SEGURIDAD® EN AMÉRICA

Año 23 / No.136
Enero-Febrero

Especial:

Seguridad en *e-commerce*

Seguridad en hospitales

Reportaje: Videovigilancia y drones

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

ASIS INTERNATIONAL

redconocer

ISO

BAC

ema
entidad mexicana de acreditación, a.c.

ANERPV

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

Año 23 / No. 136 / enero-febrero / 2023

Portada:
MULTIPROSEG

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:

EDITORIAL

El periodista mexicano Ciro Gómez Leyva sufrió en la noche del 15 de diciembre del 2022 un ataque armado cuando viajaba en su camioneta, en Ciudad de México. “A las 11:10 pm, a 200 metros de mi casa, dos personas en una motocicleta me dispararon, al parecer con la clara intención de matarme. Me salvó el blindaje de mi camioneta que yo manejaba y ya enteré del asunto a las autoridades”, señaló a los medios.

Luego del atentado con arma de fuego que sufrió el periodista, vale la pena hablar de dos temas: las agresiones contra periodistas en México y la importancia del blindaje automotriz.

BLINDAJE DE AUTOS

La empresa de blindajes certificados que realizó de dicho vehículo, miembro de la Asociación Mexicana de Blindadores de Automotores (AMBA), lanzó un comunicado donde recordó la importancia de considerar materiales de calidad empleados en el blindaje.

“Quedó comprobado que la calidad de los materiales empleados en el blindaje automotor es primordial, pues deben responder para lo que fueron creados: proteger y salvar vidas. Tal es el caso en el reciente atentado a tiros contra un connotado periodista mexicano, quien salió ileso al viajar en una camioneta acorazada por la empresa miembro de la AMBA”.

Por su parte, el presidente de la AMBA, Esteban Hernández López, destacó la importancia de adquirir unidades blindadas, sobre todo cuando prolifera la venta de automotores acorazonados con materiales “pirata” y la aparición de empresas de dudosa procedencia.

Mencionó que el blindaje más comercializado en México es el Nivel III, el cual llega hasta el 65% de participación en el mercado, protegiendo contra ataques perpetrados con armas cortas. Los precios del blindaje en este nivel que son fabricados con empresas reconocidas y materiales certificados, oscilan para los vehículos sedanes entre 33 y 43 mil dólares y los SUV entre 35 y 45 mil dólares.

VIOLENCIA CONTRA PERIODISTAS EN MÉXICO

Los profesionales de la comunicación son un blanco seguido de los pistoleros en México, el país más mortífero del mundo para los reporteros, sin estar en una situación de guerra. Es la forma que usan el crimen organizado, los empresarios o los políticos para silenciar voces incómodas. En esta ocasión, el ataque, afortunadamente sin que haya conseguido su objetivo, le tocó a Gómez Leyva.

En 2022, México alcanzó una cifra récord de 17 muertes de periodistas, 12 de ellos directamente por su trabajo, según la asociación Artículo 19. Esto, pese a que algunos han pedido protección del Estado para salvaguardar su vida.

En un informe sobre el primer semestre de este año, Artículo 19 estima que los actos de intimidación y hostigamiento contra los reporteros han aumentado un 52% respecto al mismo periodo de 2016 y señala a las autoridades mexicanas de todos los niveles como los principales agresores.

¿Usted qué opina, estimado lector?

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 Hermelindo Rodríguez Sánchez, CPO, CSSM, DSI, DES, CEO y fundador de la Consultoría en Seguridad y Protección Integral (Cosepri), 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

Rafael Abreu Ponce,

director general de Seguridad Privada Gorat

¿Qué aspectos considera que se requieren para mejorar la seguridad del país, antes de militarizarlo?

Que los gobiernos municipales y estatales asuman su responsabilidad, destinando recursos a la capacitación, equipamiento y dignificación de la cartera policial. Trabajando con la sociedad para revalorar y reivindicar la labor de los oficiales. Mejorar sus condiciones salariales, generar alianzas con los empresarios locales para dotar de beneficios en sus comercios a los policías, entre muchas otras. Por su parte, la seguridad privada es un aliado para fortalecer a cualquier país en coadyuvancia con las autoridades. ■

AppController

SISTEMA DE GESTIÓN

DE SERVICIOS OPERATIVOS

PARA HOSPITALES

CON APPCONTROLLER PODRÁS:

- *Facilitar el balance financiero.*
- *Optimizar trámites y servicios administrativos.*
- *Agilizar la documentación de los pacientes.*
- *Agilizar las labores del personal médico.*

Contáctanos y permítenos brindarte una solución modular que elevará a otro nivel la gestión y control de tus procesos hospitalarios.

¡CONOCE MÁS!

SISSA DIGITAL

55 6651 0200

ÍNDICE

enero-febrero 2023

ÍNDICE

enero-febrero 2023

ESPECIAL

LA ENTREVISTA CENTRAL

SEGURIDAD PRIVADA

SEGURIDAD PUBLICA

EL PROFESIONAL OPINA

FOROS Y EVENTOS

ENTREVISTA CON EL EXPERTO

NOVEDADES DE LA INDUSTRIA

TIPS

MILESTONE KITE

PARA PEQUEÑAS Y MEDIANAS EMPRESAS Y ORGANIZACIONES

DINAMARCA

Cimentada en el ADN de la plataforma abierta de dispositivos de Milestone, Milestone Kite™ es compatible con más de seis mil modelos de cámaras de más de 100 fabricantes

Milestone Kite™, con tecnología de Arcules, es una solución en la Nube, fácil de implementar, segura, escalable y económica, que ofrece actualizaciones automáticas y no requiere mantenimiento

Milestone Systems continúa expandiendo su oferta de soluciones de tecnología de video basadas en datos, con instalación local, de Nube híbrida y nativa. El nuevo servicio VSaaS (videovigilancia como servicio) Milestone Kite™ complementa la implementación de XProtect en AWS (Amazon Web Services). Milestone Kite™, la oferta en la Nube más reciente de Milestone, es una solución fácil de implementar, segura y escalable para la gestión de video (VMS) en la Nube, orientada a pequeñas y medianas empresas. En este servicio la implementación de XProtect en AWS ha sido optimizada para el mercado empresarial.

Milestone Kite™, con tecnología de Arcules, es una solución en la Nube, fácil de implementar, segura, escalable y económica, que ofrece actualizaciones automáticas y no requiere mantenimiento. Es la opción ideal para organizaciones con múltiples sedes, con implementación de sitio único o multisitio, que necesitan un método fácil para gestionar de forma centralizada todos sus sitios en un sistema unificado. Los negocios y las compañías de alto valor, menor complejidad y varias ubicaciones geográficas, como bancos, cadenas minoristas, escuelas y edificios residenciales, pronto descubrirán que Milestone Kite™ es la opción ideal para sus necesidades de seguridad.

"Milestone comprende la importancia de ofrecer una amplia variedad de soluciones de Nube híbrida para responder a los diferentes segmentos del mercado de la seguridad. Llevamos muchos años invirtiendo en ofertas de VSaaS (videovigilancia como servicio) para prepararnos para el futuro. Un número cada vez mayor de pequeñas y medianas empresas buscan un VMS en la Nube que sea fácil de implementar y de usar, que tenga pocos requerimientos de ancho de banda, que sea escalable entre ubicaciones y que sea seguro. Para ellas, Milestone Kite es la opción ideal. Milestone y Arcules han unido fuerzas para atender este segmento del mercado", aseguró Thomas Jensen, director ejecutivo de Milestone Systems.

COPARMEX®
CIUDAD DE MÉXICO

En COPARMEX CDMX bajar la cortina ¡no es opción!

www.coparmexcdmx.org.mx

¡AFÍLIATE!

PLATAFORMA CONECTA, CRÉDITOS, NETWORKING, E-COMMERCE, ETC.

COPARMEX Ciudad de México

La causa prioritaria de la Coparmex CDMX ha sido apoyar a las empresas para que por ningún motivo bajen la cortina y sigan creando los empleos que demandan las familias capitalinas.

Armando Zúñiga Salinas ha venido trabajando de la mano con representantes diversos de la Cámara de Diputados para dar impulso a la primera Ley Federal del Emprendedor, para que quede establecido en un marco legal el necesario apoyo a las y los emprendedores, en acciones concretas como capacitación y créditos, así como el fomento a las ideas emprendedoras desde las universidades.

Si quieres aprovechar todos los beneficios que ofrece COPARMEX CDMX para hacer crecer tu empresa y formar parte de las mujeres y hombres que de manera comprometida están buscando transformar a la Ciudad desde su actividad empresarial, entra a:
www.coparmexcdmx.org.mx o llama al 55 4184 2371.

55 5515 2511

Sponsor
IPS
GRUPO IPS

"Arcules se fundó con el propósito de estar a la vanguardia en innovación, centrándose en la creación de una nueva oferta en la Nube que fuera potente y fácil de usar para organizaciones más pequeñas o más grandes, geográficamente dispersas, con sucursales o ubicaciones remotas", Andreas Pattersson

"Arcules se fundó con el propósito de estar a la vanguardia en innovación, centrándose en la creación de una nueva oferta en la Nube que fuera potente y fácil de usar para organizaciones más pequeñas o más grandes, geográficamente dispersas, con sucursales o ubicaciones remotas. Lo que hemos logrado es una solución de Nube nativa preparada para responder a los desafíos futuros, que es escalable y que se caracteriza por su facilidad de uso e implementación. Los clientes de Milestone ya no necesitan desplazarse físicamente hasta múltiples ubicaciones ni dedicar tiempo al mantenimiento, basta con

que instalen la pasarela. Milestone Kite™ integrará automáticamente los datos de control de acceso con los datos de video entrantes a fin de permitir la verificación de video de acceso, visualizar las imágenes de las cámaras y lograr un reconocimiento inmediato del entorno", concluyó Andreas Pettersson, director ejecutivo de Arcules.

ACERCA DE MILESTONE KITE™

Milestone Kite™ es una solución de Nube nativa de videovigilancia como servicio, diseñada para pequeñas y medianas empresas y organizaciones. Cimentada en el ADN de la plataforma abierta de dispositivos de Milestone, Milestone Kite™ es compatible con más de seis mil modelos de cámaras de más de 100 fabricantes.

Milestone Kite™ es una solución de rápida instalación, fácil implementación y ágil escalabilidad, características que la hacen igualmente apta para implementaciones de vigilancia en uno o múltiples sitios. Milestone Kite™ ofrece además almacenamiento de video híbrido flexible, que requiere poco ancho de banda y permite almacenar datos de video en la Nube o de forma local, según el ancho de banda disponible.

La solución, diseñada pensando en la ciberseguridad, ofrece actualizaciones de seguridad continuas y respaldo global de protección contra fallos. Viene con una opción para almacenar datos de video en el borde de red y cuenta con detección de personas y vehículos, mapas de calor y búsqueda con propósitos judiciales, características que convierten el video en datos inteligentes que mejoran la seguridad y aumentan la eficiencia operativa. ■

Fotos: Milestone Systems

Ellos Entretienen.

NOSOTROS PROTEGEMOS.

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

PD 6500i PINPOINT DETECTION

GARRETT

PLANTA SOLAR HÍBRIDA EN CUAMBA, MOZAMBIQUE

El proyecto, de 32 millones de dólares, constituye un hito y un gran avance para el futuro del almacenamiento de la energía a gran escala en Mozambique

MOZAMBIQUE

Esta planta solar híbrida está situada en la ciudad de Cuamba (Mozambique) y es el primer proyecto del país que integra un sistema de almacenamiento de energía a escala de servicio público

RETO

Bajo el lema "Energía para todos", el Gobierno de Mozambique lleva a cabo la construcción de esta planta solar híbrida cuyo objetivo es el acceso universal a la energía para 2030, en un nuevo paso hacia un futuro de energía limpia.

Esta planta solar híbrida está situada en la ciudad de Cuamba (Mozambique) y es el primer proyecto del país que integra un sistema de almacenamiento de energía a escala de servicio público.

El diseño, suministro y puesta en marcha de esta planta solar es ejecutado por la empresa española TSK, compañía líder en ejecución de proyectos EPC o "llave en mano" en los campos industriales, energéticos y medio ambientales. Desde hace más de 8 años, TSK tiene presencia en el país.

Para la protección física de esta planta solar, TSK cuenta con el apoyo de SCATI, fabricante de sistemas de video inteligente, con el que desde hace años colabora para proteger los proyectos en los que participa.

TSK

SOLUCIÓN

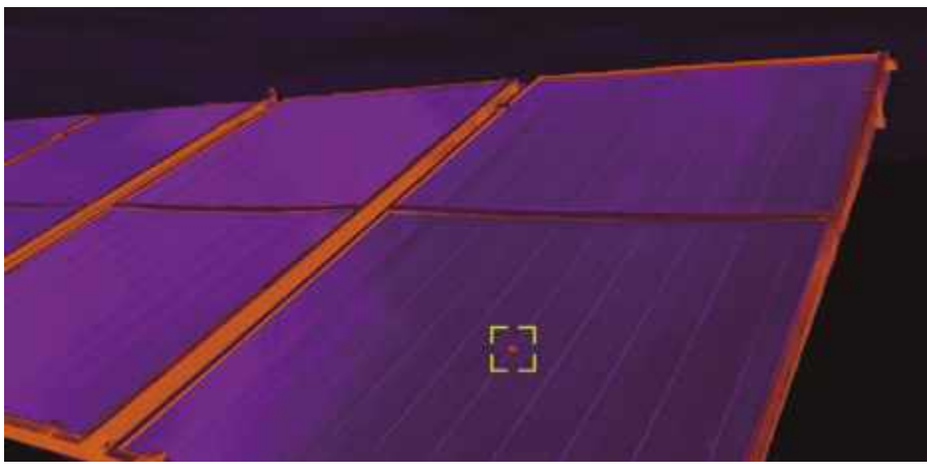
Para la protección y el control total de la planta, se han instalado 37 cámaras térmicas con diferentes lentes modelo SET-14C10-EYA y dos cámaras domo PTZ para exteriores de cuatro megapixeles.

Estas cámaras térmicas son utilizadas principalmente para detectar puntos calientes que se desarrollan debido a celdas defectuosas en los paneles solares.

Los cambios de intensidad de la radiación solar en los parques solares pueden provocar anomalías térmicas que, si no son controladas de una forma minuciosa, pueden tener un impacto negativo en el módulo completo.

Estas cámaras térmicas permiten visualizar imágenes bajo cualquier condición lumínica, climatológica o ambiental, ofreciendo una gran calidad de imagen.

Por otro lado, estas cámaras térmicas también permiten una protección perimetral de la planta solar, logrando mantener a intrusos o personas no autorizadas alejadas y son capaces de detectar incendios enviando alertas en tiempo real para poder reaccionar a tiempo, logrando incluso anticipar situaciones de riesgo con la máxima fiabilidad.



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

Las cámaras térmicas también permiten una protección perimetral de la planta solar, logrando mantener a intrusos o personas no autorizadas alejadas y son capaces de detectar incendios enviando alertas en tiempo real para poder reaccionar a tiempo

RETO

Bajo el lema "Energía para todos", el Gobierno de Mozambique lleva a cabo la construcción de esta planta solar híbrida cuyo objetivo es el acceso universal a la energía para 2030, en un nuevo paso hacia un futuro de energía limpia.

Esta planta solar híbrida está situada en la ciudad de Cuamba (Mozambique) y es el primer proyecto del país que integra un sistema de almacenamiento de energía a escala de servicio público.

El diseño, suministro y puesta en marcha de esta planta solar es ejecutado por la empresa española TSK, compañía líder en ejecución de proyectos EPC o "llave en mano" en los campos industriales, energéticos y medio ambientales. Desde hace más de 8 años, TSK tiene presencia en el país.

Para la protección física de esta planta solar, TSK cuenta con el apoyo de SCATI, fabricante de sistemas de video inteligente, con el que desde hace años colabora para proteger los proyectos en los que participa.

SOLUCIÓN

Para la protección y el control total de la planta, se han instalado 37 cámaras térmicas con diferentes lentes modelo SET-14C10-EYA y dos cámaras domo PTZ para exteriores de cuatro megapixeles.

Estas cámaras térmicas son utilizadas principalmente para detectar puntos calientes que se desarrollan debido a celdas defectuosas en los paneles solares.

Los cambios de intensidad de la radiación solar en los parques solares pueden provocar anomalías térmicas que, si no son controladas de una forma minuciosa, pueden tener un impacto negativo en el módulo completo.

Estas cámaras térmicas permiten visualizar imágenes bajo cualquier condición lumínica, climatológica o ambiental, ofreciendo una gran calidad de imagen.

Por otro lado, estas cámaras térmicas también permiten una protección perimetral de la planta solar, logrando mantener a intrusos o personas no autorizadas alejadas y son capaces de detectar incendios enviando alertas en tiempo real para poder reaccionar a tiempo, logrando incluso anticipar situaciones de riesgo con la máxima fiabilidad.

Estas cámaras son gestionadas por un Sistema de Gestión de Video (VMS) SCATI FENIX que permite una conexión de hasta 64 cámaras IP y con una capacidad de gestión de hasta 100 clientes simultáneamente a través del CMS SCATI FENIX.

Cuando una cámara detecta una fuente de calor no controlada, envía una alerta para que los operadores puedan verificarla y tomen medidas para evitar incidentes que pueden suponer pérdidas millonarias.

BENEFICIOS

TSK vuelve a apostar por la tecnología de SCATI, invirtiendo en sistemas que le permiten no sólo proteger las instalaciones de este proyecto de actos vandálicos o situaciones peligrosas. Con las soluciones de SCATI también es capaz de controlar y prevenir todos los problemas que pueden ocasionarse por fallos en los paneles fotovoltaicos, de una manera más eficiente y sostenible.

La alta disponibilidad de los sistemas de grabación de SCATI permite que el cliente pueda acceder a imágenes, datos y almacenamiento incluso en las situaciones más críticas donde los servidores puedan desconectarse.

SCATI ofrece una solución abierta y escalable que puede integrarse con otros sistemas por lo que el cliente puede incorporar nuevos sistemas de video en cualquier momento sin realizar inversiones adicionales. ■

Enlace al video:

https://www.youtube.com/watch?v=-NOW6bFiqs0

Fuente y fotos: SCATI

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

Soluciones Integrales para RASTREO SATELITAL

Recuperación 98.5%
Aviso en menos de 30 minutos*

TRUST ID

VERIFICACIÓN Y CERTIFICACIÓN DE PERSONAL

EXPERTOS EN:

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

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

¿Estás seguro de quién maneja tu Logística?

TRUST ID es una Solución de Grupo UDA y Tracking Systems dedicada a la validación de personal logístico como: Operadores, Monitoristas y Técnicos Instaladores.

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

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

Contáctanos

55-5374-9320

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

Socio Amesis
amesis.org.mx

- Análisis de datos de confianza en línea.
- Validación Fotográfica y Prueba de Vida.
- Análisis de contenido en declaraciones.
- Estudio Socioeconómico.
- Validación de antecedentes laborales.
- Antidoping y Polígrafo.

DESCARGA LA APP

UNA SOLUCIÓN: Grupo UDA

trustid.mx

55 5374 9340

55 4141 6451

CUATRO PUNTOS QUE AYUDAN A MEJORAR LA EXPERIENCIA DEL CLIENTE EN TIENDAS

Las soluciones de videovigilancia pueden ser herramientas muy eficaces para recopilar y procesar datos numéricos que ayuden a potenciar las experiencias de los clientes

Foto: Freepik

MÉXICO

Con la pandemia, la población se vio obligada a permanecer en casa durante el 2020 o incluso hasta 2021, por lo que, a pesar del crecimiento de las ventas *online*, los clientes están en busca de nuevas experiencias de compra en el mundo presencial. Por ello, ahora es necesario consolidar la efectividad de las experiencias de compras físicas con estrategias de *marketing* y soluciones tecnológicas que aporten una mejor experiencia de compra a los clientes.

Según la ANTAD (Asociación Nacional de Tiendas de Autoservicio y Departamentales), hasta el cierre de 2021 se reportaron más de 46.6 mil tiendas en nuestro país, para las que es necesario mejorar el rendimiento a través del análisis y actualización de los datos que puedan recopilar en sus diferentes pisos de venta, y de la utilización de herramientas con las que puedan brindar seguridad y mejores experiencias a sus clientes.

Axis ofrece una gran variedad de soluciones de videovigilancia para recopilar datos y que ayudan a garantizar una buena experiencia de compra, ante lo cual Alejandro Aguirre, *National Sales Manager* en Axis Communications, resaltó los siguientes puntos:

1. **Filas en cajas:** detecta la cantidad de personas en una fila y busca asignar más personal cuando sea necesario de forma automática, con altavoces en tienda o alertas personalizables.
2. **Zonas de exposición de artículos de gran valor:** detectan cuando una persona está dando vueltas por las zonas con artículos de mayor valor y avisa a los empleados con alertas de audio.
3. **Zona de ventas:** identifica las áreas en las que permanecen más tiempo los clientes y optimiza la distribución de la zona de ventas, enviando mensajes de audio específicos o anuncios promocionales en el momento y el lugar adecuados.
4. **Entradas y salidas:** informa sobre la cantidad de personas que entran y salen del establecimiento para identificar los momentos de mayor actividad, asignar personal de manera eficiente y optimizar el servicio.

De acuerdo con el estudio "El futuro del retail" de Euromonitor, en los próximos cinco años el comercio electrónico representará el 58% del crecimiento total de las ventas, mientras que el 42% restante es de las tiendas físicas, por lo que estas últimas están lejos de desaparecer; por tanto, es necesario enfocarse y encaminarse hacia el crecimiento y satisfacción del cliente.

"Nuestras soluciones siempre buscan resolver los retos a los que se enfrenta la industria, por ejemplo, la analítica AXIS Store Reporter genera estadísticas, representaciones gráficas e informes sobre el tránsito de la tienda, la longitud de las filas o los niveles de ocupación, entre otros aspectos", destacó Aguirre. "Además nuestra tecnología opera con estándares abiertos, por lo que es compatible con un gran número de aplicaciones de terceros y la colaboración de nuestros socios nos permite crear soluciones a la medida de sus necesidades".

Sin duda, en América Latina muchos consumidores siguen anhelando la experiencia de compra en una tienda, ver y tocar los diferentes productos; por eso, el servicio al cliente y su permanencia en los diferentes locales comerciales debe cumplir con sus expectativas para realizar las mejores compras, ayudarles a tener la mejor orientación de la tienda, garantizar seguridad y la mejor atención. ■

Fuente: Axis Communications

GSI
SEGURIDAD PRIVADA

GSI Seguridad Privada, S.A. de C.V.
Profesionales en Seguridad Privada

Oficiales de Seguridad

- *Servicios de contratación segura.*
- *Seguridad móvil al comercio y zona residencial.*
- *Capacitación y formación de equipos de seguridad.*

- *Oficiales de seguridad.*
- *Protección ejecutiva.*
- *Rastreo y monitoreo.*
- *Oficiales de seguridad armados.*

SOMOS GRUPO GSI
Orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx
atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

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

VIDEOVIGILANCIA, CLAVE PARA FAVORECER LA SEGURIDAD PÚBLICA DE GRANDES CIUDADES

Foto: Freepik

Un sistema de videovigilancia inteligente genera grandes beneficios a la movilidad de una ciudad, porque reduce los tiempos de traslado y la emisión de contaminantes y, sobre todo, mejora la seguridad pública

Todas las ciudades se encuentran en un constante e interminable proceso de evolución y transformación. Actualmente, el 55 por ciento de las personas en el mundo habita en ellas y datos de la Organización de las Naciones Unidas estiman que esta proporción aumentará hasta en un 13 por ciento para el 2050. Estas ciudades han demostrado que, al utilizar herramientas de videovigilancia, logran mejorar la gestión del tráfico y la movilidad urbana, obteniendo calles más seguras y eficientes para todos los transeúntes. Las soluciones de videovigilancia, junto con el análisis de video, son claves para monitorear carreteras, intersecciones y la movilidad de las personas a pie a través de la ciudad.

El análisis de video logra que las soluciones de videovigilancia reconozcan eventos extraordinarios de tránsito, accidentes y embotellamientos, emitiendo a las autoridades alertas en tiempo real con las que puedan actuar adecuadamente y de manera oportuna, enviando ayuda, planificando rutas alternativas o retirando los vehículos colapsados; proporcionando así una clara solución a estos problemas de las grandes urbes.

"El paradigma de las ciudades inteligentes se puede crear con enfoques cotidianos de futuros urbanos que ayuden a fomentar nuevas formas de urbanismo y economías basadas en el conocimiento, pasando por el desarrollo y la planeación urbana en tiempo real, hasta el aprovechamiento de soluciones tecnológicas como principal socio en la comprensión de problemas; teniendo siempre a sus ciudadanos y necesidades reales en el centro de su transformación", comentó Diana Ardila, gerente de Ventas Regionales para Sudamérica en Axis Communications.

Estimaciones de la firma Marketsandmarkets indican que el mercado global del análisis de video tendrá un valor de 20 mil 300 millones de dólares para 2027, lo que sin duda ayudará a dar solución a los problemas urbanos que se viven en el presente y que se esperan para el futuro, y que apoyarán al crecimiento de las ciudades inteligentes.

Los sistemas de vigilancia de Axis Communications logran una vista en tiempo real del flujo de tráfico y los incidentes, incluidos los accidentes, filas de gestión de multitudes, que pueden interrumpir el flujo libre de movimientos en una ciudad, incluyendo la gestión de estacionamiento que se puede mejorar sustancialmente con estas soluciones.

UN ELEMENTO DE SEGURIDAD PARA LAS CIUDADES MÓVILES

Las soluciones de videovigilancia logran convertirse en un mecanismo para resolver y prevenir hechos criminales, garantizar y gestionar el orden y la convivencia en las ciudades, lo que sin duda ha logrado generar un crecimiento, lo cual se atribuye a las iniciativas gubernamentales para adoptar tecnologías emergentes y mejorar la infraestructura de seguridad pública de las grandes ciudades.

Durante la Cumbre de Negocios 2022, realizada en Querétaro, se comentó sobre la importancia de contar con una estrategia nacional que permita a las ciudades reducir los costos en materia de accesibilidad y seguridad pública que ayude a impulsarlas hacia la tecnología inteligente, además de una ley de ciberseguridad nacional, con lo que se podrían aprovechar al máximo las ventajas que proporciona la inteligencia artificial, las soluciones de video, el Internet, entre otros.

El uso de las nuevas tecnologías es un arma eficaz para superar los desafíos de las grandes ciudades. Las 50 mayores urbes del mundo destinaron en 2018 cerca de 80 mil millones de dólares a tecnologías de ciudades inteligentes, según IDC. ■

Fuente: Axis Communications

DOORMAN

ALGUIEN EN QUIEN CONFIAR

SEGURIDAD PRIVADA

PARTE MUY IMPORTANTE DENTRO DE NUESTRA ORGANIZACIoN ES LA CAPACITACIoN, QUE SON 30 HORAS DIVIDIDAS EN 5 SECCIONES:

- Combate de incendios
- Primeros Auxilios
- Defensa Personal
- Protección Civil
- Atención al cliente
- Servicios de Seguridad Integral

En Doorman, estamos comprometidos por salvaguardar tu seguridad adaptándonos a los constantes cambios y condiciones del país, ofreciendo como empresa de seguridad, una propuesta integral de servicios, capacitando constantemente a nuestros elementos, así como actualizándonos en nuevas tecnologías de la seguridad.

