organización. Brindamos aquí, una recopilación mínima de conceptos y situaciones que podrían darse en el desempeño de las funciones del personal de Seguridad Privada y que se resumen en unos breves párrafos debajo. Pueden sonar como "Verdades de Perogrullo", pero no por eso, dejan de tener vigencia y podrán ayudar en el desarrollo de las tareas del referido personal.

1. Ser siempre honrados, leales y veraces. Actuar con Integridad. Quien así no proceda, vale muy poco para el servicio.
2. Ser siempre eficientes y confiables, en síntesis, ser profesionales.
3. Obrar siempre guiado por las virtudes de la prudencia, la fortaleza, la templanza y la justicia.
4. Operar siempre con certeza de lo que se está haciendo. Los "Actos de Fe", no son para cuando estamos en funciones.
5. Conducirnos siempre con extrema fineza y suma cortesía. Pero sepamos actuar siempre con restricción cuando corresponda en el ejercicio de nuestras tareas/funciones. "Lo cortés, no quita lo valiente".
6. Atender las obligaciones. "Sin prisa, pero sin pausa". La calidad no siempre se lleva bien con la velocidad. Pero cuando las cosas urgen, siempre se debe procurar estar a la altura de los acontecimientos. "El Tiempo pasa y la Misión fracasa".
7. Tenga su presentación personal, vestimenta, equipamiento, en impecables condiciones de empleo. Todo debe estar operativo y sin novedad. Un equipo de comunicaciones que no funcione, porque no tiene suficiente batería o no se escuchó, porque el nivel del volumen estaba bajo y aconteció una emergencia, es de muy difícil explicación después, ante las consecuencias negativas de la misma, siendo que hubiera podido evitarse, si todo estaba en pleno empleo.
8. Siempre estar en conocimiento pleno de las políticas, normas y procedimientos que haga a nuestro quehacer como Personal de Seguridad Privada. Nunca, quedarnos con inquietudes de cómo se debe proceder profesionalmente. Preguntar antes, es de persona inteligente.
9. Siempre y relacionado con el punto anterior entregue las novedades, documentación, sistemas de seguridad electrónica, equipos y elementos de empleo diario, asegurándose que su relevo haya comprendido y visto lo suficiente para continuar con la misión, sin que se originen los negativos: "Yo no sabía", "Nadie me avisó", tan propios de las actividades de cambios de turnos y que desgraciadamente, producen daños y pérdidas de todo estilo, amén del perjuicio al prestigio profesional de nosotros mismos y de nuestro equipo de trabajo.
10. Si alguien desea ingresar a una instalación y no posee una autorización para esto, es conveniente expresarle que, a pesar de no tener esa autorización, se realizará la gestión para averiguar sobre la misma. Preguntarle los datos filiatorios (de ser posible que la persona quede bajo CCTV y/u obtener imagen del documento de identificación personal; preguntar a qué empresa pertenece o si es visita particular; a quién viene a ver; motivo de dicha visita, etc.). No se le está diciendo que no directamente, pero tampoco se le está permitiendo el ingreso, a la vez que vamos recabando datos.
11. Si alguien está en una situación de espera y comienza a reclamar airadamente para que se le atienda rápido, nunca acceder a esa forma de presión, pues no sólo estaríamos siendo injustos con el resto, sino que le estamos promocionando hacerlo en un futuro, amén de que el resto, pueda imitar esa inconducta. Por el contrario, en forma calmada y prudente, ponerlo en evidencia ante el resto de que ellos también están vivenciando la misma circunstancia, por dar un ejemplo de respuesta a brindar.
12. Siempre, si recibe algo en guardia y custodia, trate de efectuar que eso quede asentado por escrito, fotografiado, recibido bajo CCTV, con testigos, acuses de recibo con firma y aclaración y DNI, o cualquier otra forma que permita brindar pistas de auditoría, en caso de tener que deslindarse responsabilidades ulteriores o intentar aclarar lo acontecido de forma cristalina, con lo que hemos recibido, tanto para el momento en que lo recibimos, como para cuando lo entregamos.
13. "Res, non verba", "Hechos, no palabras". Claramente, esta verdad milenaria, es lo que hace la diferencia entre un profesional de la seguridad y alguien que

MONTERREY / CANCÚN / VERACRUZ / / COATZACOALCOS / VILLAHERMOSA

GORAT SEGURIDAD PRIVADA

ALARMAS

GPS

CCTV

GUARDIAS

ESCOLTAS

CUSTODIA DE TRANSPORTE

SERVICIOS INTEGRALES DE SEGURIDAD

800 00 46728 / www.tecuidamos.mx

OFICINA C4 RIVIERA / +52 229 193 5519

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

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

Siempre, si recibe algo en guardia y custodia, trate de efectuar que eso quede asentado por escrito, fotografiado, recibido bajo CCTV, con testigos, acuses de recibo con firma y aclaración y DNI, o cualquier otra forma que permita brindar pistas de auditoría

vive poniendo excusas, respecto del resultado que se espera de su desempeño.

14. "Verba volant; scripta manent", "Las palabras vuelan; los escritos perduran". Otro antiquísimo axioma, que nos infiere a que debemos evitar "los dimes y diretes", tan propias de las personas y, en particular, cuando algo no salió o no está bien o se anteponen errores de interpretación.
15. Siempre, es preferible "Hacer decir lo nuestro y no permitir que digan por nosotros". Esto en particular, si quien puede enviar el escrito que sea, no es claro, no se lo ve que haya comprendido el asunto o, se observen aviesas intenciones. Escribamos nosotros. Tampoco sobrecargarnos y mal acostumbrar a terceros.
16. La actividad de Seguridad, conjuga generalmente en el diario quehacer cinco verbos: saber, caminar, controlar, informar y escribir. Dice un viejo adagio que "El que no sabe, es como el que no ve". Y al informar, efectuemos esta tarea sin magnificar, ni poner pareceres, ni inventar datos. Luchemos por ser lo más objetivos posibles.
17. Un modo de ayudar en lo anterior, es la siguiente regla nemotécnica: "ni que te toque", donde:

- **Nombre:** cargo / nombre y apellido / instalación.
- **Informe:** urgente o Importante. Grupo fecha hora del informe.
- **Qué:** oportunidad (grupo fecha hora de cuándo sucedió o cuándo se encontró la novedad), sujeto (si es persona: nombre e identificación. Si es cosa: lugar donde se encuentra o identificación), verbo ("está" – "se están" – etc.), predicado (explicar qué pasa en forma breve y clara).
- **Testigos:** todos los que estén involucrados y puedan informar. Medios de registro tecnológicos (videos; control de accesos, etc.).
- **Todo dato de interés:** cómo sucedió. Opinión. Certezas y supuestos. Medidas adoptadas hasta el momento.
- **Qué pretendo con esa información:** Acciones y consecuencias.

EJEMPLO

- N: Vigilador XXXXXX ZZZZZZ – Sucursal HHHH.
- I: Importante – 191500 Dic. 22.
- Qué: El 191300 Dic. 22 el contratista CCCC de la Empresa EEEE dentro de Sucursal HHHH, me entrega una caja de herramientas cerrada, para que le entregue al Sr. Operario OOO de su firma en el día de mañana a fin de terminar los trabajos de mantenimiento. Se recibe dicha caja bajo cámara y se envía *mail* al área de Seguridad y a la Empresa EEEE, además del Sr. JJJJ que encargó el trabajo dentro de Sucursal HHHH.
- Te: Vigilador NNNNNN MMMMM – Sucursal HHHH.
- To: Se recibió bajo CCTV de Cámara N° 4 y se guardó dicha caja de herramientas, en el *locker* N° 3 con N° de Precinto 123456.
- Qué: para ser abierto por el turno diurno de mañana, constatado lo actuado e informado y entregada dicha caja al Sr. Operario OOO, enviando *mail* para formalizar dicha entrega a los involucrados en el correo original.

18. Nunca confundir la debida actitud de servicio con el servilismo. Asumir siempre nuestras responsabilidades. No buscar nunca evadirlas y hacerlo con un alto nivel de compromiso. Si cometemos un error, brindar las disculpas del caso y más rápidamente, solucionar las consecuencias del mismo de ser posible o minimizar su impacto. Tener presente la "Originalidad en los Errores", es decir "No caer 2 veces en el mismo pozo". Que ese error, sea una verdadera lección aprendida. Internalicémoslo y no lo repitamos.
19. Siempre apoyar al equipo o a quien esté con un problema.
20. Aplicar siempre el trabajo en equipo y la debida empatía.
21. Tener siempre sentido del deber y la satisfacción del deber cumplido. Junto a los deseos de superación, son conceptos que llevarán a alcanzar la excelencia en el cumplimiento de nuestros deberes.
22. Siempre tengamos independencia de juicio. Pero si va a discutir, que no sea disputar. La discusión, es un intercambio de inteligencias. La disputa, en cambio, un intercambio de ignorancias. Siempre hacerlo con respeto, buenas maneras y principalmente, con fundamentos sólidos. Seamos asertivos, pero no necios.

Finalmente, las áreas de Seguridad, en algunas oportunidades, son utilizadas para descargar responsabilidades que no les son propias. Por eso, insistimos, nunca confundir la debida actitud de servicio vs. servilismo. Si el tema no es de nuestra responsabilidad, clarificar a quien corresponda, que lo que efectuemos —y de estar en alcance de ejecutarlo de nuestra parte—, lo haremos a modo de colaboración y siempre que esa carga adicional de trabajo, no constituya ni un traslado de responsabilidades, ni que se haga costumbre sobre nuestro sector y, lo más importante, no nos haga desatender nuestras verdaderas responsabilidades.

Es cierto también que las áreas de Seguridad, pueden ofrecer un valor agregado en el desempeño de sus funciones, pero como expresamos, no perdiendo el norte de sus misiones que le son propias y eso, debe ser debidamente analizado previamente. ■

Óscar Mario Díaz, gerente de Seguridad de la empresa Ecocarnes, S.A.
Más sobre el autor:

CONTROL®

SEGURIDAD PRIVADA INTEGRAL

ÁREAS DE NEGOCIO

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

SÚPER EMPRESAS EXPANSIÓN 2023 TOP companies

ASIS · ESR EMPRESA SOCIALMENTE RESPONSABLE · ISO 9001:2015 OC-0080/13 · AMESP

@segcontrol

www.seguridadcontrol.com.mx

Columna de
Enrique Tapia Padilla, CPP

etapia@altair.mx

Socio Director, Altair Security Consulting &Training.

Más sobre el autor:

SÉ EL CAMBIO QUE QUIERES VER

LATINOAMÉRICA

En esa constante inquietud que me invade al estar seguro que en Latinoamérica podemos hacer un montón de cosas para mejorar de manera inmediata nuestras sociedades, es que comparto con ustedes ahora este artículo.

COMPARTIENDO ANÉCDOTAS

En mi estancia de cinco años en la hermosa Riviera Maya en México, por ejemplo, no sólo fui socio fundador y presidente de la Comisión de Seguridad de Coparmex Riviera Maya (aún sigo siendo consejero directivo de esa hermosa asociación), sino también apoyamos fuertemente la creación de ASIS Capítulo Península de Yucatán e hicimos nacer el Diplomado de Seguridad Integral de la UDLAP.

Como titular de la Comisión de Seguridad en Coparmex, atendimos en la zona casi 40 casos de extorsión por cobros de derecho de piso con éxito (que no se llevara a cabo la extorsión); desde las típicas llamadas a los comercios, pasando por visitas presenciales de los malos para iniciar una extorsión permanente o incluso, los casos más complicados, cuando ya tienen años extorsionándote y te tienes que quitar el alacrán de la espalda. Hicimos muchas estrategias, en conjunto con la Fiscalía del estado y los empresarios fue que logramos que muchos de éstos tuvieran confianza en las autoridades, cosa que no era fácil, pero siempre hacía yo un acompañamiento a los empresarios para mostrarles que, aunque riesgoso, no podíamos quedarnos cruzados de brazos. Lográbamos a más gente empoderada y convencida de que ellos debían defender sus espacios. Sacamos a varios grupos delictivos de las calles. Todo lo logrado me llevaba a una satisfacción silenciosa enorme y que ahora comparto en estas líneas, saber que, si cada quien hiciéramos la parte que nos corresponde, sin duda podríamos contrarrestar muchísimos de los delitos y estaríamos en un mejor lugar.

Como titular de la Comisión de Seguridad en Coparmex, atendimos en la zona casi 40 casos de extorsión por cobros de derecho de piso con éxito (que no se llevara a cabo la extorsión)

Hicimos muchas estrategias, en conjunto con la Fiscalía del estado y los empresarios fue que logramos que muchos de éstos tuvieran confianza en las autoridades

Así también, en el paraíso tropical limpiábamos de basura una vez al mes los dos kilómetros de calle que llevaba hasta nuestro condominio y además, siempre que visitabamos la playa los fines de semana en nuestras caminatas nos acompañaban unas bolsas para recoger basura *(plogging)*. Penosamente salían varias bolsas de basura e incluso alguna vez me preguntaba algun vecino para qué limpiaba la calle si en los siguientes días la iban a volver a ensuciar; eso me hacía recordar a mi mamá cuando de chico me pedía le ayudara con el quehacer de la casa y yo le respondía que para que limpiaba si al rato estaría de nuevo sucio, a lo que mi mamá me respondía sabiamente "para qué comes si al rato vas a tener hambre", nunca lo olvidaré.

Decidía siempre hacer un cambio aunque a veces fuera efímero, otras veces de largo plazo, en lugar de quedarme de brazos cruzados ante esos actos de anarquía. Aunque la mayoría alrededor no hizo mucho, siempre hubo alguien que se unió al esfuerzo y eso ya valió la pena; sumamos a alguien más a tener una nueva conciencia que podría perdurar en el tiempo.

Todos los trabajos anteriores son constantes y consistentes, de largo plazo. No es sólo un gran esfuerzo y pensar que ya cambiarán las cosas, en el caso de la extorsión, vendrán y vendrán diferentes grupos o los mismos a insistir, tendremos que defendernos constantemente.

SÉ EL CAMBIO QUE QUIERES VER

Pongo estos ejemplos, no para vanagloriarme sino porque desde hace muchos años entendí que para lograr los cambios que uno quiere ver, hay que ser parte de ellos, arremangarse y trabajar hombro con hombro con sociedad y gobierno. Ir abriendo brecha, sumando esfuerzos en el camino y hacer que las cosas sucedan. Cambiar conciencias. Nadie me lo platicó, yo lo he vivido en carne propia.

Sean el cambio que quieren ver en la sociedad, comienza por nosotros. Piensa colega, ¿cómo puedes colaborar como profesional de seguridad en mejorar las condiciones de la sociedad, además de la actividad pagada a la cual te dedicas. Hay un montón de asociaciones sin fines de lucro en donde puedes poner un grano de arena y hacer un cambio, hay muchas organizaciones civiles e inlcuso de vecinos donde ya muchos colegas están realizando labores honorarias, pero se necesitan más esfuerzos, ¿te sumas? ¡Comencemos ahora! ■

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

Fotos: Cortesía Enrique Tapia

Columna de *GEMARC*

Héctor Coronado Navarro, presidente de Grupo de Ejecutivos en Manejo de Riesgos Corporativos, A.C. (GEMARC) para el periodo 2023-2025. Más sobre el autor:

UN REFERENTE DE LA **SEGURIDAD CORPORATIVA**

Sus orígenes se remontan hace más de dos décadas, en el que un pequeño grupo de ejecutivos de seguridad se reunían para compartir mejores prácticas en sus corporativos y lo que principalmente los unía era su amistad

El 31 de mayo del presente año, el Grupo de Ejecutivos en Manejo de Riesgos Corporativos, A.C. (GEMARC), realizó las elecciones para escoger al nuevo presidente, para el ciclo junio de 2023 – mayo de 2025, quedando seleccionado como su nuevo representante Héctor Coronado Navarro, *Sr LP Manager Sec Ops LATAM* en Mercado Libre, quien reemplazó a Dagoberto Santiago, *Sr Director Corporate Security LATAM* en PepsiCo y quien tuvo una muy distinguida labor durante su periodo.

Héctor Coronado, en este nuevo ciclo estará colaborando con Fernando Gómez Villarreal, director de Seguridad Global en Gentera, como secretario; y Lourdes Morales Aguilar, *Prevention Tribe Lead* para Walmart México y Centroamérica, como tesorera de dicha asociación, y obviamente con el apoyo de más de 115 socios activos de GEMARC, siendo todos ellos los líderes de Seguridad Corporativa del más alto nivel en sus empresas en México.

• **La Misión:** coadyuvar a la generación y mantenimiento de condiciones seguras en nuestro país y en las empresas que representan, por medio de la comunicación eficiente con todos los niveles que conforman el medio de la seguridad, a través de propuestas y postulados que logren los contrapesos necesarios para ser la voz de la Seguridad Corporativa.

• **La Visión:** ser el grupo de profesionales más reconocido en México en temas de Manejo de Riesgos Corporativos, incluidos, pero no limitados, a la Seguridad Física y Lógica, Continuidad de Operaciones, Investigaciones y Protección Ejecutiva a través de estándares, publicaciones y conferencias donde se compartan las mejores prácticas relacionadas a la Seguridad Corporativa.

Sus orígenes se remontan hace más de dos décadas, en el que un pequeño grupo de ejecutivos de seguridad se reunían para compartir mejores prácticas en sus corporativos y lo que principalmente los unía era su amistad; sin embargo no estaban constituidos como una figura jurídica como tal, pero sí con el nombre de GESC (Grupo de Ejecutivos de Seguridad Corporativa). Continuaron por años trabajando de manera informal, hasta que en el año 2019 se constituyeron ya de forma legal como GEMARC (Grupo de Ejecutivos en Manejo de Riesgos Corporativos), siendo el primer presidente Kael Malo Juvera (2019-2021), posteriormente le sucedió Dagoberto Santiago (2021-2023) y actualmente Héctor Coronado Navarro (2023-2025).

¿QUIÉN ES HÉCTOR CORONADO NAVARRO?

Héctor Coronado es Licenciado en Derecho, cuenta con una Maestría en Seguridad Corporativa y diversas Especialidades en Derecho Procesal Penal, Seguridad Integral y otras certificaciones nacionales e internacionales de seguridad.

Cuenta con experiencia con más de 30 años de carrera profesional en seguridad, comenzando su carrera profesional como Ministerio Público por Ministerio de Ley en la Procuraduría General de la República y posteriormente en la Procuraduría General de Justicia del Distrito Federal.

Posteriormente inició su carrera laboral en el sector privado, en donde ha estado a cargo por más de 18 años en posiciones de América Latina y Globales en empresas multinacionales como Amazon, HP, Dell, Mercado Libre, entre otras.

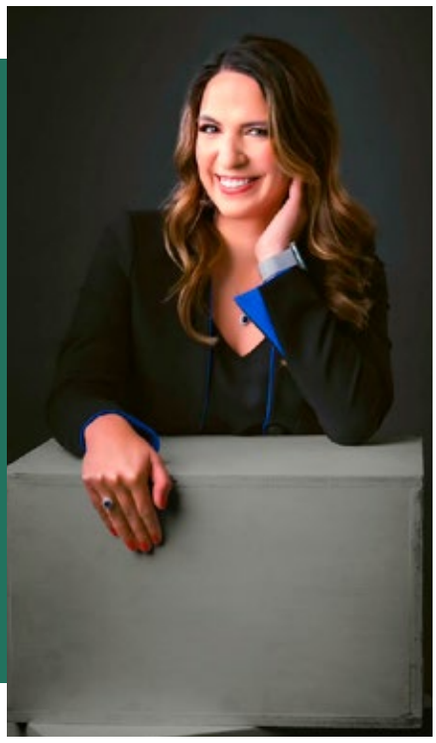
Héctor también es catedrático en la Universidad Anáhuac, en donde imparte la materia de Seguridad Corporativa y es conferencista a nivel nacional e internacional, recientemente publicó su primer libro *"Una Segunda Oportunidad"*, en donde habla de manera práctica de sus experiencias en Seguridad Corporativa. Ha sido distinguido en un par de ocasiones como parte de "Los 100 más influyentes de la seguridad privada".

Ha participado de forma directa e indirecta en diferentes asociaciones de seguridad, en donde fue presidente de ASIS Capítulo México en el año de 2017 y en el 2018 fue *Regional VP* de la región de ASIS.

¿QUIÉN ES FERNANDO GÓMEZ VILLARREAL?

Fernando Gómez Villarreal es egresado del Tecnológico de Monterrey como Ingeniero en Electrónica y Comunicaciones y como Maestro en Administración, ambas con Mención Honorífica. Ha trabajado en diferentes empresas como cabeza de Seguridad para Latinoamérica como: HSBC, FEMSA, Transportación Marítima Mexicana, Grupo Posadas y TV Azteca actualmente se desempeña como *Chief Security Officer* para Grupo Gentera a cargo de Seguridad Física, Investigaciones, Protección Civil, Comité de Crisis, Continuidad del Negocio, Prevención de Fraudes y Seguridad de la Información.

Está certificado como CPP, PSP, PCI y EP por ASIS; como CFPS por la National Fire Protection Association, CISSP por la Asociación (ISC al cuadrado) y CBCP por el Disaster Recovery Institute International. Reconocido en dos ocasiones como uno de "Los 100 más influyentes de la Seguridad Privada", por la revista **Seguridad en América**, y es ganador del premio Thoughtful Leadership en Berlín, Alemania, por International SOS. Ha sido profesor de la UDLAP en diversas ocasiones y ha dado conferencias en diversos temas en México y el extranjero. Ha salido en televisión con Ana María Salazar siempre hablando de temas de seguridad.



¿QUIÉN ES LOURDES MORALES AGUILAR?

Lourdes Morales es una criminóloga costarricense con 18 años de experiencia, especializada en Seguridad Corporativa e Investigaciones. Durante los últimos 14 años, Lourdes ha laborado en Walmart donde ha tenido oportunidad de pertenecer a los equipos de: Seguridad Corporativa, *Global Investigations, Global Security y Global Compliance*, adicionalmente ha colaborado con diferentes Comités de Equidad y Género e incluso fue Mentora del Programa Pequeños Productores.

Cuenta con una Licenciatura en Criminología, graduada *"Summa Cum Laude"*, además de Diplomados en Investigación Criminal, Seguridad Organizacional, Investigación y Control de Drogas y Desarrollo de Habilidades para el Directivo de la Seguridad Integral.

Lourdes fue la primera mujer miembro de la Junta Directiva de ASIS Capítulo 271: Costa Rica y del Comité de Seguridad de la Cámara de Industrias de Costa Rica. En mayo de 2020, Lourdes fue designada como *Prevention Tribe Lead* para Walmart México y Centroamérica, impulsando la transformación de Seguridad Corporativa, estableciendo la misión de crear las condiciones para trabajar en un ambiente seguro a través de una estrategia efectiva de seguridad e investigación, en beneficio de los clientes, colaboradores y proveedores.

Seguridad Corporativa, Seguridad Operaciones, Seguridad Logística, Investigaciones Corporativas, Prevención de Fraudes, Protección Ejecutiva y el Centro de Atención de Emergencias son los equipos que actualmente lidera Lourdes. Su responsabilidad incluye la seguridad de más de 2 mil 800 tiendas, 21 Centros de Distribución y siete instalaciones corporativas en todo México. Su equipo está compuesto por 120 asociados ubicados en seis países y más de seis mil terceros.

GEMARC será referente para establecer los lineamientos y requerimientos en Seguridad Corporativa en México

PLAN DE ACCIÓN DE GEMARC 2023-2025

El plan de acción para este periodo se conforma bajo tres pilares fundamentales:

1. Posicionar a GEMARC como la mejor y más reconocida asociación de seguridad en México y hacer el cambio que se requiere de acuerdo a las necesidades actuales. GEMARC será referente para establecer los lineamientos y requerimientos en Seguridad Corporativa en México.

2. Reforzar la esencia que es la unidad de esta asociación, historia que se empezó a contar desde hace más de 25 años, en la de ser un grupo de "amigos y profesionales" que se han venido acompañando y apoyando en este sector de la seguridad, generamos sinergia, compartimos mejores prácticas.

3. Dejar un legado y apoyar para que tengamos mejores niveles de seguridad en el país. Construyendo para ahora y el mañana, y teniendo el compromiso de ser actores y no sólo espectadores en este escenario que llamamos Seguridad Corporativa.

¿CÓMO SE LLEVARÁ A CABO?

1.- Ser la mejor asociación de Seguridad.

- Reforzar y ampliar los convenios de colaboración.
- Estar presentes en los foros más importantes del gremio, buscando la mayoría de la representación de cada uno de los miembros de GEMARC.
- La información es una de las fortalezas de GEMARC.
- Estableceremos los estándares y parámetros de la seguridad en el mercado.

2.- No perder la esencia y unidad de GEMARC.

- Reforzar la participación siendo incluyentes.
- Se fortalecerán los Comités (Admisiones, Ética, Equidad e Inclusión, Inteligencia, Desarrollo Profesional, Logística, entre otros).
- Presencia nacional.
- Continuar con *networking*-sociales.

3.- Dejando un legado.

- Fortaleciendo el "*mentoring*".
- Alianzas con universidades y asociaciones, acciones altruistas a la sociedad (apoyo a fundaciones sin fines de lucro). Ejemplo:
- Apoyo a la comunidad.
- Reforzar el tema de diversidad e inclusión.
- Apoyar y promover los nuevos estándares de seguridad en México (influyendo en propuestas de solución).

GEMARC sin duda es la asociación de Seguridad Corporativa que existe en el país y su fortaleza la conforman por todos y cada uno de sus socios, siendo imposible nombrar a todos ellos por motivos de espacio, pero no por eso no dementar su peso e importancia en la asociación. ■

Fotos: Antonio Venegas / SEA

OFRECEMOS SOLUCIONES EN LA CADENA LOGÍSTICA CON UN ENFOQUE EN LA SEGURIDAD PRIVADA, CREANDO ESTRATEGIAS PARA PROTEGER LOS BIENES DE CADA UNO DE NUESTROS CLIENTES.

SEGURIDAD EN
LA CADENA LOGÍSTICA

CORPORATIVO EN SEGURIDAD

ALFIL

ADMINISTRADORES EN SERVICIOS INTEGRALES DE SEGURIDAD, S.A. DE C.V.
SEGURIDAD PRIVADA

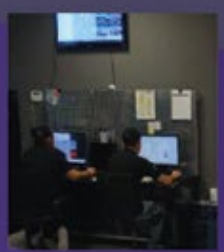
Custodia de mercancías, bienes y/o valores:

- Patrullas y/o Motos con sistema GPS
- Custodia civil o armada
- Sistema de video a bordo
- Tripulación de 2 elementos
- Sistema de comunicación seguro
- Flota con modelos recientes 2021a 2023
- Monitoreo dedicado y activo 24/7
- Candados de seguridad
- Candados GPS

- Consultoría especializadas.
- Escolta ejecutiva.
- Sistemas integrales GPS.
- Aplicaciones de seguridad.
- Análisis de riesgo.

Monitoreo Logístico, prevención, control de predidas e investigaciones.

Protegemos con estrategia e inteligencia



Equipo Centurión

Acciones
Seguimiento
Reducción de costos

CERTIFICACIONES

ISO 9001-2015 EMPRESA CERTIFICADA

CERTIFIED ISO 28000

Alce Blanco 55 Fracc. Industrial Alce Blanco, Naucalpan de Juárez, 53370. Estado de México

www.corporativoenseguridadalfil.com

informes@corporativoenseguridadalfil.com

Tel. 55 53 58 97 59

SOCIO

ASIS INTERNATIONAL CAPITULO MÉXICO 217

mesis

FEPASEP

TSR Certified TAPA

GNSP

Columna
EL TIGRE TIENE RAYAS

ballesteros.barrera@hotmail.com

Más sobre el autor:

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

OLA DE INSEGURIDAD EN LEÓN, GUANAJUATO

Foto: - Wikimedia Commons

El verdadero liderazgo se nota en la persona desde su actuar, comportamiento, porte, la forma en que habla, da un aire de autoridad y respeto, y en ocasiones de miedo, se nota el liderazgo al estar en la fila del banco, en el cine, en la banqueta, etc.

MÉXICO

Amigos, les envió un cordial saludo a la vez que les mando a todos un fuerte abrazo, esperando estén bien y logrando sus metas.

Saben que como cada edición en mi columna EL TIGRE TIENE RAYAS, busco darles conocimientos, anécdotas, y cualquier cosa que les permita crecer como los líderes que son en su campo, puesto, empresas, etc.

En esta ocasión quiero marcar la pauta sobre el tema de la delincuencia desbordada, que se vive en todo el país, no existe un solo municipio y estado de la república que esté libre de esta pandemia, que a diferencia del COVID-19 ya tiene más de una década, cada vez está más grave y sigue subiendo en el estado donde actualmente vivo, que es Guanajuato.

Foto: - Wikimedia Commons

Foto: - Wikimedia Commons

> No podemos decirle a la gente que no salga, el dinero no llega a casa del aire, tienen que tomar cursos, pláticas, conferencias, etc., de cómo responder al peligro

Los gobiernos locales manejan cifras nada creíbles, ya que, en las noticias, redes sociales, periódicos, etc., se ven los incidentes delictivos que sólo permiten denotar que ninguna cifra está bajando, todo esta al alza, es muy fácil decir que las cifras bajan cuando eres dueño del sistema, pero no se vale que nos traten como personas que no pensamos y como crédulos sólo diciendo que los crímenes son cada vez menos. ¿En qué realidad alterna es eso?

El liderazgo no es algo que se tome a la ligera, personalmente me tomo el liderazgo como un estilo de vida, y lo aplico siempre en cada aspecto de mi vida, no sólo en el trabajo, recordemos que el liderazgo no andar de mandón y que la gente te haga caso por obligación o por el sueldo.

El verdadero liderazgo se nota en la persona desde su actuar, comportamiento, porte, la forma en que habla, da un aire de autoridad y respeto, y en ocasiones de miedo, se nota el liderazgo al estar en la fila del banco, en el cine, en la banqueta, etc., por lo anterior puedo decir que el liderazgo, si es que alguna vez lo hubo en León, Guanajuato, en materia de seguridad pública, se fue hace mucho, se nota el hartazgo en una persona, y así se nota en el jefe de policía de esta ciudad.

Como empresarios, hemos ido desarrollando un sentido crítico, de tal manera que nos permita analizar lo que pasa a nuestro alrededor, y no nos "chupamos el dedo" tan fácil en lo que dice la autoridad.

En una entrevista que tuve con el periódico Milenio acá en la ciudad en León, el reportero Pablo Carrillo, me preguntaba lo siguiente:

¿Cómo es posible que las autoridades no puedan con la inseguridad, porque esta mal todo?

"Es simple amigo, no hay voluntad política, es decir, no quieren ni les interesa solucionar el problema, como empresarios de seguridad, vivimos la delincuencia desde nuestra trinchera, y vemos con tristeza, que el dinero destinado para seguridad pública, no tiene resultados, peor nos ven como el problema cuando la vía pública no es nuestro ámbito. Si pides a las autoridades que te informen de su 'estrategia' para solucionar este problema, sólo te dejan en visto".


$12.00

am

LAS NOTICIAS COMO SON

Síndico acusa soberbia de Jefe de Seguridad

Reclama a Seguridad ¿qué hace?

PROTESTA

Exigen seguridad empleados del Poder Judicial Federal

JUDICIAL DE LA FEDERACION

Arranca App de taxis

Lo convoca el Secretario

¡Viene Alejandro Sanz!

vivir+

León, técnico en sus manos

deportivo

A partir de hoy, los resultados de la Lotería Nacional en su sección AM 2

¿Cómo sociedad que tenemos que hacer para disminuir el crimen? Es insoportable.

"¡Alzar la voz! Todos comentan lo que se sabe del crimen, pero nadie quiere hacer nada, todas las noticias que se ven parecen que son series de Netflix, es decir, nadie cree que pasen porque no les pasa, todos tenemos una posición cómoda y comodina, así no se puede hacer un cambio".

DELITOS EN LEÓN

(Comparativo enero 2022 vs. 2023)

MÁS HOMICIDIOS...

Delito	Variación
• Homicidio doloso +feminicidio	37.1%
• Violencia familiar	28.3%
• Robo c/ violencia	20.2%
• Lesiones dolosas	12.3%
• Robo a negocio	8.6%

MENOS ROBOS DE AUTOS

Delito	Variación
• Violación	-26.9%
• Homicidio culposo	-76.5%
• Robo a transeúnte	-50%
• Robo de vehículo	-38.3%
• Robo a casa habitación	-28.1%
• Narcomenudeo	-1.0%

Fuente: Observatorio Ciudadano de León (OCL) con base en delitos denunciados.

El secretario de Seguridad, Mario Bravo Arrona, en reunión ayer por la tarde con el síndico José Arturo Sánchez Castellanos, luego de los señalamientos de este último. / Foto: Twitter Secretariado Seguridad de León

Foto: - Wikimedia Commons

León es una referencia de inseguridad para nosotros, ¿el secretario de Seguridad Pública de León, deberá seguir en cargo?

"No, ya tiene mucho tiempo como el secretario del estado, y si nos basamos en la ciencia de la psicología, te puedo decir que si comenzaron el puesto con un ideal, ese ideal se fue hace mucho, pueblo hablar por León, que el jefe de policía Mario Bravo Arrona, no tiene ningún interés en solucionar la delincuencia, ni atiende a la ciudadanía por voluntad, si lo mandan a dar la cara lo hace, pero si por él fuera no lo haría nada, sólo está calentando un asiento, hace poco salió que se negó atender a un síndico del ayuntamiento de León de nombre José Arturo Sánchez. ¿Qué podemos esperar los demás? Con autoridades así, no se puede solucionar nada, por eso decía que se requiere voluntad política, y no la hay".

¿Cuáles son los delitos que en la ANESP ven que están fuera de control?

"Nada está controlado, nunca lo estuvo, pero los delitos que son muy notorios son: homicidio, robo-asalto y secuestro".

¿Qué recomendaciones podemos darle a la ciudadanía para que no sean víctimas de la delincuencia?

"No podemos decirles que no salgan, el dinero no llega a casa del aire, tienen que tomar cursos, pláticas, conferencias, etc., de cómo responder al peligro, ya ni siquiera hablar del asunto de la prevención, nadie prevé nada, pero cuando el problema se presente saber cómo debemos responder para minimizar el impacto emocional y economico".

Finalmente amigos, el crimen-delincuencia es responsabilidad de todos en México, no podemos hacer oídos sordos, y alzar la voz sólo cuando nos convenga, las estrategias de seguridad no están funcionando y todos los problemas del crimen nos van a golpear en la cara con fuerza, porque cuando la policía no puede con la urbe, la urbe se mete a tu casa. ■

VERGARA & ASOCIADOS
BUFETE

Somos expertos en establecer las estrategias más idóneas en Prevención de Delitos; **limitando los posibles daños** que atenten contra su Integridad y su Patrimonio.

Somos una firma especializada en:

- **Prevención del Delito.**
- **Litigio Penal.**
- **Seguridad Corporativa.**

Nuestra Firma le brinda tranquilidad, ya que contamos con amplia experiencia por más de veinte años en todo el territorio nacional así como en el extranjero.

Insurgentes Sur 730. Piso 2,
Col. del Valle. CP 03100. CDMX.

contacto@vergarayasociados.com.mx

55 7698 6817

/VergaraBufete /bufetevergarayasociados /bufetevergarayasociados company/bufete-vergara-y-asociados

MONITOREO 360:

CALIDAD, CONOCIMIENTO Y PENSAMIENTO PREVENTIVO

MÉXICO | Antonio Venegas / *Staff* Seguridad en América

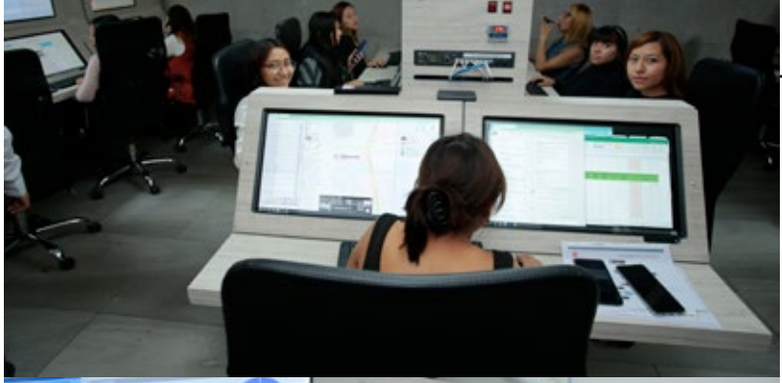
Una empresa que reconoce la importancia del conocimiento dentro del proceso preventivo en contra del riesgo al transporte

Una parte fundamental dentro de la seguridad privada es el área de logística y transporte, la custodia de mercancías es un gran elemento dentro del sector económico de una empresa, la seguridad de éstas durante el trayecto es primordial para las tres partes involucradas en la prestación de este servicio: el cliente, el proveedor y el transportista encargado del servicio, ya que se debe preservar los dos aspectos primordiales para la empresa, el producto y la vida humana.