AMESP · ASIS INTERNATIONAL · COPARMEX · AMEXSI

25 AÑOS

CONTÁCTANOS

T. 5555468229 | 5555367725 | 5572589139 | 5556519580

Cóndor No. 100, Col. Los Alpes, Álvaro Obregón, CP 01010, CDMX

www.doorman.com.mx

VIDEOVIGILANCIA EN LOS ESTADIOS: AL SERVICIO DE LOS AFICIONADOS PARA QUE NO SUCEDA "NADA"

Los beneficios de la videovigilancia son muchos, desde garantizar la seguridad y protección para la gente, mejorar los sistemas de prevención de pérdidas, prevenir responsabilidades potenciales antes de que ocurran, utilizar el material para mejorar la capacitación del personal y la optimización de las labores del personal, entre otros

Foto: Freepik

MÉXICO | Manuel Zamudio

El mundial de futbol, así como todos los eventos deportivos, de entretenimiento, y de cualquier índole que se realicen en grandes recintos como estadios, requieren un gran trabajo previo y detrás, desde la logística hasta la seguridad de los asistentes.

En temas de seguridad, cuando no sucede "algo" es difícil evaluar el resultado de un buen trabajo. Mientras más tiempo pase sin suceder ese "algo", existen mayores probabilidades de que suceda. ¿Y qué puede suceder? Bueno, hagamos una lista de los incidentes que ya han ocurrido: desde el ingreso de personas o grupos que representan una amenaza a la seguridad de los asistentes, conductas no deseadas, violencia, venta y/o consumo de drogas o de alcohol a menores, entro otras.

Algunas otras situaciones que pueden ocurrir son los comportamientos negligentes de los propios organizadores, que pueden provocar una sanción al estadio, como permitir el ingreso de armas, errores en el cálculo de aforo o fallas en el control de accesos, en la protección de los perímetros, la obstrucción de rutas de evacuación, escaleras, corredores, tolerancia al vandalismo, el comercio ilegal, etc. Todo esto debe ser considerado previamente, y apoyarnos en la tecnología para prevenir estos incidentes, y más, en este caso los sistemas de videovigilancia.

HERRAMIENTA DE APOYO

Si bien, los sistemas de videovigilancia no reemplazan al personal de seguridad ni a la gestión de esta, se trata de una herramienta que puede ser muy útil en la detección de los incidentes o problemas potenciales, así como para evaluar la situación al momento e investigar cualquier eventualidad, con el fin de deslindar responsabilidades o simplemente como parte del proceso de mejora continua.

Un ejemplo que puedo compartir es del estadio Centenario de Uruguay que, desde 2018, combinó cámaras IP con sistemas de reconocimiento facial, lo que ha permitido la identificación y restricción de acceso al estadio a individuos que se han visto involucrados en robos, peleas o están vinculados al tráfico de drogas.

A través de este sistema, el personal de seguridad del recinto recibe notificaciones automáticas generadas mediante verificación cruzada de antecedentes, que permiten comprobar la presencia de alborotadores o personas que tienen prohibida la entrada al estadio, todo gracias a una lista unificada que comparten la Asociación Uruguaya de Fútbol, el Ministerio del Interior y los clubes de futbol. Este sistema permite efectuar 25 identificaciones faciales

por segundo y adoptar las medidas necesarias, lo que ha cambiado el comportamiento de los espectadores del futbol en Uruguay.

Después de ver hasta 200 personas detenidas en distintos incidentes en el mismo partido de futbol, este número se ha reducido a una media de 10 detenciones por partido. Ahora el público sabe que, si algo sucede, habrá pruebas documentales y consecuencias. Esta nueva realidad ha animado a las familias con niños y adultos mayores —que, poco a poco, habían dejado de acudir a las gradas por sentirse inseguras— a volver a disfrutar de los partidos de futbol.

Además de evitar el daño a la imagen pública del estadio y de los organizadores, y por supuesto, de reducir el riesgo que corren los asistentes, el sistema de videovigilancia permite la optimización de procesos, la automatización de algunas actividades, búsquedas eficientes, alertas tempranas y la generación de datos estadísticos que permitan enriquecer la experiencia de todos los que participan en los eventos.

Los sistemas de seguridad existentes tienen la capacidad de visualizar situaciones e incluso de detectarlas automáticamente mediante analíticas de video que son aplicaciones de *software* que generan automáticamente descripciones de lo que ocurre en el video, es decir, "metadatos". Esa información puede utilizarse para enumerar personas, coches y otros objetos detectados en el flujo de video, así como su aspecto y movimiento. Después, puede usarse para ejecutar acciones, como decidir si se envía una notificación al personal de seguridad o si se inicia una investigación.

BENEFICIOS DE LA VIDEOVIGILANCIA

Un ejemplo de los beneficios de las soluciones de videovigilancia fue en la ciudad de Houston, en Estados Unidos, que en 2017 se preparaba para recibir a más de un millón de asistentes y garantizar la seguridad del Super Bowl, así como las atracciones del centro urbano. Sin embargo, las estructuras móviles y temporales habían dado lugar a un despliegue caótico, y las interferencias de la conexión inalámbrica en el centro de la ciudad suponían un problema a la hora de transmitir los datos de las cámaras a los dos puestos de control principales de la ciudad: el Centro de Delitos en vivo y el Centro de Operaciones de Emergencia.

Una amplia cantidad de agencias gubernamentales y locales utilizaron el sistema general de cámaras fijas, PTZ y térmicas para sus propias necesidades. Entre ellas se encontraban los cuerpos de policía, bomberos, gestión de emergencias y transporte. El evento fue un éxito para la ciudad de Houston. Las cámaras y la red de socios añadieron una necesaria herramienta de análisis que, además de respaldar las operaciones terrestres relacionadas con el acontecimiento, estableció la plataforma con la cual pueden seguir avanzando en el uso de tecnología para fines generales de protección en la ciudad.

Además del uso de los equipos para ayudar en múltiples tareas de seguridad, supervisión de la operación de los recintos y para la protección de la gente, también se puede utilizar la infraestructura de videovigilancia para otros fines, como lo hace la Liga de Hockey de Ontario. Para facilitar la toma de decisiones sobre goles y sanciones (caos entre bastones, patines y jugadores, el disco con velocidades superiores a los 145 km/h), se instalaron cámaras de alta resolución y de 60 fps, *software* de administración de video (VMS), señales de video de las cámaras de televisión, incluyendo el sistema de repetición instantánea. Todo eso permitió a los jueces revisar cada penalti y cada gol desde varios ángulos de cámara antes de tomar la decisión final sobre una acción del árbitro.

Como vemos, los beneficios de la videovigilancia son muchos, desde garantizar la seguridad y protección para la gente, mejorar los sistemas de prevención de pérdidas, prevenir responsabilidades potenciales antes de que ocurran, utilizar el material para mejorar la capacitación del personal y la optimización de las labores del personal, entre otros. Además, el uso de tecnología moderna no sólo minimiza posibles multas, sino que mejora la experiencia de los aficionados, socios y proveedores, lo que incrementa, la confianza, la demanda y la asistencia a los eventos. ■

El estadio Centenario de Uruguay, desde 2018, combinó cámaras IP con sistemas de reconocimiento facial, lo que ha permitido la identificación y restricción de acceso al estadio a individuos que se han visto involucrados en robos, peleas o están vinculados al tráfico de drogas

Foto: Freepik

Manuel Zamudio, gerente de Asociaciones Industriales para el Norte de América Latina y el Caribe en Axis Communications.

Más sobre el autor:

Foto: Creativeart - Freepik

OJOS EN EL CIELO

Los Vehículos Aéreos No Tripulados (VANT), conocidos como "drones", han mejorado las capacidades de vigilancia para seguridad, en particular en cuanto a la rapidez y amplitud en la cobertura de un espacio. Pero como todo recuso de tecnología, tiene ciertas características de funcionalidad que imponen condiciones a su aplicación a las tareas de vigilancia, y por ende demandan ciertas destrezas y habilidades en el usuario-observador

Foto: Wikimedia

Los drones ofrecen una alternativa para la observación aérea con mejores perspectivas de eficiencia en términos de costo - beneficio ya que, al no requerir los sistemas de supervivencia para una tripulación, puede incrementar su carga útil o bien reducir sus dimensiones y costo

MÉXICO | David Chong Chong

La observación aérea ha sido un recurso de vigilancia muy importante por la mayor amplitud de visualización que se proporciona desde la altura, aunque con limitaciones en la apreciación de detalles a la distancia, y ha sido utilizado con fines primordialmente militares a partir el surgimiento de los globos aerostáticos desde la Batalla de Fleurus (1794) durante las guerras revolucionaras francesas, pasando por la Guerra de Secesión (1981 - 1865) en Norteamérica y la Guerra Franco Prusiana (1870 – 1871) y hasta los inicios de la Primera Guerra Mundial (1914).

Con el advenimiento del aeroplano, durante la Primera Guerra Mundial (1914 – 1918), la observación aérea adquirió nuevas dimensiones, por el uso de equipos como el biplano Caudron G3 de Francia, pasando por el PBY Catalina en la Segunda Guerra Mundial, hasta los más sofisticados como los Lockheed U-2 y el SR-71 "Blñackbird" norteamericanos, y los An 30 y M 55 soviéticos.


Caudron


PBY


U - 2


SR - 71


An 30


M - 55

Fotos: Wikimedia

La autonomía se materializa por el tiempo de vuelo, que en principio está determinado por la capacidad de la planta motriz del vehículo, pero decrece por la magnitud de la carga útil y la complejidad de las maniobras como los patrones y velocidad de sobrevuelo, el tiempo estacionario, la altitud y el arrastre

De hecho, cualquier vehículo aéreo, tripulado o no con personal humano, puede ser utilizado como plataforma de observación aérea, sólo con instalarle dispositivos de vigilancia, que pueden ser, tanto de tipo visual (cámaras), como de señales electrónicas, como es el caso del RC-135.

Fotos: Wikimedia

Las plataformas más avanzadas para la observación aérea son las satelitales, que pueden ser con fines militares como los modelos Key Hole norteamericanos o el Razdan soviético, aunque también se destinan a usos no militares, como el monitoreo meteorológico.

Fotos: Wikimedia

Los drones ofrecen una alternativa para la observación aérea con mejores perspectivas de eficiencia en términos de costo – beneficio ya que, al no requerir los sistemas de supervivencia para una tripulación, puede incrementar su carga útil o bien reducir sus dimensiones y costo. Pero también detentan características muy particulares en su funcionalidad que demandan ciertas destrezas en los usuarios. Entre estas características, se pueden destacar las siguientes, cuya concatenación determina su capacidad de vigilancia:

MANIOBRAVILIDAD

Depende del tipo de dron con que se opere, de ala fija o de ala rotatoria, lo que determina la dinámica de vuelo. En el primer caso opera con un patrón de sobrevuelo continuo y a una velocidad al menos superior a la velocidad de pérdida del vehículo, lo cual puede dificultar darse cuenta de los detalles, si no se cuenta con facilidades para modificar la orientación de los medios de observación (las cámaras). Otro factor en este caso es la amplitud de giro para virar, incluso de regreso, si se requiere volver para observar algún espacio ya recorrido, lo que implica menor rapidez de detección y por ende de reacción.

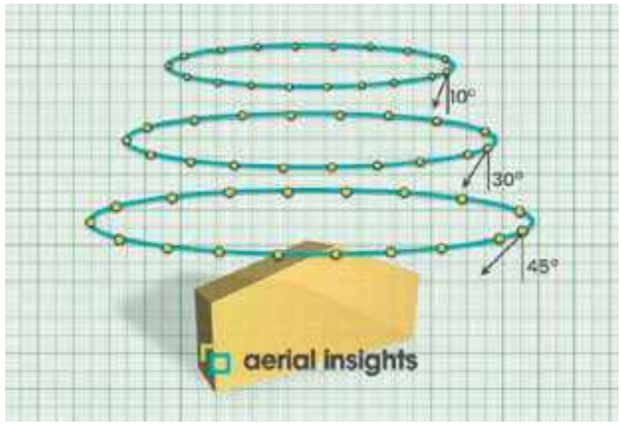
Por su parte, en el segundo caso, se tiene la facilidad para un sobrevuelo a mucho menor velocidad o estacionario *(hovering),* que le permite una mejor apreciación de detalles, así como mayor rapidez de detección y por ende de reacción, pero consume más energía de la planta motriz. Finalmente se tiene que, para el manejo del dron se tiene el problema de una visión confinada del entorno por el "efecto túnel" de lo que muestren los instrumentos a bordo a un operador remoto.

Fotos: Wikimedia

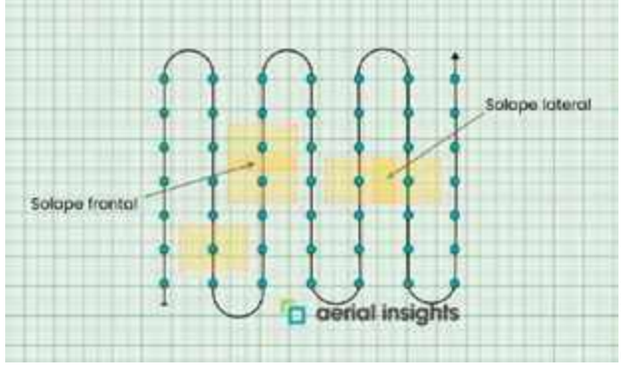
AUTONOMÍA

Se materializa por el tiempo de vuelo, que en principio está determinado por la capacidad de la planta motriz del vehículo, pero decrece por la magnitud de la carga útil y la complejidad de las maniobras como los patrones y velocidad de sobrevuelo, el tiempo estacionario, la altitud y el arrastre *(drag)* por las condiciones atmosféricas adversas. Un factor vinculado en este aspecto es el alcance de la cobertura, que depende del patrón de vuelo, que es máximo con un patrón lineal entre un origen y un destino aún alejados, y más reducido en recorridos de tipo "circuito" o "barrido".

Otro aspecto importante es que se renga capacidad de retorno origen para reabastecimiento, recarga de baterías o de combustible según sea el caso, para lo cual algunos modelos disponen de mecanismos que detectan el límite de alcance y activan automáticamente una trayectoria de retorno, pero en otros casos, el operador tendrá que determinar el momento de esta maniobra.



Fotos: Wikimedia



Fotos: Wikimedia

CARGA ÚTIL

Comprende las facilidades que determinan la capacidad operativa del dron, depende del tipo y potencia de la planta motriz y acota su autonomía. En este aspecto se puede tratar de quipos con poca potencia, como lo drones de consumo de poco peso, que sólo pueden transportar una cámara fija de corto alcance que requiere de muchas maniobras para cubrir un detalle en el espacio de interés, lo que acorta su autonomía, hasta equipos de grado militar de alta potencia capaces de transportar dispositivos sofisticados con facilidades PTZ y de largo alcance, que requieren menos maniobras de vuelo y por ende pueden extender su autonomía.

La concatenación de estas y otras características obligan al usuario - observador a desarrollar una capacidad de detección "al paso"

Fotos: Wikimedia

durante el sobrevuelo, es decir durante el desplazamiento del vehículo, para decidir las maniobras pertinentes, ya sea movimientos de exploración PTZ con los equipos de vigilancia, o bien modificaciones a la trayectoria de vuelo con el propio vehículo para una visualización específica enfocada en un detalle en particular dentro del espacio de cobertura.

Y entre menos facilidades se dispongan en el equipo, se requerirá mayor agudeza en esta destreza, la cual es indispensable cuando se utilizan drones de ala fija por su patrón de vuelo continuo, y una deficiencia o mal manejo de dicha destreza puede anular la ventaja de la mayor rapidez para el recorrido del área de cobertura al operar el vehículo a una menor velocidad o con muchos posicionamientos estacionarios. Y la efectividad de esta destreza se puede comprometer si el usuario – observador también es responsable de la operación aérea del dron.

Un dron puede ofrecer una mayor capacidad de captación ("ver más") por su movilidad aérea que le permite superar los obstáculos del terreno, pero si no se dispone de una capacidad de detección acorde, su utilidad será muy reducida. Y esa última capacidad dependerá como cualquier otra cámara, del factor humano, aunque se cuenten con sistemas analíticos que necesariamente estarán limitados a lo que les permita hacer su diseño y su programación. ■

Ver más NO asegura ver mejor.

David Chong Chong, secretario general para México de la Corporación Euro Americana de Seguridad (CEAS) México.

Más sobre el autor:

MILESTONE SYSTEMS LLEVA A CABO MIPS 2022

En el marco de MIPS 2022, la marca presentó su solución Milestone Kite™

EUA

Redacción / *Staff* Seguridad en América

Milestone Systems organizó el esperado evento Milestone Partner Summit (MIPS 2022), que se desarrolló en Minneapolis, Estados Unidos, el 24, 25 y 26 de octubre, en el Hotel Hyatt Regency, donde asistieron los principales socios de la marca para presentarles un interesante programa de conferencias con discursos inspiradores, conectarse con el liderazgo de la marca y experimentar las más recientes innovaciones, productos y soluciones.

Por su parte, Thomas Jensen, CEO de Milestone Systems, habló sobre la importancia de la evolución de la marca, asegurando que "la búsqueda en la que estamos con ustedes, nuestros socios, es un cambio de juego para esta industria, para nuestros clientes y para la sociedad. Nuestra aspiración es junto con ustedes, para hacer de la sociedad un mejor lugar para vivir".

"Para convertirnos en un líder mundial en tecnología de video basada en datos, tanto dentro como fuera de la seguridad, debemos hacer las cosas de manera diferente a como lo hemos hecho hasta ahora. Necesitamos hacer las cosas de manera que podamos cambiar colectivamente la forma en que opera esta industria, cambiar la forma en que nuestros clientes obtienen valor de nuestros productos y soluciones. Para revolucionar una industria que viene con oportunidades pero también con obligaciones", indicó.

También habló sobre cuatro aspectos en los cuales la marca busca concentrarse: "Nuestros clientes utilizan la tecnología de video en formas que nunca habían imaginado posibles. Y lo vamos a hacer de nuevo. Vamos a hacerlo junto con ustedes. ¿Nuestra aspiración? Convertirnos en el líder mundial en *data-drive*, en *software* de tecnología de video, dentro de la seguridad, que es nuestro *core business*, y más allá de la seguridad. Esos son cuatro aspectos cruciales".

MILESTONE KITE

Durante el evento, la marca reveló su más reciente lanzamiento, Milestone Kite™, se trata de la oferta en la Nube más reciente de la marca, una solución fácil de implementar, segura y escalable para la gestión de video (VMS) en la Nube, orientada a pequeñas y medianas empresas. En este servicio la implementación de XProtect en AWS ha sido optimizada para el mercado empresarial.

Milestone Kite™, con tecnología de Arcules, es una solución en la Nube, fácil de implementar, segura, escalable y económica, que ofrece actualizaciones automáticas y no requiere mantenimiento. Es la opción ideal para organizaciones con múltiples sedes, con implementación de sitio único o multisitio, que necesitan un método fácil para gestionar de forma centralizada todos sus sitios en un sistema unificado. Los negocios y las compañías de alto valor, menor complejidad y varias ubicaciones geográficas, como bancos, cadenas minoristas, escuelas y edificios residenciales, pronto descubrirán que Milestone Kite™ es la opción ideal para sus necesidades de seguridad.

MIPS 2022 también ofreció un espacio de muestra comercial donde los socios de la compañía participaron presentando sus más recientes productos y soluciones. Además de una programación de conferencias presentadas por los socios y por otros invitados expertos en tecnología y en experiencias motivacionales. ■

Fotos: Milestone Systems

VIDEOVIGILANCIA Y DRONES:

SOLUCIONES MÁS ALLÁ DE LA SEGURIDAD

La inteligencia artificial continuará siendo la innovación más utilizada en los sistemas de videovigilancia del mundo, mientras que en el caso de los drones, cada vez más estos facilitarán el cuidado y protección de bienes y personas

Foto: @Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Iniciamos el año con nuevos retos de seguridad y avances tecnológicos que no sólo contribuirán al desarrollo y operaciones de las industrias, sino que también estas herramientas tecnológicas de seguridad continuarán adaptándose y abriendo más posibilidades para su uso en beneficio de las compañías, para áreas ya no sólo que protegen y resguardan bienes y personas, sino también para aquellas que mercadean y ofertan, para Recursos Humanos, entre otras, a continuación les presentamos dos de las mejores opciones en materia de videovigilancia y drones para este 2023.

PELCO, UNA EMPRESA DE MOTOROLA SOLUTIONS

Pelco es un proveedor global de soluciones de videovigilancia con más de 63 años de experiencia en la industria. A mediados de 2020 Pelco fue adquirido por Motorola Solutions, líder global en comunicaciones de misión crítica. Las oficinas principales de Pelco están ubicadas en Fresno, California, y atienden a clientes de todo el mundo mediante oficinas regionales en las principales ciudades. En Latinoamérica cuentan con personal en los países de Brasil, Chile, Argentina, Colombia, Perú, Costa Rica, México y el Caribe. Para conocer un poco más sobre la oferta en videovigilancia para este 2023, Alejandro Rodríguez Quintero, director comercial para México de Pelco nos brindó una entrevista.

Seguridad en América (SEA): ¿Cuáles considera que serán las tendencias en videovigilancia para el 2023?

Alejandro Rodríguez Quintero (ARQ): la adopción de cámaras de alta definición (dos megapixeles o más) es un hecho en la industria. Los usuarios finales están almacenando cada vez más días de video, aprovechando la reducción de costos de los dispositivos de almacenamiento masivo. Lo que sigue es convertir ese "océano de datos" almacenados en información y conocimiento útil para el usuario.

Muchos sistemas siguen dependiendo de que el operador o vigilante se dé cuenta que algo está sucediendo y reaccionen. En los siguientes años, el análisis inteligente de escena basado en inteligencia artificial *(Machine Learning)* corriendo de forma distribuida en las cámaras, se volverá parte integral de cualquier sistema profesional de video.

La ciberseguridad también está tomando un papel relevante en los sistemas. Cada vez son más los ataques a la seguridad lógica de las empresas, por lo que cualquier dispositivo de red que se instale (cámaras, servidores, almacenamiento, controles de acceso, intrusión, etc.) deberá contar con seguridad comprobada para evitar que se utilicen como vectores de ataque.

SEA: ¿Qué soluciones de videovigilancia ofrece Pelco para los hospitales?

ARQ: los hospitales presentan el reto particular de lograr un delicado balance entre hacer que los usuarios del servicio se sientan seguros y a salvo vs. no sentirse acosados o vigilados de forma excesiva. Adicional a esto, se debe contar con sistemas confiables que garanticen tener la evidencia almacenada para revisar cuando suceda algún evento.

Las cámaras con lentes ojo de pez *(fisheye)* de Pelco permiten cubrir áreas amplias de forma eficiente. Integran análisis de escena inteligente que permite detectar la presencia de personas en el área y enviar la "metadata" para ser almacenada en los grabadores y facilitar la búsqueda posterior de eventos.

La familia de cámaras Sarix multisensor de Pelco (múltiples sensores de imagen en una carcasa tipo domo) permiten obtener video de diferentes direcciones, utilizando la infraestructura de red como si fueran una cámara convencional (un sólo puerto en el *switch* de red, una fuente de energía, un sólo cable de red) logrando un excelente balance entre costo de instalación vs. cobertura.

Para áreas amplias, exteriores, estacionamientos, etc., se pueden combinar las cámaras panorámicas Optera con las cámaras PTZ Spectra Enhanced. Cuando una cámara panorámica detecta un objeto de interés en el área, notifica a la cámara PTZ para que haga un acercamiento al área de interés y brinde evidencia detallada del suceso. Esa funcionalidad se llama Pelco Camera Link.

Las cámaras Sarix Modular son productos pequeños, sumamente discretos, que brindan una excelente calidad de imagen. Se pueden instalar en recepciones, áreas de urgencia, salas de neonatos, cualquier lugar donde se requiera una vigilancia sumamente discreta y confiable.

Un punto importante es que las cámaras Pelco están diseñadas para ser utilizadas al 100% por múltiples plataformas de video, son productos de estándar abierto compatibles con múltiples VMS como Milestone, Genetec, ISS, Axxon, etc. Todas las funcionalidades de los productos están disponibles mediante el estándar ONVIF; Pelco trabaja con los fabricantes de VMS para realizar pruebas y asegurar la completa compatibilidad de los productos.

SEA: ¿Cuáles son los principales diferenciadores de Pelco?

ARQ: Pelco busca distinguirse en el mercado por brindar una atención de primer nivel a nuestros clientes, combinado con tecnologías de vanguardia en los productos y servicio de soporte post venta superior. Nuestros asesores comerciales cuentan con habilidades técnicas para realizar un servicio de consultoría a todos nuestros clientes, ofreciendo el producto adecuado de acuerdo a las necesidades y el presupuesto disponible.

Contamos con plantas de manufactura de productos propias de Motorola Solutions en Norteamérica, lo que nos permite lograr un desarrollo de nuevos productos más ágil y ofrecer tiempos de entrega sumamente competitivos.

En el ramo de servicios hospitalarios, este año hemos proporcionado más de 600 cámaras para su instalación en diferentes proyectos en Centroamérica y Colombia. En el ramo de Petróleo y Energía, los productos ExSite para zonas con riesgo de explosión se están utilizando en múltiples proyectos en refinerías en Brasil y México.

"Pelco busca distinguirse en el mercado por brindar una atención de primer nivel a nuestros clientes, combinado con tecnologías de vanguardia en los productos y servicio de soporte posventa", **Alejandro Rodríguez Quintero**

Foto: @Freepik

OSAO

Los drones son herramientas que pueden resultar muy útiles en seguridad con una buena estrategia y planeación. Una de las empresas de seguridad privada en México que ofrece el servicio de venta y renta de drones, es OSAO, quien también ofrece soluciones de videovigilancia especializada con inteligencia artificial para vehículos de carga; sistemas de alarma residenciales, para oficina, naves industriales siempre con monitoreo 24/7 con apoyo y reacción en caso de emergencia.

Así como sistemas de control de acceso, Renta, venta de sistemas de videovigilancia de todo tipo; chapas de fabricación OSAO, para cajas de unidades de transporte con manipulación remota desde su centro de monitoreo; candados de seguridad para cajas de transporte; trabapatines de seguridad para manivela de cajas de transporte; guardias intramuros y monitoristas con un servicio integral con sistemas y tecnología.

Foto: OSAO


Foto: @Freepik

También ofrece la venta, renta, instalación de GPS vehiculares, con la especialidad del monitoreo 24/7 con apoyo y reacción en caso de emergencia, con monitoristas certificados y siempre en constante capacitación.

José Manuel Cadena Moya, jefe de Aplicaciones y Proyectos Tecnológicos nos compartió las bondades y beneficios del uso de drones en seguridad.

SEA: ¿Cuáles son los beneficios de los drones en la seguridad?

José Manuel Cadena Moya (JMC): nosotros hemos encontrado en los drones, un aliado en seguridad con muchos beneficios, los usamos en operativos de seguridad con algunos clientes que manejan masas de gente, así desde un centro de monitoreo móvil, podemos estar vigilando zonas de acceso, zonas de estacionamientos, zonas de mayor acumulación de gente, para evitar mandar a un elemento y no tenga el campo de visión como el de un dron.


Foto: @Freepik

Los usamos para vigilar terrenos de clientes, estructuras en edificios de clientes y verificar cómo se encuentran, de la mano con sus constructoras, buscando daños que requieran reparación inmediata. También en algunos eventos que llegamos a tener en carreteras, como medio de búsqueda de cajas de transporte entre terrenos de difícil acceso, siempre pilotando desde un área segura.

SEA: ¿Cuáles son los drones con los que cuenta OSAO?

JMC: tenemos drones de todo tipo, usamos la marca DJI que es muy amigable con los pilotos, tienen muchas ventajas para su uso, entre algunas características con gran funcionalidad son las cámaras térmicas con las que cuentan, para poder hacer vuelos nocturnos y tener una visión sin dificultades gracias a ellas; altavoces para dar avisos en tiempo real en las zonas donde estés volando el dron, cámaras con zoom por si es una zona de difícil vuelo bajo, volamos a una altura considerable y con la cámara con zoom podemos acercar la vista y tener una mejor visión en vivo así como la grabación.

SEA: ¿Cuáles son las normas o leyes que regulan el uso de drones en México?

JMC: desde 2017 la Dirección General de Aeronáutica Civil de la SCT (Secretaría de Comunicaciones y Transportes), estableció prohibiciones para operar los drones en zonas restringidas o peligrosas, se habla también de que debemos contar con una póliza de seguro de responsabilidad civil por daños a terceros; la misma marca DJI ya viene con bloqueos para evitar vuelos en zonas de aeropuertos, zonas militares, zonas gubernamentales, todo ello por medio de actualizaciones de *firmware* de los equipos, así mismo, los pilotos capacitados, siempre vuelan respetando la privacidad de los espacios por donde volamos y aprovechando las máscaras de privacidad con las que cuentan los drones.

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

A continuación el experto nos compartió los cinco tips para mejorar la seguridad con un dron:

1. Lo primero es preparar a un piloto para vuelos seguros y así poder brindar el servicio óptimo.
2. Hay muchos tipos y marcas de drones, es importante definir cuáles son sus necesidades de seguridad y qué uso le dará, para así elegir el dron lo más adecuado posible a lo requerido y le saque el máximo provecho.
3. Si son drones de batería, siempre tener consigo al menos cinco materias cargadas y conforme las vayas usando, ir cargando para siempre tener la disposición de energía para los vuelos.
4. Para la visión en vivo y vuelo del dron, para el piloto usar googles de la marca, así mismo, montar un centro de monitoreo móvil para que el cliente tenga la visión en una pantalla grande de los vuelos que está haciendo.
5. Realizar los vuelos con el mayor cuidado posible, siempre respetando los espacios aéreos de los demás, sólo volando donde tenga permitido por su cliente, tomando video y fotografías para tener evidencia de los vuelos.

Foto: OSAO

Tenemos claro que queremos ser reconocidos como la empresa líder en seguridad electrónica, cumpliendo siempre con los estándares de calidad y responsabilidad social, y ¿cómo lo vamos a lograr? Brindando servicios con la más alta calidad, amplia cobertura y constante innovación, protegiendo los bienes humanos, económicos y tecnológicos de nuestros clientes, siempre a través de la excelencia, efectividad y el desarrollo de nuestros colaboradores.

Actualmente tenemos cobertura en toda la república mexicana, podemos instalar y proveer el servicio en cualquier estado; contamos con más de 30 colaboradores, y nuestra matriz se ubica en Lomas Verdes, Estado de México. ■

SEA: ¿Cuáles son los principales diferenciadores de OSAO?

JMC: en OSAO, estamos comprometidos con ofrecer y brindar servicios y productos con la más alta calidad, siempre buscando se adapten a las necesidades de nuestros clientes, innovando y creando gracias a nuestro personal calificado y con la experiencia necesaria para ello. Siempre buscando la mayor satisfacción del cliente con excelencia, responsabilidad, transparencia, pasión, lealtad y puntualidad.

"Queremos ser reconocidos como la empresa líder en seguridad electrónica, cumpliendo siempre con los estándares de calidad y responsabilidad social", **José Manuel Cadena Moya**


Foto: @Freepik

PEMSA

SISTEMAS DE SEGURIDAD PRIVADA

EVOLUCIONA
LA SEGURIDAD
DE TU HOGAR Y NEGOCIO
AL SIGUIENTE NIVEL

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

222 141 12 30

gerenciacomer@pem-sa.com

ALAS

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

Achilles No. 329,814

COPARMEX

WWW.PEM-SA.COM

REGISTRO FEDERAL DGSP/303-16/3302 PERMISO SSP PUEBLA

SSP/SUBCOP/DGSP/114-15/109

REPSE AR10508/2021

USO DE DRONES
EN LA INDUSTRIA DEL *RETAIL*

El dron es muy útil para mapear grandes áreas sin sacrificar detalle y precisión y mucho más eficiente que los métodos tradicionales

MÉXICO | José Luis Sánchez Gutiérrez

En la industria del *retail* desde el punto de vista de la seguridad patrimonial nos encontramos con diferentes áreas de oportunidad continuamente con el uso adecuado de los recursos físicos tecnológicos y de procesos de apoyo que nos ayudan a identificar, transferir, asumir, contener e incluso eliminar diferentes situaciones de riesgo en la unidad de negocio donde estamos.

En esta ocasión hablamos de los drones como herramienta: en la actualidad su funcionamiento esta aplicado principalmente para que nos ayuden operativamente en el conteo de inventarios; debido a la rapidez de sus movimientos y a su tamaño pueden acceder a lugares de difícil acceso e incluso facilitan la rapidez de ubicar algún tipo de mercancía especifica.

Pero desde el punto de enfoque en la seguridad patrimonial y la prevención y gestión de riesgos, como valor agregado vemos y utilizamos el uso de los drones en el *retail* (en las unidades de negocio de todo tipo: almacenes, centros de distribución, tiendas de todo tipo de formato, edificios de oficinas, parques y deportivos empresariales, etc.) obteniendo el máximo provecho como lo hacen grandes empresas con el habilitamiento de esta herramienta en:


Foto: Freepik


Foto: Freepik

Los drones pueden usarse para inspecciones nocturnas, búsqueda y rescate, hay una versión térmica disponible de dron que también la podemos utilizar en la extinción de incendios en las unidades de negocio

a) Recorridos virtuales tanto internos y externos a la unidad de negocio (lo que comúnmente conocemos como rondines).

b) Inspecciones a vehículos de transporte propio y de terceros, tanto al ingresar como al salir de las unidades de negocio a cargo.

c) Análisis de vulnerabilidad (tanto análisis de riesgo y análisis de entorno 24/7).

d) Inspecciones de predios y zonas inaccesibles a simple vista como azoteas, equipos de refrigeración locales técnicos, etc. Identificando tipo de desgaste ha sufrido tanto el techo, los equipos ahí colocados y buscar signos de problemas adversos que podrían surgir en el futuro.

e) En el caso de uso compartido con autoridades para sobrevolar mítines y marchas como las del gasolinazo en 2018, los movimientos por vandalismos (02 de octubre), movimientos por los 43 de Ayotzinapa, etc.

f) También con trabajo en conjunto con autoridades el uso de los drones se ha utilizado para dar seguimiento a robos en progreso para no perder la flagrancia cuando el presunto delincuente entra a una unidad de negocio, comete un delito y sale huyendo de la misma (en el interior se tiene registrado el evento con el equipo instalado en sitio y con el dron se le da seguimiento al mismo evento en el exterior).

g) Incluso en una emergencia con un dron equipado con un megáfono puede ayudar a salvar vidas si das instrucciones sobre cómo realizar primeros auxilios a alguien y se coloca sobre una persona lesionada para que los profesionales médicos puedan encontrarla más fácilmente.

h) Para inspecciones nocturnas, búsqueda y rescate e inspecciones hay una versión térmica disponible de dron que también la podemos utilizar en la extinción de incendios en las unidades de negocio.

i) Inspecciones industriales al interior y al exterior de cualquier tipo de infraestructura industrial como chimeneas industriales, torres de

También con trabajo en conjunto con autoridades el uso de los drones se ha utilizado para dar seguimiento a robos en progreso para no perder la flagrancia cuando el presunto delincuente entra a una unidad de negocio, comete un delito y sale huyendo de la misma

telecomunicaciones, torres eléctricas, gasoductos, puentes etc.; para realizar inspecciones seguras sin interrumpir las operaciones de la unidad de negocio que con software especializado para el análisis de datos y con AI (Artifitial Intelligence) se pueden hacer predicciones en el mantenimiento de la infraestructura a futuro.

j) Para la reconstrucción de un accidente o si se necesita un modelo detallado de un área para topografía, la mejor opción es una nube de puntos. Los drones crean nube de puntos de alta precisión, detalle y resolución, los cuales son elementos importantes en la creación precisa de modelos 3D.

VENTAJAS

Algunos beneficios de la implementación de inspecciones con drones:

a) La exactitud: no importa qué tan profesional sea nuestro personal que supervisa, el error humano es inevitable, con un dron que puede automatizar las rutas de vuelo, se elimina la posibilidad de tener un error humano.

b) El tiempo: las inspecciones con un dron reducen la inversión de tiempo, ya que con ellos los inspectores asignados permanecen en un lugar, haciendo una ruta de vuelo y dejando que el software haga el resto.

c) La seguridad: con un dron, se puede tomar imágenes desde puntos de vista que los humanos no pueden alcanzar sin correr el riesgo de que alguien se lastime en el proceso.

d) El costo: al utilizar drones, se pueden reducir los costos de mano de obra, así como realizar más trabajos de inspección en menos tiempo.

Foto: Freepik

Foto: Freepik

Los drones pueden proporcionar reconocimiento remoto y monitoreo aéreo, así como identificar puntos críticos y amenazas para las personas y la propiedad. Con cargas útiles adicionales, los socorristas pueden identificar a las personas lesionadas, determinar los problemas de exposición y determinar el problema principal, todo mientras mantienen una distancia segura del incidente. Los drones también se pueden usar para vigilar de forma segura y alertar a los respondedores sobre condiciones cambiantes o potencialmente peligrosas para aumentar la conciencia situacional en tiempo real. Los drones también pueden crear mapas del área que pueden ayudar en las evaluaciones de daños posteriores al incidente y la planificación de la limpieza.

EN CONCLUSIÓN

El dron es muy útil para mapear grandes áreas sin sacrificar detalle y precisión y mucho más eficiente que los métodos tradicionales.

Es innegable el trabajo que hacen en la actualidad los drones para contribuir con la seguridad patrimonial, la prevención y gestión de riesgos en el *retail*, incluso para la seguridad pública y ayudar a policías, bomberos y equipos de rescate que se han encargado de actuar como soluciones rápidas, prácticas y altamente eficaces frente a escenarios críticos. Actualmente los drones ofrecen grandes e innovadoras soluciones ante este panorama, desde equipos para cuestiones de vigilancia, hasta drones que pueden servir para ayudar a reconstruir la escena de un desastre y drones con cable (en lugar de baterías) con duración continua de vigilancia (con más de 24 horas continuas de vuelo). ■

José Luis Sánchez Gutiérrez, gerente nacional de Protección Laboral y Patrimonial en Cadena de Suministro OXXO y Nuevas Avenidas de Negocio.

Más sobre el autor:

CON SOLUCIONES ESPECIALIZADAS

MILESTONE SYSTEMS

CONCENTRA SU ATENCIÓN EN INDUSTRIAS ESENCIALES

La tecnología de video basada en datos de Milestone será el centro de una nueva oferta para el sector de la salud, cuyo lanzamiento está programado para este 2023

DINAMARCA

Milestone tiene las condiciones idóneas para enfrentar los desafíos de la industria de la salud. Su sistema de gestión de video de plataforma abierta XProtect admite actualmente más de 11 mil dispositivos de seguridad de más de 500 fabricantes

En la actualidad, las organizaciones están buscando nuevas formas de utilizar la tecnología de video en aplicaciones que van más allá de la seguridad y la protección. Se están dando cuenta de que es posible acceder a un gran volumen de datos que se pueden aprovechar para generar valor agregado. En el sector de la salud, Milestone Systems pondrá en marcha una estrategia que desembocará, en última instancia, en el desarrollo de soluciones que permite a la tecnología de video generar valor en sectores específicos.

Partiendo de una comprensión más profunda de los objetivos, las necesidades y los desafíos de los clientes dentro de sectores específicos, Milestone planea ofrecer de manera gradual soluciones de video específicas, de comprobada eficacia, para la industria de la salud y la hotelera. El sistema de gestión de video (VMS, por sus siglas en inglés) de plataforma abierta XProtect de Milestone es la herramienta ideal que reúne las mejores integraciones de video y datos, análisis de video y soluciones en la Nube para atender las necesidades de las industrias esenciales.

"Para poder generar verdadero valor y resultados comerciales es necesario adoptar una estrategia sólida orientada al cliente. Las interacciones específicas que tenemos con los clientes dentro de estas industrias nos ayudan a desarrollar soluciones de tecnología de

video especializadas para cada sector, que van mucho más allá de la seguridad", aseguró Thomas Jensen, director ejecutivo de Milestone Systems. "Milestone cuenta con el ecosistema más grande de socios de desarrollo y tecnología, dentro y fuera de la industria de la seguridad. Estamos en una posición excepcional para trabajar con los líderes del mercado a fin de crear soluciones que respondan a las necesidades operativas y de seguridad únicas de industrias específicas".

La nueva solución garantizará la seguridad tanto de los pacientes como de los empleados y protegerá los activos y bienes de las instituciones, con prestaciones especializadas que cumplen con los requerimientos normativos y se ajustan a los entornos de trabajo únicos del sector de la salud

CREAR ENTORNOS DE ATENCIÓN EN SALUD MÁS SEGUROS Y EFICIENTES

En 2022, el Servicio Nacional de Salud (NHS, por sus siglas en inglés) del Reino Unido reportó un déficit de 90 mil empleados de tiempo completo. Para 2030, los Estados Unidos experimentarán una reducción de más de medio millón de plazas de enfermería. Enfrentados como están a las cargas de trabajo agobiantes y a los innumerables pormenores operativos y administrativos que deben atender, los hospitales y centros de atención en salud deben explorar nuevas tecnologías que les permitan optimizar todos los recursos que tienen a su disposición.

La tecnología de video basada en datos de Milestone será el centro de una nueva oferta para el sector de la salud, cuyo lanzamiento está programado para este 2023. La nueva solución garantizará la seguridad tanto de los pacientes como de los empleados y protegerá los activos y bienes de las instituciones, con prestaciones especializadas que cumplen con los requerimientos normativos y se ajustan a los entornos de trabajo únicos del sector de la salud.

La nueva oferta para el sector de la salud de Milestone se propone:

- Mejorar la atención, el resultado y la experiencia de los pacientes.
- Maximizar la eficiencia del personal y resolver los problemas de gestión de los recursos hospitalarios.
- Mejorar el reconocimiento del entorno sin necesidad de asignar personal adicional.

Milestone tiene las condiciones idóneas para enfrentar los desafíos de la industria de la salud. Su sistema de gestión de video de plataforma abierta XProtect admite actualmente más de 11 mil dispositivos de seguridad de más de 500 fabricantes. Adicionalmente, el ecosistema de socios tecnológicos de la compañía incluye proveedores de cámaras de video en red, servicios en la nube, equipos de almacenamiento, control de acceso, sistemas de alarma y detección, análisis de video, tecnología GPS, escáneres láser y cabinas para llamadas de emergencia, por nombrar sólo algunos.

En 2023 la compañía publicará más información sobre la solución de Milestone para el sector de la salud. ■

Fotos: Milestone

6 TECNOLOGÍAS DE IDENTIFICACIÓN PARA EVENTOS DEPORTIVOS MASIVOS

Los escaneos de boletos son más eficientes, rápidos y sencillos, lo que hace que el proceso de admisión o ingreso a los escenarios deportivos sea más conveniente

Foto: Freepik

HID Global, líder mundial en identificaciones seguras, preparó el siguiente análisis para mostrarnos las tecnologías con el fin de controlar el acceso a este tipo de eventos

SUIZA | Andrés Chenevard

Finalizó uno de los eventos deportivos más importantes del planeta: la Copa Mundial de Fútbol de la FIFA 2022™, el cual —en su pasada edición de Rusia 2018— tuvo un total combinado de 3 mil 572 millones de espectadores, equivalentes a más de la mitad de la población mundial (según cifras oficiales de la FIFA) sumados a los más de 2.5 millones de aficionados que asistieron a los estadios hasta la fase de octavos de final.

Para esta edición del torneo en Qatar se esperaba que las cifras fueran equivalentes o mayores, dado que el aforo estimado de los ocho estadios que acogieron los encuentros —que se prolongaron por un mes— sumó 388 mil 600 espectadores, por lo que la tecnología jugó un papel preponderante en la seguridad, logística y al final, en la calidad de la competencia.

Pues bien, a continuación, presentaremos algunas de las tecnologías más importantes que ofrece el mercado en la actualidad para que los organizadores de eventos deportivos, puedan garantizar una autenticación segura, eficiente y ágil de todos los involucrados.

Las plataformas de gestión de eventos ayudan a que los asistentes eviten largas esperas y filas en las zonas de ingreso a los escenarios, asimismo previenen la falsificación de las entradas físicas y virtuales, no sólo de los aficionados, sino del personal de logística, organizadores, directivos o del ciudadano común.

1. BOLETERÍA DIGITAL

Existe la posibilidad de adoptar una boletería cien por ciento digital para el ingreso a grandes acontecimientos de orden deportivo, como el que corre en tierras árabes, consistente en credenciales alojadas al interior de dispositivos móviles, la cual brinda altos estándares de seguridad, comodidad y beneficios como los siguientes:

a) Elimina la necesidad de boletos físicos, credenciales y/o brazaletes, susceptibles de ser hurtados o extraviados.

b) Al comprar un boleto, los usuarios descargan la aplicación del evento en su teléfono móvil, reloj inteligente u otro dispositivo móvil para luego transferirlo a su billetera digital.

c) Los escaneos de boletos son más eficientes, rápidos y sencillos, lo que hace que el proceso de admisión o ingreso a los escenarios deportivos sea más conveniente.

Los boletos inteligentes integran opciones de pago y control de acceso para una comodidad superior. Es posible combinar una solución de pago y un token de control de acceso seguro para brindar a los asistentes una experiencia sin contratiempos

Con la aplicación, los asistentes pueden usar sus teléfonos móviles como "entradas inteligentes" para acceder. También pueden comunicar detalles del juego antes, durante y después.

Este modelo entre pares crea un sentimiento de comunidad. En lugar de impulsar la comunicación unidireccional de arriba hacia abajo, los organizadores cuentan con aficionados que interactúan entre sí generando interés. Después del evento, los asistentes pueden guardar sus "tarjetas inteligentes de membresía" como recuerdo.

Del mismo modo, los fans pueden seleccionar entre múltiples eventos; chatear con otros seguidores, encontrar amigos en el recinto, publicar fotos y contenido, así como recibir información y promociones de los promotores y patrocinadores.

De esta manera, el patrocinador del evento puede fomentar la publicidad y promociones exclusivas para los asistentes. A su vez, el organizador puede proporcionarles información sobre el evento antes, durante y después e incluir contenido multimedia como videos, fotos y fondos de pantalla.

Algo para destacar es que el teléfono móvil con tecnología NFC (comunicación de campo cercano), se puede usar sin conexión a una red.

2. BILLETERAS ELECTRÓNICAS PARA MAYOR COMODIDAD

Los boletos inteligentes integran opciones de pago y control de acceso para una comodidad superior. Es posible combinar una solución de pago y un token de control de acceso seguro para brindar a los asistentes una experiencia sin contratiempos.

El tiquete inteligente puede también cargarse previamente con un monto mínimo de dinero para utilizarse en transacciones dentro del lugar y evitar el uso de dinero físico; además el usuario puede usar puntos o descuentos de cualquier tipo, para obtener premios, promociones, etc.

Sumado a esto, también es posible realizar transacciones en línea usando los teléfonos móviles con tecnología NFC, lo que los convierte en terminales de punto de venta. Así, los usuarios pueden verificar el estado de su cuenta en sus móviles.

Por último, pero no menos importante, el usuario puede llevar a cabo la conciliación de cuentas y el manejo de saldos en tiempo real.

Foto: Freepik

3. BOLETOS FÍSICOS CON TECNOLOGÍA RFID

Si la alternativa es seleccionar boletos físicos para el ingreso a un escenario, la tecnología de identificación por radiofrecuencia (RFID) incrustada en las entradas en forma de boletos, tarjetas, PVC, papel, prendas o accesorios electrónicos es la indicada.

Las entradas que contienen esta tecnología transmiten la identidad única del boleto y del titular a través de ondas de radio, lo que previene su falsificación, a diferencia de los boletos con código de barras.

Los escáneres RFID no necesitan una línea de visión con los chips, lo que significa que los asistentes pueden simplemente acercar sus boletos a un lector para validarlos y obtener acceso, acelerando de manera significativa el proceso de admisión. Además, los datos almacenados en el chip RFID de un boleto están encriptados y firmados digitalmente.

4. LECTORES SIN CONTACTO

Imagine este escenario: ochenta mil espectadores listos y a la espera de que se abran las puertas del Estadio Lusail para ingresar a presenciar la final de la Copa Mundial de Futbol de Qatar, o decenas de miles de espectadores en la prueba de los 100 metros planos en los Juegos Olímpicos o el Super Bowl. ¿Qué tipo de lectores deben ser instalados para garantizar un ágil ingreso de los asistentes?

Para superar este tipo de desafíos, los lectores sin contacto son los indicados. Estos se especializan en combinar múltiples soluciones de identidad y verificación en dispositivos de uso intuitivo. Sumado a que previenen la falsificación de la identidad del usuario, estos dispositivos brindan velocidad, precisión y confiabilidad, lo que los hace perfectos para organizadores de eventos masivos que buscan eficiencia en el rendimiento.

La cartera que ofrece actualmente el mercado brinda flexibilidad a los organizadores para escoger la identificación que más se ajuste a sus necesidades, con la posibilidad de incorporar diferentes tipos de lectores, diseñados para leer tokens RFID/NFC, códigos de barras 1D/2D y boletos desde teléfonos móviles, tabletas, dispositivos portátiles, boletos con RFID o tarjetas sin contacto.

Además, los propietarios de los boletos (espectadores) se benefician de la velocidad de rendimiento, lo que se traduce en una mejor experiencia de ingreso porque no tienen que seguir instrucciones específicas para la presentación del boleto cuando se acercan a una puerta o a un torniquete.

La cartera que ofrece actualmente el mercado brinda flexibilidad a los organizadores para escoger la identificación que más se ajuste a sus necesidades, con la posibilidad de incorporar diferentes tipos de lectores, diseñados para leer tokens RFID/NFC, códigos de barras 1D/2D y boletos desde teléfonos móviles

Los asistentes pueden simplemente presentar su boleto a los lectores en cualquier orientación para que ocurra una lectura positiva.

5. GESTIÓN DE IDENTIFICACIONES

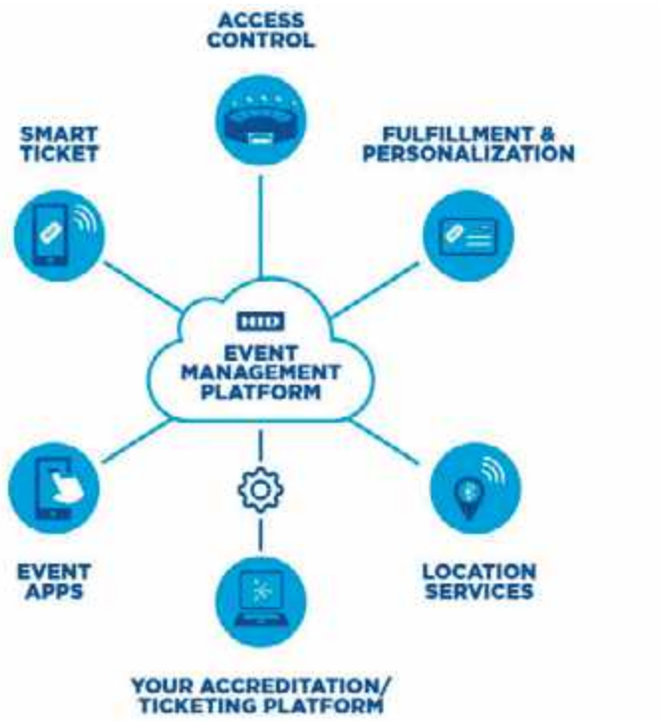
Existe, también, un conjunto de aplicaciones de administración de acceso de identidades digitales y físicas, con las que es posible automatizar los flujos de trabajo de credencialización, bien sea para empleados, contratistas, voluntarios o invitados especiales, eliminando los ineficientes procesos manuales.

Los visitantes y contratistas se pueden agrupar en una variedad de dimensiones para que su experiencia y la supervisión sean mejores para todas las partes.

Cuando es necesario, es fácil obtener información sobre las credenciales emitidas: quién las tiene, para qué sirven, por qué se han acreditado y por cuánto tiempo, por lo que es posible que estas tecnologías basadas en la Nube permitan a los organizadores o administradores de eventos masivos automatizar y simplificar el procedimiento de identificación oficial.

Para reducir el riesgo de amenazas internas, la revocación de credenciales es igual de fácil de automatizar. Esto garantiza el cumplimiento basado en las reglas de acceso de visitantes y el registro basado en políticas.

Entre otros datos que pueden ser emitidos por medio de estas plataformas y los cuales son relevantes para los organizadores, se encuentran los informes y estadísticas con análisis en tiempo real durante o después del evento; la cantidad de accesos por entrada, el número de accesos por intervalo de tiempo, el número de tiquetes no autorizados en las entradas, porcentaje de acceso comparado con tiquetes vendidos, número de tiquetes ingresados por intervalo de tiempo y otras estadísticas personalizables.



6. SALIDAS DE EMERGENCIA INTELIGENTES

El mercado también ofrece módulos que se pueden integrar a las puertas salida de los escenarios deportivos para leer RFID, de esta manera se pueden crear soluciones personalizadas que garanticen la salida de los espectadores de los estadios sin problemas y facilitar las evaluaciones de emergencia.

Tener los datos en tiempo real de cuándo los poseedores de los boletos entran y salen de perímetro es crucial para que los organizadores garanticen la mejor experiencia a los aficionados, así como para obtener inteligencia sobre dónde una puerta en particular necesita más atención en términos de control de multitudes y evacuación de emergencia.

Gracias a la experiencia por haber sido designado como emisor oficial de tiquetes en el mundial de futbol Rusia 2018, en HID brindamos soluciones versátiles para la lectura de boletos y credenciales. Además, ofrecemos la tecnología para la recepción de pagos sin contacto, integrando estos productos con máquinas expendedoras de boletos, torniquetes o puertas de acceso, lo que hace de los procesos logísticos más simples, seguros y confiables, no sólo en justas deportivas, sino también en cualquier otro tipo de evento de carácter masivo. ■

Andrés Chenevard, director de Ventas y Desarrollo de Negocio de EMS (Event & Mobility Solutions) para HID Global en las Américas.