Al analizar estos factores, nos damos cuenta de cómo hay más partes que influyen en el desarrollo de este servicio y que son de igual importancia, una de ellas es el área de monitoreo. Al hablar del transporte de mercancía por carretera los riesgos que existen abundan, el panorama tan solo en México para el desarrollo de este negocio se ve amenazado cada día, la delincuencia y el crimen organizado, factores naturales están a la orden del día. Teniendo en cuenta estos riesgos, la seguridad privada implementa nuevas medidas de prevención y reacción ante estos sucesos, las empresas encargadas de brindar seguridad y monitoreo a estos servicios crecen y se adaptan a estos retos, un ejemplo de esto es Monitoreo 360.

Fundada con los mayores estándares de calidad y compromiso, Monitoreo 360 es una empresa que, desde sus cimientos, está conformada por expertos en seguridad privada quienes conocen el campo de trabajo y la forma de laboral, así como por colaboradoras capacitadas para el ejercicio de la prevención del riesgo. Tan solo en México, el aumento al robo de transporte ha sido exponencial, un tema desafiante que cada vez requiere mayores compromisos, conocimientos e inversiones.

Algo que Monitoreo 360 ha implementado recientemente es elevar el nivel de los estándares de infraestructura que se utilizan al nivel de cualquier operación de tecnología, han puesto los componentes claves como son: energía, comunicaciones, ambiente y ergonomía al nivel de cualquier tipo de instalaciones de IT o de un centro de control de transporte terrestre, entendiendo así que el nivel del desafío ya iguala ese tipo de aspectos.



EQUIPO DE TRABAJO

El área de monitoreo, el núcleo de la empresa, es una parte muy importante dentro del servicio, técnicamente se pueden dividir sus aspectos en energía, ambiente, comunicaciones y tecnología, representadas en las computadoras dentro de las oficinas que monitorean el transporte. Dentro de esto, cada maquina es independiente, se conoce cuanta energía consume cada una, se tiene redundancia en comunicaciones, se controla la temperatura todo el tiempo y se evita el uso de aire acondicionado por un tema ecológico y de consumo de energía, dado que las personas encargadas del monitoreo generan calor, las computadoras se encuentran encerradas para concentrar el calor y expulsarlo. La innovación tecnológica esta presente en el área de computadoras con estas características, éstas se encienden automáticamente dependiendo de la temperatura.

PROCESOS Y PERSONAS

Sobre la infraestructura se encuentran dos aspectos: los procesos y las personas. Desde el punto de vista de las personas, tener métricas sobre la confiabilidad de las personas se ha vuelto más crítico; saber cuál es el nivel de conocimiento y experiencia, el entrenamiento, las pruebas de confiabilidad son procesos recurrentes y periódicos dentro de la empresa, todo esto para asegurarse que el actuar no solo está condicionado por un protocolo o una orden, sino está condicionada de manera continua y operada por el conocimiento y la confiabilidad de una persona.

No sólo es el actuar, sino cómo ese actuar estuvo condicionado por un entrenamiento y una prueba de confiabilidad. En el aspecto de procesos se necesita innovar continuamente por encima del ritmo que avanzan los grupos delictivos. Hablando acerca de transportes de alto riesgo, Monitoreo 360 ha implementado servicios de monitoreo por CCTV o videovigilancia de forma continua 24/7, algo que generalmente solía hacerse sólo con inmuebles, esto representa muchos desafíos en tres áreas: la instalación y mantenimiento de esas cámaras, ya que se deben adaptar a las condiciones del transporte, es el mantenimiento de toda una infraestructura de equipamiento funcionando todo el tiempo; la configuración y gestión de la comunicación, por los altos costos que conlleva.

Por último, el entrenamiento, ya que no hay muchos precedentes para hacer videovigilancia focalizada en buscar cosas, los precedentes que existen son casos muy específicos, entrenarse para hacer videovigilancia de vehículos requiere de un entrenamiento especializado, lo cual implica un enfoque completamente preventivo donde la reacción requiere una revisión de procesos, todo esto motivado por muchas razones, por ejemplo, la expansión del transporte derivado del *e-commerce* en la época de la pandemia, algo que todavía continúa creciendo y que evidentemente genera una oportunidad que se está manifestando en el incremento de la delincuencia en esa área.

SOLUCIÓN AL PROBLEMA

En el caso antes mencionado, las personas están acostumbradas con el *e-commerce* a conocer el fin del proceso, pero no se tiene en cuenta que el proceso del producto continúa existiendo, la logística es igual o más compleja que antes. Todos los procesos que hay detrás de esto representan oportunidades de merma, de delincuencia y para cada uno de ellos se tienen que desplegar operaciones específicas. Monitoreo 360 afronta estos retos, primero con capacitación, ellos estudian el proceso, se cuenta con una orientación 100% preventiva, si la empresa contara con un eslogan oficial este sería "pensamiento preventivo", el equipo se preocupa de qué se va a hacer cuando ocurre un siniestro, pero los ocupa que no suceda, para esto se requiere un alto grado de conocimiento sobre el proceso que se esta vigilando.

Algo que pareciera una pregunta simple como "¿qué es un vehículo detenido?", si no se cuenta con el conocimiento técnico de la ingeniería, es difícil de responder. Hasta la cosa más simple requiere un conocimiento técnico y un método científico de prueba, ese es el sello distintivo del equipo de Monitoreo 360, esa es la forma en la que se aborda cualquier tipo de problema, esos son los valores en los que la empresa cree.

Toda actividad tiene un proceso, algo que se tiene que valorar. Es por esto por lo que la capacitación y evaluación periódica, así como el conocimiento adquirido del enfoque, es vital dentro de la empresa. ¿Cómo solucionan los problemas? Concentrándose en entender el problema y no en que la solución llega por sí sola, quien estudia el problema eventualmente encontrará la solución. ■

Fotos: Mónica Ramos / SEA

DECÁLOGO BÁSICO DE LA SEGURIDAD PRIVADA

PARA IMPLEMENTAR EN CORPORATIVOS Y RESIDENCIALES

Foto: - Freepik

MÉXICO | David Makoto Nancarrow Sugiura

Es importante señalar que además de los siguientes 10 puntos básicos que se deben tener en cuenta al implementar un servicio de Seguridad Privada en estas edificaciones, también debemos seguir las políticas y procedimientos establecidos en las consignas específicas de cada empleador para así mantener una actitud responsable y diligente en el ejercicio de nuestras funciones como elementos de seguridad privada.

1. **Vigilancia constante.** Mantener una vigilancia constante en las áreas asignadas para prevenir y detectar cualquier actividad sospechosa o posible incidente.
2. **Protección de la propiedad.** Garantizar la protección de la propiedad y los activos asignados, evitando robos, vandalismo u otros daños que vulneren la seguridad general del inmueble.
3. **Control de accesos.** Controlar y supervisar los accesos a las instalaciones, verificando la identidad de las personas y asegurándonos de que tengan los permisos necesarios para ingresar.
4. **Prevención de incidentes.** Adoptar medidas preventivas para evitar situaciones de riesgo, como la implementación de sistemas de seguridad, alarmas, cámaras, analíticas y protocolos de emergencia.

Foto: - Freepik

Foto: - Freepik

5. Respeto a los derechos humanos. Tratar a todas las personas con respeto y dignidad, asegurándonos de no violar sus derechos humanos mientras realizan su labor de seguridad.

6. Colaboración con autoridades. Al ser coadyuvantes de la Seguridad Pública, debemos colaborar y coordinar con las autoridades competentes, proporcionando información relevante y asistencia en situaciones de emergencia o delitos.

7. Comunicación efectiva. Mantener una comunicación efectiva con el personal de seguridad y con otros departamentos de la organización, transmitiendo información relevante de manera clara y oportuna.

8. Formación y capacitación. Mantenerse actualizado sobre las técnicas, procedimientos y tecnologías de seguridad, participando en programas de formación y capacitación para mejorar nuestras habilidades y nuestra eficiencia.

9. Confidencialidad. Resguardar la información confidencial a la que se tenga acceso durante nuestro trabajo, evitando divulgarla o utilizarla indebidamente.

10. Integridad personal. Mantener una conducta ética y profesional en todo momento, evitando comportamientos indebidos o situaciones que puedan comprometer la integridad personal o la de otros. ■


Foto: - Freepik

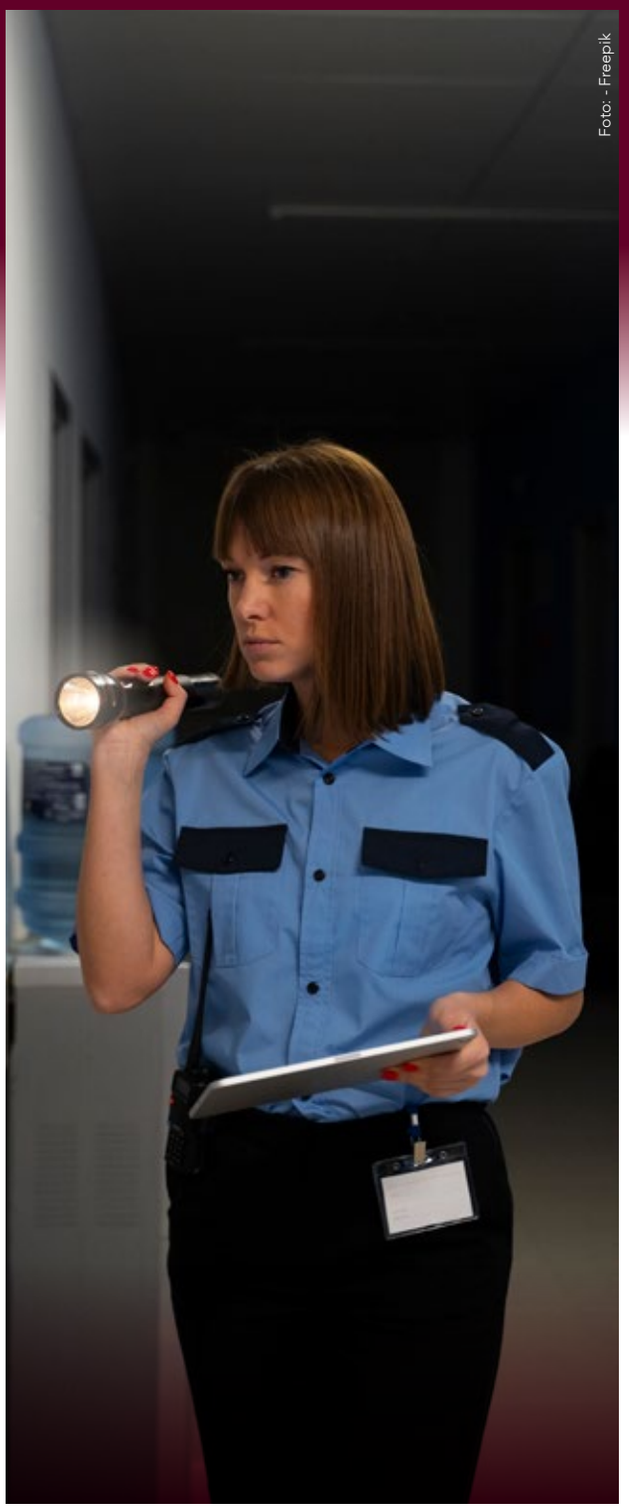


Foto: - Freepik

David Makoto Nancarrow Sugiura, director general de Doorman. Más sobre el autor:

Foto: - Freepik

GRUPO SALUS:
SOLUCIONES SIMPLES A PROBLEMAS COMPLEJOS

Con el software FACEit no sólo hay control de asistencia, sino efectividad, calidad y seguridad en cada servicio

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Grupo Salus es una empresa que se ha especializado en el desarrollo de un *software* que en primera instancia estaba enfocado para el control de asistencia, pero que requeriría de mayor complejidad y herramientas para uno de sus clientes. FACEit, se implementó en 2022 en una de las empresas de seguridad privada con mayor prestigio en el país: Galeam Security Services, y lo que empezó como una solución para la asistencia y control de sus elementos de seguridad, actualmente se ha convertido en una herramienta de asistencia, control, monitoreo, productividad y garantía del servicio.

"Este *software* que implementamos de la mano de Grupo Salus, no sólo informa y controla quién es el guardia que llega al servicio, sino que además nos indica en tiempo real cuál es el estado de cobertura del servicio, que el guardia se presenta perfectamente uniformado, y que está realizando los rondines; de igual manera nos informa si el supervisor llegó al lugar, y uno de los beneficios es que toda esa información también la tiene el cliente, lo que nos obliga a nosotros a dar un servicio de calidad, además de que va ligado con un centro de monitoreo, por lo que la capacidad de reacción ante una situación de riesgo es muy alta", comentó Francisco Javier de Lago Acosta, director general de Galeam Security Services.

Este *software* se ha ido robusteciendo de acuerdo a las necesidades de Galeam, según Eduardo Castillo, socio director de Grupo Salus, uno de los grandes retos en cualquier implementación de procesos y tecnología nueva siempre es romper la barrera de la resistencia al cambio, sin embargo con Galeam se lanzaron comunicados, involucrando a las personas de todos los niveles dentro del proceso de implementación, lo cual hizo que el cambio fuera mejor aceptado, explicándoles para qué es y cuáles son sus objetivos.

"Algo que caracteriza a Grupo Salus y nuestro modelo de negocio, es que siempre tratamos de aprender de nuestros clientes para mejorar nuestro *software* e ir avanzando; con el tiempo, Galeam ha sido un ejemplo de este proceso, nos han ayudado mucho a ir fortaleciendo el *software* con base en las diferentes necesidades que ellos mismos nos han planteado, por ejemplo toda la parte de los tableros de control en tiempo real para la visualización de operación en diferentes sentidos, para la parte de rondines, de control de presencia, herramientas que no se tenían originalmente en el *software* y que con la imagen y la funcionalidad que Galeam nos hizo que podía funcionar mejor para su centro de monitoreo, las implementamos y eso nos ayudó mucho a robustecer la solución, añadió Eduardo Castillo.

MÁS QUE UN CONTROL DE ASISTENCIA

Este *software* nació como un control de asistencia de personal remoto, a través de una *app* que funciona en cualquier celular Android, cualquier guardia que esté en servicio puede hacer su asistencia la cual es con reconocimiento facial y se envía en tiempo real a la Nube, esa información es procesada. Dentro de los principales módulos están el inventario de personal donde aparece el registro de los guardias, su documentación digital y se puede acceder a ella desde cualquier lugar, para consultar por ejemplo sus antecedentes penales; para guardias armados, está digitalizado el permiso de portación de armas.

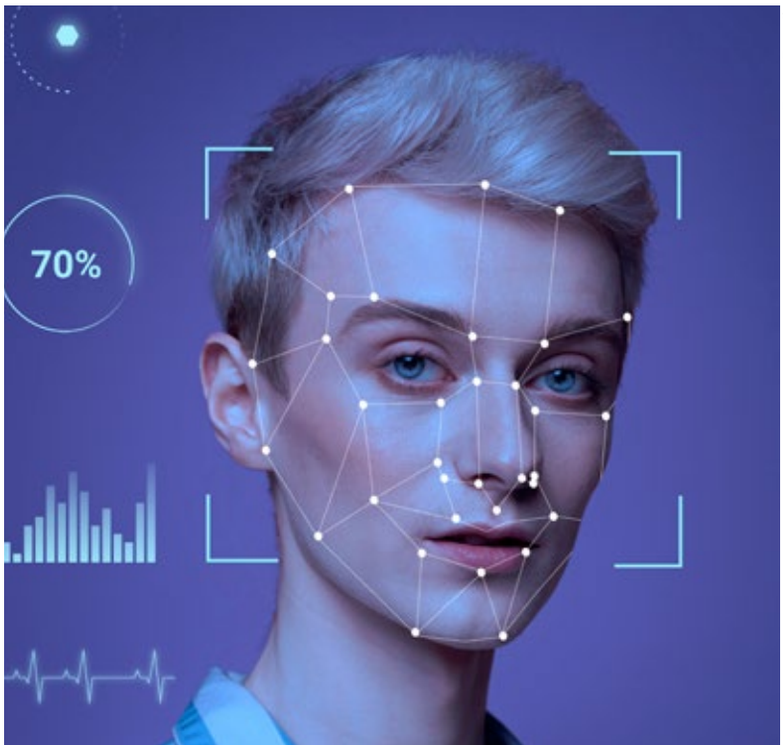


Foto: - Freepik

También existe un módulo de rondines y eventos con sus bitácoras y la parte de rol de incidencias en los servicios, ya sean derivados de los rondines o incidencias especiales a través de una bitácora electrónica donde se puede grabar el tipo de evento, en qué lugar, la geolocalización y se le puede agregar archivos multimedia de video, audio y fotografía para tener un reporte completo de los diferentes eventos que van sucediendo en la operación. Existe también un módulo completo para custodias con vehículos, control de los custodios, de los viajes y la programación de éstos, entre otros. Todo esto bajo un esquema muy robusto, ya que Grupo Salus utiliza servidores con varios proveedores de servicios de hosteo a nivel mundial, dentro de un esquema de seguridad muy importante, el acceso a la información está completamente restringido y la privacidad de los datos está muy bien resguardada.

"Principalmente existen tres beneficios de este *software* y que le han dado un valor agregado a Galeam: uno, eficiencia en el conocimiento del estatus del servicio en el menor tiempo posible; dos, capacidad y calidad en el hecho de que estamos ciertos sobre cómo están operando nuestros elementos en cualquiera de nuestros servicios en tiempo real, y tres, crecimiento. Todo lo que se nos ha ocurrido con base en los servicios se lo planteamos a Grupo Salus y él lo materializa. Tengo que reconocer que les hemos puesto la vara muy alta y ellos han respondido muy bien. Ha costado trabajo, pero lo han logrado y eso nos llena de orgullo, porque somos una empresa de seguridad privada que exige excelencia y contamos con esta solución, sin embargo, lo mejor sería que todos lo tuvieran para beneficio del cliente y del sector", comentó Francisco de Lago.

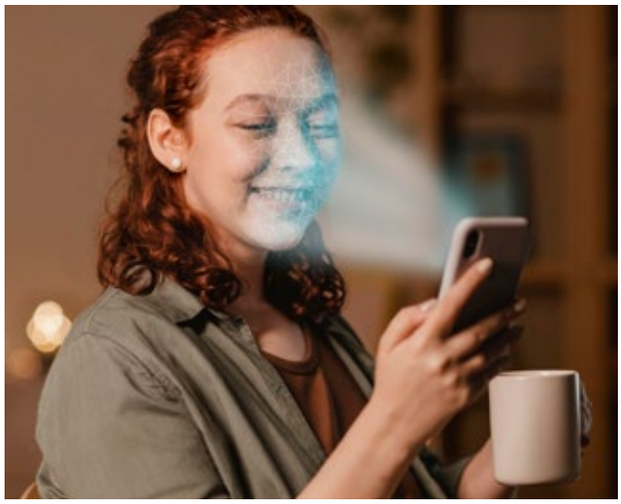


Foto: - Freepik

"En Grupo Salus escuchamos a nuestros clientes y con ello robustecemos a nuestro *software* de acuerdo a sus necesidades; nosotros no vendemos solamente la solución, sino que la mejoramos para cada cliente; todos nuestros algoritmos de inteligencia artificial y reconocimiento facial son propios de Grupo Salus, lo que brinda una certeza para su funcionamiento. La experiencia con Galeam ha sido de mucho éxito, hemos implementado la solución con diversos servicios y eso le ha generado un valor agregado en el mercado, una mayor competitividad, y eso es lo que nosotros buscamos con cada cliente, el poder generar a través del uso de la tecnología un diferenciador y que ellos con la tecnología puedan darle un mejor servicio a sus clientes", puntualizó Eduardo Castillo. ■

"Algo que caracteriza a Grupo Salus y nuestro modelo de negocio, es que siempre tratamos de aprender de nuestros clientes para mejorar nuestro *software* e ir avanzando", **Eduardo Castillo**

"Uno de los beneficios es que toda esa información también la tiene el cliente, lo que nos obliga a nosotros a dar un servicio de calidad", **Francisco Javier de Lago Acosta**

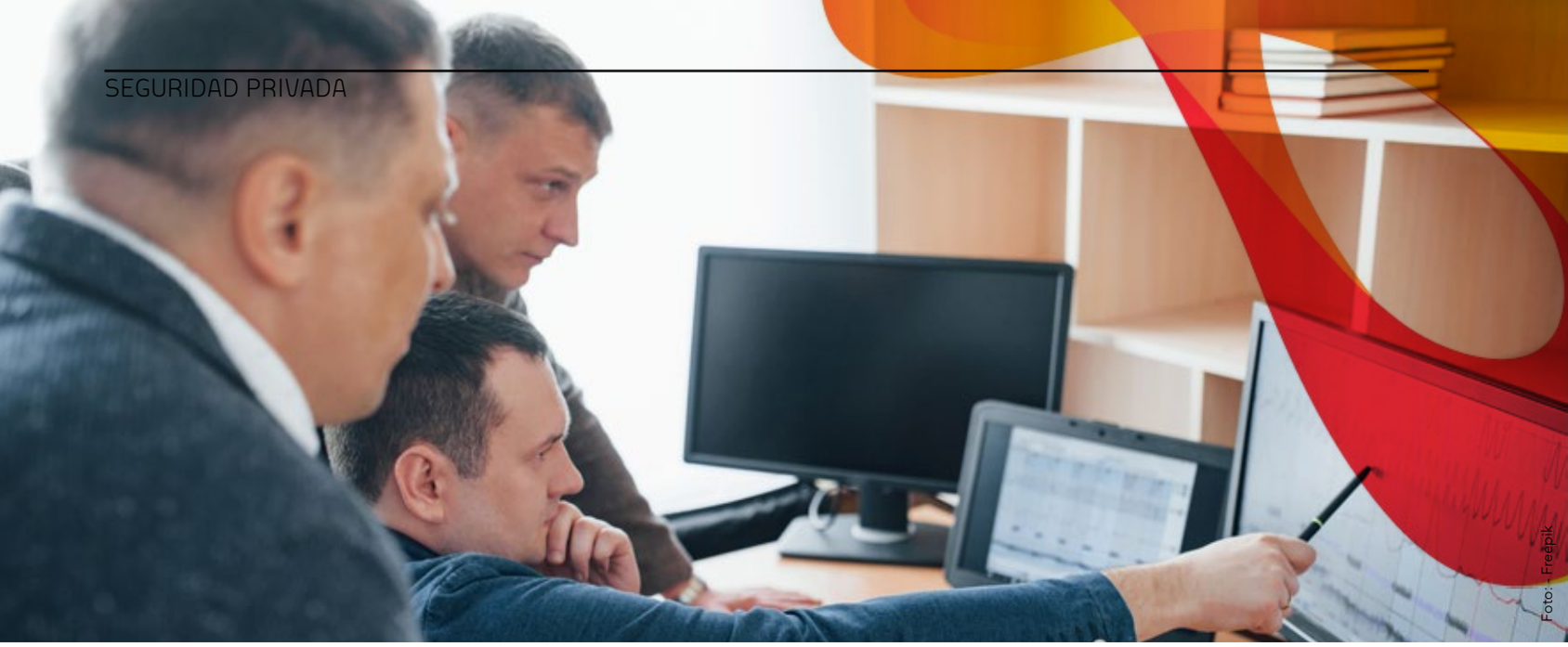


Foto: Freepik

CARACTERÍSTICAS Y HERRAMIENTAS
PARA UN BUEN SUPERVISOR DE SEGURIDAD

En esta ocasión el autor da las bases y características que un buen supervisor deberá contar y aplicar en su día a día, para proteger instalaciones y la vida de las personas en paralelo con sus herramientas en su trabajo

MÉXICO | Hermelindo Rodríguez Sánchez

Da gusto que alguien tenga tan en claro cuál es el rol de un verdadero supervisor de Seguridad. En la realidad, la cosa generalmente pasa por otros meridianos.

Para muchas empresas (sean prestadoras de servicios del ramo y/o tomadores directos), el tema es visto en forma notoriamente más acotada, como modo de justificar las limitadas remuneraciones que están dispuestos a reconocerles, si se los compara con respecto de los percibidos por todos aquellos a su cargo y responsabilidad.

Los resultados saltan a la vista. No es casual que las principales quejas de gran mayoría de los clientes de las prestadoras apunten principalmente hacia los supervisores, y estos temas que muy razonablemente consideran como de su incumbencia:

1) Falta de concurrencia y/o continuidad en la supervisión.

2) Escaso conocimiento del terreno y/o de sus consignas específicas.

3) Ausencia de ideas para ejercitaciones / simulaciones y evaluación.

4) Falta de iniciativa en el ajuste de las prestaciones.

5) Tardía respuesta ante sugerencias y/o reclamos del cliente.

6) Tardía o nula reacción en casos de emergencias.

7) Escasa o nula formación específica, y ausencia de iniciativa para su corrección tanto de parte de supervisor como del prestador.

Además, el supervisor de Seguridad (en el caso de prestadoras de servicios del rubro) es aquí una figura y categoría laboral que en México sólo aparece formalmente reconocida en la legislación específica de seguridad privada.

En el resto del país la figura del supervisor aparece con un lacónico vigilador (guardia) principal + adicional por supervisión, lo que devalúa gravemente su rol ante sus subordinados.

De más está decir que no es tarea de los propios supervisores de Seguridad el mejorar cierta parte de lo citado, y para aquello que sí está a su alcance no hay incentivos. Algún día veremos otro horizonte en este tema, pero el actual aparece bastante nublado.

En empresas especializadas en vigilancia o en compañías que utilizan sus propios guardias de seguridad, la actividad de supervisión tiene una incuestionable importancia. Son los supervisores los principales responsables de la correcta y eficiente ejecución de las tareas cotidianas de vigilancia y también de proteger las vidas de quienes contratan los servicios de los profesionales bajo supervisión.

Si observamos las diferentes empresas de vigilancia, constataremos que la denominación de "supervisor" es utilizada de manera muy indistinta. Pero, ¿cuáles son realmente las misiones que, casi obligatoriamente, debe desempeñar un supervisor?

El supervisor es el vínculo entre la gerencia de la empresa (en el caso de las empresas de vigilancia hablamos de la gerencia operacional), que es el escalón superior, y los equipos que se desempeñan en el nivel de ejecución de las tareas

OBJETIVO DEL SUPERVISOR

El supervisor es el vínculo entre la gerencia de la empresa (en el caso de las empresas de vigilancia hablamos de la gerencia operacional), que es el escalón superior, y los equipos que se desempeñan en el nivel de ejecución de las tareas. La actividad de supervisión en el campo de la seguridad tiene que ver directamente con la prestación de los servicios, la organización de la vigilancia en los puestos, el establecimiento de normas, entrenamiento, adiestramiento y evaluación del nivel de satisfacción del cliente con los servicios que ha recibido.

Las misiones de un supervisor no se deben confundir con las de un "administrador" o "capataz". El supervisor, obligatoriamente tiene que preocuparse por los resultados del trabajo, y según los conceptos de calidad vigentes, debe esmerarse para que esos resultados sean cada vez mejores. Cuando se trata de la actividad de seguridad, los profesionales involucrados trabajan en medio de presiones, incomprensiones, carencia de recursos, por lo tanto, para que el servicio sea de calidad, el supervisor debe tratar de superar tales obstáculos.

El supervisor no sólo tiene que llevar a cabo un conjunto de misiones (resultados), sino también preocuparse por la forma en que esas misiones se desempeñan (procesos). En la medida en que los subordinados logran reconocer el esfuerzo en el trabajo cotidiano, se constata una sensible mejora del patrón de desempeño del equipo de seguridad.

Foto: - Freepik

El supervisor de seguridad debe ser capaz de inspirarle a sus subordinados el "amor al arte" por la tarea que realizan, haciéndoles entender que es excepcionalmente importante. Se trata de un serio esfuerzo de carácter "educacional", en el que no sólo se debe enseñar las técnicas del servicio de vigilancia sino surgir en los hombres (que muchas veces no le dan la debida importancia a la actividad que desempeñan) valores y sentimientos de profesionalismo y búsqueda de la perfección en lo que hacen. Sólo de esa manera podrán inspirar en todos los demás funcionarios y en el público en general, el consecuente respeto por quienes arriesgan su vida al desempeñar una actividad de alto riesgo.

EL BUEN SUPERVISOR DE SEGURIDAD DEBE:

1. Conocer perfectamente su actividad, buscando el perfeccionamiento constante y la actualización técnica. Tener en mente que su actividad profesional exige una gama de conocimientos que no se agotan, por lo que deberá estar en constante aprendizaje.
2. Conocerse a sí mismo. Tener capacidad de autocríticas y tratar de ser mejor como ser humano.
3. Conocer a sus hombres, preocuparse de su bienestar y tratarlos con dignidad y respeto.
4. Mantener a sus hombres bien informados, dentro de lo que permite el principio de compartimentación de la información.
5. Verificar siempre si las órdenes han sido bien comprendidas, ejecutadas y fiscalizadas.
6. Inspirar el profesionalismo y el espíritu de equipo en sus subordinados.
7. Tomar decisiones en el momento adecuado y de manera acertada.
8. Asumir total responsabilidad por sus actos
9. Inspirar respeto y confianza a los subordinados.
10. Nunca pedirle a su equipo aquello que esté por encima de su capacidad.
11. Convertirse en un verdadero ejemplo de aquello que espera de sus subordinados.

El supervisor no sólo tiene que llevar a cabo un conjunto de misiones (resultados), sino también preocuparse por la forma en que esas misiones se desempeñan (procesos)

ACTIVIDADES QUE DEBE DESEMPEÑAR UN BUEN SUPERVISOR DE SEGURIDAD

1. Ejercer un control rígido sobre aquello que se encuentran bajo su supervisión directa.

2. Verificar las condiciones generales en los puestos de servicio.

3. Mantener un registro completo y actualizado de los puestos de servicio bajo supervisión/fiscalización, donde aparezcan datos como: nombre y dirección del puesto, teléfonos del puesto, nombres y teléfonos de los responsables con los que debe comunicarse en caso de emergencia, nombres de los guardias de seguridad, cantidad, tipo y número de serie del armamento de servicio, así como también otro detalle que se considere oportuno.

4. Verificar, si es posible diariamente, la asistencia y puntualidad de los subordinados.

5. Inspeccionar los servicios de seguridad prestados.

6. Establecer, cuando se necesite, los horarios de los efectivos de seguridad.

7. Desarrollar un análisis de los riesgos de seguridad en los puestos de servicio. Determinar qué posición debe ocupar cada vigilante e indicarle como debe actuar en su trabajo cotidiano y en casos de emergencia. Elaborar procedimientos sobre cómo actuar en casos específicos.

8. Crear y hacer cumplir las órdenes de servicio.

9. Entrenar a los vigilantes (si es posible diariamente) en las órdenes de servicio y cualquier procedimiento pertinente a la seguridad del puesto de servicio. Asegurarse de que las conocen y las cumplen.

10. Mantener en los puestos de servicio archivos actualizados que contengan las órdenes de servicio, manuales técnicos, oficios o comunicados emitidos o recibidos, libros de registro de incidentes, planillas de control, etc., esclareciendo a los subordinados que tales documentos son información de carácter reservado, cuyo contenido no debe darse a conocer a ninguna persona ajena a la labor de seguridad.

11. Instruir y motivar a los profesionales bajo su mando para desempeñar la actividad de seguridad. Tratar de compensar las deficiencias técnicas de los individuos a través de conferencias, cursos, etc.

12. Convocar a reuniones periódicas con el personal bajo su mando para analizar el desempeño de todos los miembros del equipo, analizar sugerencias, formular críticas, revisar procedimientos y establecer nuevas rutinas de trabajo.

13. Preparar notas de instrucción, organizar murales o cualquier otra forma de poner información técnica al alcance de los subordinados.

14. Tratar a los subordinados con urbanidad, pero sin transigir en lo que tiene que ver con la disciplina, el cumplimiento de las órdenes de servicio y cualquier falla motivada por indolencia, negligencia o mala fe, que pueda poner en riesgo el buen funcionamiento del servicio o la integridad física de terceros.

15. Aplicar ejemplarmente las medidas disciplinarias que se necesiten, dejando constancia, de manera detallada, de la causa que motivó la sanción.

16. Cada vez que se reemplace un vigilante, debe dedicarle el tiempo necesario a orientar al nuevo agente para que rápidamente esté en condiciones de realizar su trabajo.

17. Desarrollar una política de concientización de la necesidad de cooperar con todo lo que tiene que ver con seguridad, mostrando los beneficios que a todos les trae esa actitud.

18. Verificar el estado de conservación y el funcionamiento del armamento, municiones y equipos existentes, comunicando de inmediato las irregularidades.

19. Al registrar cualquier incidente en las operaciones, utilizar el formulario aprobado o, si este no existe, dejar constancia detallada por escrito. Tratar de ser claro, preciso y minucioso en la explicación de los datos importantes. No olvidar que el registro de incidentes y los reportes constituyen documentos legales de alto valor jurídico De ahí la necesidad de redactarlos con corrección.

20. Tener siempre a la mano copias de las diferentes legislaciones relacionadas con la seguridad privada, en el ámbito nacional, departamental y municipal.

En resumen, la supervisión en seguridad debe caracterizarse por el respeto a la dignidad humana, debe tener en consideración la complejidad de los individuos, sus diferencias y limitaciones en lo físico, intelectual y moral.

El buen supervisor es aquel cuya autoridad emana de su propio ejemplo, habilidad, conocimiento técnico, capacidad de ejecución, y se basa en el elevado patrón de disciplina y eficiencia que se exige a sí mismo y a sus subordinados. Es el profesional que consigue que las personas bajo su mando realicen las tareas más difíciles, motivados muchas veces tan sólo por la admiración, la confianza y el ejemplo. ■

El supervisor de seguridad debe ser capaz de inspirarle a sus subordinados el “amor al arte” por la tarea que realizan, haciéndoles entender que es excepcionalmente importante

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

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

25 AÑOS DE EXPERIENCIA

- **25 años** de experiencia como líderes en el sector
- Más de **50 mil equipos** instalados
- Infraestructura sustentada por **AWS y Azure**
- Contamos con puntos estratégicos en todo el país
- Atención y soluciones personalizadas

amesis

Socio Amesis
amesis.org.mx

Contáctanos
55 5374 9320

*APLICAN RESTRICCIONES.
ALGUNOS ACCESORIOS Y EQUIPOS REQUIEREN ACTUALIZACIONES Y/O CONFIGURACIONES ESPECIALES.

TRUST ID

VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL

¿Estás seguro de quién maneja tu Logística y Distribución?

- Análisis de datos de confianza en línea
- Validación Fotográfica y Prueba de Vida
- Análisis de contenido en declaraciones

- PROCESOS ULTRA RÁPIDOS
- ACEPTADA EN LOS PRINCIPALES CEDIS
- CREDENCIAL CON QR
- PROCESO EN LÍNEA DESDE TU CELULAR
- CERTIFICADO IMPRIMIBLE

TRUST ID es una Solución de Grupo UDA y Tracking Systems dedicada a la validación de personal logístico como: Operadores, monitoristas, almacenistas, montacarguistas, guardias de seguridad, intramuros y demás.

Utilizamos tecnología de punta para agilizar el proceso de verificación y certificación de los datos del personal de su empresa.