Más sobre el autor:

SISSA
Monitoring Integral

Integramos una amplia gama

DE ANALÍTICAS DE VIDEO

flexibles, escalables, intuitivas y abiertas para optimizar las acciones de videovigilancia:

- **Detección** de rostros.
- **Detección** de intrusiones.
- **Reconocimiento** de matrículas.
- **Detección** de movimiento inteligente.
- **Clasificación y detección** de objetos.
- **Detección** de agrupación.
- **Protección perimetral** escalable y de alta seguridad.

Contáctanos y permítenos brindarte una solución personalizada de videovigilancia en función de tus características y requerimientos específicos.

55 6651 0200 WWW.SISSAMX.COM.MX

LOS BLINDADOS DEL EJÉRCITO

Foto: wikipedia

MÉXICO | Ricardo Daniel Guzmán Reyes

Nuestro colaborador invitado nos comparte la historia del blindaje en aquella época

El 22 de febrero de 1914 el presidente Mexicano Francisco I. Madero y el vicepresidente José María Pino Suárez fueron asesinados bajo la ley fuga cerca de Lecumberri, el verdugo fue un porfirista simpatizante de Victoriano Huerta quien fue el autor intelectual del magnicidio. Este evento fue conocido como la "decena trágica" por los hechos que ocurrieron desde el 9 de febrero con el golpe de estado hasta la muerte de Madero y Pino Suárez. Huerta fue reconocido por el Congreso de la Unión, la Suprema Corte de Justicia, así como por la mayoría del ejército. Por su parte, el Gobernador de Coahuila, Venustiano Carranza se negó a reconocer la autoridad de Huerta, en su estado fue reuniendo fuerzas militares y recursos económicos, que fueron los inicios del movimiento que conocemos como constitucionalista.

Al triunfo del movimiento constitucionalista sobre la dictadura de Huerta, le siguió una lucha de igual naturaleza entre los tres grupos del movimiento revolucionario; carrancistas, villistas y zapatistas. Los enfrentamientos exigían contar con el mejor armamento posible y los vehículos blindados jugaron un papel importante en esos eventos, hasta ahora poco estudiados por la falta de registros y fuentes documentales, aún así actualmente es posible darnos una idea con la información que hay.

Recordemos que también en 1914 comienza la Segunda Guerra Mundial y el ejército del entonces Imperio Ruso comenzó a formar unidades de vehículos blindados, ya que su capacidad de producción era limitada, decidió comprar al Reino Unido las plataformas sobre las cuales se fabricarían los llamados "Austin" debido a que precisamente fue la firma Austin Motor Company la armadora de los automóviles. Cabe la mención de estos blindados porque son muy similares en su forma a los usados por el ejército constitucionalista.

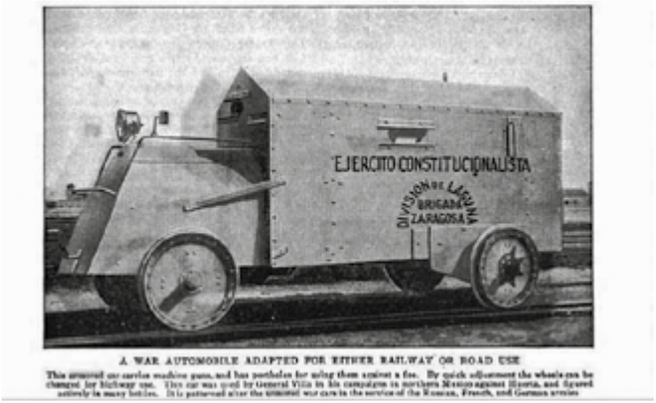
Ayudados por las imágenes que aún se conservan en archivos históricos se puede concluir que una de las plataformas usadas en ese entonces fue la de Protos de la firma alemana Siemens-Schuckertwerke (SSW).

La planta de Protos en Berlín había comenzado a fabricar vehículos desde 1899 y al inicio sólo se enfocaba en vehículos de pocos pasajeros, sin embargo, las nuevas necesidades de movilidad exigieron desarrollar automóviles de transporte de personal y camiones para los ejércitos a partir de 1914. Por lo menos un par de vehículos Protos fueron usados en México.

EL CARRO BLINDADO DE VILLA

El historiador Ilhuicamina Rico Maciel, experto en temas de la Revolución Mexicana, en su blog llamado Batallas en el Desierto narra que entre las armas de la División del Norte está el carro blindado que usó el General Francisco Villa. Este singular carro blindado que llevaba siete ametralladoras estaba inspirado en otros vehículos que estaban en servicio en los ejércitos rusos, franceses y alemanes. Sin embargo, era un armamento experimental, no hay evidencia de que haya sido utilizado en alguna batalla. En el costado estaba escrito "Ejército Constitucionalista División de Laguna, Brigada Zaragoza" que estaba bajo el mando de Eugenio Aguirre Benavides. Al Parecer había otro, pues hay una foto donde aparece el nombre del Ejército Constitucionalista escrito en forma diferente.

Así mismo, Rico Maciel menciona un artículo periodístico del 20 de febrero de 1914 donde prácticamente describe la ficha técnica del acorazado; dice que el carro blindado tenía las siguientes dimensiones: medía unos 20 pies de largo, ocho pies de alto y seis pies de ancho. El techo y las paredes eran de acero, para proteger a los operadores. La carcasa de acero construida en el camión era impenetrable, ya fuera por Máuser o fuego de ametralladora. Se le había hecho pruebas exhaustivas.



A WAR AUTOMOBILE ADAPTED FOR EITHER RAILWAY OR ROAD USE

Foto: batallaseneldesierto-blogspot.com

Foto: wikipedia

El ejército del entonces Imperio Ruso comenzó a formar unidades de vehículos blindados, ya que su capacidad de producción era limitada, decidió comprar al Reino Unido las plataformas sobre las cuales se fabricarían los llamados "Austin", debido a que precisamente fue la firma Austin Motor Company la armadora de los automóviles

El historiador Ilhuicamina Rico Maciel, experto en temas de la Revolución Mexicana, en su blog llamado Batallas en el Desierto narra que entre las armas de la División del Norte está el carro blindado que usó el General Francisco Villa

El revestimiento del coche está hecho de pared de chapa de acero entre las que se encontraba una capa de fieltro. Se podía operar ya fuera en vías de ferrocarril, en carreteras o en el campo. Estaba equipado con ruedas especialmente fabricadas, para que se pudieran desmontar los neumáticos y utilízalo en el trabajo de carretera y en su lugar un conjunto de bridas conectadas a la máquina para que pudiera funcionar en vías de ferrocarril. Podía correr a una velocidad de 20 millas por hora en carretera y 40 millas en las vías. Los protectores de acero se construyen sobre el lado de las ruedas para evitar que los rayos y las ruedas se dañara, y una placa de acero se colocó en de la parte inferior del coche para proteger la maquinaria en caso de que minas explotaran debajo de ella.

Bajo el suelo de la máquina se construyeron cajas que transportaban más municiones, aceites, piezas adicionales y suficiente combustible para hacer funcionar la máquina por 200 millas. Además, tenía al frente un poderoso reflector giratorio, hacía posible operar el coche por la noche. En la nota periodística menciona que también incluía un equipo inalámbrico (posiblemente un telégrafo inalámbrico) para mantener al coche en comunicación con el cuerpo principal de las tropas.

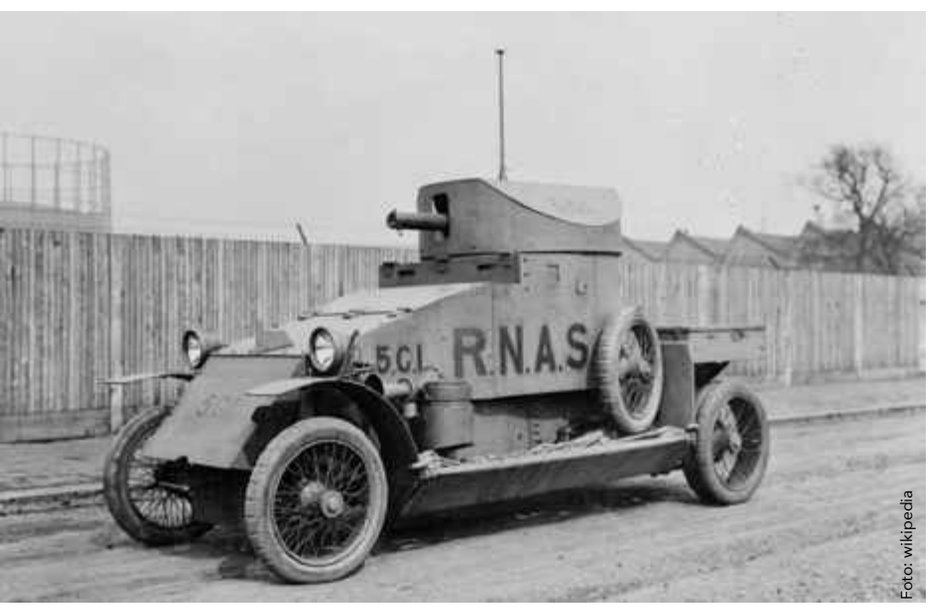


Foto: wikipedia

Según esta información, era un auténtico vehículo multipropósito con el equipamiento propio de la época, desafortunadamente se desconoce si las adaptaciones fueron locales o así venia de origen. Nada se sabe del destino de aquellos vehículos o si realmente tuvieron alguna participación importante en alguna batalla, lo cierto es que al triunfo del movimiento constitucionalista se terminó con un país agotado, una economía dañada y sin instituciones fuertes. Se abría un periodo de reorganización política y social, donde el desarrollo de los vehículos blindados por lo menos en México, tendrían que dormir el sueño de los justos para despertar muchas décadas después. ■

Foto: wikipedia

Ricardo Daniel Guzmán Reyes, director de Operaciones en Vínculo Estrategas Comerciales.

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:

¿DÓNDE SON REQUERIDAS LAS PRUEBAS INTEGRADAS DE LOS SISTEMAS DE SEGURIDAD CONTRA INCENDIOS?

EUA

La Prueba Integrada se refiere a la prueba de todos los sistemas de seguridad contra incendios para confirmar la operación, interacción, y coordinación de los múltiples subsistemas independientes, buscando ratificar la operación prevista en función de otros sistemas de seguridad contra incendios y los objetivos de protección

Uno de los cambios más importantes en la normativa de la NFPA (Asociación Nacional de Protección Contra Incendios) tiene que ver con el proceso de aceptación de los sistemas de seguridad humana y protección contra incendios en los edificios. Esto no quiere decir que en el pasado, a un sistema de protección contra incendios, no se le requiriera una prueba de aceptación, sino más bien que ahora la normativa requiere que "todos" los sistemas que tienen que ver con la seguridad humana y la protección contra incendios en el edificio pasen por una prueba de aceptación "concurrente".

Esto se llama la "Prueba Integrada", la cual está regulada por la NFPA 4, Norma para Pruebas Integradas de Sistemas de Protección Contra Incendios y Seguridad Humana. Esta Prueba Integrada es hoy día requerida en todos los edificios nuevos, antes de su apertura, con la única excepción de un edificio uni o bi- familiar.

¿QUÉ ES UNA PRUEBA INTEGRADA?

La Prueba Integrada se refiere a la prueba de todos los sistemas de seguridad contra incendios para confirmar la operación, interacción, y coordinación de los múltiples subsistemas independientes, buscando ratificar la operación prevista en función de otros sistemas de seguridad contra incendios y los objetivos de protección. Por ejemplo, en un edificio de gran altura, la activación del interruptor de flujo del sistema de rociadores automáticos, en cualquier piso, debería:

Foto: IFSC

- Activar la alarma de evacuación sonora, de voceo y visual en el piso donde se gestó la alarma y si se requiere, en otros pisos. Esta alarma de evacuación debe tener un nivel apropiado de frecuencia y presión de sonido, inteligibilidad y visibilidad.
- Si la evacuación es por fases, se debería recibir una alarma de alerta sonora, de voceo y visual en los otros pisos del edificio que no se evacuen en la primera fase. Esta alarma de alerta deber tener un nivel apropiado de frecuencia y presión de sonido, inteligibilidad y visibilidad

Las Pruebas Integradas de los sistemas de protección contra incendios y seguridad humana deben ser efectuadas en presencia de los contratistas de los distintos sistemas, quienes deben operar los equipos en presencia de un Agente de Prueba Integrada (API), quien debe liderar y ser responsable por las pruebas

- Enviar los elevadores al piso de evacuación y deshabilitarlos para que sólo puedan ser usados por los bomberos. Deshabilitar las escaleras mecánicas, si existieran.
- Apagar el sistema de aire acondicionado en el piso donde se inició la alarma.
- Iniciar el sistema de presurización de las escaleras.
- Posiblemente iniciar funciones de extracción de humos si el edificio tiene, por ejemplo, un atrio.
- Cerrar puertas y exclusas en ductos de aire según sean necesario.
- Posiblemente la bomba contra incendios también habría operado, y los paneles de alarma deben también recibir un mensaje supervisor. Paralelamente se debería documentar que otras alarmas de supervisión en el cuarto de bombas funcionan correctamente como nivel de diesel, recarga de baterías, funcionamiento de la bomba "*jockey*" y nivel del tanque de agua, entre otras.
- Por otro lado, el panel de alarma principal y los paneles remotos deben recibir una alarma sonora y los paneles deben identificar exactamente el origen de la alarma, en español simple.
- También se deben efectuar pruebas a carga completa sin "*bypass*", silencio o desconexiones entre sistemas. Esto incluye pruebas de los sistemas de protección contra incendios y seguridad humana conectados a la energía de emergencia o de reserva, para replicar una emergencia de la manera más realista posible.

Es decir, como se muestra en este simple ejemplo de Prueba Integrada, se debería confirmar la interacción y coordinación entre el sistema de alarma y detección, el sistema de rociadores, el sistema de elevadores, el sistema de bombeo de agua contra incendios y los sistemas de manejo humo, manejo de aire y compartimentación del edificio, entre otros.

MATRIZ CAUSA-EFECTO

¿Cómo se define que debe ocurrir con los sistemas de seguridad contra incendios cuando un elemento de iniciación opera, o un elemento está desconectado, apagado o cerrado? Esto debería estar indicado en la matriz causa-efecto del proyecto, llamada también matriz de entradas y salidas o "*input-output matrix*" en inglés. Esta matriz refleja la secuencia de operación basada en la filosofía operativa del edificio y los códigos y normas de seguridad contra incendios aplicables.

La matriz causa-efecto es por consecuencia parte integral de las Pruebas Integradas y es típicamente desarrollada, en la fase de diseño, por el ingeniero de protección contra incendios del proyecto y generalmente está incluida en los planos de alarma y detección. Quiero enfáticamente reiterar la importancia de la existencia de la matriz causa-efectos en cualquier tipo de edificio. Sin ella es imposible programar el panel y efectuar correctamente las Pruebas Integradas.

Agentes de Pruebas Integradas planeando las pruebas de los sistemas contra incendios en una central eléctrica (Foto: Cortesía IFSC)

¿QUIÉN DEBE EFECTUAR LAS PRUEBAS INTEGRADAS?

Las Pruebas Integradas de los sistemas de protección contra incendios y seguridad humana deben ser efectuadas en presencia de los contratistas de los distintos sistemas, quienes deben operar los equipos en presencia de un Agente de Prueba Integrada (API), quien debe liderar y ser responsable por las pruebas. El API es una entidad identificada por el dueño del edificio, que planifica, coordina, documenta, implementa y aprueba las Pruebas Integradas. El API es típicamente una firma de ingeniería de protección contra incendios calificada, que debe ser distinta e independiente a cualquier instalador de los sistemas contra incendios. Las Pruebas Integradas deben quedar documentadas en formularios de prueba que deben indicar el protocolo de prueba y sus resultados. El API debe indicar, si las Pruebas Integradas son satisfactorias, si el edificio es apto para su ocupación u operación.

Durante la reciente pandemia, las Pruebas Integradas se empezaron a efectuar, con éxito debo mencionar, de manera virtual (ver imagen anexa). Aunque el proceso de prueba virtual es generalmente un poco más largo, estas pruebas pueden tener un costo más económico para el dueño del edificio.

FRECUENCIAS DE LAS PRUEBAS INTEGRADAS

Las Pruebas Integradas se deben efectuar en proyectos nuevos, antes de la apertura del edificio, pero también es requerida en proyectos existentes donde originalmente no se efectuaron Pruebas Integradas. La NFPA da un periodo de cinco años para que los edificios existentes lleven a cabo esta prueba, a partir de la fecha donde la NFPA 4 fue adoptada. También se requiere que los edificios tengan una Prueba Integrada Periódica y su frecuencia depende de la importancia del edificio. Para un edificio como por ejemplo una

Comisionamiento es un proceso sistemático bajo el cual se asegura, verifica y documenta que los requerimientos de seguridad humana y protección contra incendios están correctamente ejecutados durante la concepción, diseño, instalación y arranque del proyecto

industria, edificio de altura, hospital o aeropuerto, la Prueba Integrada Periódica debería ser cada tres a cinco años, pero en ningún caso, para otros edificios, a intervalos mayores a 10 años.

DIFERENCIA CON COMISIONAMIENTO

El tema de la puesta en marcha de los sistemas contra incendios se empezó a regularizar en seguridad contra incendios desde el 2012, cuando NFPA emitió su primer documento sobre Comisionamiento (Cx). Esto se normó con la edición de la NFPA 3, Práctica Recomendada para el Comisionamiento de Sistemas de Protección Contra Incendios y Seguridad Humana[1].

En un edificio, el Comisionamiento se refiere al procedimiento bajo el cual se verifica que los sistemas de seguridad contra incendios cumplen los objetivos del usuario y las normas de referencia, en todas sus fases, desde su concepción, pasando por sus fases de planeación, diseño y construcción/instalación, hasta su puesta en marcha, y que al término del proyecto los sistemas de seguridad contra incendios sean efectivos y funcionales. Comisionamiento es un proceso sistemático bajo el cual se asegura, verifica y documenta que los requerimientos de seguridad humana y protección contra incendios están correctamente ejecutados durante la concepción, diseño, instalación y arranque del proyecto. Es como el ISO 9000 de los sistemas de seguridad contra incendios de un edificio.

Sin embargo, el Comisionamiento de los sistemas contra incendios no es mandatorio y se considera algo "aspiracional", es decir que "sería bueno hacerlo" pero no como algo requerido o recomendado en los códigos de incendios. Hoy día sólo en proyectos muy grandes, plantas nucleares o proyectos militares se ejecuta comisionamiento por pedido del dueño de la instalación. Es importante entonces entender que las Pruebas Integradas son requeridas, mientras que el Comisionamiento no es mandatorio en ningún edificio. ■

Referencias:

1 La NFPA 3, edición 2012, incluía además del tema de comisionamiento, las pruebas integradas de los sistemas de protección contra incendios y seguridad humana. A partir de 2015, este documento se subdivide en NFPA 3, Recommended Practice for Commissioning of Fire Protection and Life Safety Systems y una nueva NFPA 4, Standard for the Integrated Testing of Fire Protection Systems and Life Safety Systems, extrayendo los capítulos referentes a Pruebas Integradas de la NFPA 3 original. La última edición de estos documentos es de 2021.

GRUPO
CORPORATIVO
DE PREVENCION

NUESTRA EXPERIENCIA
DA
RESULTADOS

20 AÑOS

AÑOS DEDICADOS A LA SEGURIDAD
DE NUESTROS CLIENTES

LEALTAD, COMPROMISO, CONFIANZA, EFECTIVIDAD

SON LA BASE DE NUESTROS SERVICIOS

CONTACTO

Leona Vicario No. 6 Cuautitlán Izcalli

ventas@grupogcp.mx

55 4890 8325

SÍGUENOS EN REDES SOCIALES

@grupocorporativodeprevencion

@grupocorporativodeprevencion

@GCP_seguridad

contamos con las afiliaciones:

ASIS INTERNATIONAL

AMESP

CNSP

DECÁLOGO

DE BUENAS PRÁCTICAS DE INSTALACIÓN EN SISTEMAS DE DETECCIÓN Y ALARMAS DE INCENDIOS

MÉXICO | Perla Liliana Ortega Porcayo

Foto: @Freepik

Los instaladores de sistemas fijos de detección de llamas y gases deben estar calificados, tener su licencia y comprender qué es lo que están instalando

1. Capacitación. La formación en el sistema a instalar es fundamental, para ello debes asegurarte de contar en tus equipos de trabajo con personal certificado y con experiencia de campo.

2. Planeación. Asegúrate de que tu instalación cuente con todas las herramientas necesarias y los análisis de riesgos para determinar el equipo de protección personal a utilizar y las medidas de control que mantengan a tu personal seguro en todo momento.

3. Instalación eléctrica regulada y en buen estado. Si dentro de tu alcance realizarás el suministro eléctrico al panel de incendio desde el centro de carga que te asigne el cliente, asegúrate de utilizar código de colores que establece la norma y que el suministro venga preferentemente de un UPS.

4. Evita sabotajes a tu sistema. Asegúrate de que en tu instalación se respete la distancia que debe existir entre los dispositivos del sistema contra incendio (detectores de humo) y los aires acondicionados para que no existan interferencias que eviten que el sistema detecte correctamente un incendio incipiente.

5. Aplica la normatividad. Utiliza materiales listados para instalaciones de sistemas contra incendio, por ejemplo, para elegir el cable adecuado, consulta el apartado 760-179 la NOM-001-SEDE-2012, asegúrate también de que el sistema contra incendio vaya en tubería independiente, es decir que no esté compartido con servicios de luz, videovigilancia, redes, etc.

6. Cuida tu instalación. Asegúrate de que en el cableado no existan empalmes entre dispositivos, y en caso de tener que hacer una derivación en T, ubícala en el plano. Esto no sólo mejora el desempeño del sistema, sino que además facilita la localización de fallas.

7. *Back up.* Asegúrate de que el sistema cuente con respaldo de baterías a partir del cálculo de capacidad de las mismas, para que en caso de falla de alimentación de corriente alterna siga operando por 24 horas en *stand-by* y 5 o 15 minutos en condición de alarma (conforme lo dicte la autoridad competente).

8. Cuida la salud de los demás. El equivalente a "come frutas y verduras" en un sistema contra incendio es asegurarte de que las luces estroboscópicas de las alarmas estén sincronizadas, para evitar causar ataques epilépticos a personas con este padecimiento.

9. Recomendación al cliente. Asesora a tu cliente para que cuente con un pequeño *stock* de dispositivos periféricos del sistema, que le permita reemplazarlos en el menor tiempo en caso de falla, bajo la consigna de que la prioridad de estos sistemas es la protección de la vida de las personas.

10. Accesibilidad del panel de incendio. Asegúrate que el panel de incendio esté instalado en un lugar seguro, monitoreado por personal autorizado, debidamente capacitado y con accesibilidad para el proveedor de mantenimiento y brigadas de incendio. ■


Foto: @Freepik


Foto: @Freepik

Perla Liliana Ortega Porcayo, directora general de MAK Extinguisher de México S.A. de C.V.

Más sobre el autor:


Más que una empresa
de seguridad...
SOMOS GRIP
Traslados VIP
Protección Ejecutiva
Gripers
(Especialistas en
Seguridad Intramuros)
Capacitación
en Manejo de
Armas de Fuego
Auditoría
y Consultoría
Análisis
de Riesgos
Análisis
de
Confianza
Vigilancia,
Detección de Vigilancia
y Contravigilancia
CERTIFICADOS
ISO 9001:2015
redconocer
ASIS
CNS
AMESP
EXECUTIVE
PROTECTION
SUMMIT 2022
www.grip.mx
GRIPsecurity
soygriper
Global Risk Prevention
130 Años
OFRECIENDO
soluciones
#SOYGRIPER
Río Frío 143, Colonia Magdalena Mixhuca, Alcaldía Venustiano Carranza C.P. 15850 CDMX
Tel. 55 5335 1632 / 55 4336 4090

LOS ATAQUES QUE VIENEN: PREDICCIONES SOBRE CIBERSEGURIDAD 2023

Foto: Freepik

Es fundamental que tanto a nivel personal, empresarial y gubernamental haya un mayor conocimiento sobre la importancia de la ciberseguridad

MÉXICO | Carlos Ortiz Bortoni

Se terminó un año en el que los ataques cibernéticos, las violaciones de datos, estafas digitales y los ataques de *ransomware* fueron una constante. Durante años, las grandes empresas eran los principales objetivos de los ciberdelincuentes, pero el comenzar a apostar por tecnología más sofisticada para protegerse dificultó los intentos de ataque. Sin embargo, este fue el escenario perfecto para que los atacantes voltearan a ver en 2022 a las pymes como un nuevo objetivo sabiendo que muchas de estas empresas cuentan con un entorno no tan protegido.

Para 2023, hay un factor extra que entra en juego tanto para las grandes empresas como para las pymes: las condiciones macroeconómicas desafiantes a nivel mundial harán que las organizaciones opten por reevaluar el dinero destinado al área de TI tradicional y a ciberseguridad. Será crucial en 2023 que se priorice y, en medida de lo posible, aumente el gasto en seguridad en lo relacionado con los sistemas de tecnología operativa (OT) debido a que los ataques a la infraestructura van en aumento. Para que los entornos de OT actuales estén mejor protegidos, es necesario que las áreas de TI tengan visibilidad, seguridad y control completo para garantizar un funcionamiento continuo y seguro de las instalaciones, reduciendo los riesgos.

MIGRACIÓN A ESQUEMAS HÍBRIDOS

Otro factor de riesgo que vemos para 2023 es que los empleados que trabajaban de forma remota poco a poco seguirán migrando a esquemas híbridos, por lo que tener muchos empleados cambiando de lugar diariamente "abrirá puertas" a vulnerabilidades relacionadas con dispositivos de acceso o credenciales comprometidas. Los atacantes son conscientes de esto y es por ello que los usuarios finales continuarán siendo en 2023 uno de los objetivos más frecuentes para intentar vulnerar los datos de una organización de cualquier tamaño, por lo que la capacitación por parte de las empresas será fundamental para prevenir riesgos.

Los usuarios finales continuarán siendo en 2023 uno de los objetivos más frecuentes para intentar vulnerar los datos de una organización de cualquier tamaño, por lo que la capacitación por parte de las empresas será fundamental para prevenir riesgos

En 2022, vimos explotar la tendencia de robo a información protegida por diversos gobiernos, por lo que para 2023 esperamos que en América Latina se apueste por reconocer la importancia de OT y se busque la implementación o mejora de las políticas relacionadas con ciberseguridad. A medida que los gobiernos consideren que es un tema crucial, se establecerán estándares y mejores prácticas para el manejo y uso de información y datos en la región.

Otro de los temas fundamentales para el 2023 es lo relevante que se ha vuelto para las organizaciones el *smart budgeting*. Los costos de inversión en ciberseguridad son uno de los pilares más importantes a medida que los intentos de ataques se vuelven cada vez más frecuentes y sofisticados, por lo que el precio de mitigar un incidente aumenta rápidamente. Un millón de dólares invertido a tiempo puede ahorrar costos de hasta 25 millones más tarde si una organización es víctima de un ataque de *ransomware*, aunado a los graves daños que crea a la reputación de una empresa, la pérdida de clientes y costos legales, de acuerdo con el Centro de Quejas de Delitos en Internet del FBI.

Finalmente, una tendencia que seguirá en incremento para 2023 será la extorsión como una de las tácticas más "sencillas", pero efectivas para llevar a cabo el robo de datos. La notoriedad y el éxito que alcanzaron este año grupos como Lapsus$ al robar el código fuente e información valiosa de las empresas para después pedir grandes cantidades de dinero marcó un precedente para que otros grupos imiten sus tácticas a nivel mundial.

Recapitulando, esto es lo que esperamos para 2023 en materia de ciberseguridad:

- Mayor intento de ataques a pymes a nivel mundial.
- Los esquemas híbridos de trabajo abrirán más brechas de seguridad.
- Una mejora en América Latina en políticas relacionadas con ciberseguridad.
- Mayor conciencia en inversión destinada a ciberseguridad en las organizaciones de todos los tamaños.
- Intentos de extorsión para robar información valiosa de las empresas.

Así que, en definitiva, es fundamental que tanto a nivel personal, empresarial y gubernamental haya un mayor conocimiento sobre la importancia de la ciberseguridad, lo que cada uno puede hacer desde su trinchera y cómo generar una cultura de prevención más que de soluciones reactivas ante un ataque inminente. ■

Los costos de inversión en ciberseguridad son uno de los pilares más importantes a medida que los intentos de ataques se vuelven cada vez más frecuentes y sofisticados, por lo que el precio de mitigar un incidente aumenta rápidamente

Foto: Freepik

Carlos Ortiz Bortoni,
director general de Tenable México.

Más sobre el autor:

CONTROL®

SEGURIDAD PRIVADA INTEGRAL

ÁREAS DE NEGOCIO

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

EMPRESA SOCIALMENTE RESPONSABLE

ISO 9001:2015 OC-0080/13

BASC

SUPER EMPRESAS EXPANSIÓN 2022 TOP

www.seguridadcontrol.com.mx

@segcontrol

PHISHING A CUENTAHABIENTES PODRÍA CULMINAR EN UN ATAQUE DE *RANSOMWARE* EXITOSO A LA INSTITUCIÓN FINANCIERA

Los ataques de phishing contra los servicios financieros registraron un incremento del 47% durante el segundo trimestre de 2022

Foto: Freepik

MÉXICO

La microsegmentación interrumpe la cadena de ataque de *ransomware* en las fases más tempranas antes de que se produzcan los daños

Los ataques de *phishing* en el sector financiero pueden representar pérdidas de hasta 17 mil 700 dólares por minuto. Por otro lado, la gran recompensa económica de los ataques de phishing exitosos en los servicios financieros es una de las muchas razones por las Enemy at the Gates (Enemigo en Puerta), realizado por Akamai Technologies, la empresa de tecnologías en la Nube que potencia y protege la vida en línea (que adquirió Guardicore recientemente).

Oswaldo Palacios, *Senior Account Manager* para Guardicore, ahora parte de Akamai, destacó que el alza en los ataques de *phishing* contra los servicios financieros sigue siendo muy preocupante, ya que de acuerdo con dicho estudio se presentó un aumento significativo del primero al segundo trimestre del 2022, pasando del 32% al 47%, además el directivo advirtió que un *phishing* exitoso puede culminar en un ataque de *ransomware*.

El *phishing* es una de las herramientas más utilizadas por los atacantes quienes mayormente se dirigen a los clientes de las instituciones financieras más que a la institución como negocio. Este informe indicó que un 80.7% de las campañas de ataques de *phishing* se dirigieron a consumidores en lugar de a cuentas de negocio (19.3%).

Dicha demanda se debe a las cuentas comprometidas de consumidores en la Dark Web que se utilizan para lanzar ataques de segunda fase relacionados con el fraude. Mientras que los ataques dirigidos a cuentas de negocio pueden hacer que la red de una empresa se vea comprometida con *malware* o *ransomware*, o que se filtre información confidencial.

Oswaldo Palacios resaltó que un ataque que comienza cuando un empleado hace clic en un enlace en un correo electrónico de *phishing* puede terminar con la empresa sufriendo importantes daños financieros y de reputación. El eslabón más débil en un sistema de seguridad no es un fallo oculto en el código informático, sino una persona que no comprueba la procedencia de un correo electrónico.

"Para la mayoría del *ransomware*, parece que el vector de infracción más común es el *phishing*, que hace que el usuario abra un correo electrónico o mensaje de texto haciéndose pasar por una institución de confianza para engañarle y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial. Gracias a la venta de kits de *phishing* fácilmente disponibles en el mercado clandestino a precios económicos, los ciberdelincuen-

tes pueden lanzar ataques a sus objetivos previstos", explicó el especialista.

Otro dato revelador del informe Enemy at the Gates es que los ataques de *phishing* eluden la autenticación de dos factores (2FA). Kr3pto fue el kit de *phishing* más utilizado en el segundo trimestre de 2022 dirigido a instituciones financieras. Una vez comprometidas, las credenciales objetivo pueden dar lugar a un acceso no autorizado a redes seguras o actividades fraudulentas mediante la introducción de técnicas que esquivan las soluciones 2FA utilizando tokens de contraseña de un solo uso o notificaciones automáticas.

La investigación de Akamai reveló que las empresas requieren la adopción de protecciones multifactor más sólidas. FIDO2, por ejemplo, es el último estándar que ofrece una mejor seguridad, ya que no requiere contraseña y solicita que los usuarios se autentiquen localmente (usando biometría, por ejemplo) para visitar sitios web o realizar transacciones en línea. Debido a que ya no requiere ningún nombre de usuario o contraseña, no hay más credenciales para permitir ejecutar un ataque de *phishing*.

MICROSEGMENTACIÓN, INTERRUMPE LA CADENA DE ATAQUE

El *ransomware* es uno de los ataques más devastadores que los clientes y cualquier organización financiera podrían sufrir y que afectaría la confianza del usuario. Es un vector de amenaza que debe ser rastreado y mitigado de cerca; de acuerdo con el estudio Enemy at the Gates, así es la cadena de ataque del *ransomware:*

1. **Infección inicial:** el *hacker* deberá primero vulnerar el perímetro, los entes maliciosos deben conseguir un punto de apoyo inicial.
2. **Movimiento lateral:** el *ransomware* también usa técnicas comunes de movimiento lateral para moverse a través de la red que cubre MITRE, como WMI, PsExec, tareas remotas programadas, RDP, WinRM y PsExec, así como *exploits* de día cero como EternalBlue y BlueKeep.
3. **Exfiltración:** una vez que los ciberdelincuentes obtienen privilegios de nivel superior, el siguiente paso es robar nombres de cuenta y contraseñas. Las vulnerabilidades de día cero también son fundamentales durante esta etapa para obtener credenciales en la red.
4. **Cifrado:** si el *ransomware* entra de alguna manera en un equipo de destino, una política de segmentación adecuada minimiza el daño.
5. **Nota de *ransomware*:** en la pantalla secuestrada aparecerá un texto y archivo txt pidiendo el rescate.
6. **Ganancia monetaria para el atacante:** se recomienda no pagar.

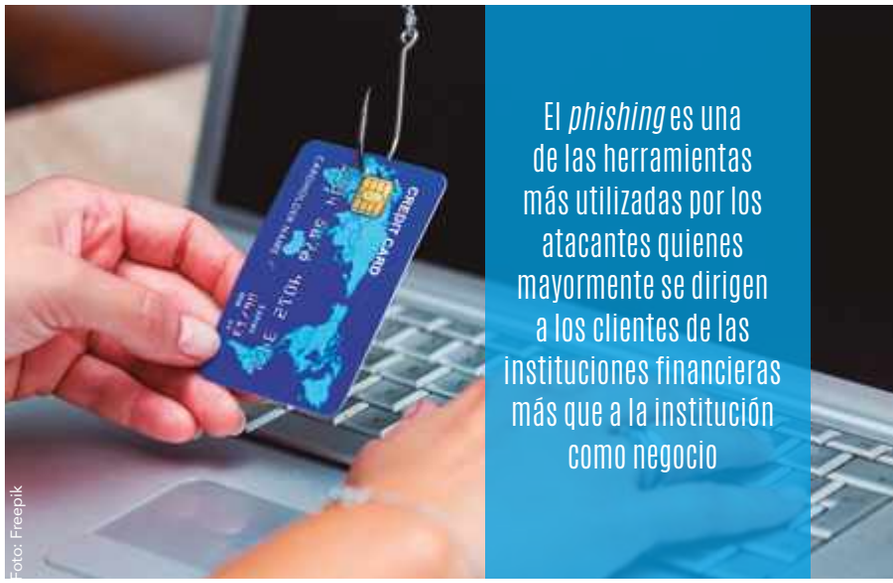


Foto: Freepik

El *phishing* es una de las herramientas más utilizadas por los atacantes quienes mayormente se dirigen a los clientes de las instituciones financieras más que a la institución como negocio

Además de adoptar las mejores prácticas y procesos de la industria como Cyber KillChain, la arquitectura Zero Trust 800-207 de NIST y el estándar FIDO2 más reciente, Oswaldo Palacios destacó que la microsegmentación se está convirtiendo en una herramienta cada vez más importante para los equipos de TI que se enfrentan al reto de mantener las políticas de seguridad y el cumplimiento en consonancia con el rápido ritmo de cambio de los centros de datos dinámicos, y los entornos de Nube y de Nube híbrida actuales.

A decir de Palacios, la microsegmentación interrumpe la cadena de ataque de *ransomware* en las fases más tempranas antes de que se produzcan los daños. Además ofrece tres ventajas principales: 1. una visibilidad completa del centro de datos a nivel de proceso; 2. crear políticas que permitan tener un ambiente Zero Trust, y 3. visualización y control en el proceso de comunicación.

Uno de los grandes obstáculos a los que se enfrentan muchas organizaciones es la falta de una visión clara de la actividad en todos los entornos locales y en la Nube. "La microsegmentación recopila y muestra información granular sobre los usuarios, los sistemas y los flujos de comunicación, utilizando la inteligencia artificial y las integraciones con las fuentes de datos existentes para añadir contexto", explicó Oswaldo Palacios.

Por último, el especialista reiteró que la combinación de visibilidad completa y la creación de políticas impulsadas por el contexto es lo que hace que una solución de microsegmentación aporte un gran valor a las instituciones financieras y ofrezca más oportunidades para interrumpir la cadena de ataques de *ransomware* en las fases más tempranas. ■

Fuente: Guardicore

Foto: Freepik

PRONÓSTICO DE AMENAZAS INFORMÁTICAS PARA EL 2023

Estafas con criptomonedas e inversiones, préstamos falsos, Inteligencia Artificial, entre otras, son las actividades pronosticadas por el equipo de McAfee Thread Labs que serán las favoritas de los cibercriminales el próximo año

Foto: Freepik

MÉXICO

El 2022 está por terminar y nunca está de más prepararnos para ver qué nos deparará el año nuevo en cuanto a estafas digitales para hacer nuestro entorno *online* más seguro. Es por eso que el equipo de McAfee Threat Labs ha hecho algunas predicciones sobre el panorama de amenazas informáticas de 2023 y así mantenernos alerta ante estas situaciones.

Este pronóstico prepara el terreno para un 2023 que promete avances no sólo en la forma en que interactuamos con la tecnología, sino también en la forma en que ciertos delincuentes pueden explotarla, y perjudicarnos.

A continuación, te presentamos las situaciones a las que debes estar atento para no caer en ellas y mantenerte protegido mientras navegas en línea:

1. **Aplicaciones de Inteligencia Artificial:** en los últimos meses de 2022, varias aplicaciones de IA se pusieron a disposición del público, ahora cualquiera que tenga un teléfono celular o una computadora puede aprovechar esta tecnología. Esto significa que los avances proporcionaron beneficios a los delincuentes, al permitir una mejor falsificación y una manipulación más realista de las imágenes, datos, etc.
2. **Estafas financieras:** el panorama financiero de 2023 será difícil para la mayoría de las personas, esto puede generar vulnerabilidad ante los mensajes de las redes sociales y los anuncios en línea que ofrecen inversiones y préstamos falsos que pueden llevarlos a perder todo. Tan solo en el primer semestre del 2022, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) recibió 3.5 millones de reclamaciones relacionadas con fraudes financieros, por lo que los usuarios deben estar alerta de las páginas y enlaces que consultan.
3. **Criptomonedas:** este año vimos varias estafas en línea que usaban contenidos existentes para hacer más creíbles las estafas de criptomonedas. Se espera que esta práctica siga evolucionando en 2023 y que haga uso de videos falsos profundos, así como audio, para engañar a las víctimas para que les entreguen su dinero ganado con esfuerzo.
4. **Metaverso:** los llamados "metaversos" como Horizon de Facebook permiten que usuarios exploren mundos en línea que antes eran inimaginables. Cuando se lanzan estas plataformas y están en una fase inicial, los malhechores suelen intentar explotar la falta de conocimiento de su funcionamiento y aprovecharse para estafar a la gente.
5. **ChromeOS:** la capacidad de ChromeOS para ejecutar aplicaciones de Android, combinada con su amplia adopción, crea el clima para que quienes tienen malas intenciones le presten más atención. En 2023 se prevé que los usuarios de Chromebook estén entre los millones de víctimas desprevenidas que descargan y ejecutan contenido peligroso, ya sea de aplicaciones Android maliciosas, de aplicaciones multiplataforma o de extensiones de la Chrome Web Store.
6. **Web3:** los servicios descentralizados de Internet como las NFT, Blockchain y Bitcoin ahora son muy populares, pero a medida que incremente la conciencia sobre este tema, los consumidores comenzarán a explorar estas ofertas de la Web3 sin entender completamente lo que significan o los peligros que deben conocer, dejándoles expuestos a las estafas mientras invierten tiempo y dinero en las cripto o en la creación de sus propias NFTs.

Ahora que conoces cuáles son algunas de las estafas que estarán rondando durante 2023, no olvides mantener tu conexión segura, no darles clic a enlaces sospechosos y tener una conexión VPN segura. ■

Fuente: McAfee

SAFEWAY CORPORATION

Servicios:

- Servicios de monitoreo inteligente, logístico y telemetría.
- Asesorías y Consultorías en procesos logísticos, cadena de suministros y seguridad.
- Distribución de periféricos en el transporte enfocados en soluciones en seguridad y rentabilidad del negocio.
- Asesorías y Consultorías en continuidad de negocio tomando como base el contexto actual de la seguridad en la cadena de suministro.
- Custodias virtuales de monitoreo.
- Monitoreo en protección ejecutiva.

ASUME · Circulo Logistic · ASIS · ALAS Asociación Latinoamericana de Seguridad · COPARMEX Ciudad de México · ASIS International · Seguridad por México

Tel. 55-6631-6397
55-8791-8659

hector.romero@safeway.mx

Autopista México- Querétaro 3069 – C Industrial Tlanepantla
CP 54030 Talnepantla Edo. De México.

www.safeway.mx

VER A LA CIBERSEGURIDAD COMO ALGO PERSONAL

El mundo digital ofrece múltiples bondades, aunque a veces las personas olvidan que la vida en línea es intrínsecamente riesgosa y siempre potencialmente peligrosa

Foto: Freepik

MÉXICO | Roberto Ricossa

Según Javelin Strategy and Research, en su estudio de fraude de identidad de 2021, el fraude de apropiación de cuenta (Account Take Over) resultó en más de 6 mil millones de dólares en pérdidas totales en sólo 12 meses

Se define a la reputación como la opinión, idea o concepto que la gente tiene sobre una persona, una cosa, incluso sobre una organización o empresa.

Se podría pensar que para ciertas personas una mala reputación no representa problema alguno. Aunque se debe tomar en cuenta que tarda tiempo en construirse, y que puede perderse de un instante a otro. Por ello, vale la pena preguntar ¿Qué tan importante es tu reputación?

Hoy día los cambios tecnológicos han permitido un acceso rápido e instantáneo a la información. Asimismo, la disponibilidad de múltiples dispositivos han facilitado la movilidad y la comunicación interpersonal, donde las redes sociales han jugado un papel transcendental.

Hablamos de un mundo totalmente dinámico, ágil y muy cambiante, que al mismo tiempo ha provocado que la reputación de muchas personas se vea afectada de la noche a la mañana.

¿Quién no ha recibido el mensaje de algún amigo, familiar o conocido diciendo: "Si te llegó una solicitud en Facebook, o en Instagram de mi parte, por favor no la aceptes. No soy yo"? Incluso la notificación de un amigo cercano asegurando: "Acabo de ganar 10 mil dólares haciendo un negocio con Bitcoin, se los recomiendo ampliamente. Haz clic aquí".

O en su defecto mensajes con amenazas diciendo que si no se entrega algo a cambio, divulgarán información personal; o simplemente restringen el acceso a los dispositivos dejando al afectado completamente fuera de línea.

Según el IRTC (por sus siglas en inglés - Centro de Recursos de Robo de Identidad de Estados Unidos), en 2021 hubo un incremento de más de 1000% en robos de credenciales o cuentas de redes sociales.

De igual manera 85% de los encuestados, mostraron que su cuenta de Instagram había sido comprometida, 25% los de Facebook, 48% recuerdan haber hecho clic en el link que algún amigo envió, 22% respondieron a alguna solicitud de algo relacionado con criptomonedas, y 27% reportó haber perdido ingresos por esa situación.

La encuesta también mostró que 66% informó haber experimentado fuertes reacciones emocionales al perder el control de su cuenta de redes sociales: 92% se sintió violado, 83% preocupado y ansioso, 78% enojado, 77% vulnerable y 7% suicida.

BIENESTAR EMOCIONAL

Si bien para algunos el robo de identidad en las redes sociales es sólo un mero inconveniente, estas cifras demuestran cuán estrechamente vinculada está la reputación en línea de una persona con su bienestar emocional.

Un ataque se vuelve personal cuando toman los ahorros de toda una vida, y desaparece el entorno de seguridad no sólo del individuo sino también de su familia. La seguridad es una necesidad humana básica, de acuerdo a la jerarquía de necesidades de Maslow, sólo los alimentos y el agua están por encima de ella.

Quien se sienta aliviado por no ser usuario de las redes sociales, tal vez deba tomar en cuenta algunos aspectos que le pueden ser muy familiares. 52% de las personas utilizan el mismo *password* tanto para sus cuentas personales como para las de su trabajo. Se plantea que se utiliza el mismo *password* en al menos 13 sitios o aplicaciones diferentes.

¿Y qué ocurre cuando se afecta la reputación de un negocio? Según el estudio de Intellicheck, 28% de los consumidores dejarán de usar un sitio web o una aplicación si su cuenta fue pirateada. Es un dato relevante si se toma en cuenta que la mayoría de las empresas interactúan con sus clientes a través de una página web o alguna aplicación, quienes esperan que estos canales de contacto tienen como máxima prioridad la privacidad y seguridad.

Los ataques de credenciales basados en la identidad son la principal fuente de ataques web automatizados que típicamente conducen al fraude. Información que posteriormente estará disponible para su compra en foros de ciberdelincuencia.

La tasa de éxito de los ataques basados en credenciales oscila entre 0.2 % y 2%. Si bien estos porcentajes pueden parecer pequeños, es importante recordar que miles de millones de credenciales están disponibles de forma gratuita o a un costo nominal.

Según Javelin Strategy and Research, en su estudio de fraude de identidad de 2021, el fraude de apropiación de cuenta (Account Take Over) resultó en más de 6 mil millones de dólares en pérdidas totales en sólo 12 meses.

Entonces podemos afirmar que la ciberseguridad es la mayor amenaza individual para la sociedad actual. El robo de identidad, el *ransomware* y las fugas de información a gran escala dominan los titulares hoy día, haciendo evidente que nadie es inmune, ni los individuos, ni las pequeñas ni las grandes empresas e incluso los gobiernos.

Ante dicho panorama la batalla contra estos ataques digitales se ha convertido en algo personal, de ahí la necesidad de hacer todo lo posible para protegernos de las devastadoras consecuencias del ciberdelito.

El mundo digital ofrece múltiples bondades, aunque a veces las personas olvidan que la vida en línea es intrínsecamente riesgosa y siempre potencialmente peligrosa. Creemos que es posible un mundo digital mejor, donde podamos disfrutar libremente de sus beneficios, sin comprometer nuestra seguridad, privacidad y reputación.

Es con el apoyo de la misma tecnología como toda organización puede adaptarse a un entorno cambiante, ser eficiente y garantizar transacciones seguras, cuidando la reputación y el valor de su negocio, a través de protección tanto de sus aplicaciones como de la integridad de sus clientes.■

Roberto Ricossa, VP de Latinoamérica de F5.

Más sobre el autor:

52% de las personas utilizan el mismo *password* tanto para sus cuentas personales como para las de su trabajo

Foto: Freepik

Si bien para algunos el robo de identidad en las redes sociales es sólo un mero inconveniente, estas cifras demuestran cuán estrechamente vinculada está la reputación en línea de una persona con su bienestar emocional

LA NUBE **IMPULSA A LOS NEGOCIOS**, PERO **LA SEGURIDAD** SIGUE SIENDO UN **RETO PARA LAS EMPRESAS**

La encuesta realizada por Fortinet y Cybersecurity Insiders a más de 800 profesionales de la ciberseguridad de todo el mundo revela las experiencias y planes de las organizaciones respecto a la Nube

MÉXICO

La adopción de la Nube va en aumento, actualmente 30% de las empresas ejecutan ahí más de la mitad de sus cargas de trabajo, lo que representa un aumento de 6% respecto al año pasado, mientras que un 58% adicional espera alcanzar este nivel en los próximos 12 a 18 meses.

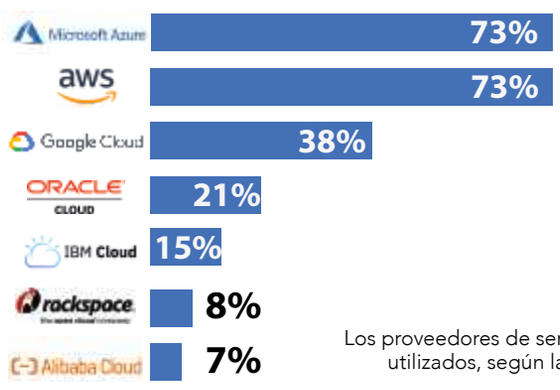
Esto de acuerdo con datos recopilados dentro del Informe de Seguridad en la Nube 2022, publicado por Fortinet, líder mundial en soluciones de ciberseguridad amplias, integradas y automatizadas, y la comunidad *online* Cybersecurity Insiders, a partir de una encuesta mundial realizada en marzo de este año a 823 profesionales de la ciberseguridad de organizaciones de diversos tamaños e industrias.

Según el estudio, entre los beneficios que obtienen las empresas al migrar a la Nube se encuentran una mayor rapidez de comercialización (51%), una mayor capacidad de respuesta a las necesidades de los clientes (50%) y un ahorro dentro de los costos (39%). Además, los encuestados confirman que la Nube está cumpliendo la promesa de capacidad y escalabilidad flexibles (53%), más agilidad (50%) y mayor disponibilidad y continuidad del negocio (45%). Los servicios y cargas de trabajo más implementados en la Nube son los de seguridad (58%), seguidos de los de computación (56%), almacenamiento (55%) y virtualización (53%).

Por otro lado, los principales imprevistos que frenan o impiden la adopción de la Nube son la falta de visibilidad (para el 49% de los encuestados), el elevado costo (43%), la falta de control (42%) y la falta de seguridad (22%). La encuesta también reveló que los mayores retos a los que se enfrentan las organizaciones no están necesariamente relacionados con la tecnología, sino con las personas y los procesos. La falta de personal capacitado es el mayor obstáculo para una adopción más rápida, según el 40% de los encuestados (frente al 37% del año pasado), seguido del cumplimiento de la legislación y la normativa (33%) y los problemas de seguridad de los datos (31%).

"La Nube ya ha demostrado ser un importante facilitador para las empresas de todos los tamaños e industrias, pero sigue siendo un reto para las empresas en varios aspectos. Abordar temas como la seguridad y la gestión es fundamental para acelerar el proceso de su adopción y aprovechar el negocio, así como invertir en la formación de profesionales para este segmento ya que esto puede representar un punto de inflexión en la búsqueda de los beneficios que la Nube puede traer", dijo Rafael Venancio, director de Negocios de la Nube de Fortinet para América Latina y el Caribe.

Actualmente, el 76% de las organizaciones utilizan dos o más proveedores de Nube. AWS y Microsoft Azure lideran la lista empatados, aunque Google y Oracle están aumentando rápidamente sus inversiones y su cuota de mercado.

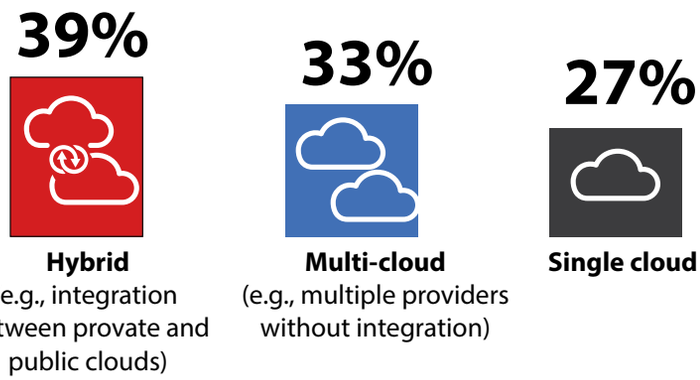


Los proveedores de servicio de Nube más utilizados, según la investigación

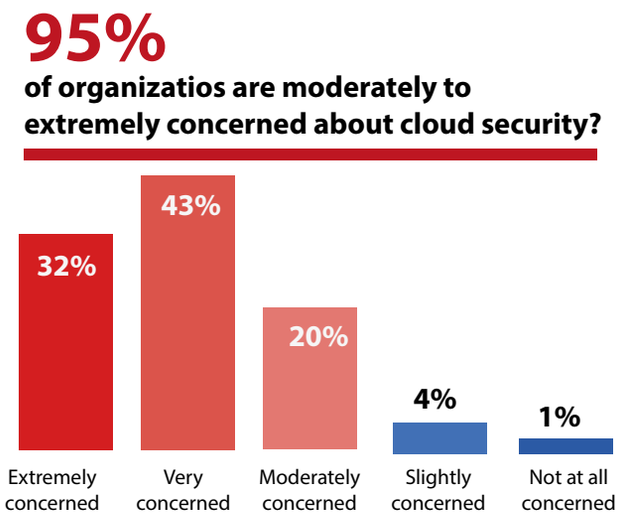
Foto: Freepik

Pero, ¿cuáles son las amenazas a la seguridad en la Nube que más preocupan a las empresas? Según la encuesta, la desconfiguración de la plataforma en la Nube sigue siendo el mayor riesgo para la seguridad (62%), seguido de las interfaces/API inseguras (52%, frente al 49% del año pasado), la exfiltración de datos confidenciales (51%) y el acceso no autorizado (50%).

El informe también revela que, para integrar servicios variados, proporcionar escalabilidad o garantizar la continuidad del negocio, el 39% de las organizaciones está optando por un enfoque de despliegue de Nube híbrida —un 3% más que el año 2021— o multicloud (33%).



El Informe de Seguridad en la Nube del año pasado se produjo en un contexto de ataques de *ransomware* cada vez más audaces y costosos y de la revelación de una grave vulnerabilidad de día cero en la popular herramienta de registro Apache Log4j, utilizada en muchas aplicaciones empresariales y plataformas en la Nube. No es de extrañar que el 95% de las organizaciones estén preocupadas por la seguridad.