- Estudio Socioeconómico
- Validación de antecedentes laborales
- Antidoping y Polígrafo

Grupo® UDA

trustid.mx

55 5374 9340

55 4141 6451

EXPO SEGURIDAD MÉXICO 2023

El 18, 19 y 20 de abril se llevó a cabo la vigésima edición de Expo Seguridad México, evento que reunió a más de 15 mil 300 asistentes por día y un sinfín de tecnología e innovaciones en esta industria

MÉXICO | **Mónica Ramos, Antonio Venegas y Tania G. Rojo Chávez / *Staff* Seguridad en América**

Este año Expo Seguridad México llevó a cabo su vigésima edición en el ya conocido Centro Citibanamex, en la Ciudad de México. Este año se contó con la presencia de más de quince mil 300 asistentes, en conjunto con Expo Seguridad Industrial, y se contó con la participación de más 350 empresas proveedoras, 40 por ciento globales, de diferentes especialidades sin dejar de lado las más de 45 conferencias, algunas de tallas internacional que se impartieron en los tres escenarios, de la mano de ASIS Capítulo 217.

La inauguración del magno evento contó con la presencia de más de 200 invitados y se realizó posterior a la conferencia titulada "¿Hay terrorismo en México? El impacto de la comunicación del miedo y sus efectos psicosociales", impartida por Mauricio Meschoulam, analista y consultor de paz y seguridad internacional. El evento comenzó con los honores a la bandera, acompañados por la banda de guerra de la Policía Bancaria e Industrial en conjunto con su escolta, posteriormente se entonó el Himno Nacional Mexicano.

Después se presentó a los miembros de presídium que incluyeron al arquitecto Víctor Manuel Aguilar Talavera, secretario ejecutivo del Sistema Estatal de Seguridad del Estado de México en representación del maestro Rodrigo Martínez, titular de la Secretaría de Seguridad del Estado de México; Héctor Morfín Chong, director de Expo Seguridad México; James Rothstein, *Chairman Security Industry Association*; Armando Zúñiga, presidente de ASUME y de COPARMEX Ciudad de México; Hermenegildo Lugo Lara, subsecretario de Inteligencia e Investigación de la Secretaría de Seguridad de la Ciudad de México; Hugo de la Cuadra Mendoza, titular del C5 Estado de México; y Jorge Antonio Ortiz Torres, asesor legal de la Secretaría de Gestión Integral de Riesgos y Protección Civil.

Héctor Morfín agradeció a los patrocinadores, expositores, y a todo el equipo detrás de la exposición ya que, gracias a ellos, el evento es uno de los más grandes de la industria de la seguridad en toda Latinoamérica, y recalcó los cuatro ejes por los que se rige la Expo; el primero consiste en generar encuentros de negocios exitosos entre proveedores y profesionales donde se vean las novedades de la industria; el segundo, es fomentar la profesionalización y capacitación; tres, fortalecer las alianzas entre sector público y sector privado, y por último, fomentar la cultura de la prevención y la concientización.

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

CONTRA INCENDIOS

Perla Ortega, directora general de MAK Extinguisher

Categoría: Equipos de Seguridad en Incendios y Control de acceso.

Empresa: MAK Extinguisher.

Entrevistado: Perla Ortega.

Cargo: directora general.

Soluciones en Expo: ante la constante demanda del cliente y aprovechando las innovaciones tecnológicas, MAK Extinguisher está presentando tres plataformas de control de acceso y riesgos, una de ellas llamada Vortex para sistemas de protección, tecnología de preingeniería recién llegada a México. También enfocándose en la Nube, MAK presenta los controles de acceso integrados con cámaras sin la necesidad de contar con un servidor, la plataforma esta nombrada Avigilon Alta, la cual permite el control de acceso a visitantes con cámaras que contienen inteligencia artificial con agilidad de grabación y almacenamiento de video. Por último, presentan las chapas y cerraduras de seguridad electrónicas en colaboración con Salto, que con su estructura robusta son más difíciles de vulnerar, ideal para sectores como la industria hotelera.

CONTROL DE ACCESO

Rogerio Coradini, Director of Sales - Latin America and Caribbean Physical Access Control – Emerging Markets Regional Business Unit de HID Global

Categoría: Control de acceso.

Empresa: HID Global.

Entrevistado: Rogerio Coradini.

Cargo: *Director of Sales - Latin America and Caribbean Physical Access Control – Emerging Markets Regional Business Unit.*

Soluciones en Expo: HID Global presentó las últimas novedades de control de acceso, como los lectores, las tarjetas virtuales como HID Mobile Access, que transforman el *smartphone* en credencial de acceso para ingresar a las áreas seguras. Esta solución es para el mercado general, pero especialmente para las verticales como educación, salud, hospitales, infraestructura crítica, puertos, aeropuertos y edificios corporativos.

Alejandro Loera Harfush, gerente de Ventas de Latinoamérica de Keri Systems

Categoría: Control de acceso.

Empresa: Keri Systems.

Entrevistado: Alejandro Loera Harfush.

Cargo: gerente de Ventas de Latinoamérica.

Soluciones en Expo: Keri Systems presentó la novedad Borealis, que es un *software* que controla los productos de la marca y que está alojado en la Nube, esto permite controlar desde cualquier dispositivo móvil, esto libera de alguna forma el hecho de tener un servidor alojado en nuestra propia Nube con toda la seguridad de encriptación de datos y antihackeo, de tal manera que el cliente ya no se tiene que preocupar de la actualización de *software*, *firmware* y sobre todo del respaldo de sus equipos.

David Montoya, director regional de Paessler América; y Jorg Altenheimer, CEO de Key Business

Categoría: Monitoreo y Control de Acceso.

Empresa: Key Business.

Entrevistado: Jorg Altenheimer.

Cargo: director general.

Soluciones en Expo: Key Business Process Solutions presentó su nuevo producto en colaboración con Paessler, una plataforma para monitoreo de dispositivos IoT, de redes y para cualquier sector de la industria capaz de dar alertas antes de situaciones de riesgo garantizando un servicio de calidad en la logística.

VIDEOVIGILANCIA

Mauricio Swain, director de Ventas para Latinoamérica de Milestone Systems

Categoría: Videovigilancia.

Empresa: Milestone Systems.

Entrevistado: Mauricio Swain.

Cargo: director de Ventas para Latinoamérica.

Soluciones en Expo: Mauricio Swain señaló que en esta vigésima edición de la Expo, Milestone cumplió 25 años haciendo VMS (*Video Management System o Video Management Software*) para la videovigilancia, por lo que además de presentar su aniversario, también lanzó su *release* 2023 R1, que ofrece una mejor experiencia para los usuarios finales, dentro de las mejoras que trae está *picture in picture* para poder ver una imagen dentro de una imagen más pequeña, una experiencia mejor para los usuarios, sobre todo para los usuarios móviles.

Ian Juárez, director comercial para México en Hanwha Vision

Categoría: Videovigilancia.

Empresa: Hanwha Vision.

Entrevistado: Ian Juárez.

Cargo: director comercial para México.

Soluciones en Expo: este año la marca presentó el nuevo nombre de la empresa, Hanwha Vision (antes Hanwha Techwin), porque toda la marca está cambiando al tema de visión, sensores, inteligencia artificial y sustentabilidad para los usuarios finales, integradores y clientes en general. También mostró una cámara que es un servidor, donde además de grabar también se puede administrar cinco cámaras adicionales, se tiene un sistema pequeño en donde nunca se tendrá un grabador, no se necesita un espacio para un servidor y no se requiere la infraestructura para alojar un servidor.

David Lira, gerente de Desarrollo de Negocios para México en QNAP

Categoría: Videovigilancia.

Empresa: QNAP.

Entrevistado: David Lira.

Cargo: gerente de Desarrollo de Negocios para México.

Soluciones en Expo: QNAP presentó soluciones de última generación de cuatro, ocho y diez discos, enfocados mucho más en videovigilancia, pero también tomando en cuenta la ciberseguridad. También mostró el servidor NAS (*Network Attached Storage*) QNAP TS-473A, que está enfocado en las pequeñas y medianas empresas, es un NAS que permite crear videovigilancia dentro de él y llevar hasta 15 o 16 anillos de seguridad dentro del propio servidor, ya que hoy se mezclan mucho esos dos mundos de ciberseguridad con seguridad física.

Camilo Orjuela, director comercial de Neural Labs México

Categoría: Videovigilancia.

Empresa: HERTA/Neural Labs.

Entrevistado: Camilo Orjuela.

Cargo: director comercial.

Soluciones en Expo: Herta, empresa especializada en reconocimiento facial para seguridad, control de acceso y Neural Labs, compañía enfocada en el control de acceso vehicular y logística de transportes, trae en conjunto nueva tecnología desarrollada para seguridad vial, trabajando en pro de aligerar el tráfico, prevención de accidentes, recuperación de vehículos robados y otras problemáticas que actualmente se encuentran vigentes en México.

Manuel Zamudio, Industry Associations Manager de AXIS Comunications para América Latina

Categoría: Videovigilancia.

Empresa: AXIS.

Entrevistado: Manuel Zamudio.

Cargo: *Industry Associations Manager*.

Soluciones en Expo: este año Axis presenta las ventajas de la nueva tecnología en video, audio, termografía o radar en los dispositivos, haciendo uso de la inteligencia artificial como *Deep Learning* y analíticas diversas en la búsqueda de la mejora operativa en la seguridad y la privacidad. También la posibilidad de integrarse a cualquier plataforma que esté basada con código abierto, todo esto con la finalidad de poder ayudar a los usuarios finales a diseñar soluciones a la medida de manera responsable basándose en estudios de costo total de propiedad buscando informar sobre cómo debería hacerse un análisis de costos.

SEGURIDAD PRIVADA / AMESP

Mauricio Natale, director general de City Safe

"En Expo Seguridad México presentamos una nueva solución para transporte seguro, logística, escoltas, o vehículos para transporte de valores. Es un diseño totalmente innovador, son vehículos perfectamente blindados, seguros, elaborados con materiales de alta tecnología que los hacen muy livianos, lo que se traduce en economía y dinero para las personas que usan estos vehículos a nivel operativo.

Algunas de las ventajas de un vehículo liviano es que gasta menos combustible, tiene menos desgaste de suspensión, frenos, además de que garantiza que va a tener una duración por años en muy buenas condiciones. Por ejemplo, uno de los vehículos que mostramos en la EXPO tiene instalado un blindaje nivel IIIA NIJ, para .44 magnum, 9 mm sub ametralladora y sólo agregando 180 kg de peso".

Saturnino Soria, director general de SEPSISA Seguridad Privada

"Es la primera vez que SEPSISA está presente en Expo Seguridad, y lo hicimos de la mano de AMESP, lo cual es un mensaje hacia nuestros socios comerciales y futuros socios o proyectos que tenemos en puerta, de que SEPSISA es una empresa legal, que cumple con todas las regulaciones gubernamentales tanto federales como estatales y que pertenece a la asociación más grande e importante de seguridad en México.

Considero que la participación de la AMESP en Expo Seguridad México nos da una claridad, una robustez a la industria de la seguridad privada, siendo la asociación de este rubro más grande que existe en México. Eso va a generar un sentido a la industria de la seguridad, que no sólo son guardias, en Expo nos podemos encontrar una gran cantidad de soluciones, de tecnología, y creo que hacía falta la presencia de una asociación en un gran *stand* como el que tuvo la AMESP en esta ocasión, siendo la primera vez, en representación de la seguridad privada, de los guardias, los custodios y de todos los que llevamos muchos años en esta industria".

Luis Enrique Reyes, director comercial de Anngel

"Expo es un foro muy importante que reúne a todo el gremio, los cuales algunos son nuestros socios comerciales. Anngel es una empresa de tecnología y lo que hacemos es desarrollar y trabajar sobre una plataforma que conecta a unidades de respuesta con personas que tienen una emergencia, estar presente en Expo y con AMESP nos sirve para ir aumentando la red de socios comerciales con los que atendemos las emergencias, y también desde el punto de vista del negocio para mostrar nuestros servicios a posibles clientes potenciales que asisten a la Expo.

Nuestra solución única es un *Marketplace* en el que el algoritmo ubica a la persona que tiene una emergencia y hace un barrido de forma matemática de la unidad más cercana que pudiera llegar a asistirlo, a acompañarlo y responder a esa emergencia. Desde el punto de vista médico, despachamos ambulancias; desde el punto de vista de seguridad, despachamos patrullas de seguridad operadas principalmente por los supervisores de compañías de seguridad privada".

Gabriel Bernal, director general de Grupo PAPRISA

"Nosotros tenemos muchos años presentes en Expo Seguridad y consideramos que siempre debemos estar innovando y cerca de nuestros clientes. Estar ahí los tres días fue una gran oportunidad para saludar a todos nuestros clientes y posibles clientes. Nos encontramos con directores de seguridad que son grandes amigos que nos vemos sólo una vez al año en esta exposición, por eso es tan importante estar aquí cada año, contribuyendo con nuestro granito de arena.

El *stand* de AMESP fue innovador porque estuvimos seis compañías juntas, eso habla de la congruencia, de la buena amistad que hay entre compañías de seguridad para poder estar juntos y competir con calidad y yo creo que en los próximos años vamos a ver a más empresas juntas como hoy en Expo Seguridad".

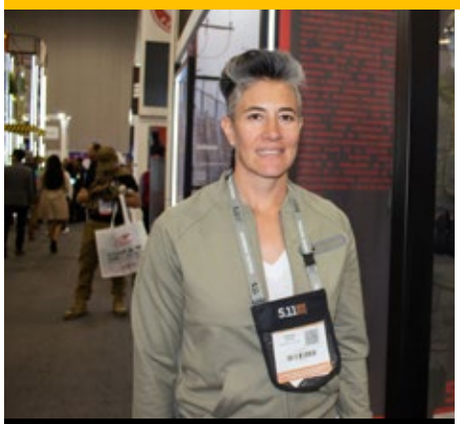
Grupo Seguridad Integral (GSI)

Grupo Seguridad Integral (GSI) cuenta con amplia experiencia en el giro iniciando operaciones desde 1976 en traslado de valores y guardias; actualmente está conformado por más de 15 empresas enfocadas en brindar servicios en el ámbito de la Seguridad Privada. Disponemos de la mayor capacidad instalada contando con 290 sucursales en traslado de valores y 52 sucursales en alarmas y guardias que cuentan con equipo de oficina y cómputo integrado a una red de comunicación directa a nivel nacional vía VPN (*Virtual Private Network*), mismas que nos permiten brindar servicios al sector financiero, gubernamental y al comercio en general, con cobertura en toda la república mexicana, Centroamérica, Estados Unidos, España y China.

Grupo Especial de Seguridad Privada México (GESPRIME)

GESPRIME es una empresa especializada en servicio de seguridad privada; con amplia experiencia en custodia de bienes de alto riesgo y valores en tránsito, desde sus inicios estableció la normatividad y sistemas operativos que tiene por objetivo minimizar las posibilidades de sufrir un evento de asalto o robo de la mercancía durante la ruta. Nuestra misión es ofrecer servicios de alta calidad orientados a la satisfacción de las necesidades de nuestros clientes manteniendo un ritmo alto de crecimiento en ventas, rentabilidad, y solidez financiera; siendo siempre socialmente responsables.

OTROS



Mariana Devesa, Marketing Leader de Latinoamérica de 5.11

Categoría: Equipo Táctico.

Empresa: 5.11.

Entrevistado: Mariana Devesa.

Cargo: *Marketing Leader* de Latinoamérica.

Soluciones en Expo: 5.11 es una empresa bastante reconocida en la parte táctica, aunque se manejan varias líneas de producto en la parte táctica PT-R que es deportiva, *Outdoor*, para actividades al aire libre y también *Life Style*, que es para el uso diario. Con más de siete asistiendo a Expo Seguridad, trae la parte táctica, 5.11 es reconocida por la calidad del producto, la resistencia y la comodidad. Es importante posicionarse en este tipo de eventos para que la gente pueda conocer las novedades que se tienen cada temporada como la línea de XTU, que consiste en un uniforme para fuerzas especiales bastante sofisticado con la última tecnología desarrollada por 5.11.

Omar Paz, director de Ventas en México Zona Centro

Categoría: Calzado.

Empresa: Riverline Ergonomic.

Entrevistado: Omar Paz.

Cargo: director de Ventas en la Zona Centro del país.

Soluciones en Expo: fabricantes de calzado ergonómico industrial, Riverline Ergonomics presentó calzado adaptable a la forma del pie, pioneros en fabricar calzado con casquillo de policarbonato y dependiendo de la labor que se realice es también el tipo de calzado. La empresa cuenta con un amplio catálogo de zapatos diseñados para diferentes sectores, pero de calidad industrial.

Richard Brent, CEO de Louroe Electronics

Categoría: Monitoreo de audio y analíticas de audio.

Empresa: Louroe Electronics.

Entrevistado: Richard Brent.

Cargo: *CEO.*

Soluciones en Expo: fuera de Estados Unidos, México representa el mercado más grande en LATAM, Richard considera que es imprescindible participar en la Expo Seguridad México 2023, ya que Louroe Electronics valora mucho al mercado latinoamericano. Este año están presentando un nuevo producto que consiste en micrófonos digitales, diferentes a los análogos, diferente a lo que vienen haciendo desde hace más de 40 años, permite al integrador una interconexión más fácil a un menor costo, además brinda un mejor entendimiento, los integradores prefieren servir al cliente y que sea rentable, queremos vender nuestro producto para que sea rentable para los integradores aquí en México.

Sergio Bravo, ingeniero Posventa de Hytera

Categoría: Radiocomunicación.

Empresa: Hytera.

Entrevistado: Sergio Bravo.

Cargo: ingeniero Posventa.

Soluciones en Expo: Hytera ofrece la parte de comunicación, a niveles de equipo de radiocomunicación tanto análogo como digital de primer nivel. Tienen soluciones también de lo que viene siendo la parte de POV O PTT sobre celular, desde los equipos más básicos hasta los equipos más avanzados llegando hasta un *smartphone*, que ya tiene integrado el botón de PTT, lo cual permite tener las mismas funcionalidades de un equipo de radio, pero a través de la red celular, lo cual implica tener equipos de soluciones de alta cobertura. También cuentan con equipo en ese desarrollo de POV que vienen siendo las *bodycams*, que ya permiten incluso tener transmisiones de video en vivo, dándole una solución completa a la empresa, porque se aprovecha todo lo que sabemos de radio y se complementa con las redes de telefonía de datos que son mensajería, poder transmitir fotos, video, tener geolocalización, etc.

POR UN SECTOR UNIDO Y UN MÉXICO MÁS SEGURO

Dentro de Expo Seguridad México, la participación de las asociaciones del sector de la seguridad ha ido en aumento. Este año hubo asociaciones que se presentaron con *stand* por primera vez y las cuales lograron con éxito sus objetivos. Algunos de sus presidentes o representantes en México, nos compartieron su experiencia y un mensaje para sus afiliados.

ALAS COMITÉ MÉXICO: COMPROMISO, VANGUARDIA, EDUCACIÓN

Carlos Martínez, presidente

Expo Seguridad México está muy enfocada a los integrantes de ALAS, ya que nuestros socios son tanto fabricantes, integradores, instaladores como usuarios finales, y la gran mayoría de los fabricantes internacionales vienen a Expo para presentar sus soluciones más innovadoras, y lo que nosotros hacemos es invitar a nuestros socios para que conozcan las nuevas tecnologías y en esta ocasión participamos con un panel titulado "*Looking in to the future*", para mostrar cuáles son las tendencias en el sector.

El objetivo de esta presidencia es crecer la membresía tanto de integradores como de usuarios finales, y hacer consciencia sobre tener siempre personal capacitado y eso nos va a ayudar a mejorar el sector y a estar siempre profesionalizados. Lo que buscamos es que siempre busquen empresas certificadas, que cumplan con todos los requisitos de la ley, y el estar asociados con nosotros les da ese respaldo de que es una empresa posicionada, con calidad y comprometida.

A manera personal, ser presidente de ALAS Comité México es una manera de poner ese granito de arena después de estar por más de dos décadas en esta industria. Y hoy tengo la oportunidad y la confianza de nuestros socios de poner en alto el nombre de la asociación, de colaborar con otras asociaciones para sumar esfuerzos y hacer sinergias y justo quienes están presidiendo esas asociaciones hoy en día, han recorrido el mismo camino que yo, arrieros somos y en el camino andamos. Para mí es un privilegio y me siento muy honrado de estar en esta industria que amo.

AMESP: INNOVACIÓN, VANGUARDIA Y TECNOLOGÍA *(ASOCIACIÓN MEXICANA DE EMPRESAS DE SEGURIDAD PRIVADA)*

Gabriel Bernal, presidente

Participar en Expo Seguridad por primera vez con un *stand* fue una experiencia muy grata y que forma parte de los objetivos de esta presidencia, ya que queremos internacionalizar a la AMESP, que la conozcan en toda Latinoamérica, y es también por eso que participamos en el "XVI Congreso Panamericano de Seguridad Privada 2023", que se llevó a cabo el 4 y 5 de mayo en Costa Rica, y que es organizado por la FEPASEP (Federación Panamericana de Seguridad Privada), siendo la primera vez que una asociación mexicana participara en un foro de este tipo en otro país.

La afluencia en el *stand* de la AMESP fue bastante concurrida los tres días de la Expo, los socios respondieron muy bien, y de hecho desde el primer día se tuvo 10 solicitudes para participar dentro del *Booth* el siguiente año, entonces la expectativa es que la siguiente edición de Expo se aumente al menos el doble el tamaño del *stand*. En AMESP uno de nuestros lemas es #HablemosBienDeLaSeguridad entonces el estar presentes en Expo, que puedan ver a las compañías que forman parte de la asociación que son de blindaje, de guardias, de custodia, eso da una imagen real de lo que es la seguridad privada en el país.

Nuestro objetivo es consolidar la imagen del sector para que todo mundo sepa lo que es y no sólo vean la parte superficial. Estamos trabajando en crear más alianzas que verdaderamente cumplan sus objetivos. La última alianza estratégica que tuvimos fue con INDEX, con los que participamos como patrocinadores del "Foro Internacional de Ciberseguridad INDEX 2023", que se llevó a cabo al mismo tiempo que Expo Seguridad; además formaremos parte de un Consejo de Ciberseguridad con Empresarios, entonces estamos abriendo nuevos canales no sólo para la AMESP, sino para que nuestros socios tengan nuevas oportunidades de negocio para crecer más

Como primicia, les queremos comentar que en el mes de octubre tendremos un foro de Ciberseguridad organizado por la AMESP y para el que tenemos ya cinco países confirmados que nos visitarán en el Estado de Nuevo León.

AMEXSI: PROFESIONALIZACIÓN, AMISTAD, ORGULLO

(ASOCIACIÓN MEXICANA DE ESPECIALISTAS EN SEGURIDAD INTEGRAL)

Ana Guzmán, presidenta

Estamos muy contentos porque es la primera vez en los 17 años que tiene la asociación, que estamos presentes con *stand* en Expo Seguridad México, lo cual es muy importante porque hemos compartido la profesionalización del gremio de la seguridad durante casi dos décadas, y hoy lo logramos gracias a todos los que nos apoyaron para estar ahí.

Este año desde AMEXSI estamos impartiendo talleres y cursos con el objetivo de profesionalizar a la industria en materia por ejemplo, de análisis de riesgos, tuvimos un taller de contratación, uno más de atracción de talento en las nuevas generaciones, porque ahora el sector está enfrentando retos muy importantes para contratar a las personas, entonces claro que la industria de la seguridad necesita capital humano y nosotros vimos la importancia de cómo las personas vamos pensando diferente a través de los años.

Tuvimos también un taller de 16 horas de los fundamentos básicos de los proyectos de seguridad con gran éxito y con integrantes de diferentes rubros del sector. En AMEXSI nos caracterizamos por reunir a empresarios, socios, integradores, clientes, aquí todos convergemos y vemos a la seguridad desde todos los ángulos y eso nutre mucho a nuestra asociación. Es increíble ver cómo cada uno aportaba diferentes cosas a la asociación.

Quiero agradecer a nuestros patrocinadores de Expo Seguridad México, que fueron: Galeam, Orion Innovation, JR, y Perla "sin pretextos". Gracias por confiar en AMEXSI y hacer esto posible. AMEXSI es una asociación de profesionales de la seguridad con calidez, amistad, nuestro principal mensaje es que la seguridad es un sector de amigos, donde podemos converger no solamente profesionales, sino también amigos que empatizamos y que queremos y amamos esta industria. Esta presidencia se rige porque todos sus socios se sientan orgullosos de pertenecer a AMEXSI.

ANERPV: EL RECUPERADOR DE VEHÍCULOS

(ASOCIACIÓN NACIONAL DE EMPRESAS DE RASTREO Y PROTECCIÓN VEHICULAR)

David Román, presidente

Expo Seguridad es el foro en donde se exponen las tecnologías y soluciones más importantes de seguridad, y es justo aquí donde visitamos y nos visitan nuestros asociados. En ANERPV trabajamos para que el sector de la seguridad y de localización sea más robusto y más confiable.

Una parte muy importante de nuestros 62 asociados, es profesionalizar al sector y justamente en Expo buscamos y contactamos a estos proveedores, fabricantes internacionales y globales para enseñarles lo que hace nuestra asociación, que efectivamente ayuda a recuperar vehículos, que opera muchos vehículos robados todos los días, que tiene 31 convenios con la autoridad, que es una fuente muy importante de información estadística y les enseñamos que estamos haciendo crecer a nuestro sector y les hicimos la invitación para sumarse. Somos la asociación más grande de este sector de la seguridad, en cuestión de localización. Dentro de los beneficios de pertenecer a la ANERPV, es que ayudamos a nuestros asociados a recuperar vehículos.

Este año cumplimos 20 años de la fundación de la ANERPV, recordando cómo hace dos décadas el Lic. Marcelo Ebrard nos dijo "hagan una asociación para que yo les pueda ayudar a recuperar vehículos de forma ordenada", de ese momento a ahorita, el ADN sigue siendo profesionalizar al sector y ser un enlace efectivo con las autoridades. En estos 20 años hemos ido explorando y cambiando de acuerdo a las necesidades de este mercado y la primera herramienta que tuvimos para el beneficio de nuestros asociados, como una gran herramienta de comunicación entre nosotros, es Centinela, la cual es una fuente de información muy importante para los medios especializados, para el mismo sector de la seguridad y para nuestros asociados.

Otro aspecto importante de pertenecer a la ANERPV es que tienes conocimiento de lo que está haciendo la autoridad para poder mejorar la situación de seguridad en carretera, en los estados y municipios; además somos la única organización civil que trabaja dentro de la Guardia Nacional, tenemos varios puntos de encuentro en los C4 y C5, en el Estado de México, en el 911, entonces cuando alguno de nuestros asociados registra un robo, tiene contacto directo con nuestro centro de monitoreo que está dentro de los C4 y C5 y ellos se dan a la tarea de informar y ayudar a la policía, porque al final es la autoridad la que puede realizar el procedimiento de recuperación. Los ayudamos con información como latitud, longitud, velocidad, *modus operandi*, etc.

A partir de 2008 empezamos a trabajar en la plataforma Centinela, que se ha vuelto hoy en día la base de datos.

ASUME: DIGNIFICACIÓN, PROFESIONALIZACIÓN Y LEGALIDAD

Herschel Schultz Chávez, director general de ASUME

ASUME estuvo presente desde la inauguración de la Expo con la participación de nuestro presidente, Armando Zúñiga Salinas, quien dirigió un mensaje importante sobre el papel actual de la Seguridad Privada en tres aspectos principales: el primero incluye proteger las cadenas de suministro; el desarrollo de la industria, y el *nearshoring* que hoy es uno de los grandes proyectos de desarrollo industrial en el país.

El segundo aspecto es cómo la industria de la seguridad privada trabaja con la seguridad pública para proteger empresas, los procesos y la continuidad del negocio.

El tercero, es cómo se coordinan las empresas de seguridad privada con los usuarios finales.

ASUME participa en coordinación con las 30 asociaciones que la integran, de las cueles algunas estuvieron presentes en Expo Seguridad México: AMBA, Misiones Regionales, ALAS, ANERPV, Círculo Logístico, ASIS Capítulo 217, AMESP, y AMEXSI. Lo que queremos en ASUME es seguir potencializando a las asociaciones para que a su vez tengan la capacidad de llegar a más empresas de seguridad privada para que se logren los siguientes puntos:

1. Regulación de las empresas.
2. Profesionalización del sector.
3. Coordinación con las autoridades.

Respecto a la creación de la Cámara Nacional de Seguridad Privada las asociaciones se busca que las asociaciones sigan incrementando su representatividad, hoy ASUME ya cuenta con las representatividad que por ley se pide para las Cámaras.

Lo que queremos hacer en 2024 es fortalecer a las asociaciones para que cada vez más se afilien más empresas de seguridad privada y así tener una mayor representatividad. Además estamos haciendo todos los ajustes con la Secretaría de Economía y la Dirección General de Seguridad Privada para que registren a todas estas empresas que ya tenemos y así ellos nos puedan dar el aval y el tercero es que estamos trabajando cada vez más fuerte con Concamin, puedo decirles que desde este momento estamos teniendo funciones de Cámara, porque nos están haciendo consulta los gobiernos, las autoridades, estamos teniendo influencia para la Ley General de Seguridad Privada y estamos esperando que la Secretaría de Seguridad Pública para que la lleven los legisladores y pueda ser votada. Nos estamos dedicando a cumplir con todos los requisitos legales para que en 2024 podamos seguir el proceso.

CÍRCULO LOGÍSTICO: SEGURIDAD, TECNOLOGÍA Y LOGÍSTICA

Héctor Manuel Romero Sánchez, presidente

Que Círculo Logístico haya estado presente en Expo Seguridad México 2023 es muestra del apoyo que les damos a nuestros socios, este espacio lo conseguimos por trabajos que desarrollamos dentro del Comité de Seguridad de la Expo en la parte académica, coordinando con autoridades, consiguiendo la banda de guerra y toda la parte de la escolta y la inauguración.

Nosotros trabajamos de la mano con Expo Seguridad, porque sabemos que es una de las mejores exposiciones de seguridad a nivel Latinoamérica, y este es un espacio para que nuestros socios vengan y expongan sus servicios y productos que brindan como operadores logísticos, empresas de custodia, de seguridad, de monitoreo, e inclusive usuarios finales dentro de nuestra asociación, para que conozcan cómo acompañamos la seguridad con la logística y la telemetría, sobre todo ahora que el robo a transporte ha incrementado de manera significativa en el país.

Hoy no podemos deslindar la logística con la seguridad y la telemetría, van en conjunto y eso nos ha dado muy buenos resultados. Como asociación lo que buscamos es apoyar para enfrentar la situación de inseguridad que vive el país, apoyar a las diferentes participantes que están jugando en la cadena de suministros, en los centros de distribución, al transporte, a las custodias, elementos básicos que debemos seguir trabajando para minimizar los riesgos actuales de seguridad.

Estamos convencidos de que a través de una buena logística, de una buena seguridad en el transporte podremos bajar los índices de inseguridad que estamos viviendo, un sector que padece de cobro de derecho de piso, extorsión, robo al transporte, robo hormiga, entre otros. Otra de las asociaciones a las que represento y que buscamos los mismos objetivos por el bienestar del país, es Seguridad por México, actualmente llevamos capacitados a más de dos mil policías de los diferentes niveles del gobierno. ■

ISIS SEGURIDAD INTEGRAL

Creamos entornos seguros

Servicios:

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

AFAC AGENCIA FEDERAL DE AVIACIÓN CIVIL

BASC BUSINESS ALLIANCE FOR SECURE COMMERCE

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

ASIS INTERNATIONAL

mesis

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

CONTROL SEGURIDAD PRIVADA:
UN LUGAR DONDE TODOS QUIEREN TRABAJAR

Por tercer año consecutivo somos reconocidos como una Súper Empresa

MÉXICO

En Grupo Control tenemos claro que el factor humano a todos niveles es fundamental para nuestro desarrollo, es por eso que nos complace anunciar que por tercer año consecutivo hemos sido reconocidos por TOP COMPANIES en el *ranking* Súper Empresas 2023: "Los lugares en donde todos quieren trabajar".

El sentido de pertenencia, el liderazgo, el crecimiento laboral, la motivación organizacional y la psicología positiva, son algunos de los rubros que se tomaron en cuenta para distinguirnos como una Súper Empresa.

Como lo marcan nuestros valores, la creatividad y la innovación son fundamentales para concretar ideas en acciones que impacten positivamente nuestro trabajo. Y bajo estos principios, durante el último año nos hemos ocupado en reforzar nuestra Cultura Organizacional y la comunicación con los colaboradores de todo el país, fortaleciendo así la cercanía con ellos y procurando su bienestar en el entorno laboral y la calidad de vida.

APP CONTODO CONTROL

Ahora los Guardias Control de todo el país pueden consultar su pago de nómina desde nuestra aplicación móvil Contodo Control, con la cual también tienen acceso directo a noticias y con nuestra área de Atención al Guardia en caso de surgir alguna aclaración de pago.

RUTA CONTROL

Reforzar y mantener la cercanía con colaboradores operativos es importante para nosotros, pues son ellos quienes diariamente ponen en alto el nombre de nuestra empresa en todo México. Por eso con la Ruta Control visitamos a los guardias de seguridad en sus centros de trabajo para difundir nuestra Cultura Organizacional, el uso de la *app* Contodo Control, además de los eventos y las prácticas en las que pueden participar.

Asimismo, durante estas visitas escuchamos y atendemos las dudas e inquietudes de los colaboradores, dando seguimiento a las necesidades específicas que puedan presentarse.

Como lo marcan nuestros valores, la creatividad y la innovación son fundamentales para concretar ideas en acciones que impacten positivamente nuestro trabajo

CULTURA ORGANIZACIONAL

Como parte de nuestra Cultura Organizacional, desde hace ya varios años, llevamos a cabo eventos y prácticas para el beneficio de nuestros colaboradores que promueven la unión familiar, como:

- Almorzando en Familia.
- Valorando a tu esposa.
- Evento del Día del Niño.
- Excelencia Académica.
- Día de la Madre y del Padre.

También contamos con prácticas de Cultura Organizacional con las cuales reconocemos el trabajo de los integrantes de la Familia Control:

- **Reconociendo al servicio:** acudimos a los servicios para reconocer la gran labor que desempeñan nuestros guardias de manera colectiva y que han recibido una felicitación directa del cliente.
- **Héroes Control:** son reconocidos los guardias que realizan sus consignas al 100% o detectan actos ilícitos, así como también a los colaboradores administrativos que destacan por su pasión, lealtad y disciplina al desempeñar su trabajo. Haciendo así algo ordinario: extraordinario.
- **Reconocimientos Santiago Barona:** desde hace 12 años galardonamos a los colaboradores ejemplares con la máxima condecoración de Control en un evento con el que conmemoramos a nuestro fundador y primer presidente de Control.

Para la Familia Control ser reconocidos por tercer año consecutivo como una Súper Empresa, es un objetivo más que hemos alcanzado. Por eso no queremos dejar pasar la oportunidad para hacer extensivo el agradecimiento a nuestros clientes por la confianza brindada y, por supuesto, a todos nuestros colaboradores administrativos y operativos por su compromiso y dedicación para seguir siendo un lugar donde todos quieren trabajar. ¡Vamos #Contodo hacia la cima! ■

Fotos: Cortesía Control Seguridad Integral

Con la Ruta Control visitamos a los guardias de seguridad en sus centros de trabajo para difundir nuestra Cultura Organizacional, el uso de la *app* Contodo Control, además de los eventos y las prácticas en las que pueden participar

EL CAMINO HACIA LA IMPARCIALIDAD EN SEGURIDAD (2ª PARTE)

Definir el problema, no vender nuestras soluciones

ARGENTINA | Ari Yacianci

En la primera parte de este artículo, establecimos tres pasos principales para mejorar nuestra imparcialidad como analistas profesionales de seguridad:

1) Definir el problema, no vender nuestras soluciones.
2) No personalizar los informes.
3) Fundamentar nuestros criterios de análisis.

En la anterior edición, nos concentramos en el Paso N° 1. En esta segunda parte, veremos los Pasos N° 2 y N° 3.

PASO N° 2: NO PERSONALIZAR LOS INFORMES

Incluso si un análisis de seguridad no tiene intención de conducir a la venta de una solución, aún podemos cometer un error que nos aleja de la imparcialidad: cargar la culpa de los problemas observados en una persona en particular.

En su libro *Security Risk Assessment* (2014), John M. White explica que si estamos realizando un análisis para clientes internos o externos, debemos tomar la distancia suficiente para poder demostrar que somos imparciales y sin prejuicios. Cuando los clientes son internos (es decir, que forman parte de la misma organización que nosotros), "es una de las cosas más difíciles de hacer".