Por ello, no es de extrañarse que se enfrenten a una complejidad y unos retos de seguridad cada vez mayores. La falta de conocimientos en materia de seguridad está a la cabeza (61%, frente al 57% del año pasado), seguida de la protección de datos (53%), la comprensión de cómo encajan las distintas soluciones (51%) y la pérdida de visibilidad y control (47%). Por esta razón, el 78% de los encuestados considera que es muy o extremadamente útil tener una única plataforma de seguridad en la Nube para proteger los datos de manera uniforme y completa en todo su espacio.

"Nunca se insistirá lo suficiente en que la seguridad en la Nube es una responsabilidad compartida entre la empresa y el proveedor, y que para lograr los objetivos de migración a este servicio, la seguridad es esencial. Precisamente por ofrecer una seguridad más eficiente y una menor complejidad, la gran tendencia del mercado se dirige hacia una plataforma de ciberseguridad en malla, como Fortinet Security Fabric, que agrupa la gestión, la visibilidad y la automatización, reduciendo drásticamente el tiempo de respuesta a las amenazas y el impacto que pueden causar las carencias de recursos", señaló Venancio. ■

Foto: Freepik

5 PREDICCIONES EN MATERIA DE CIBERSEGURIDAD PARA 2023

La ciberdelincuencia está en constante evolución y este año no será la excepción

Foto: Freepik

MÉXICO

Hace unos días terminamos el año 2022 y por ello, los expertos de Tenable, la compañía de gestión de exposición, te comparten a continuación algunas de las cinco principales tendencias en materia de ciberseguridad que estaremos viendo en 2023:

1. **El elemento humano:** la mayoría de los ataques cibernéticos han sido a causa de un error humano, principalmente a través de enlaces o correos electrónicos con información muy llamativa. Es por esto por lo que en este 2023 el objetivo más frecuente como punto de entrada a los ciberataques seguirá siendo el elemento humano.
"A medida que la pandemia retroceda, el empleado totalmente remoto cambiará a una forma híbrida de trabajar, con muchos empleados cambiando a diario de lugares menos seguros (hogar) a más seguros (oficinas), aumentando el riesgo de puertas abiertas y una 'puerta trasera' a los atacantes a través de dispositivos o credenciales comprometidos. Los atacantes son conscientes de esto, por lo que los usuarios finales y los servicios tercerizados incrementarán como el punto de entrada cada vez más frecuente en los ataques cibernéticos", señaló Omar Alcalá, director de Ciberseguridad de Tenable Latinoamérica.

2. **Criptomonedas:** los esquemas para hacerse rico rápido a través de inversiones en falsas criptomonedas, ha ido en aumento. El prospecto de ganar una suma millonaria a través de una mínima inversión es atractivo desde el punto de vista que se vea, sin embargo, hay que ser muy precavidos ante los estafadores cibernéticos.
"En 2023, dado que las condiciones económicas en todo el mundo siguen siendo inciertas, los esquemas rápidos para hacerse rico que involucran inversiones en criptomonedas falsas a través de las redes sociales y las citas en línea serán cada vez más exitosos, ya que las preocupaciones sobre el desempleo aumentan y el impacto de la inflación continúa afectando a los consumidores", expuso Satnam Narang, ingeniero *Senior* de Investigación en Tenable.

3. **Extorsiones:** en los últimos dos años, los grupos delictivos de *ransomware* han tomado mucha fuerza y han destacado de otras organizaciones dedicadas a los ataques cibernéticos. De acuerdo con el "Informe Retrospectivo del Panorama de Amenazas de 2021", al menos el 38% de todas las violaciones de datos en 2021 fueron el resultado de ataques de *ransomware*.
"La extorsión será una fuerza cada vez más disruptiva para las empresas en todas las industrias en 2023. En 2022, vimos a los actores de amenazas de

Foto: Freepik

La extorsión será una fuerza cada vez más disruptiva para las empresas en todas las industrias en 2023. En 2022, vimos a los actores de amenazas de todas las motivaciones pasar a ataques sólo de extorsión y renunciar a las tácticas más complejas como el *malware* de cifrado de datos

todas las motivaciones pasar a ataques sólo de extorsión y renunciar a las tácticas más complejas como el *malware* de cifrado de datos (*ransomware*). La notoriedad y el éxito de los grupos de extorsión como Lapsus$ significa que otros grupos seguirán imitando sus tácticas", explicó Claire Tills, ingeniera senior de Investigación en Tenable.

4. **Gasto en ciberseguridad:** las condiciones macroeconómicas desafiantes que se están viviendo, harán que las empresas reevalúen el gasto en ciberseguridad en los sistemas críticos de tecnología operativa (OT, por sus siglas en inglés).
"Las empresas priorizarán y aumentarán proporcionalmente el gasto en seguridad en sus sistemas de tecnología operativa (OT) mucho más críticos. Las consecuencias de eventos de alto perfil como Colonial Pipeline han demostrado que el riesgo para OT es mayor y las discusiones sobre seguridad cibernética en la sala de juntas casi siempre incluyen la protección de OT", aseguró Marty Edwards, CTO – OT/IoT adjunto en Tenable.

5. **Metaverso:** el mundo virtual que ha tomado una gran popularidad en el último año, y tomará mayor fuerza durante el año entrante, ha puesto sobre la mesa un sinfín de posibilidades inimaginables, sin embargo, también podemos esperar nuevos y desafiantes retos en materia de ciberseguridad.
"Las empresas casi siempre corren por delante de la seguridad para buscar nuevas fuentes de ingresos, y veremos mucho de eso con el metaverso en 2023. Si la migración masiva a la computación en la Nube es una indicación de qué tan bien irá, muchas organizaciones saltarán con los pies por delante sin probar las aguas de seguridad y se encuentran en la parte más profunda", indicó Bob Huber, director de Seguridad en Tenable.

Si bien estas son algunas de las principales tendencias que el equipo de Tenable espera para 2023, es bien sabido que los cibercriminales se encuentran en constante evolución. ■

Fuente: Tenable

En 2023, dado que las condiciones económicas en todo el mundo siguen siendo inciertas, los esquemas rápidos para hacerse rico que involucran inversiones en criptomonedas falsas a través de las redes sociales y las citas en línea serán cada vez más exitosos

Foto: Freepik

SEGURIDAD EN HOSPITALES, AMENAZAS Y SOLUCIONES

Altos representantes de seguridad en el sector médico comparten sus estrategias ante los retos que se presentan en los hospitales

Foto: Creativeart - Freepik

MÉXICO

Antonio Venegas / Staff Seguridad en América

El sector hospitalario es una de las áreas más utilizadas por la población, al ser una necesidad básica entre los seres humanos. La atención que se le debe ofrecer al paciente debe ser de primera calidad, sin importar el lugar o el tipo de hospital que se elija. Sin embargo, esto no impide que los hospitales sean de los principales objetivos de la delincuencia que sin importar la rama, el lugar o el tipo de hospital, buscan concretar actividades delictivas en cualquiera de las áreas del mismo. Esto sin dejar de lado los riesgos a los que están expuestos los hospitales como cualquier otro establecimiento: siniestros, accidentes, situaciones de riesgo, e incluso, contingencias médicas como la pandemia por COVID-19 que afecta principalmente y de manera directa al sector hospitalario.

Ante estas situaciones, las técnicas empleadas para mantener la seguridad tanto para los pacientes, sus familiares y visitantes como para empleados, propios, contratados y otra población que asiste a ellos deben estar en constante evolución para mantener los incidentes en el menor grado posible, así como se debe tener la capacidad de prevenirlos y de que, en caso de que se presenten, saber cómo reaccionar y ejecutar los procedimientos adecuados. Pero ante un mundo que está en constante cambio, hay que estar siempre a la vanguardia de las nuevas tecnologías que se presentan y que puedan ser de utilidad en este campo específicamente. De igual forma debe existir la visión a futuro de poder adaptarse a los cambios que existan; estas tareas podrán parecer responsabilidad de la persona encargada de la seguridad, sin embargo, es algo que se debe trabajar en conjunto con toda la organización, un trabajo en equipo.

RIESGOS Y AMENAZAS

Dado el sector que se maneja, los riesgos están presentes a la orden del día y el saber reconocerlos permite estar preparados ante la situación para permitirse actuar ante la amenaza. Es por esto que expertos en el tema comparten sus conocimientos adquiridos a lo largo de su experiencia en el área.

Jonathan Ávila Sánchez, *Country Manager* de México y Centroamérica de la empresa EVERBRIDGE, reconoce que son múltiples los que se presentan y los cataloga de la siguiente manera:

- Amenazas a la Continuidad Operativa.
- Amenazas a los Activos Físicos (edificios, ambulancias, etc.).
- Amenazas a las personas (pacientes, empleados, ejecutivos viajeros).


Foto: Creativeart - Freepik

- Amenazas a la reputación del hospital derivado de una afectación en cualquiera de los tres puntos anteriores.

Por otro lado, Daniel Vázquez Cayetano, gerente de Desarrollo Tecnológico en SISSA DIGITAL, enfatiza más en los aspectos digitales que modernizan los hospitales hoy en día. "En el momento que un hospital se conecta a la red, su principal amenaza son los ataques para obtener su información, ya sea para hacer mal uso de ella y/o secuestrarla, para obtener dinero. Se debe contar con una infraestructura suficientemente robusta con las políticas de acceso bien definidas por parte del área que lo administra, así como para los usuarios que se conectan para consultar su información. Esto es de vital importancia ya que los usuarios que normalmente hacen uso de la infraestructura del hospital no son especialistas en tecnologías de la información, y de eso se aprovecha el atacante: un archivo adjunto en un correo electrónico, una liga en una página web, un mensaje de texto notificando una promoción, etc., son suficientes para abrirles el paso para que tengan acceso a su información", mencionó.

"Las consecuencias de este tipo de ataques son muy graves, hasta catastróficas, por la importancia de la información relevante que maneja un hospital, los expedientes de los pacientes, los datos personales de los pacientes y personal activo, manejo de sustancias controladas, manipulación de sus tecnologías, entre muchas otras cosas igual o más importantes".

De igual manera, Daniel Jiménez, director de la Organización GDC Gestión, Desarrollo y Crecimiento Empresarial, se dirige más hacia lo que corresponde al ambiente laboral de los hospitales: "Sin lugar a duda estos complejos 'son ciudades dentro de las ciudades' por su operación 24 horas y tráfico de personas en toda su magnitud, lo que hace que sean variados y de diferentes tipos, hoy en día sin embargo, existe uno que preocupa a la comunidad sanitaria y a los profesionales que protegen los activos de estos ambientes y es la violencia en el lugar de trabajo, vista como las diferentes formas de agresión a las personas que laboran o se encuentran allí", explicó Daniel.

"Problema que desde diferentes sitios como la Healthcare Security Community de ASIS International y de la International Association for Healthcare Security and Safety (IAHSS), se han venido abordando con esfuerzos principalmente en la investigación de este problema, para definir las mejores estrategias y técnicas que aborden la prevención, intervención, una respuesta temprana y no menos importante, la capacitación, que coadyuven a evitar lesiones o pérdidas de vidas en estas facilidades, con un enfoque holístico y que incluya la participación no sólo del personal de seguridad, sino que además, la vinculación de médicos, enfermeros y demás personal que pueda ser parte interesada en estas situaciones".

PRINCIPALES ERRORES

De igual forma, Daniel Jiménez compartió cuáles son las fallas más comunes que se presentan en el área de seguridad del sector hospitalario: "El principal error es creer que el sector del cuidado de la salud o Healthcare, es igual que los demás segmentos de la economía, las personas que llegan a este rubro piensan que los controles, las contramedidas y los riesgos son iguales, y la verdad es que tienen particularidades que lo hacen único. Principalmente los procesos, activos, vulnerabilidades y amenazas son diferentes y podemos encontrar una amplia gama, que le dan una complejidad única. Entender esto me ha ayudado a comprometerme cada día más y encontrar en diferentes autores y diferentes profesionales una verdad nueva que ha fortalecido mis conocimientos que he sabido poner al servicio de la comunidad desde estas infraestructuras".

"Otro error es un desconocimiento de la importancia de la protección de activos dentro de la organización, especialmente por la alta dirección, desde donde su principal respuesta es que la seguridad no es el objeto del negocio, y comparto este punto, pero estaremos de acuerdo, en que si le aporta al cumplimiento de los objetivos estratégicos de los hospitales y clínicas, de lo contrario sus pérdidas podrían comprometer su reputación, a los que tengan un débil proceso de gestión del riesgo y auditoría, generándole afectación a sus objetivos", señaló.

SOLUCIONES PRESENTADAS

A la par de la innovación tecnológica desarrollada en los últimos años que ha acompañado el crecimiento de distintos sectores empresariales, el sector hospitalario está obligado a actualizarse


Foto: Freepik

de igual forma dado que es uno de los sectores que trabajan con el recurso humano, mismo que posee la más alta prioridad en un negocio y en el cual, el más mínimo error debe evitarse a toda costa, ya sea un error en la información o hasta que se presente en forma de situaciones extraordinarias, llámese un siniestro o atentado, por ejemplo.

Dicho esto, las soluciones para prevenir y mitigar estas amenazas son muchas y cada una más innovadora si se habla en materia de seguridad. Saber cómo intervenir al momento de una situación de riesgo es fundamental.

"Son múltiples las soluciones de seguridad, pero más que hablar de soluciones, lo importante es transformar digitalmente los procesos para gestionar esos riesgos y amenazas de manera automatizada, de manera colaborativa y a través de múltiples canales de comunicación y dispositivos móviles", comentó Jonathan Ávila.

Él también presentó un ejemplo de estas soluciones por medio de la plataforma EVERBRIDGE. "La plataforma de Everbridge cubre de punta a punta todo el proceso de transformación digital en hospitales a través de una sola plataforma habiendo converger de manera agnóstica los dispositivos de seguridad física, plataformas de TI que soportan la continuidad operativa del hospital, y fuentes de información de alertamiento en tiempo real en la periferia del o los hospitales y también de lo que se dice en la web y redes sociales".

Daniel Vázquez, quien en conjunto con SISSA DIGITAL trabaja con el proyecto IXMAKI (una solución de gestión de seguridad ideal para hospitales), encontró este aspecto como un área de oportunidad de desarrollo para los centros médicos: "Un hospital tiene varios puntos de mejora o vulnerables a riesgos y amenazas, que pueden ser virtuales o físicos. En cuanto a amenazas virtuales, abundan los ataques cibernéticos (*malware, ransomware*), que impiden o dificultan el acceso a la información. Lo físico puede ir desde un control de acceso hasta la administración del hospital".

"Un control de acceso te permite controlar quién pasa físicamente por las áreas autorizadas por el sistema, qué medios de identificación son utilizados (biometría, tarjetas físicas o virtuales, etc.), y el horario permitido para el ingreso por ciertas zonas; ayuda a administración del material que se maneja en un hospital, que puede ir desde material de limpieza, medicamento controlado, inventario de equipo e instrumental médico y por muestras biológicas; y facilita la vigilancia en zonas de difícil acceso con ayuda de cámaras de vigilancia con funcionalidades que le dan un valor agregado, como lo son los analíticos e inteligencia artificial, capaces de lanzar alarmas por cada nivel de evento que se pueda presentar en un hospital. Cada área tiene su tecnología que puede ser implementada y enfocada a ayudar al proceso y operación del mismo", explicó.

Por otro lado, Daniel Jiménez recalcó la importancia de entender las técnicas que se utilicen para mitigar riesgos como un trabajo en equipo de toda la organización y no solo responsabilidad de un área en específico: "Particularmente las técnicas están enfocadas a desarrollar ejercicios en los que se logre entender que son problemas de todos y no de unos cuantos; de esta manera, la capacitación, la concientización y retroalimentación hacen parte primordial en la obtención del objetivo de buscar hospitales más seguros para el personal.

Otro aspecto para tener en cuenta es que no sólo, propendemos por los riesgos de seguridad (*security*) sino que también en nuestra retina están los riesgos asociados a seguridad ocupacional (*safety*) y los de paciente seguro, por cuanto la capacitación y constante actualización respecto a los estándares especialmente los clínicos en donde puede existir participación de seguridad para que este concepto de espacios seguros y servicios de calidad se cumplan desde el segmento de seguridad", explicó.

"Un hospital tiene varios puntos de mejora o vulnerables a riesgos y amenazas, que pueden ser virtuales o físicos. En cuanto a amenazas virtules, abundan los ataques cibernéticos *(malware, ransomware)*, que impiden o dificultan el acceso a la información. Lo físico puede ir desde un control de acceso hasta la administración del centro médico", Daniel Vázquez

Foto: Freepik

TENDENCIAS TECNOLÓGICAS EN 2023

Con la finalidad de estar a la vanguardia con el progreso tecnológico, como lo antes mencionado, la seguridad en hospitales se encuentra en constante desarrollo en materia digital, con el objetivo de adaptarse a la innovación con la que vivimos día con día. Los expertos también comparten todas estas nuevas

Foto: Freepik

"Lo importante es transformar digitalmente los procesos para gestionar esos riesgos y amenazas de manera automatizada, de manera colaborativa y a través de múltiples canales de comunicación y dispositivos móviles", Jonathan Ávila

herramientas con las que se pretende comenzar el próximo año y que se espera mejoren la calidad del servicio y faciliten la lucha por erradicar situaciones delicitvas o extraordinarias.

Jonathan Ávila proyectó las plataformas digitales como buenas herramientas, aunque no descarta que se presenten riesgos a falta de una adecuada convergencia: "Las plataformas de Inteligencia de Riesgo son una de las principales tendencias, pero si no converge con Seguridad Física, ni con el ecosistema de plataformas de TI, será un ente aislado generando silos de información, la tendencia realmente es contar con una plataforma integral que me permita correlacionar eventos del mundo físico, con el mundo digital, automatizando los procesos operativos y de negocio y por ende salvar vidas y brindar un mejor servicio".

Daniel Vázquez desglosó sus ejemplos resaltando el desarrollo técnologico que se encuentra presente en el sector médico de hoy en día:

- Las normas de salud digital, que tienen el objetivo de impulsar la modernización tecnológica, algunas de las cuales ya han sido aprobadas por varios países, por ejemplo, la Identificación Única de Dispositivos o marcado de medicamento en serie, que proporciona identificadores digitales empleados en los pacientes para un mejor control y rastreabilidad.
- Automatización de procesos, para gestionar el aumento de los costos y la escasez de profesionales de la salud. Esto se transforma en una eficiencia operativa, optimización de los recursos y calidad en el servicio prestado en el hospital. Teniendo un mejor control, los datos se pueden medir, comparar y mejorar, impulsando los puntos débiles sin descuidar los puntos fuertes.

La telemedicina ha mejorado la comodidad de los pacientes, que puede ir desde un simple diagnóstico, un seguimiento controlado de la evolución de un paciente, hasta asistencia médica remota en el asesoramiento de intervenciones quirúrgicas operadas por un médico o un robot, prácticamente en cualquier momento, 24/7/365.

La Inteligencia Artificial, *Machine learning,* seguirán tomando más participación en la salud médica para hacer predicciones de posibles enfermedades que pueda tener cada persona y ayudar en los posibles tratamientos, antes, durante y después de padecer una enfermedad.

CONSECUENCIAS DE LA PANDEMIA

Sin duda alguna, la pandemia por COVID-19 que se presentó en el último par de años cambió por completo la situacion de todos los sectores a nivel mundial, perjudicando los aspectos económicos y sociales de cada nación en gran medida; sin embargo, es casi seguro que el golpe más fuerte que trajo consigo lo recibió el sector hospitalario. Los hospitales y centros médicos no estaban preparados para recibir y atender una contingencia de escala global que trajo consigo pérdidas en todos los sentidos y ante la cual no se tenía un plan de respuesta.

Hoy en día, con la enfermedad del coronavirus aún presente, aunque en mucho menor escala, la situación del mundo ha cambiado completamente, la reacción que se tuvo nos ha permitido adaptarnos a esta pandemia no sin antes estar dispuestos a seguir las restricciones sanitarias con las que vivimos, y el sector médico es el primero al frente ante estos cambios.

"La COVID-19 ha cambiado casi todos los aspectos de la vida normal, pero quizás ninguno más que los sistemas de salud. Desde el inicio de la pandemia hasta la administración de vacunas, hoy en día es necesario contar con estrategias que soporten procesos como:

- Administración de vacunas.
- Rastreo automatizado de contactos.
- Telesalud segura y protegida.
- Plataforma de gestión de eventos críticos.
- Respuesta de gestión de incidentes para riesgos de ciberseguridad.
- Orientación digital a las zonas de instalaciones COVID-19 u otras.


Foto: Freepik

Las pandemias continuarán alterando los sistemas de salud durante algún tiempo", aseguró Jonathan Ávila.

Daniel Vázquez también reconoció los cambios en los riesgos que ha dejado la pandemia: "La vulnerabilidad en todos los aspectos, la salud de las personas, la unión como sociedad, el poder económico de los procesos para combatir una pandemia mundial y/o local. Las tecnologías no estaban preparadas para una pandemia, sin embargo, desarrollasr nuevas tecnológias es tan importante como mejorar las ya existentes e impusar su uso en áreas que antes ni se pensaba o imaginaba que podrían ser útiles. Pero con lo nuevo, vienen las nuevas amenazas y riesgos: se mostró que un simple virus puede terminar con la humanidad, y esa información, si no es utilizada en beneficio de la humanidad, puede ser letal. Se pueden diseñar nuevos mecanismos de dispersión, y aunque las tecnologías evolucionan constantemente, siempre hay quien está un paso adelante", señaló.

RETOS A FUTURO

Teniendo en cuenta la situación actual del sector hospitalario, no es difícil prever los cambios y los retos que se presentarán en los años venideros, sobre todo en una industria que va cambiando día con día y que siempre está en constante movimiento.

Jonathan Ávila finalizó con la importancia de conocer estos cambios con la finalidad de saber cómo actuar cuando se presenten: "La atención médica es un sistema cada vez más complejo y colaborativo con hospitales que ya operan a su capacidad máxima diaria o cerca de ella. Durante eventos críticos, la capacidad de anticipar y responder define qué tan hábiles serán los hospitales para mitigar una serie de riesgos que pueden amenazar la resiliencia".

"Cuando los segundos importan, las vidas dependen de una respuesta coordinada en tiempo real que generalmente involucra a múltiples partes interesadas, en múltiples sitios hospitalarios, ya sea que respondan a un caso clínico diario no emergente o a un caso de alta agudeza, los hospitales generalmente tienen el desafío de administrar la capacidad y brindar atención de calidad al paciente en menos tiempo, al tiempo que superan los estándares de cumplimiento y las expectativas del paciente. Al mismo tiempo, deben mantener un entorno de atención más seguro al garantizar que los sistemas y tecnologías de TI funcionen sin problemas y que cualquier incidente relacionado con la tecnología se resuelva rápidamente con poco o ningún impacto en las operaciones hospitalarias de atención al paciente", aseguró.

Para Daniel Vázquez, la cultura de prevención es algo que no se tiene muy arraigado, como se ha señalado en foros anteriores de **Seguridad en América (SEA)**; sin embargo, también destaca la importancia de los retos hablando en materia de las personas: "no cuentan con seguro médico porque se tiene la falsa idea de que es muy caro y que mientras uno está con buena salud no se ocupa, pero las enfermedades y/o accidentes no se planean, como dice el dicho 'mejor tenerlo y no usarlo, a usarlo y no tenerlo'. Lo que mostró esta pandemia es que es muy cara una enfermedad si uno lo paga directamente del bolsillo. Para las instituciones de salud, como lo son los hospitales, esta pandemia les vino a enseñar que no se contaban con procedimientos para prevenir, tratar, controlar y mitigar un evento de esta magnitud, que aún sigue, pero la información generada en todo el mundo ayuda a generar acciones para que el impacto no sea del mismo tamaño. Si esto no nos ayudó a prevenir y estar preparados ante otra pandemia o algo peor, el impacto sería catastrófico".

Por último, Daniel Jiménez resaltó la importancia de brindar un servicio de calidad en todos los aspectos, haciendo énfasis en materia de seguridad: "¡Mantener los espacios seguros y brindar un servicio de calidad!, bueno, cada día la seguridad avanza conforme avanza el arte criminal, pero en los hospitales y clínicas la experiencia que aún hoy se vive en algunas partes del mundo, además, nos ha dejado enseñanzas muy grandes; una de ellas quizás, es la toma de decisiones informadas, el uso de la tecnología sin la consulta y recomendación adecuada podrá hacer que en algunos casos se desperdicien recursos que son valiosos y en otros escasos, el empleo de la analítica de video, ha empezado a rebajar costos en cuanto a los presupuestos de seguridad y será algo que perdurará". ■

"Principalmente los procesos, activos, vulnerabilidades y amenazas son diferentes y podemos encontrar una amplia gama, que le dan una complejidad única. Entender esto me ha ayudado a comprometerme cada día más y encontrar en diferentes autores y diferentes profesionales una verdad nueva que ha fortalecido mis conocimientos que he sabido poner al servicio de la comunidad desde estas infraestructuras", Daniel Jiménez

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

SEGURIDAD EN *E-COMMERCE:* RIESGOS VS. PREVENCIÓN

El robo de datos, el Spoofing, el Smishing, y el Phishing son sólo algunos de los riesgos en el comercio electrónico que pueden generar pérdidas millonarias o provocar la extinción de las empresas

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

El comercio en línea tuvo una gran estimulación a causa de la pandemia por COVID-19, sin embargo, con el paso del tiempo y la adopción de este, método de compra, los comercios y los usuarios lo han ido colocando como una actividad cotidiana en su día a día. Brasil es uno de los países de Latinoamérica con más auge en el *e-commerce*, tan sólo en el año 2021, las ventas *online* alcanzaron los 41 mil millones de dólares y se prevé que la cifra se duplique para 2025[1].

Si bien en un principio las compras en línea aumentaron por necesidad básica, es decir, compra de alimentos y productos para el hogar, una vez que disminuyeron los contagios y se fueron reactivando las industrias, los usuarios de Internet, se quedaron con esta práctica para cualquier servicio u objeto que necesitaran, y gracias a las plataformas que se han vuelto cada vez más amigables y que mejoran la experiencia de usuario, el comercio en línea sigue en aumento.

México ocupa el segundo lugar en América Latina en compras en línea (34 mil millones de dólares en 2021). Plataformas como Mercado Libre, han ayudado a estas estadísticas; creada en Argentina, esta tienda virtual generó más de 2 mil 100 millones de dólares tan sólo en el cuarto trimestre de 2021, convirtiéndose en el cuarto *marketplace online* más importante del mundo y líder en México y América Latina.

Pero no todo lo que ha incrementado son ganancias, las pérdidas por fraude virtual y robo de información de Tarjetas de Crédito (TDC) son la pandemia del mundo digital actual. Es por ello que realizamos una serie de entrevistas con expertos en el tema, para analizar y entender cuáles son los riesgos del *e-commerce* y cómo se pueden contrarrestar.

EVOLUCIÓN DEL *E-COMMERCE* VS. CIBERDELINCUENCIA

De acuerdo con datos de la Asociación Mexicana de Venta Online (AMVO), el valor del comercio electrónico en México en el año 2021 fue de 401 mil millones de pesos (21 mil millones de dólares aprox.), un número aún bajo en comparación con otros países como Estados Unidos en donde las ventas en línea ese mismo año representaron el 20% de las ventas totales de *retail;* en Europa cerca del 25%, y más del 50% en la región de Asia-Pacífico.

El crecimiento principalmente en países de América Latina ha sido notorio, cada vez más empresas de *retail* se unen a este método de compra (o venta), y se ve reflejado sobre todo en las ventas especiales como El Buen Fin, o las ventas de fin de año, pero qué sucede con los riesgos de seguridad en el mundo virtual, ante mayor demanda, mayor oportunidad, no sólo para las empresas.

"Los ciberdelincuentes sin duda alguna aprovecharon que muchas empresas no tenían bien establecido su *e-commerce* durante la pandemia, la cual aceleró esta digitalización y grandes marcas que aún no lo tenían implementado el comercio electrónico tuvieron

GIGI AGASSINI
Ingeniero en Sistemas, con una Maestría en Grandes Redes de Telecomunicación y Transporte. Tiene una certificación internacional como, CPP (Certified Protection Professional) por sus siglas en inglés, otorgada por ASIS Internacional. Cuenta con más de 15 años como profesional en seguridad física, consultor y desarrollador de negocios, se ha desempeñado en Corporativos internacionales, cubriendo México y Latinoamérica en todos los niveles, con amplia experiencia internacional y desarrollo profesional enfocado a nuevos mercados, ejecutando e implementando análisis estratégicos planeando y ejecutando para expandir operaciones.

Foto: Freepik

que hacerlo, pero ese desconocimiento del mercado, significó una oportunidad a través de prácticas como el *phishing, smishing, poofing,* y otros, para obtener datos confidenciales de las Tarjetas de Crédito (TDC) de los usuarios y robar información y dinero", comentó Gigi Agassini, Certified Protection Professional (CPP).

Más adelante hablaremos sobre algunos de estos riesgos cibernéticos que están atacando a la industria del *retail*, del *e-commerce* y por supuesto generando grandes pérdidas. La experta en ciberseguridad Gigi, nos dio algunos ejemplos de cómo funciona o a cuánto equivale en dólares, la información de las personas.

Una tarjeta de crédito en la dark web oscila entre los 50 centavos de dólar hasta 20 dólares, por lo que las ganancias están medidas por volumen, es decir grandes bases de datos, aunque para cada individuo la cantidad que le sea robada será un terrible suceso.

"Los ciberdelincuentes actúan a través de una cadena, roban bases de datos de un comercio electrónico que tiene toda la información de sus clientes, de sus tarjetas bancarias, y venden esas bases por volumen. Y el monto además oscila dependiendo de si la tarjeta que vas a vender tiene por ejemplo el código de verificación y también va relacionado a cuánto dinero es lo que tiene la tarjeta de crédito, en eso se basa la fluctuación del robo de información y TDC en línea", explicó.

La desconfianza que hasta hace unos cuatro años atrás existía para ciertos grupos de personas sobre las compras en línea, fue disminuyendo por el uso continuo de las plataformas durante la pandemia, situación que tanto los *retailers* como los ciberdelincuentes notaron.

"El robo de información y el fraude electrónico son delitos que desafortunadamente van en aumento, las personas que caen más en estos fraudes tienen edades entre los 30 y 39 años, seguidos por personas de entre 40 y 49 años de edad. En el último año y medio, el robo a las personas de la tercera edad se ha incrementado, las tácticas son las mismas, pero ahora los sitios web son más idénticos a los reales y ese es un gran riesgo. Además de que la ciberdelincuencia, aprovechó la pandemia para expandir sus fraudes a través de links y enlaces con supuesta información noticiosa con temas sobre dónde acudir a colocarse la vacuna contra COVID-19, los contagios del día a día, entre otras", señaló Gigi Agassini.

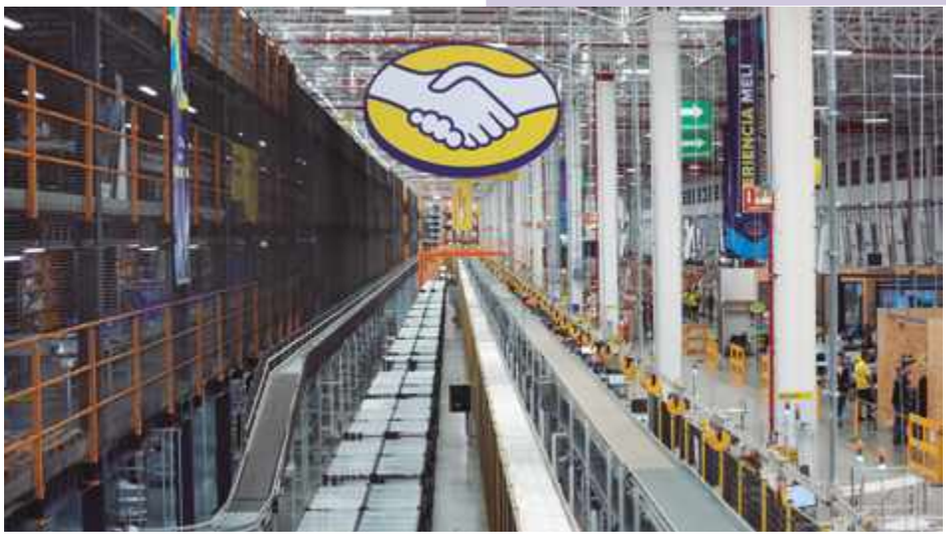
La experta nos compartió un dato alarmante, pues solamente en Estados Unidos, por citar un ejemplo, las pérdidas a través del incremento del cibercrimen, le costaron en el 2020 a dicho país, 56 billones de dólares en pérdidas. Esas pérdidas son tanto para las empresas y el gobierno como para cada individuo y representan también un daño a la imagen empresarial, situación que puede costar hasta la extinción de la empresa. El cibercrimen se ha incrementado, en parte, por esa falta de cultura de prevención en el mundo virtual, por no considerar las pérdidas posibles al ser un mundo intangible (no físico).

"México ocupa a nivel global el tercer lugar en robo de información y fraude, ahí hay una gran área de oportunidad para proteger mejor nuestros datos", comentó Gigi Agassini.

Por su parte, Guillermo Rossette Aguilar, gerente nacional de Prevención de Pérdidas en Mercado Libre México, considera que el reto principal del e-commerce, es caminar en paralelo con el equipo directivo sobre la estrategia del negocio con la finalidad de adecuar la estrategia de seguridad.

"En el *e-commerce*, es importante ser consciente de que nuestro actuar como especialistas en seguridad y gestión de riesgos es fundamental para asegurar la mejor experiencia de compra para nuestros clientes. En Mercado Libre contamos con un sistema de seguridad enfocado en proteger tres pilares principales:

1) Producto.
2) Gente .
3) Información.



GUILLERMO ROSSETTE AGUILAR
Abogado de profesión y criminólogo por la Universidad Autónoma de Nuevo León. Cuenta con la certificación avanzada en Técnicas de Interrogatorio Wicklander & Zulawsky, así como Técnicas de Perfilamiento Criminal, Análisis de Comportamiento y Conocimientos Técnicos en Criminalística y Balística Forense. Recientemente cursa la maestría en Administración de la Seguridad, en la "UDLAP Jenkins Graduate School" y cuenta con un diplomado en Coaching Empresarial. Fundó la asociación "Huellas", la cual participa en actividades altruistas en CDMX y área metropolitana. Como experto en seguridad tiene más de 13 años de experiencia en diferentes industrias como el *retail,* la logística, las fiscalías de administración de justicia, el *e-commerce* y la producción.

Estos pilares nos rigen para tener una directriz base que nos permita tomar las decisiones correctas en términos de seguridad", explicó.

PRINCIPALES RIESGOS

Retomando información de la AMVO, en 2022 se estimó que el 76.5% de las empresas invertirían en sus plataformas de *e-commerce,* sin embargo, tan sólo un 28.7% lo haría en protección contra fraude, esa ausencia de prevención se ha convertido en el principal riesgo del comercio en línea. Gigi Agassini considera los siguientes riesgos actuales en el *e-commerce:*

- Robo de datos.
- Robo de información crediticia.
- *Spoofing* (usurpación de identidad electrónica).
- *Smishing* (obtención de información privada a través de mensaje de texto o SMS).
- *Phishing* (propagandas fraudulentas por WhatsApp o correo electrónico que simulan el sitio web de empresas que ofrecen ofertas, ingresa sus datos de TDC y se realiza el fraude o robo).

Las plataformas de venta en línea se han ido adaptando cada vez más a la experiencia y satisfacción del usuario, dependiendo de dónde se esté visualizando el sitio web, para ello existen estadísticas puntuales sobre cuántas personas ingresan a Internet desde una computadora de escritorio, una laptop, una tableta o un celular, detalle que también tienen en cuenta los ciberdelincuentes.

Con datos del informe "Digital 2022" realizado por We Are Social y Hootsuite, "el número de usuarios de Internet en el mundo alcanzó los 4 mil 950 millones de personas, lo que representa al 62.5% de la población mundial (7.910 millones de personas)... En cuanto a los usuarios de Internet en dispositivos móviles, en enero de 2022 alcanzaron al 67.1% de la población, es decir, 5 mil 310 millones de personas, lo que representa un incremento del 1.8% interanual, y para tener mayor contexto sobre esta cifra, es un incremento de 95 millones de usuarios en los últimos 12 meses"[2].

"Debemos entender que el *e-commerce* se refiere a la compra y venta de mercancía a través de Internet, lo cual implica diversos problemas, entre ellos la publicidad engañosa o mal intencionada, las ofertas que el fabricante puede realizar y que pueden no ser ciertas para el usuario final, el papel que juegan los influencers en dicho tema, el cual puede ser falso. Siempre se recomienda al usuario final comprar de forma segura, validar que las ofertas sean reales, debemos poner foco en ofertas que sean muy por abajo del precio, lo cual genera sospecha de fraude, recordemos que algo que sea muy bueno y que tenga bajo precio, puede ser una estafa", comentó Víctor Díaz Bañales, socio director de RAMDIA.

Empresas como Mercado Libre, están conscientes de los riesgos de la ciberdelincuencia, de las consecuencias y que no sólo son responsabilidad del usuario que cae con engaños y descuidos ante tales estafas, sino también de la tienda en línea y del marco legal de cada país.

"En Mercado Libre creemos que la formalidad y la seguridad jurídica son pilares de la inclusión y el desarrollo. Como ciudadanos corporativos, cumplimos estrictamente con los marcos legales de los distintos países y nos esforzamos para evitar o minimizar conductas inadecuadas en nuestras plataformas. En nuestro *marketplace* siempre explicamos con claridad cuáles son los derechos y las responsabilidades de los vendedores, los compradores y los usuarios de nuestro ecosistema así como nuestras políticas sobre artículos y actividades prohibidas. Para Mercado

Libre, la transparencia es clave para ayudar a los usuarios a tomar decisiones informadas sobre los servicios que utilizan", expresó Guillermo Rossette.

HERRAMIENTAS DE SEGURIDAD PARA EL COMPRADOR

Los expertos en seguridad y ciberseguridad están en constante profesionalización para estar un paso adelante de la delincuencia, a continuación nuestra experta Gigi Agassini comparte los 5 tips para el usuario final del *e-commerce* para que sus compras sean seguras:

1) Sea muy cuidadoso con la información que recibe en WhatsApp, SMS o por correo electrónico, observe detenidamente las ofertas que recibe en línea, en el teléfono móvil, verifique que realmente sea la tienda original, no abra todo lo que recibe. Verifique la URL (https://).
2) Sea desconfiado con todo lo que reciba vía SMS, WhatsApp o correo. Revise faltas de ortografía, ponga el cursor en el link antes de dar clic, no abra nada, no descargue nada sin verificar la información, primero, en la página web oficial del comercio y verifique si realmente hay alguna oferta, o bien, puede marcar al teléfono que ahí viene, pedir información al Call Center o en sus redes sociales oficiales.
3) Al momento de hacer la transacción, cuente con una conexión segura, no lo haga a través de una red wifi pública, puesto que seguramente no tendrá protección y sus datos estarán comprometidos.
4) Verifique la información del vendedor, que el sitio sea correcto. Hoy en día la ciberdelincuencia está haciendo lo posible para comprometer la seguridad del usuario, las páginas, los links cada vez son más parecidos a las reales, simulan los candados que anteriormente ayudaban a saber que era un sitio seguro.
5) A la hora de pagar, es importante leer antes la política de privacidad, ahí nos va a mencionar cómo están ellos gestionado nuestros datos, nuestra información personal, porque ahí en las letras chiquitas dice si pueden o no compartir nuestra información, y el problema es cuando se vulneran esos sitios y nuestra información queda comprometida, y si no estás de acuerdo, mi recomendación es no continuar.

Gigi comentó que la ciberdelincuencia tiene dos cosas de manera ilimitada: tiempo y recursos. Ellos buscan, analizan y se actualizan para que sus estafas sean mucho más fáciles y creíbles. Y muy importante no guardar de forma automática las contraseñas o los datos bancarios en las plataformas de *e-commerce*. Así como el tener un antivirus tanto en el celular como en la computadora o dispositivo inteligente.

"Las recomendaciones anteriores, conjugadas con una conexión segura a Internet, más el uso de una VPN, más el uso de un antivirus con detección de *malware*, ayudarán a reducir por mucho el que tu información pueda ser vulnerada", puntualizó.

Herramientas de seguridad para el comercio en línea

La cultura de seguridad en general es un tema que hace falta implementar y adoptar en muchos países, ahora el tema de ciberseguridad tiene más lagunas pese a que el uso del Internet es diario, en aumento y con poca prevención. Después de revisar las recomendaciones de los expertos a los usuarios del *e-commerce*, ahora vamos con las estrategias de seguridad para los comercios con tienda virtual.

"El *e-commerce* debe protegerse de forma integral, la primera línea de defensa es proteger su código, el cual en diversas ocasiones puede ser modificado por terceros y generar ofertas válidas, es decir hemos tenido casos de empresas que son atacadas y alteran el código relacionado con los precios y publican teléfonos o laptops en precios muy bajos, los cuales deben ser respetados por el vendedor, es decir si una empresa X publica un teléfono X en 1 peso, debe venderlo y entregarlo por dicho precio, de lo contrario tendrá problemas con las autoridades pertinentes", comentó Víctor Díaz Bañales.

En el caso de Mercado Libre, la política de venta es más estricta para que los usuarios se sientan más seguros al momento de comprar. "Contamos con los más altos estándares de seguridad de la industria con diversas formas de proteger a nuestros usuarios a la hora de hacer una compra, que van desde el bloqueo de publicaciones ilícitas, prohibición de venta de los artículos que infringen los derechos de titulares de propiedad intelectual, hasta la protección de datos personales, entre otros. Esto gracias a nuestro mecanismo de identificación de prevención de fraude, el cual está 24/7 atendiendo diversas eventualidades y que cuenta con algoritmos sumamente avanzados para la oportuna identificación de riesgos" explicó Guillermo Rossette.

VÍCTOR DÍAZ BAÑALES
Socio fundador de Ramdia Security, apasionado por la ciberseguridad, el compartir con la mayor cantidad de personas posibles su postura, cree firmemente en que si tenemos una cultura sólida en ciberseguridad, seremos una sociedad menos vulnerable y saldremos avante de cualquier situación. Reitera que la ciberseguridad es responsabilidad de todos, todo el tiempo.

Además de que la empresa no permite productos y servicios que estén prohibidos por sus Términos y Condiciones o por imposición legal. Con sus algoritmos y una constante innovación en su plataforma, supervisan constantemente el contenido para brindar una experiencia segura y confiable a sus usuarios, al tiempo que reducen su exposición a publicaciones que atenten contra ese objetivo, explicó el experto.

Así como se incrementó la venta en línea, también las empresas de paquetería aumentaron sus servicios o se crearon nuevas compañías; hasta que el comprador recibe y verifica que lo entregado por la paquetería es lo que solicitó y está satisfecho, hasta ese momento se libera el pago, ¿pero cómo

Foto: Freepik

garantiza el comercio el servicio de un tercer participante que es la paquetería?

"Lo más importante para nosotros es la satisfacción de nuestros clientes que utilizan Mercado Libre, los *sellers* y todos los actores que forman parte de nuestra cadena logística. Con la infraestructura y los procesos de nuestros centros de distribución hacemos de la logística un proceso más ágil y eficiente para que nuestros usuarios tengan una compra y recepción segura.

Por tal motivo, tenemos estrategias que protegen el producto mediante la trazabilidad punto a punto de la vida del paquete, controles físicos para prevenir el robo interno y un sistema de monitoreo para las rutas en calle que dan protección a nuestros conductores y la carga. De igual forma, la relación con asociaciones y autoridades nos ha dado la tranquilidad de expandirnos en zonas de complejo alcance y con la certeza de llevar protegido a nuestros colaboradores y sus compras", detalló Guillermo.

BÁSICOS PARA UNA TIENDA EN LÍNEA

Para evitar ser presa de la ciberdelincuencia, es mejor estar preparado y prevenido ante cualquier posible ataque, por ende estas medidas de seguridad lograrán la confianza del comprador, empezando con acciones sencillas.

"Primero comenzaría con los básicos, que es cumplir con que la empresa debe informar sobre su identidad, nominación legal, ubicación, contacto, todo en su página web, para que el consumidor en caso de hacer una reclamación o verificación, pueda tener acceso a esta información. Debe tener sus políticas de privacidad, qué información se va a recolectar, el uso y manejo de la misma y sobre todo preguntar al consumidor si está dispuesto a recibir información como ofertas especiales, etc.", explicó Gigi Agassini.

Este es un tema muy importante, porque como usuario tenemos la responsabilidad de informarnos sobre cómo se usará los datos personales y confidenciales que ingresaremos, y precisamente debe venir en las Políticas de Privacidad, que muy pocas personas se toman el tiempo de leer y analizar.

"Las Políticas de Privacidad, señalan si se va a compartir nuestra información con terceros, ya que hay algunas marcas que son parte de un conglomerado de empresas y a veces se comparten las bases de datos. También el sitio web debe informar sobre si va a manejar cookies sin capacidad de verificación del usuario, o con capacidad de identificación del usuario, de ser así, en esta segunda tiene que ser muy claro en su política de privacidad y cuál es la información que va a retener. Unas dice que solamente por Performance, pero otras son más invasivas, identifican tus preferencias y trata de hacer el sitio con una experiencia más personalizada", comentó Gigi.

En el caso del pago con TDC, la compañía debe cumplir con PCI DSS (Payment Card Industry Data Security Standard) que es el estándar de seguridad de datos para la industria del pago de tarjeta de crédito. Este fue desarrollado por un comité de las compañías de TDC y de débito, además hay un comité que se denomina PCI SSC (Payment Car Industry Security Standards Council), es decir que si eres un comercio que va a hacer operaciones a través de tarjetas de crédito debes cumplir con este estándar adicional de otros estándares, desarrollar y mantener un *software* seguro, que debe tener un programa de gestión de vulnerabilidades.

Otros aspectos a considerar por parte de los comercios electrónicos es el proteger los datos de los propietarios de tarjetas y sobre todo implementar medidas sólidas de control de acceso, es decir restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información, monitorear tu sitio web y para eso Gigi Agassini recomendó algunas herramientas de seguridad:

- Optimizer Robot, permite saber si la web ha tenido algún fallo o está inactiva.
- DMARK, es un sistema de validación de correo electrónico, para detectar y prevenir las estafas por correo electrónico. Las estafas se hacen tanto al consumidor como a la tienda electrónica.
- Uso de estándares. Por ejemplo el ISO 9001 referente a los sistemas de gestión de la calidad; cómo puedo asegurar los temas de calidad de mi tienda virtual. Debe tener certificados como el PCI, certificados HTTPS, SSL (permite dar encriptación al momento del envío de una transacción electrónica en el sitio web). ISO 27001 (seguridad de la información), o el ISO 27005 que habla de riesgos de ciberseguridad en la protección de la información.

Y cumplir, por ejemplo en México, con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares - LFPDPPP (aplica para México) o la ley de protección de datos personales que aplique según el país que corresponda, toda esta información debe aparecer de forma pública en el sitio web, para darle mayor seguridad al usuario y que sepa que su información está tratada de manera responsable. De ahí la importancia del cumplimiento de los estándares para brindar mayor seguridad y reducir el riesgo.

"Existen también herramientas de seguridad basadas en el diseño de la


Foto: Freepik

tienda electrónica, dónde va a estar ubicada, si en la Nube o de forma híbrida; es importante colocar ese tema en el aviso de políticas y privacidad. Por diseño debemos establecer ciertas reglas para proteger y brindar la continuidad de nuestra tienda virtual, políticas, cultura interna, herramientas. Por diseño hay muchas estrategias para esto, las cuales brindan los estándares.

Si eres una empresa de *e-commerce*, mira los estándares, dale autenticación y esa encriptación a la información de tus clientes, protege tu base de datos donde almacenas información delicada de tus clientes, ten una réplica en dado caso de que tengas algún problema, puedas darle continuidad a tu operación, y si sucede una intrusión, sé honesto, sé directo y lo más importante, avisa a tus usuarios", puntualizó la CPP.

LA CIBERSEGURIDAD COMO UN ESTILO DE VIDA

El *e-commerce* llegó para quedarse, aunque ya existía hace varios años atrás, con la pandemia por COVID-19, países como Brasil, México, Chile incrementaron significativamente el uso de este método de compra.

"Sin duda alguna la sociedad no volverá a ser la misma ante la pandemia y todos sus bemoles, la hiperconectividad y las nuevas tecnologías hicieron que la gente tuviera una mayor confianza y primeros acercamientos al tema de comercio electrónico, es decir jamás imaginamos que nuestros padres o abuelos pudiesen pedir el supermercado en línea, que las plataformas de servicio de transporte pudieran enviar paquetes a nuestros amigos y familiares, sin duda alguna la pandemia cambió la forma en que las generaciones interactúan con el comercio electrónico y los envíos", comentó Víctor Díaz Bañales.

El experto también hizo un análisis sobre si esta transformación a lo virtual beneficia en su totalidad a las empresas, o bien les ha generado pérdidas , que de acuerdo de igual manera con Gigi Agassini, los riesgos de pérdidas están en la falta de una cultura de ciberseguridad.

"Los negocios existentes de *e-commerce* y los nuevos, tienen un gran desconocimiento en temas de ciberseguridad, muchos utilizan plataformas de código abierto las cuales son constantemente vulneradas y otros utilizan plataformas de paga pensando que no son vulnerables y es un error común, todas las plataformas están formadas por un conjunto de tecnologías las cuales pueden ser vulneradas a diversos vectores de ataques, el problema es el uso común de dichas plataformas las cuales pueden hacer vulnerables a muchos usuarios finales que las utilicen, es hora de que las empresas pongan el foco en el entorno digital", señaló Díaz Bañales.

Sobre este tema, Gigi Agasini enumeró tres los principales riesgos actuales de la ciberseguridad:

1) Falta de cultura.
2) Falta de concientización.
3) El exceso de confianza a lo intangible.

Adicional al phishing, *ransomware,* y la manera en que ahora están evolucionando los ataques cibernéticos. "Veo con mucha preocupación que crece mucho el *ransomware,* el robo de credenciales comprometidas, robo de identidad, el fraude, leí que en la dark web se está vendiendo por 4 millones de dólares el acceso a información de más de 527 empresas. El crimen cibernético a nivel global es más redituable por encima del narcotráfico, la trata de personas o la venta de armas. El costo pronosticado del crimen cibernético para 2025 es de 10.5 trillones de dólares, es decir hay una gran problemática frente a nosotros y seguimos viviendo en la negación de 'a mí no me va a pasar'", indicó Gigi.

Y es que pese a que seguimos viendo empresas de talla mundial que han sido vulneradas y muchas de ellas no han podido continuar, "estamos en una guerra cibernética, en una pandemia en el mundo digital, el cual converge con el mundo físico, pero como no lo palpamos es difícil para muchas personas aceptar que hay una problemática ahí. Hay que tener presente que la seguridad es una cultura, pero la ciberseguridad es un estilo de vida", finalizó la experta.

Ropa, calzado, sartenes, fruteros, anillos, tapetes, libros, cámaras, micrófonos, camas para perros, autos, motos celulares, todo lo que se piense y se pueda comprar está ahí, en las tiendas virtuales, en el comercio electrónico, pero es importante crear una cultura preventiva para el uso de esas plataformas, y en dado caso de ser víctima de alguna estafa, avisar sobre ésta o si fue un ataque cibernético, que por desconocimiento o ignorancia, por ingenuidad o falta de prevención, cayó en esta mala acción y necesita informarlo, porque una empresa puede ahorrarse hasta un millón de dólares en costos, si es que se detecta el ataque cibernético en los primeros 30 días de que sucedió.

Según el reporte de IBM, hasta que te des cuenta de la brecha de información pueden pasar más de 200 días y dependiendo el tipo de ataque puede llevarte a más de 90 días, lo que significa que puede llevarte hasta un año el detectar una intrusión, un ataque, hasta contenerlo, y es por eso que muchos negocios quiebran, porque son pocas las empresas que toman con seriedad está problemática global y están tomando medidas al respecto. Piense dos veces antes de dar clic. ■

Referencias

1 América Latina: ventas de comercio electrónico por país 2021-2025. Statista Research Department, 30 nov 2022 https://es.statista.com/estadisticas/1075464/america-latina-e-commerce-ventas/
2 El número de usuarios de internet en el mundo crece un 4% y roza los 5.000 millones (2022). Susan Galeano, 27/01/2022 Marketing4Ecommerce https://marketing4ecommerce.net/usuarios-de-internet-mundo/

HÉCTOR ROMERO SÁNCHEZ:

COMPROMISO CON LA LOGÍSTICA Y EL TRANSPORTE

Círculo Logístico es la asociación enfocada en la seguridad del transporte de carga y la Logística, encabezada por Héctor Romero, empresario y profesionista con más de 20 años en el sector

MÉXICO | Mónica Ramos / *Staff* Seguridad en América

Uno de los sectores que más se ha visto afectado por la inseguridad en México es el del transporte de carga, no ha sido fácil estar un paso adelante de la delincuencia; de la planeación y la prevención depende la seguridad no sólo de la mercancía, sino de las personas que día a día laboran en esta industria. Para ello existen profesionales que se han especializado en la protección de la cadena de suministro, de la logística, del transporte, que trabajan en conjunto con las autoridades, y crean estrategias para lograr que este país sea más seguro.

Uno de esos profesionales es Héctor Romero Sánchez, actual presidente de Círculo Logístico, asociación de seguridad privada, logística y telemetría en el transporte, Héctor es licenciado en Administración de Empresas, cuenta con una maestría, un doctorado y es egresado del IPADE *Business School* (Instituto Panamericano de Alta Dirección de Empresa), ha cursado diversos diplomados enfocados a la seguridad, logística, mercadotecnia y alta dirección, y fue reconocido como uno de "Los 100 más influyentes de la Seguridad Privada" (SEA 2022).