Foto: - Freepik

Imagen: elaboración propia.

Esto es importante, porque han existido casos de informes de análisis que contenían información correcta sobre aspectos técnicos de seguridad, pero esa información factual terminó siendo opacada por ataques personales a otros profesionales, lo que resultó en que los informes fueran finalmente descartados, y por lo tanto se ignoraron recomendaciones que podrían haber generado mejoras significativas en la seguridad.

Esos casos demuestran que la imparcialidad no sólo debe buscarse desde un punto de vista ético, sino que perseguirla hará que también valoren mejor nuestro trabajo en términos prácticos.

Y si a raíz de nuestro análisis recibiéramos un ataque verbal por parte de una persona ofendida, no debemos responder con ardor ni enojo, sino siempre de forma acorde al ámbito profesional. El colega Daniel Garibaldi suele decir: "En nuestro rol de expertos, debemos ser seres inmutables, sin nada de pasión".

Además, salvo en casos de grave negligencia o de actividades ilícitas, no es conveniente "quemar puentes" innecesariamente y perder contactos con los que se podría llegar a establecer una relación constructiva en el futuro, incluso a pesar de haber sufrido desacuerdos.

De ser conveniente, se puede mencionar en los informes el área o cargo de la persona a la que se hace alusión: por ejemplo, "el departamento de Seguridad", o "el responsable del servicio"

Algunas buenas prácticas para evitar personalizar nuestros informes son las siguientes:

a) Evadir opiniones personales; atenerse a los hechos y hacer recomendaciones exclusivamente con base en ellos.

b) Intentar prevenir posibles malentendidos, explicando el propósito del análisis tanto en la propuesta de trabajo como en el informe final.

c) No sólo enfocarse en lo que debe ser mejorado, sino también destacar lo que está funcionando bien actualmente.

d) No buscar atacar la integridad y el profesionalismo de los responsables del área que estemos evaluando, sino simplemente la efectividad de sus medidas.

e) De ser conveniente, se puede mencionar en los informes el área o cargo de la persona a la que se hace alusión: por ejemplo, "el departamento de Seguridad", o "el responsable del servicio".

f) Sólo incluir el nombre y apellido de una persona en un informe si resultara claramente imprescindible.

PASO Nº 3: FUNDAMENTAR NUESTROS CRITERIOS DE ANÁLISIS

Popularmente se dice que "cada persona es un mundo", porque cada individuo observa la realidad de una forma diferente, utiliza sus propias metodologías y aplica diversos criterios a la hora de analizarla. Entonces, se suele decir que si no existen dos analistas iguales, es evidente que tampoco existen dos análisis iguales.

Incluso si lográramos que 100 profesionales de seguridad realizarán una auditoría en un mismo momento y lugar para un mismo cliente, y hasta contarán con el mismo *checklist,* nos encontraríamos con una gran variedad de resultados y hallazgos: desde aspectos mínimamente diferentes, pero compatibles entre sí, hasta contradicciones absolutas e irreconciliables.

Esta diferencia es completamente natural, pero la subjetividad desmedida puede hacer que cuestionen nuestra calidad analítica, y en consecuencia, que se ponga en duda nuestra capacidad técnica y nivel profesional. Entonces, para poder moderar nuestra subjetividad, debemos asegurarnos de que los criterios de nuestro análisis estén sólidamente fundamentados.

Esto implica que nos hagamos a nosotros mismos las siguientes preguntas, idealmente antes de que alguien más nos las haga a nosotros.


Foto: - Freepik

Incluso si lográramos que 100 profesionales de seguridad realizarán una auditoría en un mismo momento y lugar para un mismo cliente, y hasta contarán con el mismo *checklist*, nos encontraríamos con una gran variedad de resultados y hallazgos


Foto: - Freepik

Sobre la preparación de nuestro análisis:

- ¿En qué bibliografía especializada apoyé el desarrollo de mis *checklists*?
- ¿Con base en qué estándares internacionales está organizado mi análisis?
- ¿Qué ítems incluí en mi *checklist*, y cuáles excluí? ¿Por qué?
- ¿Se adapta mi método de análisis a las particularidades del cliente?
- ¿Cómo voy a calcular los aspectos técnicos que son cuantitativos?

Sobre nuestro informe final:

- ¿Cómo puedo explicar y argumentar los aspectos que son cualitativos?
- ¿Estoy omitiendo hallazgos sólo porque creo que no quieren escucharlos?
- ¿Estoy omitiendo recomendaciones sólo porque creo que no las van a aplicar?
- ¿Mis recomendaciones están en conformidad con las buenas prácticas de la industria?

CONCLUSIÓN

Si como profesionales de seguridad hacemos un esfuerzo consciente en torno a aplicar los tres primeros pasos del Camino hacia la Imparcialidad, incluso si no lo logramos inmediatamente, ya habremos comenzado a mejorar nuestro desempeño moral y técnico.

Y tú, ¿cuál crees que debería ser el siguiente paso? ■

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

PROGRAMA DE MANEJO DE EMERGENCIAS

(D.R.A.)

El plan de emergencia es la planificación y organización para la utilización óptima de los recursos técnicos previstos con la finalidad de reducir al mínimo las posibles consecuencias sobre seres, pérdidas bienes generales y el ambiente, que pudieran derivarse de la situación

COLOMBIA | Javier Nery Rojas Benjumea

Foto: - Freepik

CRITERIOS BÁSICOS DEL PLAN:

Todo Plan de Emergencia debe ser básico, flexible, conocido y ejercitado, debiendo haber sido probado y actualizado.

BÁSICO:

Todo Plan de Emergencia debe permitir ofrecer una primera respuesta de emergencia a todos los supuestos que se consideren como razonablemente posibles. Esta respuesta, debería ser completa a pesar de su sencillez, o lo que es lo mismo, debe funcionar por sí sola. Ello supone que debe contemplar las tareas de salvamento, clasificación, atención y evacuación de los heridos.

Sobre esta respuesta inicial debe acoplarse de manera ordenada toda la ayuda exterior que vaya llegando a la zona del siniestro, permitiendo la realización de tareas más complejas y, sobre todo, dotando a la respuesta de emergencia de una mayor potencia en sus cometidos (salvamento, clasificación, atención y evacuación de heridos hacia centros hospitalarios).

LA RESPUESTA DEL PLAN A CADA UNA DE LAS FACETAS CONTEMPLADAS DEBE SER FLEXIBLE A LAS NECESIDADES DEL MOMENTO, PERMITIENDO UNA RÁPIDA TRANSFERENCIA DE LOS RECURSOS HACIA OTRAS FACETAS QUE LA PUEDAN PRECISAR OTRO TIPO DE RECURSOS O, SENCILLAMENTE, MÁS RECURSOS

FLEXIBLE:

La respuesta del Plan a cada una de las facetas contempladas debe ser flexible a las necesidades del momento, permitiendo una rápida transferencia de los recursos hacia otras facetas que la puedan precisar otro tipo de recursos o, sencillamente, más recursos. Ello supone que, si en un momento determinado no existiera fuego en la zona crítica, el equipo de bomberos debería comenzar a realizar el rescate de las víctimas, apoyando desde un inicio las tareas de clasificación y atención a los heridos. De esta misma forma, si los heridos son rescatados uno a uno, el equipo de clasificación de heridos resultará sobredimensionado, necesitando ser reajustado a las necesidades de cada momento.

El hecho de que el Plan sea flexible no quiere decir de ninguna manera que fomente la improvisación; más bien lo contrario, debe intentar contemplar las necesidades variables de cada tipo de respuesta, formando a los equipos de respuesta en las tareas más sencillas de los equipos que van a trabajar junto a ellos. De todas formas, hay que referir que la respuesta improvisada es la menos mala de las respuestas que se pueden ofrecer a un problema cuando no se ha contemplado ninguna respuesta para él.

CONOCIDO:

Si el Plan de Emergencia no es conocido por las personas que inicialmente van a responder a él, difícilmente puede ser eficaz. Este es el tan conocido concepto americano del "Plan de Papel"; un precioso plan, bien encuadernado, que adorna la estantería y se enseña a las visitas para impresionarlas, pero que no tiene ningún tipo de respuesta pues es desconocido por sus actores.

Por lo tanto, todo Plan de Emergencia que se aprecie debe contemplar la forma en que se da a conocer a las personas que van a actuar en él, así como la periodicidad de estas acciones.

EJERCITADO:

Si se pretende que una determinada persona realice una acción, es necesario, aparte de que dicha persona conozca su función en el Plan, formarle para que sea capaz de llevarla a cabo con la eficacia necesaria.

Por esto, todo Plan de Emergencia, debe llevar anexo un Plan de Formación.

Foto: - Freepik

El esquema más básico, y que ha demostrado una mayor eficacia, es aquel que contempla la comunicación directa entre las personas de un mismo equipo por un canal exclusivo, y la comunicación directa de las diferentes áreas sin necesidad de intermediación a través de un canal común

PROBADO:

Una vez que el Plan es conocido y que el personal ha sido formado en la respuesta que de ellos se espera, el Plan debe ser probado mediante Simulacros de Emergencia de una manera parcial o completa. Los simulacros parciales permiten probar la respuesta del plan en determinadas áreas, sin necesidad de movilizar a todas las personas involucradas. Los simulacros generales dan una valoración global de la eficacia del Plan, pero su organización es compleja y costosa.

Tras la realización de cualquier tipo de simulacro se debe realizar una reunión de cada una de las áreas para valorar la eficacia del Plan en esa área concreta; y finalmente una reunión de un representante de todas las áreas que valore la eficacia global del Plan, si el simulacro ha sido general.

ACTUALIZADO:

Todo Plan debe ser regularmente actualizado con objeto de ajustarse a los cambios surgidos en las instalaciones o los procesos. La periodicidad con que el Plan debe ser revisado depende de lo cambiantes de las circunstancias, pero con carácter general, se acepta como bueno el carácter anual de este tipo de revisión. Este tipo de revisiones conlleva la existencia de una Comisión de Actualización del Plan de Emergencia, que es la encargada de elaborar las modificaciones necesarias, de difundirlas y de encargarse de que lleven a cabo las actividades formativas establecidas.

FUNCIONES BÁSICAS DEL PLAN

Como ya se ha recogido; todo Plan, a pesar de su sencillez, debe funcionar por sí mismo, sin la ayuda de otros planes e instituciones. Ello supone que debe contemplar la realización de las siguientes funciones:

SALVAMENTO:
CLASIFICACIÓN DE HERIDOS, ATENCIÓN DE HERIDOS, EVACUACIÓN DE HERIDOS

Para que estas funciones se puedan desarrollar de manera ordenada y eficaz resulta necesario la existencia de las siguientes funciones integradoras: Mando, Seguridad, Punto de Reunión y Comunicaciones.

CADENA DE MANDO:

Debe estar perfectamente clara para todas las instituciones que participan en la emergencia desde el momento en el que el Plan de Emergencia es aprobado. En cualquier caso, se recordará de forma activa a todo el personal que acuda en socorro de la emergencia a la entrada al Punto de Reunión.

Tradicionalmente se ha recogido la existencia de dos Puestos de Mando.

El Puesto de Mando Avanzado, lugar de encuentro de los coordinadores de las diferentes áreas de respuesta en el lugar, se encuentra dirigido por la persona designada por la autoridad aeroportuaria. Se trata de un Puesto de Mando inminentemente operativo en aras de que los Equipos de Bomberos, Sanitarios y Policía puedan trabajar de la manera más eficaz sin interferirse.

El segundo Puesto de Mando al que se hacía referencia lo constituye el Puesto de Mando Principal, donde se encuentra la Autoridad que dirige la Emergencia y un responsable de las principales instituciones que hacen frente a la emergencia. Su ubicación debe permitir comunicarse tanto con la zona de la emergencia como con el exterior.

SEGURIDAD DE LA ZONA:

Toda la zona en la que se están realizando las tareas de extinción del fuego, salvamento, clasificación, atención y evacuación de heridos debe ser rápidamente balizada y custodiada por las Fuerzas de Seguridad del Estado, con objeto de evitar la entrada indiscriminada de personas a esta área. De la misma forma las rutas de acceso y de evacuación deben ser reguladas tan pronto como sea posible. Con este sentido, las fuerzas de seguridad del estado secundarán a los responsables de cada área con el objeto de que sean seguidas sus indicaciones.

Foto: - Freepik


Foto: - Freepik

REUNIÓN DE RECURSOS:

Ha quedado largamente demostrada la necesidad de reunir los recursos exteriores, que acuden en respuesta de la emergencia, en un lugar determinado antes de darles acceso a la zona de emergencia. Este hecho intenta simplificar la localización del lugar de la emergencia, al tiempo que pretende recordar a todos los constituyentes de estos equipos que deben seguir las pautas recogidas en el Plan de Emergencia.

COMUNICACIONES:

Las comunicaciones se han mostrado siempre como un punto crítico en la respuesta a este tipo de emergencias.

El esquema más básico, y que ha demostrado una mayor eficacia, es aquel que contempla la comunicación directa entre las personas de un mismo equipo por un canal exclusivo, y la comunicación directa de las diferentes áreas sin necesidad de intermediación a través de un canal común.

El uso de equipos de radio portátiles se ha mostrado hasta la fecha como el más operativo, sin desatender a la telefonía móvil para comunicaciones directas entre el lugar de la emergencia y el exterior del aeropuerto. Ejemplo de esta necesidad lo constituye la comunicación entre el responsable de Evacuación de Heridos y los Hospitales de Destino (en general a través de una Central de Emergencia).

Las comunicaciones del Puesto de Mando Principal se realizarán utilizando todos los recursos disponibles, basando inicialmente su mayor peso en la telefonía convencional de cara a comunicarse con el exterior del aeropuerto y en los equipos de radio para las comunicaciones con la zona de emergencia.

SUPUESTOS RECOGIDOS DENTRO DEL PLAN:

El Plan de Emergencia debe recoger los supuestos de actuación que parezcan más probables que pudieran ocurrir en estas instalaciones. *A priori*, los supuestos mínimos que debe recoger son los siguientes:

SITUACIONES DE PREALARMA:

En muchas ocasiones se producen situaciones de riesgo que terminan o no por generar una situación de emergencia. De esta forma el riesgo de accidente aéreo que se produce cuando una aeronave presenta algún tipo de problemas que le impide volar o aterrizar en condiciones de seguridad (averías de alguno de los motores, del tren de aterrizaje, etc.). También se producen estas situaciones cuando existe una amenaza de bomba tanto en una aeronave como en un edificio del aeropuerto. Por último, lo mismo sucede ante actos de secuestro y apoderamiento ilícito.

Todas estas situaciones deben ser contempladas dentro del Plan de Emergencia, permitiendo en la medida de lo posible anticiparnos a sus consecuencias.

DESASTRE ESTRUCTURAL:

El Desastre Estructural de las instalaciones del aeropuerto por fuego, atentado terrorista con explosivos, y otras circunstancias ha aumentado notablemente en los últimos años. Para estos supuestos, es preciso contar qué áreas muy transitadas por el público sufran su azote, con la producción de un gran número de víctimas y la génesis de problemas sobreañadidos en la extinción y el rescate de las víctimas para los Equipos de Bomberos del Aeropuerto, especializados en su actuación en aeronaves.

DESASTRE DE LA COMUNIDAD CIRCUNVECINA:

Me estoy refiriendo a grandes calamidades (terremotos, inundaciones, etc.) que invalidan los mecanismos de respuesta de la comunidad (carreteras, hospitales, etc.). En estos supuestos el aeropuerto, de quedar operativo, debe jugar un importante papel en la llegada de la ayuda exterior y en la evacuación de víctimas. ■

Referencias:

- Compilación y adaptación de varios autores desconocidos.


Foto: - Freepik

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

airbag

Creamos Mejores Conductores

airbag es el primer *software* de gestión y mejora de operadores.

Analizamos, calificamos y premiamos a los operadores por su manejo seguro aumentando la seguridad y reduciendo los costos de tu flota.

- Reduce hasta 40% de siniestralidad.
- Hasta 30% de ahorro en combustible.
- Reten y mejora a tus operadores.
- Reduce costos de mantenimiento.
- Aumenta la vida útil de tus vehículos.
- Ahorro de hasta el 30% en Seguros.
- Aumenta la seguridad de tu flota y tus operadores.

Por un transporte más seguro

SAFEWAY CORPORATION

airbag

Pide un **DEMO** y obtén tu **Prueba Piloto** con descuento para obtener los beneficios

www.airbagtech.io

55 3443 9597

adriant@airbagtech.io

Airbag Technologies

RESILIENCIA Y GESTIÓN DE LA SEGURIDAD

Una organización que reúne, consolida y se correlaciona de inteligencia de seguridad es capaz de detectar ataques en tiempo real, responder rápidamente, y prepararse para futuras amenazas siendo más oportuna en su actuación y resistente

Foto: - Freepik

MÉXICO
Mercedes Escudero Carmona

La resiliencia se ha convertido en un concepto clave en los sistemas de gestión de seguridad. La seguridad se incorpora como parte de la misión de la organización y la resiliencia es para asegurar la continuidad y recuperación de cualquier organización ante cualquier situación de cambio de cualquier sector.

En seguridad, la resiliencia se define como: "un proceso dinámico donde las influencias del ambiente y del individuo interactúan en una relación recíproca que tiene como resultado la adaptación positiva de la persona en contextos de gran desafío". (Melillo y Suárez, 2002).

Sin embargo, se desconoce a profundidad lo que implica la resiliencia.

RESILIENCIA

En su semántica se incluyen los conceptos de:

- **Resistencia:** en su definición queda sujeta a la disciplina en la cual sea aplicada. El término proviene del latín *resistentia*. Está compuesto por el prefijo "re", que explica la intensificación de la propia acción, y del verbo '*sistere*', que deriva del verbo '*stare*', que se traduce como "mantenerse o estar en pie".
- **Desiliencia:** situación de vulnerabilidad donde un individuo o grupo social presenta unas circunstancias desfavorables determinadas por unos niveles inadecuados de adaptación. Es la relación de equilibrio entre fortalezas y debilidades a nivel interfactorial es precisamente lo que determina la caracterización de la vulnerabilidad.
- **Desistencia:** es la acción y efecto de abandonar, desistir, renunciar, ceder, dejar o abdicar mediante un derecho, empresa o intento por alguna causa o motivo o de un proceso.

Por lo tanto, para entender la resiliencia en el Sistema de Gestión de Seguridad debemos partir por descubrir qué condiciones la permiten, es decir, la securización, la recuperación, las relaciones y la cultura (Boris Cyrulnik).

La securización es el hecho de dotar de la seguridad necesaria, hecho de hacerlo seguro o protegerlo con los medios pertinentes. Tiene el efecto de hacer creer que la seguridad nunca es suficiente y junto a la privatización del espacio público se genera la sensación de falsa seguridad en las personas, ya que supone que en espacios controlados o cerrados se puede estar más seguros, cuando sabemos que no siempre hay mayor seguridad.

CARACTERÍSTICAS

- La flexibilidad.
- La capacidad de adaptación.

EP SUMMIT '23
mexico city - oct. 10-11

EXECUTIVE PROTECTION SUMMIT

CONOCE EP SUMMIT

Únete al EP Summit 2023, un fascinante evento de 2 días dirigido a profesionales de la seguridad de todo el mundo para explorar todos los aspectos de la protección de personas en el que emprendedores, profesionales y líderes de opinión de todo el mundo se reúnen para intercambiar ideas, impulsar la innovación y establecer conexiones duraderas.

Sumérgete en talleres atractivos, discursos inspiradores y oportunidades de networking sin igual, todo en el vibrante escenario de la capital mexicana.

¡ EL MEJOR EVENTO DE SEGURIDAD EN AMERICA LATINA !

CONFERENCISTA MAGISTRAL

LEE SANSUM

Miembro del Equipo de Protección para la familia Al Fayed. Encargado de la seguridad de la Princesa Diana en Francia.

CONFERENCISTAS INVITADOS

MARIO FRANCO

JOE LASORSA

ELIJAH SHAW

CHRIS STORY

¡Únete a la elite de la seguridad en EP Summit! Una experiencia única e intensa de aprendizaje, networking y tendencias en un solo lugar.

10-11 OCTUBRE

Inscripciones en:
www.epsummit.com.mx

SISSA · GORAT SEGURIDAD PRIVADA · Density · Galeam · decysyon · FIRSTCALL · Ivan Ivanovich · AS3 DRIVER TRAINING · the box · JVP · AXIS COMMUNICATIONS · AIRBUS · AGP · CIA KAPITAL

Es importante considerar a la resiliencia como un proceso y tiene como estándar de referencia para cualquier organización la Norma ISO 22316: 2020 de Resiliencia Organizacional, la cual es la mezcla de resistencia y flexibilidad que influye sobre la capacidad para superar situaciones adversas


Foto: - Freepik

- La capacidad del sistema para recuperar su estado inicial una vez finalizada la perturbación a la que ha estado sometido.
- Incrementa su presencia e implantación permanentemente tanto en los aspectos sociales como funcionales y especialmente en materia de seguridad.

En este sentido, si bien tanto el Estado, y sus organismos autoridades; así como las empresas tienen un compromiso con sus ciudadanos y sus integrantes, respectivamente, proporcionar la seguridad en todo momento, este compromiso debe entenderse que se encuentra comprendido entre los límites establecidos por la certeza y la incertidumbre, la impredecibilidad, lo probable y lo improbable dentro de los márgenes que definen y condicionan la ejecución de las políticas de protección y seguridad.

Por ello, es importante considerar a la resiliencia como un proceso y tiene como estándar de referencia para cualquier organización la Norma ISO 22316: 2020 de Resiliencia Organizacional, la cual es la mezcla de resistencia y flexibilidad que influye sobre la capacidad para superar situaciones adversas. Destacando:

- La habilidad para impedir que se produzca algo malo.
- Habilidad para evitar que algo negativo se convierta en algo peor.
- Habilidad para recuperarse de algo malo una vez que ha ocurrido.

Asimismo, propone los siguientes principios:

- Comportamiento alineado con la visión, misión y valores.
- Entendimiento del contexto.
- Absorber, adaptarse y responder efectivamente al cambio.
- Buen gobierno y gestión.
- Diversidad de habilidades, liderazgo, conocimiento y experiencia.
- Coordinación de todas las áreas.
- Gestión del riesgo.

Sin duda, en los últimos dos años se ha demostrado la impresionante aptitud que tenemos las personas, no sólo para superar dificultades, sino para lograr obtener situaciones positivas de ellas y esto debe ser transmitirse y trabajarse con rigor científico en materia de seguridad y así lograr que las organizaciones mejoren su inteligencia de seguridad basada en la resiliencia.

La inteligencia de seguridad es la información y datos sobre vulnerabilidades y amenazas, que se analizan y permiten la priorización de acciones para maximizar la reducción de riesgos. Una mejor y mayor inteligencia de seguridad permite una mejor toma de decisiones estratégicas, mejores procesos de organización y por lo tanto una mayor protección.

Seguramente no hay un modelo perfecto y único de resiliencia organizacional y la nueva realidad nos ha puesto nuevos retos a los que debemos hacer frente. Por ello, debemos comprender la importancia de aumentar la capacidad de resiliencia con metodologías específicas. Una organización que reúne, consolida y se correlaciona de inteligencia de seguridad es capaz de detectar ataques en tiempo real, responder rápidamente, y prepararse para futuras amenazas siendo más oportuna en su actuación y resistente. ■

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

BENEFICIOS ESPECIALES

24/365 DÍAS
Atención personalizada de nuestro centro de monitoreo

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

ACCESO
Total acceso a reportes de estadísticas de robos

COMITÉS

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

NUESTROS SOCIOS

Tracking Systems · sitel Seguridad Satelital · Holkan · skyguardian · skymeduza · SECUREWITNESS · INFO TRAX · TECNO LOGISTIK · GLOBAL MIT · RAINDE · SEGURIDAD360.com · ATLANTIDA · GEOTRACKING Rastreo Satelital · GPS · TTC · DUMAY · AISIS Seguridad Integral · GEOTRUCKS · GRUPO ALFIL · SEC Soluciones · RCU Sistemas · GPS TRACKER MX Vamos contigo · MAGNI Tracking · TSVISION · BLC · SATECH

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

COMUNÍCATE
55 3334 4707

Foto: - Freepik

EL TERCER LADO DEL CONFLICTO

COMO HERRAMIENTA DE SEGURIDAD EN INSTITUCIONES EDUCATIVAS

Puede ser una herramienta que mejore la seguridad humana en las instituciones educativas junto con las medidas de seguridad tradicionales

ARGENTINA | Juan Manuel Iglesias

En el artículo del número anterior propuse la implementación del concepto del "Tercer Lado", desarrollado por William Ury, antropólogo y negociador representante de la Escuela Harvard de Negociación, para la pacificación en situación de conflictos comunitarios donde las fuerzas de seguridad tenían un rol protagónico.

Siguiendo ese desarrollo, es que propongo el mismo encuadre para aplicar a situaciones de violencia y conflictos en instituciones educativas.

Ya en varios artículos he tratado el tema de la seguridad en colegios, especialmente para la prevención de situaciones de "tiradores activos" como también el tratamiento de conflictos resultante de situaciones de *bullying*, *ciberbullying*, problemas de convivencia, discriminación por género, nacionalidad, religión, etc.

El encuadre de estrategias protectoras y preventivas desde el "Tercer Lado" descansa sobre los principios de la Paz Positiva (Galtung) y de la Justicia Restaurativa.

En el primer caso no sólo previene la violencia, sino también configura un espacio de crecimiento y transformación, no sólo para los alumnos, sino también para todos los miembros de la comunidad educativa. Y segundo, permite que los victimarios puedan hacerse cargo y responsabilizarse de sus acciones, ponderando el daño ocasionado a la víctima, desarrollando más empatía (una de los componentes de la inteligencia emocional). Por otro lado, a la víctima le permite poder salir del estado victimológico, trabajar en la superación del TEPT, y en ambos casos, asumiendo un rol protagonista y de cambio.

¿QUÉ ES EL TERCER LADO?

Para empezar, podemos retomar brevemente la definición que di para "Tercer Lado" en el artículo anterior. Ury define al "Tercer Lado" como "(...) una forma de ver los conflictos que nos rodean no sólo desde un lado, o el otro, si no desde una más amplia perspectiva: la de la comunidad que lo circunda. Es el poder de la gente. Usa el poder de la persuasión. Influye sobre las partes apelando sobre todo a los intereses de ellas mismas y a las normas de la comunidad. En los conflictos generalmente no hay una única tercera parte, sino una multitud de ellas.

La propuesta, no es solamente formar mediadores escolares para el tratamiento de los conflictos, sino transformar a la comunidad educativa en el "Tercer Lado" del conflicto para lograr un estado de paz positiva que permita la transformación y el crecimiento.

FASES DEL CONFLICTO

Recordemos que para las diferentes fases del conflicto, tal como analicé en el artículo anterior, existe una configuración característica:

- Si en conflicto está latente o no se produjo: en esta fase se trabaja a diario y de forma sistemática a través de:

El constructor de Puentes: es importante que la institución a través de los docentes, personal, y autoridades entable relaciones, no sólo con los alumnos, sino también con las familias. El trabajo en equipos y grupos de consejería educativa es muy importante para generar espacios de escucha y expresión de las necesidades de la comunidad.

La comunidad tiene un rol sanador y terapéutico, tanto para la víctima como para el victimario

La propuesta, no es solamente formar mediadores escolares para el tratamiento de los conflictos, sino transformar a la comunidad educativa en el "Tercer Lado" del conflicto para lograr un estado de Paz Positiva que permita la transformación y el crecimiento


Foto: - Freepik

El Maestro: no sólo los contenidos académicos son importantes sino también aquellos que implican valores, habilidades, nuevas perspectivas que mejoren mi forma de "estar siendo en el mundo". Una estrategia interesante es incorporar en los currículum, temas relacionados con la resolución de conflictos, el trabajo en equipo, la comunicación, la aceptación de la diversidad, etc.

El proveedor: muchas veces los conflictos surgen por necesidades básicas insatisfechas. La construcción de una red de ayuda y solidaridad para apoyar a los más vulnerables de la comunidad puede ser otra de las formas.

• Si el conflicto está manifiesto: ya sea por violencia o *bullying*, etc., el "Tercer Lado" podría configurarse como:

El Mediador: la mediación entre pares permite que los alumnos se responsabilicen y aprendan formas de resolver los conflictos sin recurrir a la violencia.

El Testigo: muchas veces, los victimarios recurren a la violencia porque necesitan sentirse importantes. El hecho de que les demos la función de testigos, que monitorean y observan el patio de juegos y las aulas en busca de situaciones conflictivas para convocar a los mediadores, puede ayudar a que se enfoquen en una actividad constructiva y puedan satisfacer su necesidad de estima y reconocimiento.

• Si el conflicto ha escalado:

El Guardián de la Paz: no sólo los docentes y autoridades, sino toda la comunidad educativa, tiene la responsabilidad de tomar las mínimas medidas de fuerza que puedan detener el conflicto dañino. Los guardianes son los que se "ponen en medio" para frenar la violencia.

• La etapa posconflicto:

El Sanador: "Las heridas pueden ser profundas. Incluso cuando un conflicto parece resuelto después de un proceso de mediación, arbitraje o votación, es posible que las heridas subsistan y, junto a ellas, el peligro de recurrencia. Un conflicto no se puede considerar totalmente resuelto hasta que haya comenzado a sanar la herida dañada".

La comunidad tiene un rol sanador y terapéutico, tanto para la víctima como para el victimario. Por ejemplo, los círculos de justicia restaurativa dónde se comparten emociones, ideas, pensamientos, imágenes de lo sucedido, acompañado de dinámicas grupales de expresión corporal, arte, dramatizaciones, etc., puede ayudar a superar esa situación de sufrimiento desde una experiencia de aprendizaje y reconocimiento mutuo.

El "Tercer Lado" puede ser una herramienta que mejore la seguridad humana en las instituciones educativas junto con las medidas de seguridad tradicionales. ■


Foto: - Freepik

Juan Manuel Iglesias, magíster en *Counseling* Humanista y Educativo, y gerenciador de Seguridad Corporativa.
Más sobre el autor:

LA SEGURIDAD ESCOLAR
EMPIEZA EN EL SALÓN DE CLASES

Todas las escuelas deben tener un plan de operaciones de emergencia organizado y sistemático para reducir los riesgos o prevenir, prepararse, responder y recuperarse de una situación de crisis

MÉXICO | David Chong Chong

Los accidentes pueden ocurrir en cualquier sitio en formas y con efectos de daños muy diversos e impredecibles, a pesar de las mejores medidas preventivas de Seguridad que se hayan adoptado. En los centros escolares el principal problema con los accidentes es que las víctimas más probables, y en ocasiones al mismo tiempo causantes de los mismos, son los alumnos, en especial de nivel básico (preescolar y primaria) que dependen totalmente de su docente, y que no suele estar preparado para enfrentar este tipo de eventos.

La seguridad de un alumno es una responsabilidad absoluta e indeclinable del centro escolar durante su permanencia dentro de sus instalaciones, y el docente a cargo del grupo es el primer responsable de ello.

Foto: - Freepik

Foto: - Freepik

LA HORA DEL RECREO

La dinámica dentro de un centro escolar suele ser de un actividad intensa, multitudinaria y simultánea que propicia la ocurrencia de accidentes y dificulta su prevención, así como una detección oportuna de dicha ocurrencia por parte de los docentes, cuantitativamente insuficientes respecto a la población escolar. Más controlable en la estancia dentro de un grupo y menos controlable en los espacios comunes en los descansos (recreo).

Es indispensable que tanto el docente como los directivos presentes en la instalación, estén preparados para enfrentar todo tipo y nivel de situaciones, desde los incidentes menores hasta eventos catastróficos, para proteger y salvaguardar la vida y la integridad de los alumnos.

Es conveniente que los alumnos, al menos los de mayor edad, tengan una preparación básica par al menos asistir al docente en la atención de contingencias.

Efecto multiplicador a nivel social. ■

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

Tu seguridad, nuestra prioridad *con excelencia*

OSAO

Seguridad Electrónica

SERVICIOS OSAO

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

55 679 834 90

55 2430 8253

Info@osao.com.mx

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


Foto: - Freepik

LA MEJOR MANERA DE GESTIONAR LOS RIESGOS DE SEGURIDAD EN LAS INSTALACIONES HOSPITALARIAS

La Seguridad es el punto central de este artículo, y es que se debe "pensar fuera de la caja" y desmitificar el rol policial o militar, de que se enfoque en actividades reactivas la gestión de seguridad

COLOMBIA | Daniel Jiménez

Sin lugar a dudas, el hecho de trabajar gestionando la seguridad de las instalaciones hospitalarias es un tema desafiante, primero el conocimiento de las instalaciones, después de ello, saber de qué manera interactúan los procesos, y además conocer la operación que es totalmente diferente a cualquier otro negocio.

Sin embargo, y recordando lo que en algún momento al empezar a trabajar en este tipo de industria, recibí como consejo "esto es igual que en cualquier otro negocio" entendí que esta se define como concreta, después de estudiar por largo tiempo esta clase de organizaciones, llegué a una conclusión, y fue que como para los pacientes que asisten allí a recibir atención, éstas, necesitan un diagnóstico específico y una cantidad de conceptos y conocimientos que verdaderamente las hacen únicas, y a quienes gestionan la protección de activos de ellas como aprendices o especialistas dependiendo de diferentes factores.

Algunos de los responsables de este rubro en mencionadas empresas, son delegados por la alta dirección para realizar un gerenciamiento misional u operativo, y probablemente lo realicen bien, sin embargo descuidan el verdadero sentir de lo que es la protección integral, por cuanto en algunas ocasiones su labor se limita sólo a aprehender a quien robó, dejar ver quien fue que lo hizo, o temas superfluos, dejando esa verdadera protección de activos y la prevención de pérdidas desde las diferentes ópticas a comentarios y percepciones falsas por los supervisores de tan importante rol en las instalaciones de atención hospitalaria.

¿DE QUÉ MANERA PODRÍA MEJORAR MI ROL?

En uno de mis artículos pasados he hablado de la triple hélice de la seguridad hospitalaria, y empezaré por ello, por mencionarlas y dentro de ellas, que poder hacer para que el cargo como tal se invista de un verdadero valor.

a) La Seguridad del paciente: es uno, si no el principal foco de atención de este tipo de industrias, es así, como desde los altos estándares clínicos, como el de "The Joint Commission" tiene en cuenta en su intención la calidad y seguridad del mismo paciente, y dentro de los cuales, seguridad tiene una importante relevancia.

En enero de 2022, este importante ente acreditador de hospitales, clínicas y centros de larga estancia alrededor del mundo, actualizó sus estándares, y quizás la inclusión más importante (en cuanto a *security* y *safety*) en ellos tiene que ver en la orientación para que se afecte e intervenga en temas de prevención e intervención de la violencia en el lugar de trabajo para este tipo de organizaciones, dentro del cual hay participación activa de los responsables de seguridad ocupacional y por supuesto de seguridad.

Entonces, nuestra participación como componente de protección juega un papel más importante, toda vez, que se propende por mejorar la consciencia y cultura no sólo de seguridad, sino que de protección.

b) Seguridad ocupacional: en este segmento podría pensarse que nuestra responsabilidad es nula, sin embargo, cada momento que pasa en las instalaciones, debe tenerse en cuenta las condiciones ambientales y como éstas, pueden en un momento determinado afectar a la misma empresa, permitiendo pérdidas que se ven reflejadas por pago de indemnizaciones, incapacidades y otros conceptos que claramente afectan el cumplimiento de los objetivos.

Algunos de los responsables de Seguridad son delegados por la alta dirección para realizar un gerenciamiento misional u operativo, y probablemente lo realicen bien, sin embargo descuidan el verdadero sentir de lo que es la protección integral

c) Seguridad: es precisamente el punto central de este artículo, y es que se debe "pensar fuera de la caja" y desmitificar el rol policial o militar, de que se enfoque en actividades reactivas la gestión de seguridad. Claramente, se paga una importante cantidad de dinero a una empresa que provee el servicio de vigilancia y seguridad privada para que bajo la dirección del responsable o delegado de la organización, actúe, pero no es su eje central. O acaso ¿la empresa paga XXX cantidad de dinero en ocasiones miles o millones a una persona para que realice un doble esfuerzo por el cual ya se está pagando?

Es entonces, donde el responsable de la seguridad debería pensar de manera gerencial y entregar un producto más concreto, que tan solo ser el representante de la vigilancia ante la organización para la que trabaja. Su enfoque debería estar centrado en aspectos más estratégicos como el análisis de las vulnerabilidades, vistas como las brechas que se presentan no sólo en las instalaciones físicas, sino que se mire la parte administrativa o procedimental, y también de la tecnología.

LOS RIESGOS

Definidos de manera clara y particular y teniendo en cuenta, como la identificación de éstos se ajusta a la operación diaria de la misma facilidad, y la manera en la cual, cada tipo de riesgo puede ser intervenido desde su posición en la empresa. La definición de las amenazas, entendiendo el comportamiento del contexto y la interacción con cada uno de los conceptos anteriores, sabiendo que cada ubicación es única, tiene personas, comportamientos y problemas únicos, que pueden en momentos particulares ser similares, pero que conservan su estatus de "único".

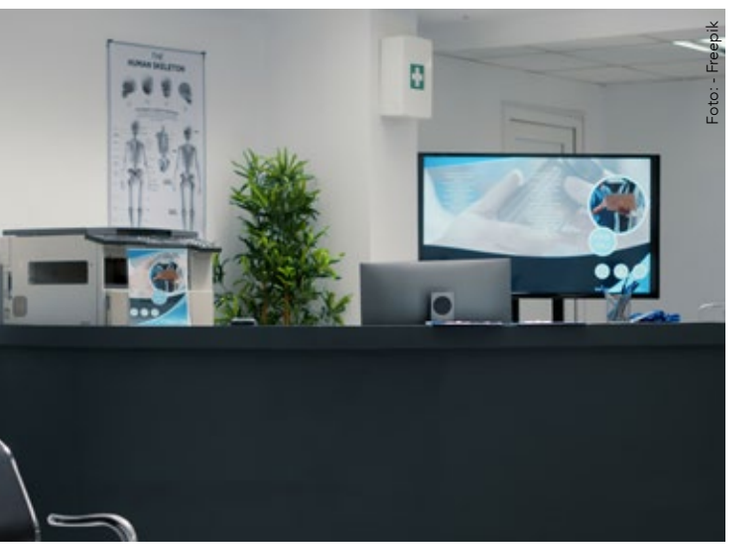


Foto: - Freepik


Foto: - Freepik

Finalmente la identificación de los activos, empezando por entender y reconocer los tipos y clases de activos (que si bien es cierto, en muchas ocasiones, creemos saber y conocerlos, pero lo que se encuentra en la realidad, deja ver en algunos casos que no es así), de esto depende que se pueda definir la cantidad y calidad de contramedidas como el componente humano (guardas y/ o vigilantes), tipo y clase de cámaras y demás elementos qué ayuden a complementar el Sistema de Protección Física (PPS, por sus siglas en inglés), pero que además dejen ver y logren suministrar elementos de juicio para saber si la seguridad de las HCF, es costo-efectiva y adecuada a lo que se pretende proteger.

Así las cosas, lo que se debería propender es porque los recursos en verdad estén sincronizados con una verdadera necesidad producto de un análisis juicioso y sistemático, que permita a la alta dirección comprender que la seguridad en un hospital o clínica es una inversión y no un gasto como en diferentes escenarios se percibe por la parte estratégica de estas facilidades. ■

Daniel Jiménez, PSP, CHSS, presidente del Capítulo 225 Bogotá ASIS International. Más sobre el autor:

EL SALVADOR CON NAYIB BUKELE

LOGRA REDUCIR FRECUENCIA Y NÚMERO DELICTIVO

Con voluntad política un país como El Salvador nos demuestra que si se puede controlar la criminalidad, del mismo modo la violencia extrema que hoy vivimos en el Perú necesita ser controlada por el Poder Ejecutivo

PERÚ | César Ortiz Anderson

Me basé en la excelente crónica de la buena periodista y redactora del suplemento dominical del diario la República Juana Gallegos Ayala "El Costo de la Paz de el Salvador", es tan buena crónica que investigue y puse muy breves comentarios.

Según el periódico digital el Faro de El Salvador, reporta que cuando en el mes de marzo del año 2022, que se implementó el Régimen de excepción impuesto por el presidente Nayib Bukele ya no se ven pandilleros, al menos ni la sombra de antes.

Recordemos que en el año 2015, El Salvador era considerado el país mas violento del mundo y las cifras hablan por sí solas 103 homicidios por cada 100 mil habitantes, en una población de aproximadamente 6.5 millones de habitantes, y una superficie de 21 mil 40 Km^2, para que el lector se pueda hacer una idea en el Perú tenemos una tasa aproximada en la actualidad de mas de 8.1 homicidios por cada 100 mil habitantes, con una población de mas de 33 millones de habitantes, y una superficie de 1,285 millones de Km^2, según el diario el Farol el año pasado en los primeros 212 días no se reportó un solo homicidio en el país, según nuestras fuentes si hubieron pero muy pocos, sin duda ha sido un gran trabajo con resultados muy positivos en la lucha contra la criminalidad, la reducción del número y frecuencia de homicidios ha sido un récord mundial en la lucha contra la criminalidad.

Foto: - Freepik

Por otro lado, el diario el Faro, que es crítico al gobierno de Bukele, resalta los buenos planes y estrategias aplicadas como:

1. El trabajo realizado para destructurar las pandillas.
2. Han desbaratado el control territorial de la criminalidad.
3. Combatir de manera permanente sus vías de financiamiento.
4. La capturas de sus líderes.

Son esos cuatro puntos la base para esa reducción drástica de crímenes, ademas ya no están ocurriendo muchos casos de extorsión a empresarios y transportistas, que antes tenían que pagar su cuota de "protección" a las pandillas, sólo con los transportistas recaudaban en promedio mas de 34 millones de dólares por año, otro punto importante son las zonas manejadas con fronteras invisibles en los distritos que impusieron las pandillas a hoy ello ya no existe y se vienen recuperando espacios públicos para los ciudadanos. Desde que empezó el régimen de excepción, hasta el mes de enero de este año 2023 y éstas son citas del propio gobierno, se han capturado a más de 63 mil personas.

COSTOS SOCIALES

Sin duda debido al trabajo realizado son inevitables los costos sociales, por ejemplo, según Erika Guevara, directora para las Américas de Amnistía Internacional, una de las tantas ONG que hay en nuestros países, señala que se han reportado casos de detenciones arbitrarias, violación de los derechos humanos como torturas o muertes de personas bajo custodia del Estado, en ese punto quisiera comentar que ayer siete valerosos policías fueron cruelmente asesinados por narcoterrorista en la zona del VRAEM, en el centro poblado de natividad en Perú y ninguna ONG de derechos humanos se pronuncian, ninguna.

Según el medio de comunicación de El Salvador, el diario el Faro, el porcentaje de pandilleros capturados no llega ni a un 30%, habría que señalar también que de acuerdo a nuestras investigaciones, algunos líderes y pandilleros se han ido a los países fronterizos como: Nicaragua, Honduras y Guatemala, los menos también han viajado algunos países de la región, con lo cual Interpol y todas las policías deberán estar muy atentas.

Un libro que refleja 30 años de experiencia

El autor tiene experiencia como Director de Seguridad Corporativa, operando a nivel global en diversas empresas asi como catedrático universitario lo que conjuga la experiencia operativa y la docencia en su libro.

El libro versa sobre los criterios que rigen en las organizaciones empresariales en materia de administración de pérdida y como el ejecutivo de Seguridad Corporativa debe aplicar un modelo de Inteligencia para entender los tiempos que vive la empresa, su naturaleza y al final lo que rige su actuación, su cultura organizacional, y una vez entendido lo anterior, estructurar una propuesta de valor tal, que sea incluida en la toma de decisiones críticas. Seguridad Corporativa, se vuelve una función crítica cuando atiende la naturaleza humana de las corporaciones en su identificar y asimilación de riesgos y como decide esta administrar sus acciones para manejar la pérdida. Donde se diferencia el cumplimiento obligatorio, del cumplimiento como cultura. Donde no se habla de la seguridad de la empresa, sino de una empresa segura.

El autor comparte esta obra, más de 28 años como alto directivo de Seguridad Corporativa, operando a nivel global para empresas de la construcción, tabaco, retail, telecomunicaciones, banca y entretenimiento, en entornos de terrorismo, guerrilla, violencia social, delincuencia organizada y desastres naturales, donde los tiempos y la naturaleza de cada empresa determinan las acciones para manejar estas condiciones. Así también como logra una transición exitosa de 20 años en el campo de la seguridad en las fuerzas armadas al mundo corporativo.

¡Cómpralo aquí!
$280 + envío

En Perú, según el profesor, abogado internacionalista, Francisco Belaúnde Matossian, realiza una opinión sobre las estrategias aplicadas por el presidente Bukele, que reconoce han servido en el corto plazo, pero se pregunta que pasará en el mediano y largo plazo, además señala que la popularidad de gobernantes de corte autoritario, no son novedad, ocurren con bastante frecuencia, recordemos cuando Alberto Fujimori dio el golpe en el año 1992.

Las situaciones límites favorecen a líderes políticos con agendas autoritarias, para Belaunde la lección que se debería sacar de la experiencia vivida en El Salvador, es que no sólo basta la mano dura como una salida para enfrentar la inseguridad, las democracias también deben ser eficientes para ello, señalando que estos fenómenos están ligados también a la lucha contra la corrupción e impunidad. No sólo se trata de atrapar delincuentes, sino que además estos sean efectivamente castigados, garantizando para ello el debido proceso.

El porcentaje de pandilleros capturados no llega ni a un 30%, habría que señalar además que algunos líderes y pandilleros se han ido a los países fronterizos como: Nicaragua, Honduras y Guatemala, los menos también han viajado algunos países de la región, con lo cual Interpol y todas las policías deberán estar muy atentas

Foto: - Freepik

Foto: - Freepik

La lección que se debería sacar de la experiencia vivida en El Salvador, es que no sólo basta la mano dura como una salida para enfrentar la inseguridad, las democracias también deben ser eficientes para ello, señalando que estos fenómenos están ligados también a la lucha contra la corrupción e impunidad

El presidente Nayib Bukele ha vuelto a la palestra al inaugurar el "Centro de Confinamiento del Terrorismo", la cárcel más grande de Latinoamérica que podrá albergar a 40 mil internos en varios módulos muy seguros, eso sí continuando con la mano firme y dura contra la criminalidad esta prisión no contará con patio de recreo y advierte que allí serán también recluidos los pandilleros.

Finalmente, un país mucho más pequeño que el Perú, con muchos menos ingresos económicos, nos está dando una gran lección con una verdadera voluntad política, con expertos que tengan una visión holística del fenómeno y con instituciones comprometidas en realizar un trabajo integral y articulado si se puede sentar las bases en nuestro país, eso sí lo señalado por el abogado internacionalista Francisco Belaúnde que de plano debemos combatir frontalmente la corrupción e impunidad, que son en mi opinión las piedras angulares de todos nuestros problemas. ■

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

FACEit

PLATAFORMA TECNOLÓGICA EN LA NUBE
PARA COMPAÑÍAS DE SEGURIDAD

GRUPO SALUS
SEGURIDAD Y BIENESTAR

Faceit es un poderoso software para dirigir y controlar la operación de su empresa beneficiando todas las áreas como:

- "**Supervisión** en tiempo real de las operaciones de seguridad."
- "**Optimización** en la gestión del personal de seguridad."
- "**Generación** de informes detallados en cuestión de minutos."
- "**Aumento** en la eficiencia."
- "**Y ahorros de tiempo** con el uso del software."

SOLUCIONES SIMPLES A PROBLEMAS COMPLEJOS

Conoce nuestros servicios en nuestro sitio web www.gruposalus.com.mx

Tel. +52 55 2560 7642

WWW

WWW.GRUPOSALUS.COM.MX/FACEIT

CONTÁCTANOS
Y SOLICITA TU DEMO

SEGURIDAD PERSONAL EN ÁREAS DE ALTO RIESGO

Consejos para no ser víctimas de la violencia urbana

Foto: - Freepik

GUATEMALA | Enrique Jiménez Soza

Nada está garantizado en un 100% cuando se trata de seguridad : 90% prevención, 5% reacción y 5% suerte.

La prevención representa un 90% en seguridad, por eso las acciones se deben concentrar en esta etapa.

PREPARACIÓN ANTE UN ASALTO

En general todo asalto tiene una cierta preparación que consiste en:

1) **Elección del blanco:** esta fase puede llevar meses, días o apenas unos segundos. Es cuando el delincuente elige a quién atacar
2) **Identificación del blanco:** esto ocurre luego de elegir el blanco. Generalmente es el más débil, el más distraído o el que tiene lo que el delincuente busca (dinero, modelo de auto, etc.).
3) **Vigilancia:** periodo en el que el delincuente evalúa la situación antes de atacar. Es el mejor momento para interrumpir la acción del delincuente.
4) **Planeamiento:** el delincuente tiene todo lo que necesita; ahora planea cómo será el ataque (día, hora, lugar, forma de abordarlo, arma, etc.).
5) **Ataque:** el delincuente ataca. En esta fase ya no es posible la prevención, y menos del 5% de las acciones de interrupción tiene éxito. Es el peor momento para interrumpir la acción del delincuente.

REGLAS

El delincuente no tiene un aspecto determinado. El modelo de delincuente mal vestido está superado.

Hoy, muchas personas cuentan que fueron abordadas en semáforos por delincuentes elegantes de traje y corbata, y al abrir el vidrio fueron asaltadas. También aumentó mucho la participación de mujeres.

Éstos:

- No quiere exponerse.
- Siempre elige sus víctimas.
- Siempre elige lo más fácil, es decir el más desprevenido.
- Durante un asalto el delincuente está nervioso y con miedo.
- Reaccionar es una actitud de altísimo riesgo.

Observe siempre:

- El comportamiento.
- Las manos (generalmente escondidas en los bolsos).
- Los ojos (dicen que los ojos son el reflejo del alma, y esto es verdad: observe los ojos y sabrá si tiene mala intención o no).

ACCIONES DE PREVENCIÓN

Está equivocado al pensar que no le va a ocurrir a usted.

Permitir que ocurra (tenga dinero separado para entregar al delincuente si ocurre un asalto).

Mientras que una actitud acertada sería actuar en forma preventiva, evitando que ocurra el asalto.

El modelo de delincuente mal vestido está superado. Hoy, muchas personas cuentan que fueron abordadas en semáforos por delincuentes elegantes de traje y corbata, y al abrir el vidrio fueron asaltadas


Foto: - Freepik


Foto: - Freepik

Busque un lugar donde protegerse, un lugar bastante concurrido, con policías o personal de seguridad

CAMINANDO POR LA CALLE

Camine observando todo lo que ocurre a su alrededor (incluso detrás de usted), si ve alguien sospechoso observe sus manos, y si es posible, sus ojos.

Para el delincuente el espacio es su enemigo. Por eso necesita "cerrar el espacio", es decir necesita acercarse para realizar el ataque. Por eso trate de mantener siempre 20 metros (margen de seguridad) entre usted y el sospechoso, ya que nadie asalta a nadie a distancia.

Cuando el sospechoso está cerrando el espacio entre ustedes (por ejemplo, caminando en dirección a usted), proceda de la siguiente forma:

- Cambie de vereda y observe cómo se comporta el sospechoso.
- Si el sospechoso cambia también de vereda, la probabilidad de que lo aborde se vuelve mucho mayor.
- No permita que el sospechoso "cierre el espacio". Si esto ocurre usted. no tendrá nada más que hacer. El delincuente habrá ganado.

Para que el delincuente no "cierre el espacio":

- Busque un lugar donde protegerse, un lugar bastante concurrido, con policías o personal de seguridad.
- Si no hay dónde protegerse, cambie la dirección en que camina. De esta forma mantiene el espacio entre los dos.

¿CÓMO PROCEDER?

- El delincuente viene en su dirección, así que cámbiela, para mantener el espacio entre ustedes.
- Él apresura el paso en su dirección, por lo que es recomendado que busque un lugar seguro y concurrido (un negocio, un supermercado, etc.).
- Si no hay lugares donde protegerse, corra y observe el comportamiento del sospechoso. Corra antes de que él pueda cerrar el espacio entre ustedes. Nunca corra después del abordaje.
- Si el sospechoso corre en dirección a donde está usted, está claro que pretende cometer un delito y en ese caso grite. Generalmente el delincuente no va a correr detrás de usted ya que no quiere llamar la atención, y prefiere elegir otra víctima menos alertada.

¿QUÉ HAY QUE GRITAR?

- Gritar "socorro" hace que las personas a su alrededor se alejen, porque está claro que hay peligro.
- Gritar "fuego" despierta el interés de las personas. Muchas salen de sus casas para ver dónde está el fuego.
- Gritar el nombre de alguien, "Coco", es la mejor opción, ya que esto es poco común y el delincuente tendrá miedo de que haya más personas en el lugar (¿quién es Coco? ¿Un amigo, un policía, un perro feroz?). Hay buenas posibilidades de que desista.

REGLA

Si usted tiene el presentimiento de que alguien lo va a abordar nunca cierre el espacio. Muchas personas que fueron asaltadas cuentan que percibieron que algo iba a suceder y no tomaron ninguna precaución. ■

Enrique Jiménez Soza, asesor profesional de seguridad. Más sobre el autor:

SEGURIDAD FARMACÉUTICA: RECOMENDACIONES PARA EL CONTROL Y RESGUARDO DE MEDICAMENTOS

Foto: - Freepik

Es necesario revisar las normas, guías y leyes que regulan los medicamentos, realizar análisis de riesgos y gestionarlos periódicamente

MÉXICO | Francisco Javier Villegas Barbosa

Las áreas de Seguridad y Protección normalmente se identifican como aquellas que se dedican a administrar a los oficiales de seguridad y el CCTV, sin embargo, existen muchas más actividades en las que estas áreas pueden aportar un gran valor para una organización, ya sea con la creación de programas de prevención de pérdidas, la gestión de riesgos e incluso con el manejo de crisis o de programas de continuidad de las operaciones.

Para generar este valor y con el objetivo de ayudar a mitigar cualquier riesgo, es indispensable que el profesional de seguridad conozca su institución —cada uno de los recovecos—, que se entere de todo lo que sucede, que tenga clara la misión y visión de la empresa, que resguarde lo más preciado y que identifique con antelación aquello que pudiera afectarla.

El profesional de seguridad debe estar siempre en la búsqueda de todo aquello que pudiera ocasionar una pérdida o le reste velocidad al negocio, y en la industria de la salud no es la excepción. De hecho, cuando hablamos de gestionar riesgos, uno de los temas más importantes dentro de un hospital o grupo hospitalario es la seguridad y protección de medicamentos.

Partiendo de que todo hospital, clínica o centro de salud, sin importar el tamaño, debe contar con un lugar o área donde se almacenan los medicamentos, el cual puede ser llamado almacén de farmacia o de medicamentos, les comparto los puntos más importantes a considerar para su correcto resguardo y control:

1) **Contar con la documentación legal.** Este punto es de suma importancia para la continuidad de operaciones, ya que al no contar con toda la documentación correspondiente, se corre el riesgo de que ante la verificación de un organismo legal se sancione a la empresa con una multa o clausura. Algunos de estos documentos son:

- Aviso de funcionamiento.
- Licencia sanitaria.
- Responsable sanitario.
- Factura y documentos de compra o venta de los medicamentos.
- Registros del monitoreo de temperatura del almacén. Esta área no debe rebasar los 30°C y no debe tener una humedad relativa mayor al 65%, los refrigeradores que conservan los medicamentos deben mantener una temperatura entre 2°C y 8°C. Estos mismos equipos deben de contar con sus calibraciones correspondientes por terceros acreditados.

2) **Sistemas de Gestión de Calidad.** Los procedimientos y políticas deben ser claras e incluir lo siguiente:

a) **Auditorías.** Los departamentos de seguridad y protección deben participar en las auditorías y revisiones mensuales. Es importante evitar que los mismos almacenes sean juez y parte, para evitar incidentes o malas interpretaciones.

b) **Gestión de riesgos.** La participación activa para la detección de riesgos y peligros a los que están expuestos los medicamentos es vital. En este proceso podemos definir planes de mitigación, además de involucrar a todos los colaboradores e incluso a los pacientes.

c) **Simulacros.** Para todas aquellas amenazas que se identifican en la gestión de riesgos se debe de contar con un plan para hacerles frente, y es menester practicar ese plan de mitigación, por ejemplo:

- **Recolección por alerta sanitaria (*Recall*).** Cuando un medicamento debe ser recolectado y sacado del almacén para ser llevado a la autoridad a consecuencia de una alerta.
- **Falla eléctrica.** Para los medicamentos refrigerados tenemos que establecer un plan B; en la mayoría de los casos se cuenta con planta de energía externa, pero si no se tiene o ésta falla, se deben planear y esbozar las alternativas.
- **Inundaciones y/o huracanes.** Se debe definir cómo se retirará el medicamento de la zona afectada, contemplar su reubicación y traslado seguro.

3) **Ciberseguridad.** En la actualidad, gran parte de los registros de transacciones de los medicamentos se realizan mediante medios de sistemas computacionales, éstos mismos deben de contar por lo menos con:

- Protección de acceso al mismo sistema mediante dos elementos distintos, como: código de identificación y claves que garanticen la integridad de la información.
- Respaldos periódicos, físicos o en la nube, para que estén correctamente protegidos y disponibles en caso de ser necesarios.
- Respaldo eléctrico a los sistemas de cómputo.

4) **Procedimientos Normalizados de Operación (PNO).** Contar con documentos vigentes donde se describan todas las actividades que nos darán garantía de estandarización y continuidad:

- Elaboración de auditorías y los departamentos participantes.
- Verificación, mantenimiento y calibración de equipos (planta de luz, extintores, termómetros, refrigeradores, detección de humo, control de acceso, CCTV, etc.). Recordemos que los equipos que garantizan la calidad e integridad del medicamento son críticos.
- Planes de emergencias, crisis y continuidad de las operaciones.
- En caso de robo, asaltos o extravíos.

5) **Personal.** Lo más importante de toda institución, y a su vez, de lo más crítico para la seguridad. Algunas empresas, desde su reclutamiento, cuentan con controles para verificar la veracidad de la documentación y competencias de los candidatos, así como pruebas psicométricas y de honestidad que ayudan a seleccionar a la mejor persona para trabajar y administrar un almacén de medicamentos. Debemos asegurarnos de:

- Garantizar el Equipo de Protección Personal (EPP) en los casos que aplique.
- Brindarles uniforme e identificación correspondiente para laborar en el área.

6) **Instalaciones y Equipo.** Todas las instalaciones como paredes, techos y puertas, deben ser construidas de material que garantice el resguardo de los materiales y equipos:

- Ventanilla de despacho.
- Control de accesos.
- CCTV.
- Luces de emergencia.
- Rutas de evacuación.
- Cerraduras en anaqueles de medicamentos controlados.
- Cerradura en refrigeradores (en los que aplique).
- Áreas segregadas de productos caducos o desechos.
- Estantería anclada en paredes o piso, y separada del piso, pared y techo por 20 cm, con el fin de asegurarlas.

7) **Productos Controlados y de Alto Riesgo.** Los medicamentos controlados tienen ciertas obligaciones y cumplimientos legales, el no cumplir con ellos deriva en amonestaciones con apercibimiento, multas, clausura temporal o definitiva (que podrían ser parcial o total) y, en algunos casos, hasta la cárcel. Todo medicamento controlado que se utilice sin autorización y sin la documentación necesaria puede incurrir en delitos federales.

Los medicamentos a los que debemos poner mayor atención son los estupefacientes y psicotrópicos; algunos de ellos requieren refrigeración y su trazabilidad debe ser muy estricta. Al ser medicamentos muy potentes, son también muy atractivos para personas sin escrúpulos que los utilizan lúdicamente o para hacer negocio sin medir las consecuencias legales y de salud.

Por tal motivo el Departamento de Seguridad y Protección debe de trabajar de la mano con los responsables de farmacovigilancia y QFB responsables de los almacenes de medicamentos para llevar un estricto control, desde la salida de almacén hasta su destino final:

- Los medicamentos controlados deben de contar con una receta firmada, con folios correspondientes en su receta y en papel seguridad.
- Se debe registrar la cantidad, lote, destino del medicamento y quién lo recibe.
- Todos los medicamentos de estas categorías deben estar resguardados bajo llave en gabinetes sólidos.
- Los utilizados en cirugía deben ser devueltos al almacén.
- Para los sobrantes se debe realizar un reporte y entregarlos al almacén para su resguardo y confinamiento.

Las cirugías es uno de los lugares o momentos más críticos en donde se disponen de los medicamentos, pues hay la posibilidad de que algunos de ellos no sean utilizados o que haya sobrantes, y con ello una oportunidad para los presentes en las cirugías de tomarlos y utilizarlos fuera de la institución. Es por esto mismo que debemos contar con personal profesional e íntegro, con alto grado de compromiso y honesto que detenga cualquier desviación subestándar y así poder evitar:

- Cargos al paciente de medicamentos no colocados/consumidos.
- Sustracción de medicamentos para uso personal, o para ser usados en otros lugares donde no se tiene acceso a estos medicamentos, y realizar un negocio con insumos propios del hospital.

La falta de seguimiento a los puntos anteriores puede derivar en un mal manejo y resguardo de los medicamentos, lo que puede llegar a provocar no sólo una suspensión de labores sino también, y más crítico aún, daños a la salud de los pacientes e incluso su muerte.

Es necesario que revisemos las normas, guías y leyes que regulan los medicamentos, realizar análisis de riesgos y gestionarlos periódicamente o cuando exista algún cambio en el entorno del país, sigamos buscando ser más fuertes y robusteciendo los procesos de seguridad y protección, adoptemos el término "anti frágil" de Nassim Taleb. ■

Referencias:

- *Cofepris: Guía para almacenes de depósitos y distribución de medicamentos y demás insumos para la salud.*
- *Cofepris: Acta de verificación Sanitaria.*
- *NOM- 059-SSA1-2015 – Buenas prácticas de fabricación de medicamentos.*
- *NOM-241-SSA1-2012 – Buenas prácticas de fabricación para establecimientos dedicados a la fabricación de dispositivos médicos y el suplemento para establecimiento dedicados a la venta y suministro de medicamentos y demás insumos para la salud.*
- *Estándares de la Joint Comission Internacional para Hospitales.*
- *Estándares para implementar el Modelo en Hospitales- Modelo de Seguridad del Paciente del SiNaCEAM.*

Francisco Javier Villegas Barbosa, CPP, DSE, CPO, CSO en Christus Muguerza. Más sobre el autor:

Foto: - Freepik

FALSIFICACIÓN DE MEDICAMENTOS: EL CÁNCER DE LA INDUSTRIA

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Entre los medicamentos que más se falsifican en México están los productos para tratar la disfunción eréctil y el cáncer, así como los antibióticos y analgésicos, lo que puede provocar desde no curarse hasta la muerte

La industria farmacéutica en México representa el 1.8% del Producto Interno Bruto (PIB) respecto al PIB de las manufacturas, teniendo un crecimiento considerable durante la pandemia por COVID-19. Precisamente en el año 2021 se logró un crecimiento de 8.4% respecto a 2020, y se generaron al menos 79 mil puestos de trabajo representando un incremento del 3.6% respecto al año 2019.

De acuerdo con el documento "Conociendo la industria farmacéutica", que forma parte de la Colección de estudios sectoriales y regionales elaborado por el Instituto Nacional de Estadística y Geografía (INEGI) con apoyo de la Cámara Nacional de la Industria Farmacéutica (CANIFARMA)[1], los medicamentos con mayor venta en el país se dividen en seis tipos de productos más importantes los cuales suman el 59.6% del valor de la producción a precios corrientes: "antibióticos (15.0%), medicamentos para el sistema digestivo y para el metabolismo (10.5%), medicamentos para el sistema nervioso (9.6%), medicamentos para uso veterinario (9.4%), vitaminas y compuestos vitamínicos (8.7%) y medicamentos para el sistema cardiovascular (6.4%)".

Ante la demanda de servicios de salud, las clínicas particulares aumentaron su número de pacientes o asistencia médica, pero también por la demanda de medicamentos y el propio desabasto de éstos, la posibilidad de falsificarlos de igual manera se incrementó.

Durante el doceavo Congreso Nacional de Farmacias 2022 (Ciudad de México), el director general de CANIFARMA, Rafael Gual Cosío, confirmó que para ese año hubo un crecimiento de 36% en la producción de medicamentos; no obstante, Juvenal Becerra, presidente de la Unión Nacional de Empresarios de Farmacias (Unefarm), en el mismo evento reveló que el tráfico ilegal de medicamentos viene en mayor medida de Centroamérica, se venden en páginas de Internet y se concentra en Ciudad de México, Estado de México, Guadalajara y Michoacán.

"Becerra estimó que el mercado irregular repuntó un 20% en 2021 hasta alcanzar un valor de 28 mil millones de pesos (cerca de 1,365 millones de dólares), entre medicinas caducas, falsificadas y robadas, además de insumos como cubrebocas o gel antibacterial sin certificaciones"[2]. Para lo que Rafael Gual agregó que el robo y falsificación de medicamentos representa un 6% del comercio total de fármacos.

El robo y falsificación de medicamentos representa un 6% del comercio total de fármacos

"#VeALoSeguro" es una campaña de prevención para identificar un medicamento original de uno falsificado, que lanzó CANIFARMA en sus redes sociales. Entre los consejos que la Cámara emite a los usuarios, está el de comprar los medicamentos en establecimientos seguros, ya que la mayor venta de los medicamentos falsificados proviene de redes sociales y páginas de Internet, que aunque sean empresas de *e-commerce* reconocidas, los vendedores son prácticamente desconocidos, así como el origen del producto.

Siendo un riesgo para la salud, realizamos una entrevista con uno de los expertos en materia de seguridad en la industria farmacéutica con amplia experiencia y trayectoria en el sector: Gerardo Corchado, consejero de la Comisión de Seguridad de CANIFARMA.

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

Gerardo Corchado (GC): los problemas de seguridad más comunes, como en todas las industrias, son: intrusiones ilegales a las instalaciones; los peligros que corren sus empleados, desde los obreros hasta los ejecutivos, por ejemplo, ser asaltados, desapoderados de sus bienes, extorsionados o peor ser víctimas de un secuestro largo o exprés, es decir, los peligros que la mayoría de las personas corremos en ciudades grandes de casi cualquier país, entre otros.

Sin embargo, la industria farmacéutica organizada en la CANIFARMA (Cámara Nacional de la Industria farmacéutica) también se preocupa por temas como el robo de sus materias primas y productos terminados en tránsito, así como por la falsificación de medicamentos, ya que ambos delitos pueden poner en riesgo la salud y la vida de los pacientes.

SEA: ¿Qué es la falsificación de medicamentos?

GC: para que todos lo podamos entender, ocurre como en casi todos los productos que son pirateados, clonados o falsificados; te venden algo con la intención deliberada de engañarte y ofreciéndotelo como un original con su marca de prestigio. Sin embargo, en la mayoría de los productos tú puedes darte cuenta si es falsificado, desde que te dicen el precio, el cual no coincide con el real: ropa de marca, tenis famosos, relojes finos, perfumes exclusivos que te venden en cientos de pesos, ¡cuando en realidad cuestan miles!

El usarlos, ponértelos o vestirlos en realidad no te causará un daño, sin embargo, una tableta, una inyección intravenosa, un dispositivo médico que estará dentro de tu cuerpo, es un riesgo de daño a tu salud inminente y de alcances potenciales incalculables que, te pueden llevar desde no curarte, enfermarte más o, incluso hasta la muerte.

Mi punto de vista personal después de ver este flagelo por más de 20 años, es que no sólo es un delito, es una acción cobarde y ruin. ¿Cómo ser capaces de abusar y dañar a una persona enferma, debilitada, disminuida, que incluso puede estar inconsciente, ser un anciano o un bebé?

SEA: ¿Qué tipos de medicamentos suelen ser falsificados con mayor frecuencia?

GC: los falsificadores seleccionan los productos más demandados, los más necesitados, los que más compra la gente, pueden ser caros o baratos, pero ellos saben que se venderán pronto, entre ellos destacan los productos para tratar la disfunción eréctil y el cáncer, también los antibióticos, analgésicos, antigripales, antitusivos y algunos dispositivos médicos de uso común como preservativos, gasas o venoclisis. Sin embargo, para ellos no hay limitaciones y son capaces de falsificar lo que sea.


Foto: - Freepik

SEA: ¿Cuáles son los peligros y riesgos asociados con los medicamentos falsificados?

GC: diversos productos falsificados, como ropa, perfumes, tintas, accesorios, etcétera, se pueden encontrar en los mercados informales: tianguis, pulgas, sobre ruedas; allí la gente los compra, sin embargo, nadie debería pensar en comprar en un lugar de estos, un medicamento para su uso o el de su familia.

Los medicamentos originales son fabricados y manejados hasta su punto de venta formal, como las farmacias, con estrictas reglas sanitarias supervisadas por la Autoridad Regulatoria. En el caso de los productos falsificados no sabemos nada de ellos, de qué están hechos, cómo fueron empacados, almacenados, distribuidos, entonces, los peligros y los riesgos son incalculables, como lo mencioné antes, puedes no curarte de lo que ya estabas enfermo y, si tu padecimiento es grave, como un cáncer, perderás el control de tu enfermedad por la falta de efecto terapéutico y simplemente no sobrevivirás, si el producto falsificado contiene virus, bacterias o sustancias tóxicas, el pronóstico es reservado, pues ya estabas enfermo y ahora pudieras enfermarte de algo nuevo y quizá peor, la muerte es un catastrófico, pero posible escenario.

SEA: ¿Cómo se pueden identificar los medicamentos falsificados?

GC: la mayoría de los medicamentos falsificados están fabricados y empacados de manera muy parecida a los originales pues, su intención es engañarnos. En realidad, la única manera formal para determinarlos como falsos es mediante un análisis de su composición química que, usualmente sólo puede hacer el fabricante al compararlo con la información guardada de un original. Existen actualmente grandes esfuerzos de la industria farmacéutica para tener en varios continentes equipos electrónicos que ayuden a detectar productos farmacéuticos falsificados.

Sin embargo, en México la industria farmacéutica ha reunido experiencia en este asunto y ahora somos capaces de detectar más fácilmente los "medicamentos sospechosos de ser falsificados", y entonces, denunciamos ante la autoridad para investigar su origen y llegar al punto de su fabricación clandestina. Se ha desarrollado un protocolo de observación de "fallas" en los empaques que los delatan como posibles falsificaciones, como por ejemplo, faltas de ortografía, errores de impresión, colores sospechosos, errores en el suaje, lotes y fechas de caducidad marcados con letras no ordinarias en estos procesos, etcétera.

La industria farmacéutica en México representa el 1.8% del Producto Interno Bruto (PIB) respecto al PIB de las manufacturas

Al identificar estos medicamentos sospechosos y denunciarlos para su investigación, estamos dando el primer y gran paso para la protección de los pacientes.

SEA: ¿Cuáles son las medidas que los fabricantes y las autoridades toman para combatir la falsificación de medicamentos?

GC: los fabricantes de los productos farmacéuticos deben cumplir con estrictos estándares de fabricación, empaque y manejo de los medicamentos, además de ello implementan principalmente en los empaques medidas de seguridad contra la falsificación como son, hologramas, etiquetas especiales, sellos de seguridad y las marcas secretas en los suajes, entre otras; sin embargo, estas medidas son también imitadas por los falsificadores y para el público en general es difícil detectar las diferencias.

La Comisión de Seguridad de la CANIFARMA, de la cual soy consejero, y hoy es dirigida por Alejandro Córdova y presidida por Jesús Islas, ha logrado el acopio de casi 20 años de información y muestras de medicamento falsificado y, con ello se ha diseñado una estrategia y un entrenamiento para capacitar a las diversas autoridades que pudieran llegar a tener de frente un caso de producto sospechoso de falsificación. Ahora estas autoridades saben detectarlos, manejarlos y avisar a los fabricantes para notificar a la autoridad sanitaria competente, que en el caso de México es la Cofepris (Comisión Federal de Prevención de Riesgos Sanitarios).

Este acervo de información está preparado y ordenado en un entrenamiento especializado y a la disposición de los grupos internos de la industria farmacéutica, por ejemplo, sus áreas de Calidad, Cadena de Suministro, Legal y Regulatorio, quienes lo nutren constantemente para después, a través de la CANIFARMA, llevar este entrenamiento a diversas autoridades para unir esfuerzos en la investigación de este delito y actuar en beneficio de la salud de los pacientes.

El entrenamiento llamado "detección y manejo de productos farmacéuticos sospechosos de ser falsificados" se ha ido perfeccionando gracias al trabajo y la voluntad de muchas personas, por ejemplo, hace 15 años se unió a nuestro equipo Javier Martínez Cañal, un especialista impresor afiliado a la Cámara Nacional de la Industria de Artes Gráficas, quien se ha convertido en un pilar de esta capacitación, explicando a los asistentes los modos correctos de impresión y enseñándolos después a detectar errores y fallas que cometen los falsificadores. Esta capacitación se ha dado a: FGR, FGJCDMX, Guardia Nacional, Aduanas, SSCCDMX, entre otros.

SEA: ¿Cómo puede un consumidor protegerse de los medicamentos falsificados?

GC: aprendiendo a observar su medicamento y distinguir diferencias de tamaño o color de las tabletas, diferencias en el empaque, forma diferente de los envases, color de cajas diferentes, pero sobre todo, adquiriendo sus productos en lugares adecuadamente establecidos y autorizados para ello y no en el comercio informal. La CANIFARMA ha desarrollado una importante campaña de comunicación para el público en general, que pretende generar esta conciencia en la población sobre los riesgos para la salud que representan los medicamentos falsificados, a través de las redes sociales de CANIFARMA y las empresas afiliadas a esta; la información es publica y está en las páginas oficiales de la CANIFARMA y en el SINGREM (Sistema Nacional de Gestión de Reciduos en Bases de Medicamentos), *www.canifarma.org.mx* y: *www.singrem.org.mx*

SEA: ¿Hay alguna tecnología o método innovador que se esté utilizando para prevenir la falsificación de medicamentos?

GC: como lo comentamos, en realidad se están haciendo esfuerzos internacionales por parte de la industria farmacéutica para evitar y detectar las falsificaciones de medicinas, sin embargo, los falsificadores son hábiles para lograr su propósito de engañar a los pacientes. La capacitación de autoridades y la información a la población sobre la falsificación de medicamentos, son las mejores herramientas.

Hubo un caso donde encontramos tabletas contra el cáncer que resultaron ser lentejas capeadas con cemento blanco, en otro caso, un jarabe infantil contra la tos que sólo eran frascos llenados con agua de la llave más colorantes y saborizantes sin ninguna sustancia activa contra la enfermedad.

Los medicamentos más falsificados en México son aquellos para tratar la disfunción eréctil y el cáncer, también los antibióticos, analgésicos, antigripales, antitusivos y algunos dispositivos médicos de uso común como las venoclisis

En otra ocasión, descubrimos que los falsificadores compraron un lote de antibiótico genérico y lo metieron en un empaque falso del mismo producto, pero de una presentación idéntica de mayor precio para obtener ganancias, hasta aquí parecería que tuvieron cierta consideración, pero los falsificadores admitieron que para poder quitar la etiqueta de origen de las ámpulas, las sumergieron en agua hirviendo, desconfigurando los efectos del producto.

SEA: ¿Qué se hace en caso de tener sospechas de falsificación sobre un medicamento, pensando en el usuario?

GC: primero, no ingerirlo, todos los medicamentos tienen una leyenda para que en caso de sospecha de falsificación o eventos adversos los pacientes puedan notificar a la Cofepris a través de un correo electrónico y/o números telefónicos. El paciente también puede llamar al laboratorio fabricante donde existe un área de farmacovigilancia que los ayudará, los orientará y dará seguimiento al caso. ■

Referencias:

1 Colección de estudios sectoriales y regionales "Conociendo la industria farmacéutica". Instituto Nacional de Estadística y Geografía (INEGI), 2022. https://www.canifarma.org.mx/uploads/descargables/inegi.pdf

2 "Las farmacéuticas en México prevén crecimiento de 36% en medio de las crisis". EFE/José Méndez- CONCANACO. 04/08/2022 https://www.concanaco.com.mx/prensa/tepuedeinteresar/las-farmaceuticas-en-mexico-preven-crecimiento-de-36-en-medio-de-las-crisis

Foto: - Freepik

Gerardo Corchado Chávez es egresado de la Licenciatura en Comunicación y Periodismo en la Escuela Carlos Septién. Fue subdelegado de la Policía Judicial Federal, director de Inteligencia en la Procuraduría del Distrito Federal (ahora Ciudad de México), y durante 20 años fue director de Seguridad Corporativa de Novartis Farmacéutica. Es CPP (Certified Protection Professional), CFE (Examinador Profesional de Fraude); también fue docente en la Escuela de Periodismo Carlos Septién. Actualmente es consejero de la Comisión de Seguridad de la Cámara Nacional de la Industria Farmacéutica (CANIFARMA), y ex-coordinador del Comité de Seguridad de la Cámara de Comercio Suizo-Mexicana.


Foto: - Freepik

BULLYING, DISCRIMINACIÓN Y TIROTEOS: LOS NUEVOS RETOS EN LOS CENTROS EDUCATIVOS

En México, siete de cada diez niños, niñas y adolescentes sufren algún tipo de acoso diariamente, colocando a México en el primer lugar a nivel mundial con el mayor número de casos de *bullying* y *ciberbullying* principalmente en las escuelas

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Tras dos años de suspensión de clases presenciales, distintos fenómenos se han ido presentando con la reapertura de los centros educativos, desde el nivel básico en donde los niños no tienen o perdieron la práctica de socializar, hasta la universidad en donde existe un atraso de conocimientos. Los retos sociales y cognitivos no son los únicos a los que se enfrenta este sector, pareciera que ahora existe una nueva pandemia y es la del *bullying* y el *ciberbullying* que trasciende de las aulas a la vida digital de los y las alumnas, de docentes y personal.

En el mundo, seis de cada diez niños, niñas y adolescentes diariamente sufren de algún tipo de acoso y ciberacoso, de acuerdo al estudio oficial de la organización no gubernamental internacional *Bullying* Sin Fronteras para América, Europa, Asia, Oceanía y África, en el periodo de enero de 2021 a febrero de 2022.

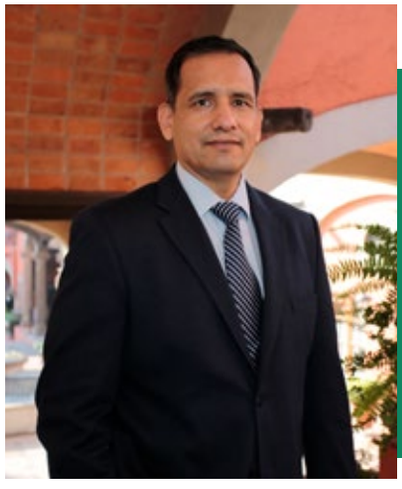
La misma organización, pero para América Latina y España, informó que en México siete de cada diez niños, niñas y adolescentes sufren acoso, presentando en ese mismo periodo 180 mil casos graves de *bullying* colocando a México como el primer lugar a nivel mundial con tipo de violencia. Las escuelas son el primer lugar donde se presentan estos hechos, seguidos de las redes sociales e Internet.


Foto: - Freepik

Para los responsables de la seguridad de los centros educativos, actualmente y tras dos años de cambios en la vida de las personas, regresar a las aulas implicó nuevos retos a enfrentar y riesgos por mitigar. Además de buscar estrategias para adaptarse a los cambios sociales y personales del alumnado, ejemplo la inclusión y respeto hacia la comunidad LGBTIQ+ (lesbiana, *gay*, bisexual, transgénero, transexual, travesti, intersexual y *queer*), o del género no binario; sin dejar de lado los riesgos de violencia, robo, y tiroteos.

Éste último, se ha agravado en Estados Unidos, de enero a marzo del presente año se tenían reportados más de 130 tiroteos, incluyendo el ataque en una escuela de Nashville, Tennessee, donde murieron tres niños y tres adultos. Lo más valioso para una persona se encuentra dentro de una escuela, vulnerables y a la vez con la oportunidad de prevenir si se cuenta con la persona indicada para proteger su vida e integridad.

En esta ocasión, **Seguridad en América** entrevistó a diferentes expertos en la materia para conocer los actuales problemas de seguridad en los centros educativos y algunas estrategias para mitigarlos.



"Nuestra misión es habilitar un entorno seguro para estudiantes y empleados, propiciando un ambiente de respeto y confianza", **Antonio Rafael Bellorín Useche**

"Uno de los principales retos que tenemos en los centros educativos es la evolución de principios de inclusión, diversidad, la posibilidad de la existencia de un tirador activo, y los sistemas de reporteo interno", **Francisco Javier de Lago**

PRINCIPALES RETOS DE SEGURIDAD

El cambio es una constante en la naturaleza y la vida de las personas, en un mundo altamente tecnológico, digital, la inmediatez es parte de la actualidad. En los centros educativos, se presentan todos estos cambios: de aprendizaje, tecnología, pensamiento, ideologías, modas, pero sobre todo y lo más importante, de crecimiento. Los docentes, los administrativos, todo el personal que integra estas instituciones crece junto al alumnado, y va modificando y adaptándose a los cambios que hay en su vida personal, social y digital.

"Uno de los principales retos que tenemos en los centros educativos es la evolución de principios de inclusión, diversidad, la posibilidad de la existencia de un tirador activo, y los sistemas de reporteo interno, es decir que si ve algo, que diga algo", señaló Francisco Javier de Lago Acosta, director general de Galeam Security Services y co-fundador de Timur Latinoamérica.

El experto recomendó entender primero qué es la inclusión y el respeto que debe existir, y por consiguiente capacitar sobre este tema a todo el personal del centro educativo, para generar un entorno seguro y respetuoso, aceptar el cambio y sobre todo el generar esa consciencia tanto en las generaciones pasadas como en las actuales.

Poco a poco tanto las leyes como las normas se están adaptando a la inclusión, los centros escolares no pueden quedar fuera y conociendo los índices de violencia y acoso actuales, el personal de seguridad debe estar capacitado para lograr ese ambiente respetuoso e incluyente.

Sobre este tema también comentó de forma resumida los cinco aspectos que no pueden faltar para la seguridad de un centro educativo:

1. Control de accesos. ¿Quién entra? ¿Quién sale?
2. ¿Qué entra? ¿Qué sale?
3. Respeto entre la comunidad estudiantil.
4. Comunicación, si veo algo, oigo algo, digo algo.
5. Capacidad de reacción ante una situación de riesgo.

ACOSO Y CIBERACOSO

La cifra a nivel mundial del acoso escolar y ciberacoso es alarmante, tomando como referencia un dato más local, el Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México, reportó que el acoso escolar creció en un 347 por ciento en el periodo enero-febrero de 2023, en comparación con el mismo periodo del año anterior.

Casos tan trágicos han sucedido dentro de las escuelas a causa de esta mala práctica. El 13 de marzo del presente año, murió una alumna de la Secundaria Oficial 0518 Anexa a la Normal, ubicada en San Juan Teotihuacán, debido a un traumatismo craneoencefálico provocado por los golpes que otra alumna le propició 15 días atrás; por lo que el *bullying*, el acoso sexual y virtual deben prevenirse y atenderse con severidad.

"Nuestra universidad cuenta con una normativa, instancias y procedimientos que velan por la Sana Convivencia Universitaria, a saber: un Reglamento de Sana Convivencia y Disciplina, una Defensoría de Derechos Universitarios, y una Comisión Consultiva y Disciplinaria", explicó Leonardo Iván Reyes Guerrero, gerente de Operación Campus Sur de la Universidad Anáhuac.

Por su parte, Adolfo Guadalupe Quintero Herrera, coordinador y asesor de Seguridad Escolar en UDLAP, platicó que cuando son detectados o reportados los casos de acoso, es el área de disciplina académica quienes toman las medidas de seguimiento o correctivas para ello. Seguridad, en estos casos sirve como apoyo, monitoreo, resguardo de evidencias o si llegara el caso de que dichas acciones rebasaran a los mencionados, es que, actúan de manera conciliatoria.

"La seguridad de los integrantes de la Comunidad Universitaria no es algo que pueda negociarse o algo que pueda ser minimizado por otros aspectos. La integridad física de una persona es prioritaria y se debe invertir todo lo que sea necesario para que el riesgo esté lo más controlado posible", **Luis Constantino Chacón**

"Nuestra universidad cuenta con una normativa, instancias y procedimientos que velan por la Sana Convivencia Universitaria",
Leonardo Iván Reyes Guerrero

MEDIDAS DE SEGURIDAD

Ante estos actuales retos de seguridad, los especialistas en el tema van modificando y adaptando las estrategias para contrarrestarlos. Milton A. Rodríguez Torres, jefe de Seguridad en la Universidad La Salle, compartió algunas medidas de seguridad que La Salle implementa para proteger a los estudiantes y personal de los centros educativos:

Fortalecimos nuestro programa permanente de Universidad Segura con las siguientes acciones:

- Instalamos arcos detectores de metal con videovigilancia digital, integrada a nuestro centro de monitoreo.
- Se agilizó nuestro sistema de credencialización de alumnos y colaboradores de nuevo ingreso, obteniendo tiempos de respuesta más cortos para entrega de credenciales al inicio de cada semestre y/o nueva contratación de colaboradores.
- Capacitación constante y permanente del personal operativo de vigilancia en materia de prevención del delito, evacuación y primeros auxilios.
- Capacitación constante y permanente de nuestros brigadistas sumándose a esta labor alumnos y colaboradores.
- Estrechamos la coordinación con la Secretaría de Seguridad Ciudadana y otras autoridades para efectos de una atención y respuesta a incidencias en las inmediaciones de las instalaciones.
- Mediante el programa Sendero Seguro, se mejora el alumbrado público y la instalación de más botones de emergencia en la vía pública.
- A lo largo de cada año llevamos a cabo simulacros con diferentes hipótesis y escenarios.

Foto: Freepik

Mientras que Miguel Ángel Martínez Ruíz, jefe de Protección Civil y Salud Ocupacional Regional en la Universidad Panamericana, comentó que ellos cuentan con un sistema de credencialización ligado a torniquetes en los accesos de los predios para evitar el acceso de personas ajenas a la universidad sin su debida acreditación y registro. Además se llevan a cabo rondines por todos los predios para detectar actos y condiciones inseguras y corregirlas para evitar cualquier tipo de incidente o accidente.

La Universidad Panamericana cuenta con sistema de videovigilancia en todos los predios de la universidad, con una cobertura en todas las instalaciones, accesos y las calles aledañas, y se tienen contratados los servicios de la Policía Bancaria e Industrial y una patrulla interna, para la custodia de las calles aledañas a la universidad, además de la implementación del Sendero Seguro con el Sector Nápoles para el apoyo en todo el perímetro de influencia por parte de Policías de Proximidad, entre otras efectivas estrategias.

En el caso del Tecnológico de Monterrey, se cuenta con una infraestructura de seguridad para la prevención de riesgos y amenazas externas, tales como barreras perimétricas, iluminación exterior e interior y puntos de atención ante emergencias, y se emplean sistemas y tecnologías de seguridad para la oportuna y efectiva detección, reacción y respuesta ante incidentes de seguridad. Incluyendo sistemas electrónicos de control de acceso, videovigilancia, sistemas de alarmas contra intrusos, sistemas de detección y supresión de incendios, GPS, entre otros.

"Estrechamos la coordinación con la Secretaría de Seguridad Ciudadana y otras autoridades para efectos de una atención y respuesta a incidencias en las inmediaciones de las instalaciones",
Milton Rodríguez Torres

"Nuestra misión es habilitar un entorno seguro para estudiantes y empleados, propiciando un ambiente de respeto y confianza para la comunidad del Tec. Para lograr nuestra misión desarrollamos procesos de prevención y respuesta que nos permiten mitigar los riesgos y amenazas que podrían afectarnos, siempre alineados a nuestro código de ética y al ambiente regulatorio de las universidades", comentó Antonio Rafael Bellorín Useche, *Chief Security Officer* del Sistema del Tecnológico de Monterrey.

Adolfo Quintero compartió cinco tips de seguridad ante un atentado dentro del centro escolar (tiroteo, terrorismo):

1. Tener en cuenta que nos puede suceder.
2. Contar con los recursos humanos y materiales para poder contener, resguardar a los miembros de la comunidad o huir de la amenaza.
3. Tener elaborados y practicados planes de actuación, protocolos y procedimientos.
4. Estar capacitados y preparados para ese momento. "Prepararnos en la paz, para cuando llegue la guerra".
5. Conocer de más a todos y cada uno de los miembros de la comunidad para ubicar perfiles y posibles blancos

PERÍMETRO SEGURO

Como hemos visto, los centros educativos forman alianzas con las autoridades y crean una sinergia para la protección del alumnado al exterior de las instalaciones escolares, Sendero Seguro es un programa de seguridad implementado por algunos gobiernos locales para la protección de alumnos y alumnas, y mujeres principalmente, que requiere de trabajo en conjunto.

"Nosotros estamos en constante comunicación con las autoridades de la Alcaldía Álvaro Obregón, aunado a esto, participamos en el programa 'Sendero Seguro AOB', mismo que cuenta con un grupo de WhatsApp, donde podemos solicitar apoyo cada vez que se requiere, además, contamos con el número telefónico de los Jefes de Sector de la Secretaría de Protección Ciudadana", expresó Luis Constantino Chacón, director de Seguridad en la Universidad Iberoamericana.

También Carlos Irecta Lecona, líder de Gestión de Riesgos en Seguridad del ITESM Campus Puebla, recomendó tener este contacto cercano con las autoridades. "En nuestra experiencia es importante tener esta línea de comunicación directa con las autoridades a los diferentes niveles, actualmente invitamos a la policía en su área de prevención del delito a visitar y dar ponencias continuas en temas de violencia familiar, feminicidios, prevención del delito, etc., y contamos con un chat que nos permite tener una respuesta inmediata".

"En la Universidad Panamericana contamos con un Programa Interno de Protección Civil para cada uno de los predios de la universidad, con un protocolo específico para cada tipo de emergencias", **Miguel Ángel Martínez**

"Ante un tiroteo, hay que estar capacitados y preparados para ese momento. 'Prepararnos en la paz, para cuando llegue la guerra'", **Adolfo Quintero Herrera**

Ahora bien, existen ciertas estrategias y herramientas tecnológicas para complementar la seguridad externa al plantel. "Lo que nosotros recomendamos son rondines continuos por toda la parte exterior de la instalación y detectar situaciones que se pueden convertir en riesgos, por ejemplo, tener tiros de cámara desde las propias instalaciones hacia las zonas críticas como paradas de autobús, puentes peatonales, al transporte público, los accesos vehiculares, peatonales, monitoreado en tiempo real. Y de preferencia coordinar todo esto con seguridad pública", recomendó Francisco de Lago.

Sobre este tema, Carlos Irecta Lecona sugirió el sistema de patrullaje con unidades caninas, ya que consideró que es un elemento de disuasión para el perímetro, así como la presencia periódica de unidades de seguridad pública. "Referente al perímetro debemos estar conscientes de no usurpar funciones, se recomienda realizar sobre vigilancia con sistema de videovigilancia, para reportar a la autoridad cualquier condición de riesgo que se identifique en el perímetro mientras sea visible", recalcó.

Y precisamente coincidió con las estrategias que se aplican en la Universidad Iberoamericana. "En lo que respecta al exterior del campus, contamos con el servicio de una patrulla que nos provee la compañía de seguridad privada, misma que realiza rondines aleatorios por todo el perímetro de las instalaciones, de igual manera, contamos con el apoyo de la Secretaría de Seguridad y Protección Ciudadana, quienes nos visitan diariamente y también hacen recorridos en la periferia. En nuestro caso particular, el campus es una 'isla', ya que está rodeado por calles, pero lo recomendable es hacer recorridos externos por lo menos dos cuadras a la redonda de las instalaciones", comentó Luis Constantino Chacón.

SELECCIÓN Y CAPACITACIÓN

Cada generación es distinta debido al contexto social y la educación que recibe en casa, las redes de comunicación y tecnológicas que le han tocado, etc. Tratar con alumnos, es tratar con sus padres, con las instituciones que regulan la educación y a las escuelas, con los problemas sociales y humanos que cada uno presenta, es por eso que no es tan sencillo ser la autoridad, la seguridad de un centro escolar, de ahí la importancia de la selección del personal adecuado.

"Nuestra área de capital humano se encarga de hacer una selección concienzuda de los candidatos con base en nuestro perfil para colaboradores de vigilancia. Se realizan pruebas psicométricas como parte del proceso de selección. Posteriormente se realiza una entrevista al candidato con base en un cuestionario de entrada para el personal de vigilancia. Si los resultados de las pruebas y la entrevista son satisfactorios se hace un estudio socioeconómico y posteriormente se hace la contratación", comentó Milton Rodríguez.

Y recalcó que el entrenamiento de los colaboradores de vigilancia, siempre es basado sus manuales de operaciones y procedimientos de vigilancia adaptados a cada unidad según sea el caso, y también se incluye capacitación en prevención de delito, prevención y combate de incendios, evacuación y primeros auxilios.

"La selección y entrenamiento del personal de seguridad es una actividad clave para alcanzar niveles de servicio, calidad y respuesta ante los riesgos de seguridad que enfrenta nuestra institución", señaló Antonio Rafel Bellorín.

RIESGOS NATURALES

Además de los riesgos antes mencionados, no se puede dejar de fuera los riesgos naturales, un claro ejemplo es el terremoto de 2017, en donde escuelas como el Colegio Enrique Rébsamen, ubicado en la Alcaldía de Tlalpan (Ciudad de México), sufrió grandes daños y pérdidas de vidas humanas. Ante esta situación, los expertos recomendaron realizar simulacros continuos y que el alumnado ubique los puntos de reunión seguros.

"Referente al perímetro debemos estar conscientes de no usurpar funciones, se recomienda realizar sobre vigilancia con sistema de CCTV para reportar a la autoridad cualquier condición de riesgo",
Carlos Irecta Lecona

"En la Universidad Panamericana contamos con un Programa Interno de Protección Civil para cada uno de los predios de la universidad, con un protocolo específico para cada tipo de emergencias; en el caso de sismos el protocolo que se sigue es el siguiente: si se escucha la alerta sísmica y se encuentra de una planta baja hasta un primer nivel se debe aplicar el protocolo de evacuación hacia los puntos de reunión previamente establecidos por cada inmueble, siguiendo las indicaciones de la Brigada Interna y la Brigada Estudiantil.

Si se escucha la alerta sísmica y se encuentra en un segundo nivel hacia arriba, se debe practicar el repliegue en las zonas de menor riesgo debidamente identificadas y señalizadas en cada edificio hasta que concluya el movimiento sísmico, una vez concluido el personal de la brigada les indicará si es posible llevar a cabo la evacuación hacia los puntos de reunión preestablecidos.

Si se percibe un movimiento sísmico antes de escuchar el alertamiento, se debe seguir el mismo protocolo, siempre que las condiciones permitan la evacuación, de lo contrario todos deberán practicar el repliegue hasta que concluya el movimiento sísmico. En el punto de reunión se debe guardar silencio y esperar las indicaciones de la brigada.

Foto: - Freepik

TRUSTGROUP MR

En Seguridad, “Nadie Conoce México Como Nosotros”.

- Protección Ejecutiva.
- Seguridad Física.
- Seguridad Logística.
- Traslado de Valores.
- Capacitación y Entrenamiento.
- Administración de Crisis.
- Estudios de Integridad.
- Proyectos Integrales de Seguridad.

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

www.trustgroup.com.mx

Más de quince años brindando servicios profesionales de seguridad

ASIS CAPÍTULO MÉXICO 217

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

El personal de la Jefatura de Protección Civil en coordinación con Seguridad y Mantenimiento realizarán la evaluación rápida de los inmuebles para determinar si es posible regresar a las instalaciones, o si se encuentran probables daños estructurales, en cuyo caso se informará al coordinador general para que ordene la evacuación de las instalaciones y se programe una revisión técnica por parte de un corresponsable de seguridad estructural. Si las condiciones lo permiten, el coordinador general con el apoyo de la Brigada Interna y Estudiantil, ordenará el regreso a las instalaciones", compartió Miguel Ángel Martínez.

HERRAMIENTAS TECNOLÓGICAS

La tecnología es sin duda un aliado para la seguridad. Leonardo Iván Reyes sugirió contar con sistemas automatizados de control de acceso y mecanismos de validación que permitan restringir el acceso a personas no autorizadas. Mientras que Carlos Irecta Lecona lo complementa con algún sistema de alertamiento, tanto de detección como de voceo, y también el apoyo de videovigilancia acompañado de un monitoreo permanente.

"Debemos contar con credenciales sin contacto, sistemas robustos de CCTV, alarma contra incendio, alarma sísmica, detectores de humo, sistemas automatizados contra incendios, cercas electrificadas, y sensores de movimiento", agregó Luis Constantino Chacón.

Y Antonio Bellorín expuso cinco tips de seguridad para el control de acceso en un centro educativo:

1. Implementar un sistema de identificación y autenticación: utilizar tarjetas de identificación o credenciales digitales con tecnología de proximidad para que los estudiantes y empleados puedan acceder a las instalaciones. Estos sistemas de identificación pueden ser asociados con códigos PIN o contraseñas para asegurar una autenticación adicional.

2. Establece zonas de acceso restringido: definir áreas específicas en el campus que requieran una autorización especial para acceder. Esto puede incluir laboratorios, áreas administrativas o salas de almacenamiento de datos sensibles. Colocar puertas con cerraduras o sistemas de acceso controlado para limitar el ingreso a estas zonas solo a las personas autorizadas.

3. Activar un módulo de control de visitantes al Sistema de Control de Acceso y al Sistema de Videovigilancia: instalar cámaras de seguridad y sistemas de registro de visitantes en puntos clave del campus. Esto permitirá un monitoreo constante y un registro de quién accede a las instalaciones en determinados momentos. Estos registros pueden ser valiosos para investigaciones de seguridad o para rastrear incidentes.

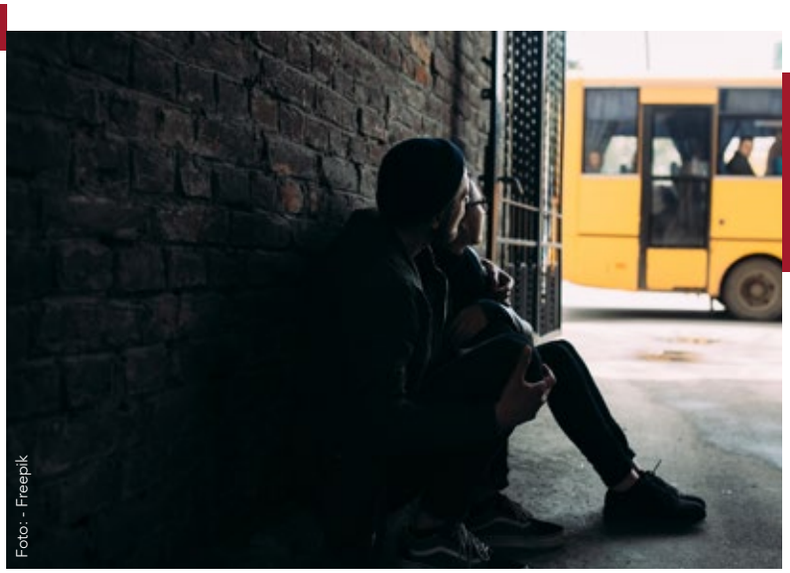


Foto: - Freepik

4. Capacitar al personal de seguridad: brindar capacitación adecuada al personal de seguridad encargado del control de acceso. Esto incluye instruirlos sobre cómo manejar situaciones de emergencia, identificar intentos de acceso no autorizados y cómo responder a ellos de manera efectiva y segura. Además, asegurarse de que el personal esté actualizado sobre los protocolos de seguridad y las políticas vigentes.

5. Realizar auditorías de seguridad periódicas y pruebas de vulnerabilidad: llevar a cabo auditorías periódicas para evaluar la efectividad de tus medidas de control de acceso. Esto puede incluir revisar la configuración de los sistemas de acceso, identificar y solucionar posibles vulnerabilidades, y evaluar el cumplimiento de las políticas de seguridad por parte del personal y los estudiantes.

Francisco de Lago concluyó en la importancia de analizar a los alumnos, la comunicación entre maestros y los sistemas de reporteo anónimo, aquellas situaciones alarmantes, extrañas que han visto y que deben notificar. Para esto actualmente se debe agregar el monitoreo constante de redes sociales y dar aviso sobre alguna publicación sospechosa. ■

Referencias:

- "Bullying en México alcanza la mayor cifra de casos a nivel mundial", El Financiero, mayo 02 de 2023. https://www.elfinanciero.com.mx/nacional/2023/05/02/bullying-en-mexico-alcanza-la-mayor-cifra-de-casos-a-nivel-mundial/

- "Reportan aumento de bullying en CDMX durante 2023", Milenio, 08 de abril de 2023. https://www.milenio.com/politica/comunidad/durante-2023-aumento-bullying-en-cdmx

Fotos: Mónica Ramos / SEA

SISSA Monitoring Integral

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

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

SOLUCIONES ESTRATÉGICAS

RE & MI
S.A. DE C.V.

SEGURIDAD PRIVADA

AFAC
AGENCIA FEDERAL DE AVIACIÓN CIVIL

Acreditación Técnica AVSEC

"Nuestro **Reto** y **Misión** es su **Seguridad**"

- **Guardias Intramuros.**

Guardias de seguridad
con experiencia y capacitación.

- **Guardias Especializados en AVSEC.**

Guardias expertos en seguridad de la aviación.
Analistas de Rastreo Satelital.

- **Guardias Especialistas en Casinos.**

- **Monitoristas de CCTV.**

Más Información
55-4178-6695

s.badilloaguilar@seremi.com.mx
www.seremi.com.mx

SEGURIDAD EN TELECOMUNICACIONES Y RADIODIFUSIÓN

Un entendimiento de los retos y las soluciones de estos sectores indispensables para el desarrollo del país

Foto: - Freepik

MÉXICO

Antonio Venegas / *Staff* Seguridad en América

La seguridad es un área en constante evolución, el cambio está presente en todo lo que vivimos y este sector no puede quedarse atrás, la innovación tecnológica se desarrolla cada día generando que el ser humano tenga que adaptarse constantemente a estos cambios, los cuales han traído consigo distintas ventajas al manejo de los sectores, específicamente con la seguridad privada, pero también como todo incluyen diferentes retos en su uso. Al escuchar la palabra "retos" tenemos la percepción de que se trata de algo difícil, algo que puede presentar complicaciones difíciles de superar, pero no hay que ver estos aspectos como amenazas, sino como áreas de oportunidad que puedan traernos una mejora continua en el desarrollo de las operaciones que realicemos.

Es por ello que **Seguridad en América** tuvo una charla con Wilfrido Robledo Luna, responsable de la Dirección de Información Estratégica de Grupo Imagen Multimedia, además dirige las áreas de Inteligencia, Seguridad Patrimonial, Protección Civil, Seguridad y Salud en el Trabajo en dicha empresa, que es una de las principales compañías de medios de comunicación en México, ya que cuenta con un canal de televisión nacional, una red de estaciones de radio y uno de los principales periódicos en el país: Excélsior, todo esto soportado por una gran estructura multimedia a través de Imagen Digital.

Wilfrido explicó que el concepto de telecomunicaciones no es igual al de medios de comunicación. Citando fuentes, describió a las telecomunicaciones como toda emisión, transmisión, o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.

En esta rama se encuentran los servicios como la telefonía, el Internet o sistemas de televisión por cable. Por otro lado, la radiodifusión se puede definir como la propagación de ondas electromagnéticas de señales de audio o de audio y video asociado, haciendo uso, aprovechamiento o explotación de las bandas de frecuencia del espectro radioeléctrico, incluidas las asociadas a recursos orbitales, por ejemplo, la radio y la televisión abierta, aquellos donde no hay un intermediado entre el generador de estas señales con el usuario.

"Las telecomunicaciones como toda emisión, transmisión, o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión"

"Los riesgos pueden provenir de fenómenos naturales; actividades delictivas; eventos químicos y sanitarios; sociales y del entorno internacional"

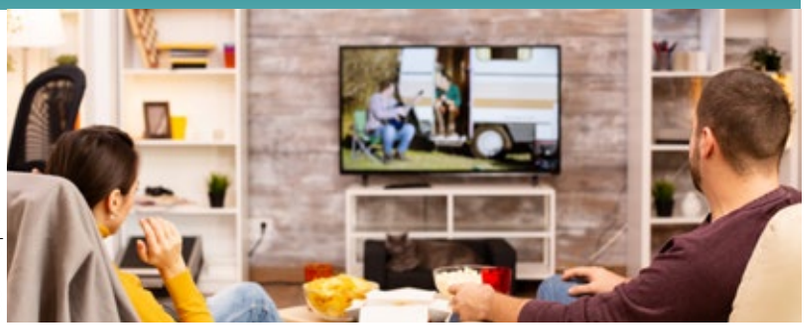


Foto: - Freepik

En cuanto a los componentes de las telecomunicaciones y radiodifusión, normalmente en casi todos los casos, se trata de sistemas dotados de un emisor que codifica y transmite la señal mediante distintos medios o canales; un medio por el que transitan pulsos o radiación electromagnética; el receptor, que es quien recibe la señal y, por último, un protocolo, que permite y regula el envío de la información entre dos entidades. En México, el ecosistema de las TyR está conformado por tres partes: un proveedor, el operador regulador, en este caso es el Instituto Federal de Telecomunicaciones, y los usuarios.

IMPORTANCIA DEL SECTOR DE LAS TELECOMUNICACIONES EN MÉXICO

Sobre la importancia del sector de las telecomunicaciones en México, Wilfrido presentó datos duros respecto a su impacto.

En México, el PIB (Producto Interno Bruto) de este sector representan 18 mil 314 de millones de pesos, lo que se traduce en una contribución de 3.4% al PIB nacional; se encuentran empleadas más de 300 mil personas y los ingresos del sector superan los 500 mil millones de pesos, de los cuales, los proveedores invierten más de 100 mil millones de pesos. En cuanto a servicios de telecomunicaciones, mencionó que se cuenta con 90 líneas de servicio móvil de Internet y 103 de servicio móvil de telefonía por cada 100 habitantes; 70 accesos de servicio fijo de Internet y 71 de televisión restringida por cada 100 hogares y 73 líneas de servicio de telefonía fija por cada 100 habitantes.

BENEFICIOS

Hoy en día, este sector nos permite acceder y consultar páginas de Internet, contenidos diversos, redes sociales, noticias nacionales e internacionales; transmitir y recibir signos, señales y datos o lo que es lo mismo, correo electrónico, mensajes de texto, fotografías, video, música, llamadas, canales de televisión gratuitos o de paga, estaciones de radio, imágenes, entre otros; y también emitir señales de televisión y radio.

Wilfrido cuestionó sobre cómo hubiéramos experimentado la pandemia por COVID-19 sin las telecomunicaciones y la radiodifusión, argumentando que, en México, ante la necesidad de continuar con los asuntos de la vida cotidiana, se recurrió a los medios electrónicos para reuniones, clases, cursos, entrevistas o simples pláticas; asimismo el Gobierno, a través de la Secretaría de Educación Pública, también recurrió al uso de canales de televisión para transmitir contenido educativo a distancia para poder llegar a todas las personas que no podían tener un sistema de educación virtual, por lo que se utilizó la televisión para poder llenar ese vacío.

INSTALACIONES ESTRATÉGICAS

Para dar contexto de la importancia de este sector, Wilfrido explicó cuál es el marco, en términos de seguridad, para incluir a las telecomunicaciones y radiodifusión en México como infraestructura estratégica. La Constitución Política de México define las áreas estratégicas, entre éstas, a las comunicaciones satelitales y las vías generales de comunicación; por otro lado, en la Ley General de Telecomunicaciones y Radiodifusión se establece como vías generales de comunicación al espectro radioeléctrico, las redes públicas de telecomunicaciones, las estaciones de radiodifusión y equipos complementarios, así como los sistemas de satélite.

Por otra parte, la Ley de Seguridad Nacional faculta al Secretario Técnico del Consejo de Seguridad Nacional para realizar el inventario de la infraestructura estratégica del país; finalmente en la Ley General del Sistema Nacional de Seguridad Pública, en la que define como instalación estratégica a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional y establece la responsabilidad de la Federación, las entidades federativas y los municipios en la protección y vigilancia de las instalaciones estratégicas, así como la constitución del Grupo de Coordinación para Instalaciones Estratégicas.

RETOS DE LOS SECTORES DE TYR

Entre los principales retos de la industria de las telecomunicaciones y radiodifusión se encuentran: es un sector altamente complejo y diverso; las zonas inhóspitas y la dispersión de infraestructura en todo el territorio nacional; es infraestructura crítica de la cual dependen otras, así como el resto de las actividades económicas; la presencia de la delincuencia organizada en las zonas de operación; los altos tiempos de respuesta institucional en algunos puntos del país; baja incidencia delictiva en el sector de radiodifusión, pero con alto impacto operacional, económico y reputacional; la complejidad para operar un sistema de seguridad integral y una mayor coordinación en el sector. Wilfrido explica que la radiodifusión depende de la infraestructura de las telecomunicaciones.

En este contexto, uno de los modelos que Wilfrido y su equipo han instrumentado es el Ciclo ESRM, Enterprise Security Risk Managment, que promueve ASIS Internacional, mediante el cual buscan identificar y priorizar los activos, a través de la criticidad de estos.

Foto: - Freepik

"En el caso de actividades delictivas, las empresas de este sector son vulnerables a ciberdelitos, robo, secuestro, amenazas, extorsión, cobro de piso, sabotaje, invasión, terrorismo, uso indebido de infraestructura, vandalismo e intervención de comunicaciones, entre otros"

Es en esta parte donde se valoran los activos para poder establecer la estrategia correspondiente, y para eso buscan ver cuánto les cuesta el activo, cuánto les cuesta reemplazarlo, el impacto operacional, el daño que puede generar si uno de estos activos es vulnerado, el tiempo de recuperación de un activo y finalmente la parte reputacional.

Posterior a esto, se trabaja en identificar y priorizar los riesgos, así como establecer el tratamiento de riesgos donde se hacen distintas propuestas para la mitigación. Es importante señalar que se busca la forma de operar con el menor riesgo, no obstante, hay que recordar que el riesgo es inherente a la operación. Finalmente, se trabaja bajo un esquema de mejora continua.

RIESGOS

Sobre los principales riesgos a los que el sector de las telecomunicaciones y radiodifusión se encuentra expuesto, Wilfrido mencionó que estos pueden provenir de fenómenos naturales; actividades delictivas; eventos químicos y sanitarios; sociales y del entorno internacional. Sobre los riesgos de fenómenos naturales, destacó que, dependiendo de la zona geográfica en México, se debe contemplar una estrategia ante sismos, tsunamis, volcanes, inestabilidad de laderas, flujos de lodo y escombros, hundimientos, agrietamientos del terreno, ciclones, nevadas, inundaciones, sequías o tormentas severas. En el caso de actividades delictivas, las empresas de este sector son vulnerables a ciberdelitos, robo, secuestro, amenazas, extorsión, cobro de piso, sabotaje, invasión, terrorismo, uso indebido de infraestructura, vandalismo e intervención de comunicaciones, entre otros.

Foto: - Freepik

"Hoy, considero que en la industria de telecomunicaciones y radiodifusión, el ciberdelito es nuestra principal amenaza, el efecto de esto tendría una afectación importante en los sectores financieros y económicos. Cada vez se incrementan más los ataques a esta industria", mencionó. También están los riesgos químicos y sanitarios como los incendios, accidentes, derrame de combustible, epidemias o pandemias, y, por otro lado, los riesgos sociales como el bloqueo y toma de instalaciones, manifestaciones, rechazo a instalaciones del sector, cambios regulatorios y falta de fuerza laboral. Finalmente hay que destacar el entorno internacional, el ambiente de incertidumbre global, las cadenas de suministro fracturadas, conflictos políticos internacionales, situaciones como la pandemia por COVID-19, migraciones y otras afectaciones de carácter global que pueden perjudicar al sector.

Antes de concluir, Wilfrido propuso un Sistema Integral de Continuidad del Negocio para recuperar el servicio esencial lo antes posible, el cual debe incluir el plan de Seguridad, planes de Emergencia, de Continuidad de la Operación y de Gestión de Crisis, donde se incluyan a las personas, los procesos y los activos de la empresa con el objetivo de tener un sistema unificado y evitar la dispersión en las estrategias, implementando la inteligencia en todos los procesos así como el trabajo de todas las áreas para reducir el tiempo de recuperación en caso de una afectación.

"Hoy esta implementación es fundamental, con la inteligencia podremos anticiparnos, reducir la incertidumbre que nuestro contexto tanto interno como externo nos puede generar y podemos generar escenarios para que nuestros planes o nuestra continuidad de negocio no se vea afectada. Todos vamos a estar expuestos a amenazas, lo importante en todo esto es la prevención, y en su momento, recuperar el servicio esencial lo antes posible con la menor afectación, una inteligencia que no sirve para tomar decisiones no es inteligencia, se queda en información", expresó.

Conociendo esto, podemos comprender que las telecomunicaciones, así como la radiodifusión son industrias esenciales con un impacto en todas las actividades que desempeñamos, se encuentran arraigadas en la sociedad en general como en las empresas; vulnerar estos sectores representa varias pérdidas en sectores económicos que pueden escalar niveles nacionales o internacionales, pero manejando buenas estrategias de recuperación se puede prevenir o reaccionar de manera adecuada, trabajando en equipo con los cuatro planes previamente mencionados se puede otorgar la información necesaria a las personas responsables para, de esta manera, disminuir el tiempo de recuperación, siempre usando la inteligencia en las soluciones. ■

Wilfrido Robledo Luna,
responsable de la Dirección de Información Estratégica de Grupo Imagen Multimedia

MAK MR
EXTINGUISHER

SISTEMA HÍBRIDO DE EXTINCIÓN DE INCENDIOS VICTAULIC VORTEX™ 1500

SE PUEDE APLICAR EN LA SUPRESIÓN DE INCENDIOS POR INUNDACIÓN TOTAL PARA ESPACIOS DE MÁQUINAS INDUSTRIALES COMO:

- Plantas de generación de energía
- Recintos de turbinas
- Fabricación de automóviles
- Fundición de acero
- Almacenamiento de líquidos inflamables
- Centros de datos
- Museos
- Bibliotecas
- Instalaciones mineras

55 57-36-92-19

makseguridad.com

ERIK ERIKSON

Y EL DESARROLLO PSICOSOCIAL DEFICIENTE COMO CAMINO A LAS CONDUCTAS ANTISOCIALES Y CRIMINALES

Foto: - Freepik

El modelo que Erikson construyó contiene los ingredientes para un desarrollo y funcionamiento sanos

MÉXICO | Wael Sarwat Hikal Carreón

DESARROLLO PSICOSOCIAL, EFECTOS POSITIVO Y NEGATIVO EN LA PERSONALIDAD

Para Erikson, las etapas se encuentran en definitiva en un desarrollo psicosocial, en el que los niños tratan de entender y relacionarse con el mundo. En efecto, Erikson hizo clara la extensión social que estaba latente, incluso algo ausente en la obra de Freud (Papalia, Wendkos Olds y Dustin Feldman, 2009).

Al tratar de seguir el curso del desarrollo social, algunos teóricos han considerado la manera en que la sociedad presenta retos que cambian a medida que madura el individuo. Según Erikson, los cambios evolutivos que se dan durante nuestra vida corresponde a una serie de ocho etapas del desarrollo psicosocial (Woolfolk, 2006).

Erikson sostiene que el paso a través de cada una de estas etapas involucra la resolución de crisis o conflictos; de acuerdo con esto, cada etapa de las ocho, representa los aspectos más positivos y negativos de las crisis de ese período (Ríos Patio, 2017). Si bien esas crisis nunca se solucionan completamente (ya que la vida se vuelve cada vez más compleja), deben superarse de manera adecuada para enfrentar los requerimientos de las siguientes etapas de desarrollo (Papalia, Wendkos Olds y Dustin Feldman, 2009).

Las primeras cuatro etapas propuestas por Erikson son basadas en las etapas psicosexuales de Freud; es decir: de la oral a la latencia. Erikson subdividió entonces la etapa genital en cuatro fases más que representan la maduración juvenil y adulta hasta la ancianidad (Martínez Ocaña, 2018). Cada una de las ocho etapas incluye su propia crisis importante, cada etapa proporciona oportunidades nuevas para que se desarrollen fuerzas del "yo" o "virtudes básicas" (Montes De Oca González, Macías Bestard, Vera Vergara, Maynard Bermúdez y Maynard Bermúdez, 2009).

Las diversas tareas descritas por el autor, se establecen con base en la tarea del infante, llamada "confianza-desconfianza". Al principio resulta obvio pensar que el niño debe aprender a confiar y no a desconfiar. Pero Erikson determina muy claramente que se debe aprender que existe un balance, y que hay más por cultivarse sobre la confianza, pero también algo de desconfianza, de manera que no nos convirtamos en adultos torpes (Restrepo, 2002).

Cada fase tiene un tiempo óptimo también, existe un lapso para cada función. Como ya se mencionó, si se supera bien por un estadio, se llevan ciertas virtudes o fuerzas psicosociales que ayudarán en el resto de los estadios de la vida; por el contrario, si no va tan bien, se podrán desarrollar maladaptaciones o malignidades, así como poner en peligro el desarrollo faltante. De las dos, la malignidad es la peor, ya que comprende mucho de los aspectos negativos de la tarea o función y muy poco de los aspectos positivos de la misma, tal y como presentan las personas desconfiadas. Por otro lado, la maladaptación no es tan mala y comprende más aspectos positivos que negativos de la tarea, como las personas que confían demasiado.

Foto: - Freepik

Los niños de ambientes sociales deficitarios, en riesgo de delincuencia, no disponen de suficientes oportunidades, por lo que resultan retrasados en su desenvolvimiento cognitivo socio-moral


ESPECIALISTAS EN
TRASLADOS VIP
Y PROTECCIÓN EJECUTIVA
NUESTROS SERVICIOS:
GRIPERS
ESPECIALISTAS EN
SEGURIDAD INTRAMUROS
AUDITORÍA Y
CONSULTORÍA
ANÁLISIS DE RIESGOS
ESTUDIOS
DE CONFIANZA
VIGILANCIA Y DETECCIÓN
DE VIGILANCIA Y CONTRAVIGILANCIA
CAPACITACIÓN EN
ARMAS DE FUEGO
grip®
global risk prevention
CONTÁCTANOS
55 1391 6570
comercial@grip.mx
SÍGUENOS EN
REDES SOCIALES
www.grip.mx

Conforme el niño crece, hay cambios en las potencialidades y capacidades, pero también un aumento en su vulnerabilidad a sufrir daño. Al aprender a hacer más por sí mismo, el niño aumenta su susceptibilidad a las frustraciones y conflictos

Erikson también tuvo algo que decir con respecto a las interacciones de las generaciones, lo cual llamó mutualidad. Ya Freud había establecido claramente que los padres influían de una manera drástica en el desarrollo de los niños, pero Erikson amplió la explicación, partiendo de la idea de que los niños también influían al desarrollo de los padres; por ejemplo, la llegada de un nuevo hijo, representa un cambio de vida considerable para una pareja y remueve sus trayectorias evolutivas.

Para Pérez Pinzón y Pérez Castro (2006):

c. El nacimiento de la conducta antisocial está relacionado principalmente con dos fenómenos:

La insatisfacción de ciertas necesidades del niño, como atención, seguridad, dependencia, interacción y experiencias.

La imposibilidad de llevar a cabo ciertas tareas inherentes del desarrollo, como aceptación del propio rol, establecimiento de nuevas relaciones, adquisición de patrones de conducta, elección y preparación para el futuro.

d. En fin, genéricamente hablando, los niños de ambientes sociales deficitarios, en riesgo de delincuencia, no disponen de suficientes oportunidades, por lo que resultan retrasados en su desenvolvimiento cognitivo socio-moral. Igualmente, fracasan a la hora de desplegar obstáculos cognitivos contra las influencias antisociales y las tentaciones (p. 76).

DESARROLLO Y FUNCIONAMIENTO ANORMAL: PROXIMIDAD A LAS CONDUCTAS ANTISOCIALES Y CRIMINALES

La teoría de Erikson de zonas y usos constituye el esquema mediante el cual pueden comprenderse ciertas formas de mal funcionamiento. Al analizar las ocho etapas de la vida según Erikson, hay que tener en cuenta que cada etapa, si es encontrada y vivida triunfantemente agrega un valor al "yo". Erikson se refiere a esas ganancias como fuerzas del "yo" (Huerta Orozco, 2018). Para Erikson, esas fuerzas del "yo" no son sublimaciones sino verdaderos logros.

Conforme el niño crece, hay cambios en las potencialidades y capacidades, pero también un aumento en su vulnerabilidad a sufrir daño. Al aprender a hacer más por sí mismo, el niño aumenta su susceptibilidad a las frustraciones y conflictos (Ríos Patio, 2017). Y aunque la correcta realización de un logro en particular prepara al niño a vivir de una manera más eficaz, puede fácilmente reincidir o regresar. No obstante, si una crisis no se resuelve con éxito en la etapa adecuada del desarrollo, las experiencias posteriores pueden aumentar el daño psicológico producido por padres crueles o negligentes.

Pero debe notarse que un logro alcanzado en la etapa apropiada puede preparar al niño en crecimiento para encargarse de las tareas de la siguiente etapa; por lo tanto, tendrá una posibilidad aún mayor de volverse una influencia continua en el desarrollo del niño, conforme sean dominadas las tareas subsecuentes.

Etapa	Edad aproximada	Resultados positivos	Resultados negativos	Virtudes del "yo"
Confianza *vs.* Desconfianza	Nacimiento a un año y medio	Sentimientos de confianza debido al apoyo del entorno	Miedo y preocupación hacia los demás	Esperanza
Autonomía *vs.* Vergüenza y duda	Un año y medio a tres años	Autosuficiencia si se promovió la exploración	Dudas acerca de sí mismo, dependencia	Voluntad
Iniciativa *vs.* Culpa	Tres a seis años	Descubrimiento de formas de iniciar las acciones	Culpa en cuanto a acciones y pensamientos	Determinación
Industria *vs.* Inferioridad	Seis a 12 años	Desarrollo de un sentimiento de capacidad	Sentimiento de inferioridad,_sentimiento de incapacidad	Competencia
Identidad *vs.* Confusión de roles	Adolescencia	Conciencia de ser único, conocimiento del papel a seguir	Falta de habilidad para identificar roles adecuados en la vida	Fidelidad
Intimidad *vs.* Aislamiento	Primera fase de la edad adulta	Desarrollo de relaciones sexuales amorosas y de amistades íntimas	Miedo de interactuar con los demás	Amor
Generatividad *vs.* Estancamiento	Fase intermedia de la edad adulta	Sentimiento de ayuda a la continuidad de la vida	Subestimar las actividades propias	Cuidado

Cuadro 1. Las etapas del desarrollo psicosocial. Fuente: Elaboración propia.

Foto: - Freepik

ELEMENTOS DE POLÍTICA CRIMINAL BASADA EN ERIKSON

DiCaprio (1989, pp. 202-205), acertadamente indica, para el interés político criminal, algunas opiniones con base en la teoría eriksoniana sobre la personalidad sana; o como él la llama "vida ideal".

CONFIANZA

El sentido de confianza no sólo es esencial para el lactante sino para todos. Un sentido de confianza capacita para tomar decisiones en situaciones desfavorables. Se requiere tener seguridad o confianza en sí mismos y en el ambiente. Sin confianza, se experimenta temor, emoción paralizante que impide la conducta. La esperanza se refiere a expectativas positivas en ausencia de pruebas que las apoyen (Restrepo, 2002).

Constantemente se toman decisiones sobre asuntos importantes, y el resultado de éstas trae consigo incertidumbre y riesgo. Erikson también incluye en el sentido de confianza el poderoso beneficio del respeto y la reverencia hacia la gente. La vida es enriquecida en gran medida por nuestras relaciones sociales, incluso por nuestra relación con seres sobrenaturales. El sentido de confianza debe abarcar la fe en la gente.

AUTONOMÍA

La capacidad de preferir, tomar decisiones y efectuarlas juega un papel importante prácticamente en todo lo que se hace. Se considera el valor de la vida: el autocontrol, autodisciplina, autoafirmación y el poder de la voluntad. La capacidad de decir: "sí" o "no" a los propios impulsos, a las presiones del ambiente y a las perspectivas futuras, es una dimensión importante de la vida efectiva (Steinberg, 2006).

Todos deben esforzarse al enfrentar las distracciones, frustraciones, las propias resistencias internas y los problemas diarios que atormentan. La persistencia y perseverancia son cualidades deseables derivadas del valor. Para ejercitar la voluntad sensatamente, se requiere tener un juicio sano en relación con la conducta correcta y la equivocada. La sensibilidad a los patrones y prácticas sociales, culturales, legales y personales contribuyen ciertamente a la vida efectiva (Marcial, 2006).

Lograr un sentido de identidad ayuda a resolver muchos conflictos importantes en la vida. Ser capaces de encontrar continuidad en los diversos papeles da cierta estabilidad y unidad

INICIATIVA

Satisfacer las necesidades y los deseos de una manera ordenada es otro espacio importante en la vida sana. Tener un propósito en la vida confiere significado. El sentido de iniciativa es auxiliado por los objetivos a corto plazo y fomenta una aproximación vigorosa a la vida.

Erikson incluye, como una característica de la iniciativa, la identificación con papeles auténticos, sentirse cómodo con los papeles culturalmente aceptados y que se adaptan a las capacidades, disposiciones y necesidades, es sin duda una ventaja valiosa en la vida (Marcial, 2006).

LABORIOSIDAD

El sentido de laboriosidad, apoyada por la competencia, en áreas necesarias de ejecución es otro logro importante en el "yo". La vida con éxito en cualquier sociedad depende de la posesión de habilidades valiosas. Se concede categoría y valor propio por las habilidades que se poseen. El éxito depende de las competencias, conocer y practicar las formalidades de la cultura fomenta experiencias de éxito. El ser víctimas o amos de las propias circunstancias depende en alto grado de la competencia.

IDENTIDAD

Lograr un sentido de identidad ayuda a resolver muchos conflictos importantes en la vida. Ser capaces de encontrar continuidad en los diversos papeles da cierta estabilidad y unidad.

La identidad define el lugar en la estructura social. Identificarse con papeles aceptables ayuda a confirmar el sentido de dignidad. La mujer valorada por sus hijos resulta ayudada a establecer su identidad como madre. Si ella es amada y respetada por su esposo, su identidad como esposa se afirma y se define. Si sus padres piensan que ella es una hija, madre y esposa excelente, su identidad recibe más apoyo y definición. Si en su profesión es estimada, se fortalece otro aspecto de la identidad (Huerta Orozco, 2018).

Dos aspectos importantes de la identidad son el compromiso ideológico y la fidelidad. Por compromiso ideológico, Erikson quiere decir tener valores y prioridades que funcionan en una sociedad en particular.

GRUPO EMPRESARIAL CASA

SEGURIDAD PRIVADA

CUSTODIA

INTRAMUROS

CONSULTORÍA

SEGURIDAD PRIVADA | INTRAMUROS

www.gecsa.com.mx

info@gecsa.com.mx

www.facebook.com/gecsa

www.twitter.com/gecsa

www.youtube.com/gecsa

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

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


Foto: - Freepik

Por la virtud de la fidelidad, quiere decir la capacidad de hacer compromisos y acatarlos. Estos son atributos esenciales para la vida efectiva (Fierro, 2006).

INTIMIDAD

El sentido de intimidad es uno de los logros humanos más distintivos. Sus beneficios son muchos. Su ingrediente esencial, la capacidad de amar, enriquece en gran medida la vida. El sentido de intimidad está formado por algunas de las más notables emociones y sentimientos. La vida es apoyada, en gran parte, por las muchas afiliaciones con otras personas. Ser capaz de participar en las relaciones sociales con una gran diversidad de personas es una ventaja valiosa.

GENERATIVIDAD

Los atributos de productividad y generatividad requieren utilizar capacidades en la ejecución del trabajo útil. La sociedad proporciona una gran variedad de papeles aceptables de trabajo, aunque varíen en categoría. Ser capaz de trabajar productivamente es una fuerza principal del "yo", que contribuye significativamente a la calidad de la vida.

El trabajo productivo no sólo se limita a un empleo remunerado, sino también a las obligaciones familiares y la vida comunitaria. La virtud del afecto hace a la familia un vehículo importante para la transmisión de la cultura. El afecto proporciona una valiosa cualidad a los papeles parentales. Erikson sostiene que la persona generacional está motivada a transmitir lo que recibió de la generación anterior, un atributo necesario para la percepción de la cultura.

INTEGRIDAD

La personalidad se fortalece a través de la sabiduría y unificación en la última etapa de la vida. Erikson parece atribuir un mayor control personal a los últimos estadios que en los primeros. El modelo que Erikson construyó contiene los ingredientes para un desarrollo y funcionamiento sanos. ■

Referencias:

- *DiCaprio, N.S. (1989). Teorías de la Personalidad. McGraw-Hill.*
- *Huerta Orozco, A. (2018). El sentido de pertenencia y la identidad como determinante de la conducta, una perspectiva desde el pensamiento complejo. IE Revista de Investigación Educativa de la REDIECH. 9(16), 83-97. https://www.scielo.org.mx/pdf/iered iech/v9n16/2448-8550-iered iech-9-16-83.pdf*
- *Marcial, R. (2006). Identidad cultural. En M. Pérez Olvera (Comp.). Desarrollo de los Adolescentes III. Identidad y Relaciones Sociales (pp. 105-125). Centros de Integración Juvenil. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/Libros_Adolecencia.pdf*
- *Montes De Oca González, Y.; Macías Bestard, C.; Vera Vergara, V.; Maynard Bermúdez, G.I.; y Maynard Bermúdez, R.E. (2009). Algunas consideraciones teóricas acerca del modelo epigenético de Erik Erikson. Revista Información Científica. 62(2), 1-11. http://www.revinfcientifica.sld.cu/index.php/ric/article/view/1235/2484*
- *Papalia, D., Wendkos Olds, S. y Dustin Feldman, R. (2009). Psicología del Desarrollo. De la Infancia a la Adolescencia. McGraw Hill. https://www.mendoza.gov.ar/salud/wp-content/uploads/sites/16/2017/03/Psicologia-del-Desarrollo-PAPALIA-2009.pdf*
- *Pérez Pinzón, Á.O. y Pérez Castro, B.J. (2006). Curso de Criminología. Universidad Externado de Colombia.*
- *Restrepo, L.C. (2002). La confianza frente a la desconfianza. Un enfoque de salud mental para la construcción de la paz en Colombia. Revista Colombiana de Psiquiatría. 31(4). 271-284. http://www.scielo.org.co/pdf/rcp/v31n4/v31n4a03.pdf*
- *Ríos Patio, G. (2017). Relaciones e implicancias del determinismo biológico, el pensamiento freudiano de psicología criminal y la nueva criminología. Horizonte Médico. 17(3). 65-72. https://www.horizontemedico.usmp.edu.pe/index.php/horizontemed/article/view/670/414*
- *Woolfolk, A.E. (2006). La obra de Erikson. En M. Pérez Olvera (Comp.). Desarrollo de los Adolescentes III. Identidad y Relaciones Sociales (pp. 29-44). Centros de Integración Juvenil. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/Libros_Adolecencia.pdf*

Referencias:
- *DiCaprio, N.S. (1989). Teorías de la Personalidad. McGraw-Hill.*
- *Huerta Orozco, A. (2018). El sentido de pertenencia y la identidad como determinante de la conducta, una perspectiva desde el pensamiento complejo. IE Revista de Investigación Educativa de la REDIECH. 9(16), 83-97. https://www.scielo.org.mx/pdf/iered iech/v9n16/2448-8550-iered iech-9-16-83.pdf*
- *Marcial, R. (2006). Identidad cultural. En M. Pérez Olvera (Comp.). Desarrollo de los Adolescentes III. Identidad y Relaciones Sociales (pp. 105-125). Centros de Integración Juvenil. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/Libros_Adolecencia.pdf*
- *Montes De Oca González, Y.; Macías Bestard, C.; Vera Vergara, V.; Maynard Bermúdez, G.I.; y Maynard Bermúdez, R.E. (2009). Algunas consideraciones teóricas acerca del modelo epigenético de Erik Erikson. Revista Información Científica. 62(2), 1-11. http://www.revinfcientifica.sld.cu/index.php/ric/article/view/1235/2484*
- *Papalia, D., Wendkos Olds, S. y Dustin Feldman, R. (2009). Psicología del Desarrollo. De la Infancia a la Adolescencia. McGraw Hill. https://www.mendoza.gov.ar/salud/wp-content/uploads/sites/16/2017/03/Psicologia-del-Desarrollo-PAPALIA-2009.pdf*
- *Pérez Pinzón, Á.O. y Pérez Castro, B.J. (2006). Curso de Criminología. Universidad Externado de Colombia.*
- *Restrepo, L.C. (2002). La confianza frente a la desconfianza. Un enfoque de salud mental para la construcción de la paz en Colombia. Revista Colombiana de Psiquiatría. 31(4). 271-284. http://www.scielo.org.co/pdf/rcp/v31n4/v31n4a03.pdf*
- *Ríos Patio, G. (2017). Relaciones e implicancias del determinismo biológico, el pensamiento freudiano de psicología criminal y la nueva criminología. Horizonte Médico. 17(3). 65-72. https://www.horizontemedico.usmp.edu.pe/index.php/horizontemed/article/view/670/414*
- *Woolfolk, A.E. (2006). La obra de Erikson. En M. Pérez Olvera (Comp.). Desarrollo de los Adolescentes III. Identidad y Relaciones Sociales (pp. 29-44). Centros de Integración Juvenil. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/Libros_Adolecencia.pdf*

Wael Sarwat Hikal Carreón, director de Proyectos en la Sociedad Mexicana de Criminología Capítulo Nuevo León, México. Más sobre el autor:

GRUPO LK

"Protegemos tu patrimonio con profesionalismo y pasión"

Oficiales de Seguridad

Custodias de Transporte

Monitoreo y Rastreo Vehicular

Estudios de Vulnerabilidad

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

55-8848-8264

grupolkseguridadprivada.com

Foto: Freepik

LA REALIDAD DE LA MUJER EN SEGURIDAD

No importa de qué cultura provenga una persona, las mujeres siguen teniendo más probabilidades que los hombres de identificar correctamente las emociones

PERÚ

Herbert Calderón

Comencemos con la familia, la cual es la célula de la sociedad y, por supuesto, es la institución más básica en el desarrollo de nuestra cultura, también es la unidad de reproducción y mantenimiento de la especie humana y en ese sentido, es el elemento que sintetiza la producción de la salud a escala micro social.

El rol de la mujer es ser el miembro fundador de la familia y al tener un papel importante en la creación, formación y mantenimiento de valores de las personas que la integran, la naturaleza de ser madre, se hace realidad; pero también es allí donde empieza su mayor responsabilidad con la sociedad.

Así mismo, en competencias verbales, en general, las mujeres tienen más talento que los hombres, como señalan diferentes investigaciones científicas que veremos más adelante.

Adicionalmente se ha demostrado que las mujeres pueden reconocer las emociones de otras personas mucho mejor a través de la mímica, que por el tono de voz. Para los hombres, parece ser que es lo contrario.

EXCELENTES GESTORAS DE SEGURIDAD

Ellas no sólo pueden reconocer las emociones a través de la comunicación no verbal, sino que también pueden decir exactamente de qué emoción se trata. El psicólogo Sokolov, de la universidad de Tübingen, por ejemplo, hizo un estudio interesante con la imagen del brazo de una persona llamando a una puerta de diferentes maneras: las mujeres pudieron interpretar las emociones exactamente, y fueron capaces de reconocer la forma agresiva de llamar mucho mejor que los hombres; que al contrario, fueron capaces de reconocer bastante bien la manera que expresa felicidad de golpear a la puerta.

Por lo tanto, y teniendo en cuenta todo lo mencionado, se reúnen ampliamente las condiciones para ser un excelente gestor de seguridad en cuanto a las

Foto: - Freepik

cualidades antes mencionadas como: percepción de la realidad, lectura de lenguaje no verbal, creación, formación y mantenimiento de valores de las personas; que son aptitudes que hacen de la mujer un excelente líder, no sólo en el desempeño como líder, sino también en los diferentes roles de la seguridad, como agente, supervisor, directivo de un sistema, etc.

Esto ha revolucionado las actividades en un mundo machista, en donde se pensaba que sólo el hombre dominaba, sin embargo, la mujer no reemplaza al hombre, sino que lo complementa y fortalece, en ello radica su mejor aporte. Muchas instituciones han comenzado a incrementar la presencia de la mujer como en las Fuerzas Armadas, Policía Nacional, empresas de vigilancia, empresas privadas en general. ■

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

¡AFÍLIATE AHORA!

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

Conoce y disfruta nuestros BENEFICIOS

REUNIONES MENSUALES SIN COSTO
PROFESIONALIZACIÓN + NETWORKING
Presenciales, Conferencias y sedes de 1er nivel

COSTO PREFERENCIAL
En cursos, certificaciones, bibliografía y eventos internacionales

ACCESO GRATUITO
En cursos, certificaciones, bibliografía y eventos internacionales

+ DE 10 COMUNIDADES ESPECIALIZADAS
Interactúa con tus colegas, intercambia conocimientos y mantente informado.

OFERTA ACADÉMICA ESPECIALIZADA
Webinars sin costo, cursos especializados, masterclasses, y programas de preparación para certificarte (CPP, PSP, PCI Y APP)

ASIS EN LOS MEJORES EVENTOS GLOBALES DE SEGURIDAD
Precios exclusivos, workshops, eventos de networking y más.

CHAT PRIVADO DE SOCIOS ACTIVOS
Intercambio de información en tiempo real con l@s expert@s de la seguridad en mx.

BOLSA DE TRABAJO
Especializada y exclusiva para soci@s

NEWSLETTER SEMANAL PADLET DE NOTICIAS

*Vigencia de membresía al 31 de diciembre 2023

COMUNICACIÓN GLOBAL

De más de 34 mil Profesionales de seguridad Alrededor del mundo

¡Mitad de año, mitad de precio!

Afiliación

ASIS MÉXICO 217
$2,825.^{00} MXN

ASIS INTERNACIONAL
$60.^{00} USD

50%

#JuntosXASIS
#PosibilidadesInfinitas

MAYOR INFORMACIÓN
(55 3437 6890
info@asis.org.mx

NEXTGEN (YOUNG PROFESSIONALS)

Una red de apoyo para los jóvenes profesionales de la seguridad

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

ASIS INTERNATIONAL | NextGen

Young Professionals es una comunidad de ASIS Internacional que integra a todos los miembros que estén interesados en temas de seguridad, pero relacionados a los jóvenes o nuevos integrantes del sector. Entre sus principales objetivos es el desarrollar nuevos talentos, capacitar y profesionalizarlos, así como el compartir conocimiento y experiencia en todo el mundo. Sin embargo para no encasillar a la comunidad y darle ese empuje que necesitaba, en octubre de 2022 se decidió cambiarle el nombre a: NextGen continuando con su enfoque hacia profesionales menores de 40 años que son nuevos en la industria de la seguridad. A continuación Ana Julieta Alvarado, líder de la comunidad NextGen (Young Professionals) en ASIS Capítulo 217, nos compartió más sobre ésta.

LA TECNOLOGÍA Y EL SOPORTE TÉCNICO

APLICADOS PARA EVOLUCIONAR TU SEGURIDAD

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA

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

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

ALAS Asociación Latinoamericana de Seguridad · Socio ALAS
SISTEMA DE GESTIÓN ISO 9001:2015 BICERT, S.C.
Achilles No. 329,814
COPARMEX

222 141 12 30
gerenciacomer@pem-sa.com
WWW.PEM-SA.COM

“La comunidad es un espacio para que los jóvenes profesionales podamos desarrollarnos a través de *webinars*/reuniones con oradores destacados”

¿Cuáles son los objetivos, valores y hacia quién está dirigida la Comunidad de Young Professionals (NextGen)?

La Comunidad Young Professionals (NextGen) tiene como principal objetivo servir como recurso para educar y desarrollar jóvenes profesionales, proporcionándoles un foro para participar y aprender de los líderes de opinión en seguridad, participar en los programas y actividades de ASIS y conectarse con colegas en todo el mundo. En ASIS Capítulo México 217 tenemos el objetivo de difundir y reclutar a más jóvenes profesionales a través de actividades que enriquezcan la experiencia profesional.

¿Cuál es su función dentro de la Comunidad?

Mi función es cumplir con las metas que se han establecido a través de un *Framework* que se desarrolló para que la ejecución sea lo más eficiente posible, además de integrar nuevas ideas que permitan que los jóvenes se sientan atraídos por los beneficios que podemos brindar.

¿Cuáles son los beneficios de pertenecer a esta Comunidad?

La comunidad es un espacio para que los jóvenes profesionales podamos desarrollarnos a través de *webinars* con oradores destacados con temas relevantes para la comunidad (especializados), eventos, programas de mentoring, becas en certificaciones (APP/CPP); y con esto generar una red de apoyo.

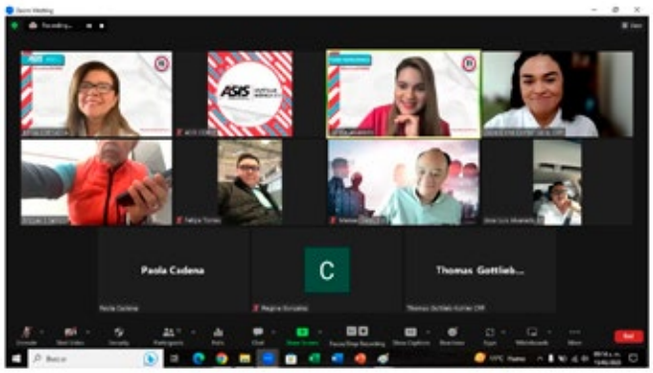
¿Cómo contribuye la Comunidad y sus integrantes al sector de la seguridad?

Innovando, integrando nuevos métodos para que cada vez más jóvenes se integren a la asociación.

¿Cuáles son los planes de la Comunidad para 2023?

La comunidad está creciendo, y queremos que ésta se enfoque en todos los aspectos que necesita un joven para desarrollarse como profesional, desde la difusión y becas en cursos de certificaciones, como estrategias y habilidades, hasta *soft skills*. ■

Fotos: NEXTGEN



MÁS SOBRE...

Julieta Alvarado es egresada del Centro de Estudios en Ciencias de la Comunicación en la carrera de Mercadotecnia, y comenzó su carrera profesional fundando su propia empresa de Mercadotecnia y Publicidad, JUMI-MKT, en el año 2019, posteriormente se unió al equipo de Multiproseg en donde desempeña diferentes actividades.

“Soy miembro de ASIS Capítulo México 217 desde 2019, mi motivación es poder crear un espacio para que los jóvenes puedan tener un sentido de pertenencia a la asociación, donde puedan aprender y aplicar dichos conocimientos a su vida laboral, es importante que sigamos innovando para que las próximas generaciones conozcan los innumerables beneficios que tiene ASIS INT a nivel profesional y personal; los invito a ser parte de esta comunidad y seguir construyendo el ASIS que tod@s queremos #JuntosXASIS”.

Potros BOOTS

VIVE LA EXPERIENCIA

Apostemos siempre por la innovación y calidad del calzado Poblano

Una empresa de calzado 100% mexicana de alta tecnología

Informes al 55 2737 2372

ACONTECIMIENTOS DE LA INDUSTRIA DE LA SEGURIDAD PRIVADA

Fecha: 27 de marzo de 2023.

Lugar: Hotel Sheraton, Ciudad de México.

Asistentes: más de 70 invitados.

La AMPCI presenta la conferencia "Las inversiones de edificaciones para las instalaciones de protección contra incendio" y reconoce a las mujeres bomberos

La Asociación Mexicana de Protección Contra Incendios (AMPCI) llevó a cabo un desayuno en el que el ingeniero Carlos Gutiérrez, impartió la conferencia titulada "Las Inversiones de edificaciones para las instalaciones de protección contra incendio", además se aprovechó el encuentro para reconocer el esfuerzo y la labor de las mujeres bomberos en el campo.

José Arturo Ortega Porcayo, presidente de la AMPCI Comité México, dio la bienvenida a los miembros de la asociación, invitados especiales y medios de comunicación. José Arturo habló acerca de los recientes incendios presentados, y de igual forma ofreció estadísticas en las que durante 2022, el Heroico Cuerpo de Bomberos Capitalino atendió 54 mil servicios, de los cuales 4 mil 20 correspondieron a incendios estructurales, dicho esto, José Arturo invitó a los presentes a seguir promoviendo las buenas prácticas y el cumplimiento de la normatividad para salvaguardar las vidas y la integridad de las personas, mismas que fomenta la asociación. ■

Fecha: 18 de abril de 2023.

Lugar: Centro Citibanamex, Ciudad de México.

Asistentes: más de 100 socios e invitados.

ASIS Capítulo México realiza su reunión mensual previa a Expo Seguridad México 2023

Manuel Rivera Raba, director general de NEKT Group

ASIS Capítulo México llevó a cabo su reunión del mes de abril en las instalaciones del Centro Citibanamex, debido a que ese mismo día inició la vigésima edición de Expo Seguridad México 2023 en dicho recinto. En esta ocasión, SISSA fue el patrocinador del desayuno mensual, siendo Isaac Valencia, director y fundador de SISSA, quien agradeció a ASIS el espacio y resaltó la importancia de profesionalizar la seguridad, además expresó la celebración de SISSA por sus 12 años de presencia en el mercado.

La ponencia principal titulada "El rol de la alta dirección en la ciberseguridad empresarial" estuvo a cargo de Manuel Rivera Raba, director general de NEKT Group. En su plática, compartió su conocimiento en cuanto a las nuevas tecnologías y lo imperativo que es implementar técnicas de seguridad en las empresas que, con la constante innovación digital, se ven vulneradas cada día de manera fácil ante la ciberdelincuencia. Hechos como conectarse a una red de wifi pública pueden poner en riesgo al usuario, ocasionando que se cometan delitos desde robo de datos personales hasta la infiltración a empresas. ■

Fecha: 19 de abril de 2023.

Lugar: Hotel Marquis, Ciudad de México.

Asistentes: más de 200 invitados.

La AMESP presente en el "Foro de Ciberseguridad INDEX 2023"

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) fue uno de los patrocinadores del "Foro de Ciberseguridad INDEX 2023", un espacio para afrontar los nuevos retos y las tendencias del mundo digital. Previo a la inauguración, el Dr. Luis Manuel Hernández, presidente de INDEX; el Ing. Agustín Tiburcio, director del Comité de TI de INDEX; el Ing. Eduardo Alvarado, vicepresidente de CANIETI; y el Dr. Arturo Ramírez, presidente de ANADIC, dieron una conferencia de prensa.

También estuvo presente el Lic. Fadlala Akabani Hneide, secretario de Desarrollo Económico de la Ciudad de México en representación de la Dra. Claudia Sheinbaum, jefa de Gobierno de la Ciudad de México; así como Gabriel Bernal, presidente de la AMESP; Verónica Torres Landa, directora general de la AMESP; y Luis Miguel Dena, vocal de la asociación, quien además se presentó más tarde ese día en el Conversatorio AMESP con una ponencia en conjunto con Pablo Gutiérrez, Alberto Friedmann y Herve Hurtado. El principal motivo es concientizar a las personas y a las empresas acerca de los riesgos y amenazas que se presentan en un mundo que avanza exponencialmente día con día en temas de tecnología y el mundo digital. ■

Fecha: 20 de abril de 2023.

Lugar: Centro Citibanamex, Ciudad de México.

Héctor Coronado presenta su libro *"Una Segunda Oportunidad"* durante la Expo Seguridad 2023

En el último día de la vigésima edición de la Expo Seguridad México 2023, Héctor Coronado Navarro, director de Seguridad de Mercado Libre en Latinoamérica, realizó la firma de su nuevo libro *"Una Segunda Oportunidad"* en el *stand* de **Seguridad en América** dentro del evento. Los asistentes acudieron al mismo para tener la oportunidad de conocer al experto en seguridad, obtener un saludo y una pequeña charla con él, acompañados de la firma de su libro.

"Este libro es con la intención de ser muy autocrítico, de aportar algo diferente. Todos hemos tenido crisis, una de las crisis que tenemos, para mí, son las áreas de mejora y de oportunidad. El libro va dedicado para cualquier persona que quisiera hacer las cosas un poquito diferente, también para los jóvenes o la gente que va empezando, que ojalá no se tropiecen con las mismas piedras que yo lo hice y para colegas como yo que compartimos mejores prácticas. Este libro lo dedico con todo el corazón, con toda la humildad y espero les agrade", expresó el autor. ■

Héctor Coronado Navarro, director de Seguridad de Mercado Libre en Latinoamérica

Fecha: 21 de abril de 2023.

Lugar: MRKTec, Ciudad de México.

PELCO y Motorola Solutions otorgan reconocimiento a José Luis Caballero de MRKTec por su excelente desempeño

Los directivos de la empresa Motorola Solutions con su marca PELCO, se reunieron en las oficinas de la empresa MRKTec para otorgarle un reconocimiento especial a José Luis Caballero, director general de MRKTec, esto por su excelente desempeño como distribuidor principal de PELCO durante el año 2022. Víctor Merino, director regional de Canales de Distribución para LATAM, expresó que el reconocimiento hacia José Luis y MRKTec funciona como una retribución por todo el apoyo y su colaboración a lo largo de los años, pero especialmente por su *performance* y desempeño en el año 2022.

Por su parte, Dean Brazenall, *Senior Director for International Distribution* de Motorola Solutions, le extendió el reconocimiento a MRKTec por su trabajo en conjunto; mientras que José Luis Caballero, director general de MRKTec, agradeció a PELCO y a Motorola Solutions, destacando que el reconocimiento es el resultado de la base del trabajo del equipo local y el apoyo de Víctor y Dean; en conjunto con su gran equipo, y además auguró más éxitos en el futuro. ■

Fecha: 27 de abril de 2023.

Lugar: Ciudad de México.

Asistentes: más de 600 participantes.

Seguridad en América realiza *Roadshow* de Seguridad en Centrales de Monitoreo y GPS

Seguridad en América (SEA) llevó a cabo una nueva edición *online* del *Roadshow* "Seguridad en Centrales de Monitoreo y GPS", en el que la charla magistral estuvo a cargo de Yolanda Bernal Sánchez, fundadora y directora comercial de Orbit Keeper, quien se presentó con la ponencia titulada "Innovación en Centrales de Monitoreo". El *Roadshow* contó también con las participaciones de Verónica Villa, de la empresa Control T y de Lucas Banda, de la empresa SoftGuard; además de palabras de José Luis Alvarado, de parte de ASIS Capítulo México, dicho foro fue presentado nuevamente por Samuel Ortiz, director general de **Seguridad en América**; y Alex Parker, *Sales Manager* de la misma casa editorial.

Yolanda Bernal Sánchez, fundadora y directora comercial de Orbit Keeper; Samuel Ortiz, director general de Seguridad en América; y Alex Parker, *Sales Manager* de SEA

PATROCINADORES

Verónica Villa Lara, directora de Proyectos de la empresa Control T, presentó la ponencia "Nuevas tecnologías para mejorar la seguridad de la carga". Verónica coincidió que los riesgos

de seguridad en el área de transporte siguen abundando, pero la tecnología y los avances digitales ofrecen nuevas posibilidades de protección para las empresas, los empleados y los clientes. Es por esto por lo que, Verónica presentó la plataforma de Control T, una herramienta digital con la finalidad de garantizar la protección en todas las áreas del servicio de transporte. Dentro de sus ventajas, la plataforma ofrece la posibilidad de no solamente monitorear los transportes, sino los viajes en general, cada aspecto del traslado, obteniendo una visión general del servicio, entre otras funcionalidades.

Posteriormente fue el turno de Lucas Banda, *Country Manager* de la empresa SoftGuard, con la ponencia titulada "¿Cómo innovar en el monitoreo sin morir en el intento?". Lucas explicó los tres puntos principales de su presentación: quiénes son SoftGuard, ¿Qué es el Monitoreo 4.0? y qué fundamentos se necesitan para sobrevivir y crecer. También habló acerca de la evolución del *software* de monitoreo, lo que ha traído en la actualidad el uso de aplicaciones digitales, una de ellas es Vigicontrol. SoftGuard presentó Vigicontrol como una aplicación diseñada para el control de guardias cuyas ventajas incluyen: alertas automáticas ante incumplimientos, *tracking* para monitoreo de objetivos móviles, control de presencia, entre otras.

Luego fue turno de Luis Giovanni Ramos Baca, supervisor de Monitoreo de la empresa Tracking Systems, con una plática titulada "*Control Rooms* en la práctica del Monitoreo GPS". La empresa dedicada al rastreo satelital está muy enfocada a la parte de la logística; habló de cómo los centros de control son vitales en el área de monitoreo y rastreo. Presentó

Luis Giovanni Ramos Baca, supervisor de Monitoreo de la empresa Tracking Systems

Trust ID, un servicio de verificación y certificación del personal encargado de esta área. Trust ID cuenta con análisis de datos de confianza en línea, validación fotográfica, análisis de contenido en declaraciones, estudio sociolaboral, entre otras herramientas.

Al finalizar el *Roadshow*, se les realizó una invitación a los presentes a asistir a la segunda edición de la Cumbre de Seguridad Corporativa, organizada por **Seguridad en América,** donde más de 30 profesionales de la seguridad corporativa estarán como panelistas compartiendo sus conocimientos y experiencias en sus distintas áreas de trabajo. El evento se llevará a cabo de manera presencial el 29 y 30 de agosto de 2023 en el Centro Citibanamex de la Ciudad de México. ■

Fecha: 04 y 05 de mayo de 2023.

Lugar: Hotel Radisson de San José, Costa Rica.

La AMESP participa en el "XVI Congreso Panamericano de Seguridad Privada"

Se llevó a cabo el "XVI Congreso Panamericano de Seguridad Privada", organizado en colaboración entre la Federación Panamericana de Seguridad Privada (FEPASEP) y la Asociación Costarricense de Empresas de Seguridad (ACES), el cual contó con la participación de diferentes miembros del gremio de varios países de Latinoamérica como México, Brasil, Colombia, Paraguay, Ecuador; siendo la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), quien representó al sector de la seguridad de México.

Los miembros del presídium fueron el Dr. Stephan Brunner Neibig, primer vicepresidente de la República de Costa Rica; el Lic. Johan Vargas, presidente de la ACES; el Dr. José Jacobson Neto, presidente de la FEPASEP; el Profe. Edgardo Frigo, director académico del Congreso y autoridades latinoamericanas de seguridad. Gabriel Bernal Gómez, presidente de la AMESP, participó con la conferencia titulada "Desafíos de la industria de la Seguridad Privada en México en los últimos 10 años". ■

Fecha: 09 de mayo de 2023.

Lugar: Bárbaro Club House del Hipódromo de las Américas en la Ciudad de México.

Asistentes: más de 150 asociados.

ASIS Capítulo México lleva a cabo su Reunión Mensual de mayo

ASIS Capítulo México llevó a cabo su reunión mensual de mayo, en la que Brisa Espinosa, presidenta del Capítulo, manifestó su reporte de actividades, entre los cuales destacan la presencia de la asociación en la Expo Seguridad México 2023, donde la asociación contó con un panel central y varias conferencias de alto nivel en el escenario principal durante los tres días de la exposición. También destacó la implementación del proyecto "Adopta una escuela", a cargo de Gerardo del Lago, coordinador de la Comunidad en Seguridad Escolar, el cual consiste en mejorar una escuela para elevar todos los estándares para que se considere una escuela segura.

En esta ocasión, Rebeca Muñoz Cornejo, *Mind Coach* y conferencista internacional, impartió la charla principal "Construyendo un liderazgo transformacional a través de la inteligencia emocional", en la que destacó varios puntos importantes de la inteligencia emocional que se pueden aplicar dentro del sector de la seguridad privada, como el hecho de tener aptitudes de liderazgo dentro de la organización para fomentar un sentimiento igual en el equipo de trabajo. El patrocinador de la reunión fue CIA Kapital. ■

Rebeca Muñoz Cornejo, *Mind Coach* y conferencista internacional

Fecha: 11 de mayo de 2023.

Lugar: Hacienda de Los Morales, Ciudad de México.

Asistentes: más de 70 asociados.

La AMESP realiza su desayuno del mes de mayo con conferencia de Sergio Aguayo

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) llevó a cabo el desayuno del mes de mayo en donde Gabriel Bernal, presidente de la asociación, aprovechó para rendir un reporte de actividades de los últimos meses que la AMESP ha desarrollado, también se presentó Sergio Aguayo, académico y analista, con una charla titulada "El peso de la inteligencia en la seguridad mexicana". Entre los puntos que destacó Bernal, estuvieron: la integración de los nuevos asociados, Isaac Valencia, de SISSA; Elisa Regina Garza, de Compañía Mexicana de Traslado de Valores S.A. de C.V.; y Eduardo Hernández, de Suministros y Consultoría Punto Sur.

También comentó sobre la apertura de las nuevas oficinas de la asociación, y sobre la presencia de las seis empresas asociadas en el panel de la Expo Seguridad México 2023 en conjunto de conferencias especiales; los representantes de la asociación también tuvieron una plática con la embajadora de México en Costa Rica durante el "XVI Congreso Panamericano de Seguridad Privada". De igual forma, se mencionó la participación de la AMESP en el Foro Internacional de Ciberseguridad INDEX. ■

Rafael Arenas Hernández, presidente de la Comisión de Asuntos Fiscales de AMESP; Cap. José Carlos Sánchez Guzmán, director general de GECSA; Sergio Aguayo, académico y analista; y Gabriel Bernal Gómez, presidente de AMESP

Fecha: 11 de mayo de 2023.

Lugar: Ciudad de México.

Asistentes: más de 500 participantes.

Seguridad en América presenta el *Roadshow* "Seguridad en Supermercados y Tiendas de Conveniencia"

Seguridad en América llevó a cabo una nueva edición de los ya conocidos *Roadshows*, esta vez el tema fue "Seguridad en Supermercados y Tiendas de Conveniencia"; en el que la charla magistral estuvo a cargo de un panel grupal con la participación de miembros de Grupo Comercial Chedraui con la ponencia titulada "El Ecosistema de la seguridad integral en supermercados". Asimismo, se contó con la participación de una ponencia de la empresa OmniCloud y palabras de José Luis Alvarado, vicepresidente ejecutivo de ASIS Capítulo México. El *roadshow* fue presentado nuevamente por el equipo de **Seguridad en América**, Samuel Ortiz, director general, Alex Parker, *Sales Manager;* y Katya Rauda, asistente de Dirección. ■

CHARLA MAGISTRAL

El panel principal estuvo a cargo de representantes de Grupo Comercial Chedraui, que incluyó a Gloria Meléndez, directora de Prevención de Pérdidas; José Mario Morales, gerente de Inteligencia; Oscar Berthier, gerente de Operaciones C5; Israel Baizabal, gerente regional de Prevención de Pérdidas; Juan Agustín Morales, gerente de Protección Civil *Compliance*; y Reynaldo Vázquez, gerente de Tecnologías para la Seguridad, quienes presentaron la charla magistral titulada "El Ecosistema de la Seguridad integral en Supermercados".

Cada miembro del panel explicó las diferentes Verticales del Ecosistema de Seguridad que mencionan, entre ellas: la Inteligencia a través de la *Data*, que es el conocimiento integral del entorno en la U.N. y mitigar el riesgo patrimonial; la Inteligencia Artificial, que se usa para facilitar la experiencia del cliente y atacar puntos de dolor con la ayuda de la *data*; el Cumplimiento Normativo, que logra identificar factores de riesgo estructural en la U.N. y posee cercanía con las autoridades; la Experiencia de los Clientes (NPS), una estrategia corporativa que funciona con agilidad y con la implementación de una propuesta de valor; y por último, el Monitoreo Estratégico y Reacción Inmediata, que hace uso de la infraestructura, los protocolos, la *data* y el capital humano.

Todo esto se debe trabajar en conjunto con las áreas responsables para garantizar un sistema de seguridad integral que funcione adecuadamente y que beneficie a las tres partes importantes del negocio: los clientes, los colaboradores y los proveedores.

PATROCINADOR

Posteriormente fue el turno de Arturo Flores, director comercial de la empresa OmniCloud, quien se presentó con una plática titulada "Innovación en la Seguridad de Supermercados con servicios *Cloud*". Reconociendo la importancia de la innovación tecnológica, Arturo comenzó hablando de la plataforma OmniView, una herramienta que utiliza toda la infraestructura existente enfocándose en mejorar los procesos de seguridad dentro de la organización.

Capaz de conectarse con la red local, la plataforma integra todos los puntos de la empresa con la finalidad de realizar un análisis recopilatorio que muestre la información requerida. Cuenta con todos los sistemas de seguridad necesarios en la parte de logística y transporte de producto dentro del supermercado, controles de acceso y paneles de alarma, así como sistemas de CCTV, ofreciendo imagen y video de calidad para su análisis. La calidad de la plataforma OmniView se ve reflejada con soluciones a la medida de la innovación actual, reflejando en el manejo de data que se transfiere a la Nube por medio de ésta.

Finalmente, Samuel Ortiz y Alex Parker despidieron la edición del *roadshow*, no sin antes realizarles una invitación a todos los presentes a asistir a la próxima edición de la Cumbre de Seguridad Corporativa que organiza **Seguridad en América,** donde más 30 panelistas expertos en distintas áreas de la seguridad corporativa presentarán conferencias magistrales para compartir los conocimientos derivados de su trayectoria y experiencia. La Cumbre se realizará el próximo 29 y 30 de agosto en el Centro Citibanamex de la Ciudad de México. ■

Fecha: 23 y 24 de mayo de 2023.

Lugar: Hipódromo de las Américas, Ciudad de México.

Asistentes: más de 50 asociados.

ALASCA realiza su Reunión Anual para miembros en la Ciudad de México

Se llevó a cabo la Reunión Anual para miembros de la Asociación Latino Americana de Seguridad de Casinos (ALASCA), en la que durante los días se brindaron pláticas para los asociados y los asistentes de Grupo Codere, impartidas por distintos miembros de ALASCA e invitados especiales. Uno de los ponentes fue Juan Carlos Rocha, director de Seguridad de CODERE Europa; así como Pablo Mariano Kovalevsky, director de Seguridad y CCTV de CODERE Panamá; Manuel Correas, director de Inspección de Riesgos y Seguridad de la empresa CIRSA Panamá y actual presidente de ALASCA.

También estuvo presente Rodolfo Prado, de la empresa IPTC; y Antonio Gaona, director de Seguridad de Grupo CODERE; Miguel Ángel Milla, gerente de Cámaras Casino Golden Palace y director del Comité de Membresía de ALASCA. José Casapía Bardales, gerente de Seguridad y Corporativo en NOVOMATIC Perú y embajador ALASCA, así como Johan Orel Gallego, gerente de CCTV y Seguridad del Royal Casino Hotel "La Hacienda" en Panamá. Finalmente se presentó John Henry Camargo, director nacional de Control Interno Seguridad de Grupo Vicca y vicepresidente de ALASCA. ■

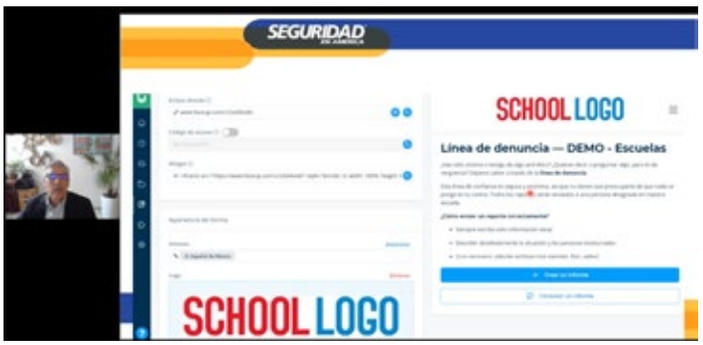
Fecha: 24 de mayo de 2023.

Lugar: Ciudad de México.

Asistentes: más de 500 registrados.

Seguridad en América presenta el *Roadshow* de Seguridad en Centros Educativos

El equipo de **Seguridad en América (SEA)** realizó una edición más de los *Roadshows*, en esta ocasión titulado "Seguridad en Centros Educativos", en el que la charla magistral estuvo a cargo de Carlos Irecta, líder de gestión de riesgos en seguridad para el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) campus Puebla, con la ponencia "Riesgos emocionales en la seguridad escolar". Además de contar con ponencias de las empresas Ética integral y Eagle Eye Networks, así como participaciones de las asociaciones ASIS Capítulo México y AMESP. El *Roadshow* fue presentado por Samuel Ortiz, director general de **Seguridad en América**; Alex Parker, *Sales Manager*; y Katya Rauda, asistente de Dirección.



CHARLA MAGISTRAL

La charla magistral impartida por Carlos Irecta Lecona, líder de gestión de riesgos en seguridad para el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) campus Puebla. La plática estuvo titulada "Riesgos emocionales en la seguridad escolar". En su charla, habló acerca de los riesgos derivados de las emociones y las conductas de la comunidad estudiantil desde el punto de vista emocional, el experto aclaró cómo desde la pandemia, cuando las escuelas adoptaron la modalidad de clases en línea, los docentes no podían atender de la manera más óptima las problemáticas estudiantiles, especialmente las personales, por lo cual, al regresar a

la modalidad presencial, los alumnos presentaron indisciplina. La falta de madurez que, Carlos señaló, se dio en la pandemia, generó esta falta de buena conducta y sentido por la rebeldía que genera riesgos, tanto personales en el alumnado y el cuerpo docente, así como físicos en la escuela, y ambas partes son responsabilidad del área de seguridad.

PATROCINADORES

Después se presentó Jaime Gómez Balderrama, socio fundador y director de Ética Integral, con la charla titulada "Herramientas certeras para fomentar un ambiente escolar seguro". Jaime retomó puntos importantes de la presentación de Carlos, explicando las conductas que amenazan el ámbito escolar: personales, patrimoniales y reputacionales. Ante esto, presentó la plataforma Enfoque Integral, una herramienta que puede implementarse en el ámbito escolar como método de denuncias ante alguna situación de riesgo, otorgándole al estudiante el canal de comunicación de manera confidencial y anónima con todos los estándares de seguridad en el manejo de datos de cuenta personalizada, mejorando el entorno escolar, la reputación y marca, así como fortalece la cultura ética.

Más tarde fue el turno de Sara Aguirre, *Market Development Representative* para LATAM de Eagle Eye Networks, con la plática titulada "Videovigilancia remota para entornos de aprendizaje seguros". Proveniente de la empresa dedicada a la fabricación de sistemas de videovigilancia en la Nube, resaltó cómo los padres de familia tienen la seguridad dentro

de sus prioridades al buscar un centro educativo. Hoy en día, la videovigilancia puede atender los cuatro riesgos más comunes en las escuelas: el *bullying*, el acoso sexual, robos y desastres naturales.

La videovigilancia de Eagle Eye puede brindar la grabación y monitoreo de cualquier área dentro o fuera del perímetro, enviar alertas en caso de situaciones peligrosas, utiliza la función de audio bidireccional, posee la búsqueda inteligente de video, así como el almacenamiento seguro en la Nube del contenido en caso de ser necesario.

Finalmente, tomó la palabra Verónica Torres Landa, directora general de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), para invitar a los presentes a unirse a la AMESP. ■

Arturo Ortiz,

CEO DE GRUPO CIPI

Seguridad en América (SEA): ¿Cuáles son los servicios que ofrece CIPI?

Arturo Ortiz (AO): Grupo CIPI cuenta con cuatro divisiones: DIVISIÓN PROTECCIÓN EJECUTIVA, DIVISIÓN SEGURIDAD PRIVADA, DIVISIÓN BLINDAJE y FUNDACIÓN CIPI, con la cual nos sentimos muy orgullosos, puesto que nos ha permitido colaborar en la capacitación de instituciones de seguridad de los tres niveles de gobierno en nuestro país, aunque actualmente ya también los civiles buscan este tipo de capacitación que nosotros brindamos, como manejo táctico, defensa personal, antisecuestro, manejo de armas, etc., para nuestra sorpresa en otros países en los que hemos tenido la fortuna de ir a capacitar, como Serbia y Italia, recientemente son más civiles quienes acuden a nuestros cursos.

SEA: ¿Cómo Grupo CIPI fortalece las habilidades de prevención y protección ejecutiva con sus clientes?

AO: Grupo CIPI está muy enfocada en la profesionalización del escolta, es por eso que nos ocupamos en brindar las mejores doctrinas a nivel nacional e internacional, a lo largo de mi experiencia he tenido la oportunidad de conocer varias de éstas y he podido hacer un extracto de todas ellas para que nuestros cursantes estén capacitados y, puedan servirles en su campo de acción, de nada me sirve ni es mi propósito darles mil técnicas si muchas de ellas no son aplicables, ya que es importante conocer los recursos con los que cuentan para hacer su labor.

SEA: como experto, ¿cuáles considera que son los principales problemas de seguridad en el país?

AO: actualmente nuestro país tiene un grave problema de inseguridad; las estadísticas presentadas y la percepción de seguridad de los ciudadanos no van de la mano, considero que el crimen organizado, homicidios dolosos, feminicidios, y la violencia de género, es algo que nos hace falta trabajar en todas sus aristas, y es necesaria reforzar la prevención primaria, reforzar la cultura de respeto hacia el otro, de esta manera no tendríamos que luchar por los derechos de las personas vulnerables, en la que la mujer, de la orientación de uno u otras banderas que necesitan levantadas exigiendo respeto; la prevención y la atención a estos , temas es sin lugar a dudas lo que como gobierno y ciudadanía nos estamos debiendo.

El secuestro y la extorsión también son temas que dañan y laceran al individuo, son un parteaguas en la vida de cualquiera, una vez que te sucede es complicado recuperarse, es un tema un poco más complejo, pero considero que el gobierno ahora tiene buena atención en este tema, aunque lamentablemente la prevención está muy lejos de lograrse.

SEA: ¿Cuáles son los aspectos más importantes a considerar ante la presencia de un posible secuestro?

AO: ante la primera llamada y duda tratar de localizar al familiar, la buena comunicación entre la familia será primordial, ya que la estrategia de los delincuentes es justo la información que nosotros mismos les brindamos, ellos se vuelven expertos en aprovechar este tipo de información.

Lo segundo es confiar en nuestras autoridades, dar aviso, por supuesto que es lo primero que nos pedirán no hacer, pero es necesario que alguien experto nos asesore en este proceso, ya que ante este hecho podemos llegar a ser más vulnerables emocionalmente.

LOS 5 TIPS DE ARTURO ORTIZ PARA LA PROTECCIÓN DE FUNCIONARIOS

1. Contar con el personal capacitado y certificado para la protección del ejecutivo.
2. Es necesario contar con un análisis de riesgo para definir el nivel de seguridad y el perfil del personal a cargo de su seguridad.
3. Contar con los recursos necesarios para su protección (número de personal, blindaje, inteligencia, etc.), el cual dependerá del análisis de riesgo.
4. La seguridad del ejecutivo también debe ser responsabilidad del mismo, ya que es necesario que éste conozca la función de cada uno de su personal de seguridad y no obstaculizar con tareas no afines a la labor del escolta.
5. Asegurarse que el personal a cargo de su seguridad cuente con una capacitación continua en las diversas áreas de la protección ejecutiva.

SEA: ya que Grupo CIPI es un Centro Evaluador CONOCER, ¿cuáles son sus funciones, qué certificaciones manejan, hacia quiénes están dirigidas, y cómo lograron ser un Centro Evaluador?

AO: es uno de nuestros logros para la certificación de nuestros instructores, así como de nuestros cursantes; también hemos logrado certificarnos con tres ISOS internacionales: ISO9001-2015, ISO18788, y ISO17024, ya que como mencionamos anteriormente nos interesa la profesionalización de nuestros cursantes, estamos muy contentos y orgullosos de estos ISOS, porque muestran nuestro compromiso hacia ellos, el escolta ya está muy lejos de sólo ser el más alto o el más corpulento, ya las certificaciones que brindamos respaldan su preparación. ■

Fotos: Curso High Level Protection, en Serbia.

Arturo Ortiz es experto en seguridad integral, ha colaborado en la seguridad de diversas personalidades de la política, artistas internacionales, empresarios así como ex mandatarios de diversos países, entre los que podemos mencionar Mijaíl Gorbachov, Lech Walesa, Rigoberta Menchú, entre otros.
Se ha profesionalizado en diferentes países lo que le ha permitido crear sus propias técnicas de defensa y protección ejecutiva.

CONSEJOS DE SEGURIDAD PARA LOS DÍAS DE CAMPO Y REUNIONES FAMILIARES

Los fines de semana son una buena oportunidad para convivir con la familia y amigos, para salir de viaje o día de campo o simplemente permanecer en casa sin nada más que hacer, que disfrutar de su tiempo libre. Si usted opta por viajar, por ir de paseo o planear reuniones familiares, no olvide considerar los siguientes aspectos extraídos del "Manual de Seguridad" de David Lee, para que dichas reuniones tengan éxito y no se conviertan en tragedias.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1) **Planeación**. Investigue las rutas de acceso al lugar por visitar, rutas alternas, sitios seguros en el trayecto (costos de casetas de peaje, estaciones de servicio y restaurantes), las recomendaciones de las autoridades y encargados del lugar a visitar, procurando que sea concurrido, tenga presencia de autoridades, y puede buscar noticias sobre sus índices de inseguridad.
2) **Equipamiento.** Adquiera prendas o distintivos con un color llamativo (camisetas, gorras o pañoletas) a fin de identificar perfectamente a los integrantes del grupo y detectar extraños a su alrededor. Considere llevar radios de intercomunicación, así como crear un grupo de WhatsApp con todos los miembros de la familia o amigos, y compartir ahí toda la información del viaje. Agregue herramientas que puedan ser útiles para el paseo, botiquín de primeros auxilios, protector solar, bebidas y alimentos bien conservados.
3) **Vestimenta y transportación.** Sugiera a su grupo que vistan con ropa y calzado cómodos y adecuados al lugar, evitando el uso de tacones y prendas o accesorios de lujo que denoten un alto perfil, así como bolsos grandes; idealmente deben portar una bolsa tipo "cangurera" sujeta a la cintura por debajo de la camisa. Sugiere a los invitados llevar dinero en efectivo, con billetes de baja denominación y cambio suficiente en monedas.
4) **El día de campo.** Programe las actividades de tal manera que salgan y regresen, todos, con luz de día. En el trayecto, considera las recomendaciones de seguridad en caso de que exista algún retén para revisión de vehículos. Al llegar al lugar establezca un punto de reunión para casos de extravío o emergencia. Que cada menor de edad esté acompañado siempre de un adulto.
5) **Seguridad del vehículo.** Estacione su vehículo en un lugar adecuado y vigilado. Evite dejar objetos a la vista, guarde sus cosas en la cajuela, instala o active o coloque sus dispositivos de seguridad: alarma, bastón, inmovilizador. Si hay servicio de "*valet parking*", solicité identificación y pida su boleto sellado. ■

FOMENTE LA CULTURA DE LA SEGURIDAD
Consulte la revista digital en
www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

SEGURIDAD EN AMÉRICA

ÍNDICE DE ANUNCIANTES

COMPROMETIDOS CON LA SEGURIDAD DE NUESTROS CLIENTES Y LA CALIDAD EN EL SERVICIO

Capacidades globales
Con experiencia local

Nuestros servicios:

- **Personal de Seguridad**
- **Asesoría de Riesgos**
  - 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

Nuestro compromiso es contribuir a la construcción de una cultura de trato igualitario y no discriminación y por ello nos sumamos al **Consejo para Prevenir y Eliminar la Discriminación de la Ciudad de México (COPRED)**, *siendo la primera empresa de seguridad privada que se suma a este gran acuerdo.*

GRAN ACUERDO
POR EL TRATO IGUALITARIO
CDMX

Contáctanos

www.ausecurity.mx

(+52) 55 5337 0400

ALLIED UNIVERSAL®
SECURITY SERVICES
There for you.

incluye gastos de envío

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. (Marque así X)

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA 2023	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en banco Banorte, SEA MEDIA GROUP, S. de R. L. de C. V. Cuenta: 1095 5437 37

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe **0721 8001 0955 4373 78**

_____
Firma

DATOS DEL CLIENTE (para el envio de la revista):

Nombre: _____

Compañía: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envío de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato vía: → e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2023

29 | 30 AGOSTO 2023

CENTRO CITIBANAMEX CDMX

CUMBRE DE SEGURIDAD CORPORATIVA

II EDICIÓN

ACTUALICE SUS CONOCIMIENTOS Y CONOZCA LAS NUEVAS TENDENCIAS EN MANEJO DE CRISIS Y CONTINUIDAD DE NEGOCIOS.

13 CONFERENCIAS MAGISTRALES

CON LA PARTICIPACIÓN DE MÁS DE 30 PROFESIONALES DE SEGURIDAD CORPORATIVA

Juan Antonio Bernal, CPP

Director *Senior* de Seguridad y Gestión de Crisis para Latam

Salvador Morales, CPP, CPO, DSE

Senior *Director Security and Resiliency* México y Costa Rica para Flex

Paulina Bustos, CPP

Directora de Seguridad Patrimonial para Clase Azul México

Orlando J. Poncelis, DSE

Corporate Security Manager para Diageo

Gonzalo Enrique Alamillo

Director de Seguridad Integral para Grupo Alsea

Gustavo Melo, CPP, DSE

Corporate Security Manager para Daimler Trucks México

Dora Elena Cortés, CPP

Associate Director of Asset Security & Crisis Management- Latam

Darío Preza

Brand Protection, Security & Resilience Director North Region para Flex

Kael Malo Juvera, CPP

Regional Security Manager para IBM

Enrique de J. Higuera, DSI

Director de Prevención de Riesgos para Médica Sur

Pedro A. Castolo R. CPP

Regional Security Director Latam. Regulatory Compliance para Geodis

Mercedes Escudero

Presidenta de CPTED México ICA Chapter

Ivan Gustavo Islas Castillo

Subdirector de Prevención de Pérdidas para Logística y Transporte

Juan Ramón Becerra

Gerente Nacional de Inteligencia y Prevención del Delito para Grupo Coppel

Francisco Javier Villegas, CPP, DSE, CPO

Subdirector de Protección Patrimonial para Christus Muguerza

Jorge Rodríguez Ramírez, DSE

Director de Seguridad para Soriana

Midori Llanes, CPP

Comisaria de ASIS Capítulo 217 CDMX

Arturo Martínez Avalos, CPP, PCI, DSI

Director general adjunto para MSPV

Oscar Arias

LATAM Regional Security Officer para Danone

Ana Guzmán, DSI

Directora de Seguridad Corporativa para GICSA

Gloria Meléndez Paredes

Directora de Prevención de Pérdidas para Grupo Chedraui

Coral Meza Hidalgo Monroy, CPP

Gerente de Seguridad y Resiliencia Latam para Levi Strauss & Co

Rodrigo Funcia, CPP, DSI

Country Security Manager para Abbvie Farmacéuticos

Fabiola Enríquez, CPP

Gerente general de Prevención para Grupo Presidente

Lourdes Morales

Líder tribu de Prevención para México y Centroamérica

Jorge Luis Acatitla, CPP, DSE, DSI

Director Corporativo de Seguridad Integral para Grupo Xcaret

Erick Mancera

Corporate Director of Security para Karisma Hotels & Resorts

Alicia Sorroza

Directora de Seguridad Corporativa para DHL Supply Chain

Antonio M.-Laib

Head of Security, Latin America Senior Director, Deutsche Post DHL Group

José Arturo Moreno Ferrusca

Gerente de Prevención de Pérdidas para Palacio de Hierro

Marco Alejandro Hernández Licona DSI

Director de Prevención de Pérdidas y Siniestros para Grupo Salinas.

Carlos Mera Cepeda

Gerente de Seguridad para *McDonald's*

PARA MÁS INFORMACIÓN CONTÁCTANOS

55-5965-4582

telemarketing@seguridadenamerica.com.mx

CONTROL · SISSA · CIA CAPITAL · Density · SCATI · Tracking Systems · Altair · Protectio · M36 · PEOPLE TRUST · PSI · DILME

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.®

Guardias, guardias armados, custodias, custodias blindadas y custodias armada.

Cobertura a nivel nacional.

www.sepsisa.com.mx comercial@sepsisa.com.mx 55 5351 0402