DE CAMINO A LA SEGURIDAD

La espacialización es una herramienta que ayuda a cualquier profesional a abrirse camino en las industrias, aprender cada vez más sobre un tema sin dejar de vista el contexto, mejora el desempeño de las personas en su medio laboral. Héctor Romero puede que haya llegado por una oportunidad laboral al sector del transporte, pero con los años y capacitación, se ha vuelto experto en seguridad en logística y transporte.

"Soy transportista desde hace más de 10 años, inicié esta formación en grupo ADO, hasta ser director y fundador de un concepto novedoso en nuestro país y que aún está vigente, que es el viajar por la noche con un concepto tipo avión y a un bajo precio; este proyecto fue traído desde Brasil, Europa y USA y se implementó con éxito en Méxi-

Más allá de la seguridad	
Pasatiempo favorito:	Ejercicios para el cuidado físico y mental.
Grupo de música o cantante favorito:	Enrique Guzmán.
Programa o serie de TV favorito:	Género policíaco.
Libro favorito:	Don Quijote de la Mancha.
Destino favorito de vacaciones:	Acapulco.
Bebida favorita:	Jugo de tomate.
Comida favorita:	Salmón.
Personaje favorito:	José Cárdenas.
Actriz o actor favorito:	Tania Rincón.

co; éste me permitió hacer mi primer plan estratégico de negocios, innovador y que revolucionó el transporte en nuestro país, este fue mi primer contacto con la seguridad, ya que este era uno de los principales valores dentro de este giro", explicó Héctor.

Después de terminar su ciclo laboral en ADO, el empresario tuvo su primer contacto con la seguridad privada al formar el Consejo Nacional de Seguridad Privada (CNSP) junto con grandes empresarios de la seguridad, esto hace más de 25 años.

"Gracias a ello y los grandes maestros que tuve, aprendí parte comercial, operativa y administrativa de una empresa de seguridad privada, así mismo, participé en los primeros diplomados que se desarrollaron en diversas universidades privadas como fue la UVM, Universidad Anáhuac y la Universidad Iberoamericana".

Posteriormente fue invitado al sector de transporte de carga, desarrollando diferentes proyectos de logística, seguridad y telemetría, lo que le permitió hacer una mezcla de aprendizajes para la seguridad en el transporte de carga.

"Después de unos años, regresé al transporte foráneo de pasajeros mediante el grupo IAMSA (dueños de Viva Aerobús) para hacerme cargo de manera operativa de Omnibus de México, empresa representativa en el sector tanto nacional como internacional, y tuve oportunidad de laborar para diferentes empresas del grupo en transporte urbano, foráneo y suburbano; con grandes experiencias, como el haber fundado Transportes y Autobuses del Pacífico (TAP), una empresa que recorre de occidente a norte el país, una experiencia grata, que trabajé desde su conceptualización hasta su operación".

Desde sus inicios en la vida laboral, Héctor siempre tuvo la inquietud de ser un empresario, actualmente se dedica a la asesoría, consultoría y capacitación con un enfoque en la seguridad en el transporte, así como a la comercialización de diferentes periféricos enfocados a la seguridad en el transporte en sus diferentes modalidades, y también a los procesos de monitoreo inteligente de seguridad de personas, objetos, muebles inmuebles y transporte.

CÍRCULO LOGÍSTICO

Las asociaciones son sin duda alguna, una plataforma y un espacio para la profesionalización y mejora de cualquier sector, industria o grupo social. Círculo Logístico, nació a través de una serie de necesidades detectadas por un grupo de empresarios dedicados al transporte, seguridad, capacitación, telemetría, integración de tecnologías, y comercialización de periféricos, con el objetivo de crear estrategias y encontrar herramientas para ser más predictivos y planificadores en cuanto a seguridad.

Dicha asociación tiene un enfoque prospectivo y preventivo, apoyándose de la colaboración de Cámaras, asociaciones, universidades y autoridades que les han dado la oportunidad de ir sumando diferentes empresarios, académicos, transportistas.

"Para mí, Círculo Logístico representa un gran reto para sacar adelante las áreas de oportunidad que tenemos actualmente en la Logística, con el crimen organizado en la cadena de suministro derivado de los problemas internacionales, como lo es la guerra entre Rusia y Ucrania, la inflación, y es un gran reto que tenemos para formar una gran comunidad de logísticos, integradores, académicos, transportistas y personas", puntualizó Héctor Romero, quien también es socio fundador y director general de Transportación y Logística Romero S.A. de C.V.

"Gracias a ello y los grandes maestros que tuve, aprendí la parte comercial, operativa y administrativa de una empresa de seguridad privada, así mismo, participé en los primeros diplomados que se desarrollaron en diversas universidades privadas como fue la UVM, Universidad Anáhuac y la Universidad Iberoamericana"

"Uno de mis objetivos como persona y empresario es seguir apoyando a las diferentes asociaciones a las que pertenezco, aportando conocimiento, experiencia, y mi apoyo para salir adelante ante la vulnerabilidad del entorno en el que estamos viviendo, versus delincuencia, inflación, guerras, falta de valores"

EL DÍA A DÍA DE UN EMPRESARIO

Hijo menor de cuatro, único varón, admirador de la madre Teresa de Calcuta, por su humildad, sencillez, dedicación compromiso, transparencia, por su acción conocida de dar sin recibir nada a cambio; concentrado en consolidarse como un especialista en la Logística y la seguridad en el transporte para poder apoyar a las diferentes comunidades, asociaciones, Cámaras, y profesionales que se dediquen a estos y diferentes sectores, así es Héctor Romero en su día a día.

"Uno de mis objetivos como persona y empresario es seguir apoyando a las diferentes asociaciones a las que pertenezco, aportando conocimiento, experiencia, y mi apoyo para salir adelante ante la vulnerabilidad del entorno en el que estamos viviendo, versus delincuencia, inflación, guerras, falta de valores. Durante la pandemia cambiamos nuestros hábitos, las formas de laborar, aprendimos más sobre el uso de la tecnología, el cuidado físico, y muy importante el mental; en lo personal, aprendí a valorar el minuto a minuto y el día a día, de lo importante que es vivir feliz, quitarse de apegos y valorar la vida", concluyó nuestro entrevistado. ■

Asociación de palabras	
México:	Compromiso
Seguridad:	Preventivo.
Presidente:	Mentira.
Gobierno:	Autoridad.
Policía:	Respeto.
Familia:	Vínculo.
Amigos:	Lealtad.
Círculo Logístico	Compromiso.

CONTROL®
SEGURIDAD PRIVADA INTEGRAL

CUIDAMOS A NUESTROS GUARDIAS, PARA QUE CUIDEN TU PATRIMONIO

En Control reconocemos y dignificamos la labor que realizan nuestros guardias de seguridad

MÉXICO

En Control nos apasiona la seguridad de nuestros clientes y de sus bienes, así como que nuestros colaboradores se desarrollen positivamente en el ámbito personal, profesional y familiar. Sabemos que nuestros colaboradores son parte fundamental para seguir brindando un servicio de calidad a nuestros clientes, por lo cual contamos con una Cultura Organizacional con la reconocemos y dignificamos la labor que realizan todos los días nuestros guardias de seguridad.

Nuestros oficiales de seguridad ponen en alto el nombre de Control, trabajando siempre con pasión, lealtad y disciplina. Todos ellos reciben una capacitación adecuada que les brinda los conocimientos indispensables para desarrollar sus actividades de la mejor manera y ofrecer siempre un servicio de calidad a nuestros clientes y a los miles de usuarios de centros comerciales, corporativos e industrias en las que tenemos la responsabilidad de proveer seguridad a lo largo y ancho del país.

En Control destacan cientos de guardias ejemplares por la gran pasión con la que desempeñan su labor y cumplen al 100 por ciento con los protocolos y las consignas en sus servicios. Es por eso que, cada semana llevamos a cabo eventos y prácticas para reconocer la entrega y profesionalismo de nuestros colaboradores, lo cual nos permite mantener una cercanía de primera mano con ellos e incluso, con sus familias, a las que también integramos en actividades y las consideramos parte de nuestra organización.

Con prácticas como “Reconociendo al Servicio” y “Héroes Control” distinguimos el trabajo individual y en equipo con el que nuestros oficiales de seguridad se desenvuelven de manera destacada en sus centros de trabajo y que los lleva a ganarse también el reconocimiento de nuestros clientes. Estas prácticas son también una oportunidad de visitarlos en los servicios, conversar con ellos y conocer sus inquietudes o áreas de oportunidades en las que podemos trabajar para nuestra mejora continua.

Somos conscientes de que la labor de los guardias de seguridad demanda pasar mucho tiempo fuera de casa, dedicando incluso fines de semana lejos de sus familias. Por eso en Control promovemos prácticas y eventos que refuerzan la unión familiar de todos nuestros colaboradores que dedican su valioso tiempo y esfuerzo a esta loable profesión para llevar el sustento a sus familias.

CULTURA ORGANIZACIONAL

Como parte de nuestra cultura organizacional, llevamos a cabo nueve prácticas de manera mensual y bimestral y anualmente realizamos nueve eventos para nuestros colaboradores y sus familias. Desde los inicios de Control, hace más de 21 años, hemos reconocido a más de 6 mil 500 colaboradores y familiares y hemos tenido una asistencia a los eventos y prácticas mayor a las 29 mil personas.

Con las prácticas “Valorando a tu esposa” y “Almorzando en Familia” tenemos la oportunidad de visitar los hogares de nuestros guardias ejemplares para convivir en su núcleo familiar y reconocer todo el apoyo incondicional que en el hogar les brindan sus esposas(os) e hijo(a)s para que puedan desarrollarse profesionalmente en Control.

De igual forma promovemos los valores y la unión familiar permanentemente con eventos a los que pueden acudir los Guardias Control con sus familias, en celebraciones como el “Día del Niño”, nuestra “Peregrinación Anual Control” a la Basílica de Guadalupe, el evento de “Fin de Año” y “Excelencia Académica”. Con este último evento buscamos también motivar a los hijos de nuestros colaboradores a nivel nacional en el ámbito académico, otorgando una mochila y un kit de útiles escolares a quienes hayan obtenido un promedio mínimo de 9.0 en el ciclo escolar, así como un regalo especial a los alumnos que alcanzaron la excelencia académica con promedio de 10.





El apoyo a la educación continua es muy importante para nosotros, no sólo para los más pequeños, pues además buscamos que nuestros colaboradores sigan preparándose académicamente. En conjunto con la capacitación de actualización que les brindamos, les damos la oportunidad de crecer profesionalmente dentro de la organización como parte de nuestro Plan de Carrera Control. Con este enfoque hemos desarrollado el programa "PREPÁrate en Control", con el que buscamos que todos nuestros guardias de seguridad concluyan sus estudios a nivel medio superior y también tengan la oportunidad de estudiar una licenciatura y especializarse en el ramo de la seguridad privada.

De esta forma, en Control trabajamos con calidad humana que se refleja en nuestra cultura organizacional, que tiene como prioridad el desarrollo personal, familiar y profesional de nuestros colaboradores. Nuestros guardias son el motor de la empresa mediante el cual podemos seguir brindando el mejor servicio a nuestros clientes y usuarios. Porque en Control amamos lo que hacemos y todo lo que hacemos, lo hacemos con pasión.

Cada semana llevamos a cabo eventos y prácticas para reconocer la entrega y profesionalismo de nuestros colaboradores, lo cual nos permite mantener una cercanía de primera mano con ellos e incluso, con sus familias, a las que también integramos en actividades y las consideramos parte de nuestra organización

Reconocemos el trabajo que hacen los integrantes de la Familia Control con prácticas y eventos dirigidos a los colaboradores y a sus familias:

9 prácticas mensuales y bimestrales.
9 eventos anuales.
+ 6 mil 500 reconocidos.
+29 mil asistentes.

Fuente y fotos: Control Seguridad Privada Integral








Columna de
Enrique Tapia Padilla, CPP

etapia@altair.mx

Más sobre el autor:

Socio Director,
Altair Security
Consulting &Training.

LATINOAMÉRICA

¿CÓMO PACIFICAR AL PAÍS?

(PRIMERA PARTE)

Cortesía Enrique Tapia

El día que escribí esta columna, antes fui a jugar padel y me encontré con tristeza una cancha con basura dentro y fuera de ella, cuando a escasos cinco metros está el bote de basura y un señalamiento que dice: "No tires basura, cuida las áreas verdes y las especies protegidas".

Me puse a pensar, qué puede motivar a esas personas (porque no fue sólo una) a dejar su basura ahí, afectando el entorno y a otras personas, donde por cierto también ellos jugaron, ¿será por falta de conciencia, desconocimiento o por puro desinterés y "valemadrismo"?

Lo que es un hecho es que todos los días tenemos cada uno de nosotros la oportunidad de crear cambios sociales que impacten a la sociedad directamente y con ello a la seguridad ciudadana. Impactos negativos o positivos: todo delito grande comienza por uno pequeño, la falta de conciencia, de civilidad y de empatía en una nación es el iniciador de violencia y de delitos en un futuro.

Vemos como en el día a día, puede afectar positivamente en las personas una zona cuando se encuentra ordenada y limpia, cuando hay disciplina, no importa si la zona sea modesta o rica. En términos técnicos esto es parte del CPTED (Prevención del Crimen a Través del Diseño Ambiental, por sus siglas en inglés), aunque en términos del día a día comienza con la civilidad.

La calle más limpia no es la que se limpia todos lo días, sino es la que no se ensucia, ni siquiera con colillas de cigarro o con heces de mascotas. El respeto a las reglas básicas, como las reglas de buena vecindad y de convivencia, influyen directa y drásticamente en las conductas presentes y futuras de una sociedad. Pero también los "árbitros" que corrigen esas conductas a través de la conciencia o sanciones forman parte importante de ello. Vivimos en una sociedad y la responsabilidad es de todos. Y todos simplemente con el hecho de hacer la parte que nos corresponde podemos ayudar a mejorar esta sociedad. ¡Imagina que cada familia lo hiciera! Estaríamos sin duda en otras condiciones, de mayor seguridad y tranquilidad.

> *El respeto a las reglas básicas, como las reglas de buena vecindad y de convivencia, influyen directa y drásticamente en las conductas presentes y futuras de una sociedad*

> *La creación de una cultura de seguridad comienza desde las bases y echando mano de todos los recursos disponibles para lograrlo, pero también con constancia y consistencia para crear hábitos, que el día de mañana nos saquen del boquete en el que estamos*

LA EDUCACIÓN COMIENZA EN CASA

La educación, la conciencia, la civilidad, la seguridad empieza en nuestro seno familiar. Aún recuerdo cuando niño en la escuela primaria pública donde asistí llegaron unas personas del gobierno a darnos clases de civismo. También recuerdo cuando en esas fechas coleccioné un álbum de la ardilla de Barcel que te enseñaba los principios básicos de buena vecindad; pero también vienen a mi mente mis padres, que desde niños nos inculcaron principios de respeto hacia los demás, de honestidad, momentos que me dejaron tatuado esas condiciones en mi vida. Lamenté cuando a inicios de este siglo quitaron de las clases de secundaria la materia de Civismo, materia que me encantó cursar en la década de los ochenta.

Mi interés por ello y las razones de cómo es que en este mundo hay naciones ahogadas en la violencia y otras que son bastante pacíficas, se incrementaron con el pasar del tiempo. Los viajes, que son mi pasión, me ayudaron a entender eso, me encanta sentarme en un parque, jardín o cafetería y simplemente observar las acciones de los demás, tomar notas y reflexionar sobre ello.


Cortesía Enrique Tapia


Cortesía Enrique Tapia

Acerca de este tema estaré escribiendo todo este año en SEA, porque la seguridad comienza desde casa. El Internet está lleno de información sobre cómo mejorar una sociedad y, sin embargo, lo vemos tan lejos, pero la realidad es que está tan lejos como empezar hoy mismo en cambiar algo nosotros mismos. Se requiere sólo de voluntad para lograrlo y quienes estamos en algún lugar en puestos de liderazgo, podemos influir directamente en decenas o cientos de familias. Los invito a hacer cada uno de nosotros algo desde nuestra trinchera. Un anónimo dijo: "Quien no hace nada por el lugar en el que vive, no merece vivir ahí". Si al menos no afectas negativamente, ya estás haciendo algo positivo.

La creación de una cultura de seguridad comienza desde las bases y echando mano de todos los recursos disponibles para lograrlo, pero también con constancia y consistencia para crear hábitos, que el día de mañana nos saquen del boquete en el que estamos; es un tema de largo plazo y no sólo de esfuerzos aislados y temporales.

Por ejemplo, ¿cuáles son los sonidos que te gustan del lugar donde vives? ¿cuáles son los sonidos que no te gustan y quisieras que se quitaran? Mucho de ello es cambiar nuestra mente, nuestra forma de pensar y saber que cada uno de nosotros tenemos la capacidad de crear un cambio, de externar nuestras inquietudes y de que se sumen otros para lograrlo. Algo tan básico como los ruidos que nos estresan, influyen en nuestra andar en el día a día.

Y es que la violencia, es la consecución de un montón de cosas y actitudes que se hicieron o dejaron de hacer en el pasado. Tenemos que comenzar ya, con los niños, desde las etapas tempranas, pero con el ejemplo y no solo con palabras que se las puede llevar el viento. Tenemos que evolucionar como sociedad, ser mejores de lo que fuimos ayer y eso está más cerca de nosotros de lo que creemos. Desde hace mucho decidí intentar hacer un cambio, algunos en foros públicos me han llamado soñador o utópico, pero prefiero intentarlo y estoy convencido que podemos lograrlo, porque he visto como lo han logrado en otros países, tengamos voluntad.

¿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/enriquetapiapadilla/.* ■

HABILIDADES GERENCIALES

PARA EL DIRECTIVO DE LA SEGURIDAD PRIVADA

MÉXICO | Hermelindo Rodríguez Sánchez

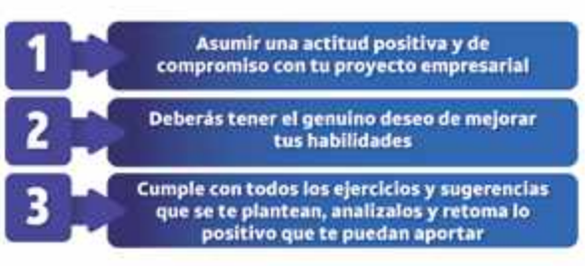
Foto: @Freepik

No importa la edad que se tenga para estudiar, todas las personas tienen la misma capacidad (un joven de 19 años que uno de 50). La diferencia entre un mediocre y un triunfador, es el estudio

El objetivo de este artículo es proporcionar los elementos necesarios a los emprendedores para el desarrollo de las siguientes habilidades gerenciales: comunicación, liderazgo, motivación, trabajo en equipo, negociación y toma de decisiones, para su desarrollo personal y profesional.

RECOMENDACIONES PARA EL DESARROLLO EXITOSO DEL DIRECTOR

Para cumplir con el objetivo planteado en el artículo, te recomendamos:



Este material informativo está enfocado a brindar a los emprendedores una serie de herramientas para el perfeccionamiento de sus habilidades gerenciales, con lo cual se concluye su proceso formativo extracurricular, que, aunado al desarrollo de un prototipo, a la conclusión de un plan de negocios preliminar y a la exposición de su proyecto en algún evento de emprendedores y empresarios, los prepara para avanzar al proceso de Incubación Empresarial.

El tema de las Habilidades Gerenciales está orientado a desarrollar y mejorar la comunicación, el liderazgo, el trabajo en equipo, la motivación, las negociaciones y la toma de decisiones.

Son las destrezas que poseen los jefes, gerentes y dueños de las empresas para dirigir de manera eficiente y productiva al personal de su empresa, para lograr los objetivos organizacionales

Con ello seguramente su empresa saldrá beneficiada al ser más productiva y eficiente. Es así, que este último constituye una gran experiencia para usted.

MÉTODOS Y HABILIDADES DE APRENDIZAJE

Proporcionar estrategias en el arte de aprender.

- Metas principales:
- Ser efectivo como estudiante independiente.
- Leer eficiente y adecuadamente al estudiar.
- Obtener las más altas calificaciones que se requieren para certificarse como Profesional de la Seguridad.

HÁBITOS DE ESTUDIO

No importa la edad que se tenga para estudiar, todas las personas tienen la misma capacidad (un joven de 19 años que uno de 50). La diferencia entre un mediocre y un triunfador, es el estudio.

Todas las personas son distintas, no hay una fórmula ideal de estudiar y aprender, sólo se proporcionan técnicas para el desarrollo de habilidades.

Foto: @Freepik

Para diseñar un plan que te permita desarrollar tus habilidades gerenciales, necesitas definir objetivos vitales y profesionales que marcan el proceso para tu desarrollo

TÉCNICAS PARA EL APRENDIZAJE

Pasar tiempo estudiando no garantiza un aprendizaje eficaz. Actualmente no se conoce ningún medio de aprendizaje sin dedicarle:

Método PQRST:

PREVIEW - Vista previa
QUESTION - Preguntar
READ - Leer
STATE - Estado
TEST - Examen

P - Examen Preliminar
Q - Formularse preguntas
R - Ganar información mediante lectura
S - Hablar para describir o exponer los temas leídos
T - Investigar los conocimientos que se han adquirido

Con cualquier tiempo que le dedique, si lo divide entre lectura y meditación, como se ha descrito anteriormente, podrá aprender y recordar más, que si omite la parte relacionada con la meditación.

Si para estudiar emplea breves periodos desligados entre sí, y no sigue un plan sistemático de estudio, el tiempo empleado no le dará buenos resultados como los que obtendría con el total de ese mismo tiempo si lo distribuyera y lo usará sistemáticamente.

PROCESO DE APRENDIZAJE

El aprendizaje es una ciencia basada en principios y procedimientos bien definidos. Consiste en adquirir nuevas formas para hacer las cosas o para satisfacer los deseos. Solamente estudiamos por una razón: para aprender.

Para que los conocimientos sean útiles deben aprenderse, en relación con algo que pueda hacer, (aplicar los conocimientos).

Poca gente aprende con eficiencia. No es difícil hacerlo, pero pocos lo intentan.

¿QUÉ SON LAS HABILIDADES GERENCIALES?

Son las destrezas que poseen los jefes, gerentes y dueños de las empresas para dirigir de manera eficiente y productiva al personal de su empresa, para lograr los objetivos organizacionales.

El conjunto de técnicas específicas para poder administrar eficientemente al personal.

IMPORTANCIA DEL DESARROLLO DE LAS HABILIDADES GERENCIALES

Solamente quien es capaz de asumir responsabilidades es capaz de tener autoridad real y dirigir al equipo de manera eficiente.

De la actitud que presentas y de la manera como evalúas las situaciones personales depende tu éxito como dirigente.

Requisitos para definir un plan para el desarrollo de Habilidades Gerenciales:

Para diseñar un plan que te permita desarrollar tus habilidades gerenciales, necesitas definir objetivos vitales y profesionales que marcan el proceso para tu desarrollo.

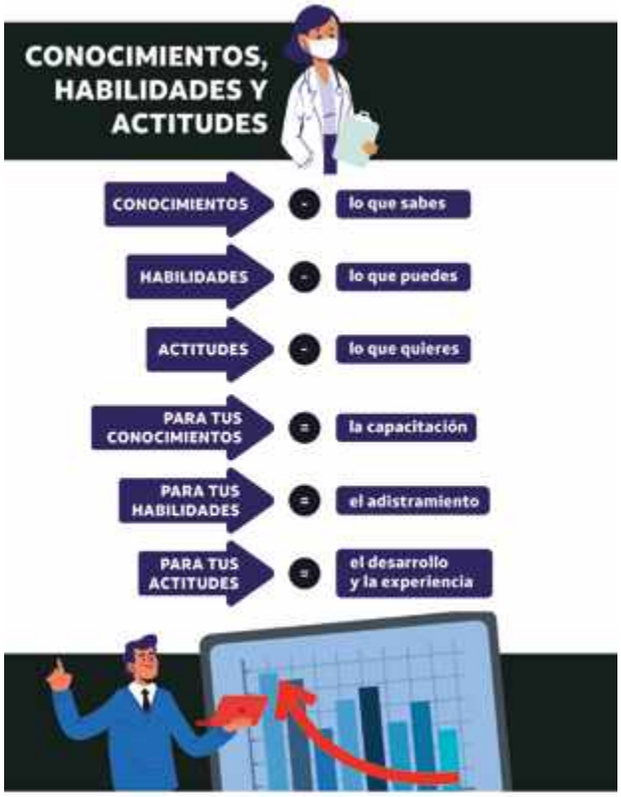
Necesitas tener muy claro:

- Un compromiso contigo mismo.
- Responsabilidad para asumir retos.
- Capacidad para aprender y ser mejor.
- Actitud positiva y constructiva.

La comunicación a nivel gerencial consiste en saber escuchar, propiciando la participación de los colaboradores, específicamente es participar y dejar participar

El proceso de transmitir información de un emisor a un receptor es fundamental en toda organización, sobre todo si la intervención de la Gerencia como líder del proceso genera la identidad, efectividad y comprensión de los objetivos organizacionales al grupo que pretende influenciar

EL PROCESO ADMINISTRATIVO



La Dirección como parte del Proceso Administrativo:

Ubiquemos ahora el área específica, con un orden y sentido que nos ayudara a desarrollar nuestras Habilidades Gerenciales.

Definiendo el Proceso Administrativo, la administración es la ciencia social que persigue la satisfacción de los objetivos institucionales, contando para ello con una estructura a través del esfuerzo humano coordinado.

Su herramienta fundamental es el mapa genérico del proceso administrativo y éste se configura de la siguiente manera:

2.1 Mapa Genérico del Proceso Administrativo

COMUNICACIÓN

La reina, la emperatriz, la soberana de las Habilidades Gerenciales es la comunicación. Hacer partícipes a los demás de nuestras ideas, pensamientos, actitudes y sentimientos. La comunicación a nivel gerencial consiste en saber escuchar, propiciando la participación de los colaboradores, específicamente es participar y dejar participar.

La comunicación no sólo hace factible la transferencia de ideas o sentimientos, sino que a través de ella se constituyen los grupos, las empresas, las instituciones y en general toda la vida de relación, la comunicación es un proceso vital de transferencia de información del emisor al receptor, tratando de influenciar en este para los fines de compartir objetivos comunes. Es necesario que exista una comunicación efectiva entre el líder y sus colaboradores, y aún más, no solamente comunicarse con los miembros del grupo, sino con aquellas personas que no forman parte del mismo.

La comunicación es un medio de ligar a las personas (futuros clientes, proveedores, compañeros, etc.) sin ella no pueden establecerse, ni concretarse los objetivos, la planeación, la coordinación, el control y lo más importante generar una actitud hacia el cambio.

El proceso de transmitir información de un emisor a un receptor es fundamental en toda organización, sobre todo si la intervención de la Gerencia como líder del proceso genera la identidad, efectividad y comprensión de los objetivos organizacionales al grupo que pretende influenciar.

¿Qué podemos hacer para mejorar la comunicación?

Existen tres factores simples que pueden ayudar:

1. Uso de un lenguaje común, utiliza palabras que puedan entenderse fácilmente y dilo en forma amable.
2. Buscar un interés común, el hecho de que trabaje en la misma empresa genera un interés común entre los miembros de esta, por ejemplo, formar un equipo de fútbol con integrantes de diversas áreas, puede romper el hielo, estableciendo las bases para una buena relación, otra herramienta podría ser implantar círculos de calidad.
3. Buscar Sinergia o Empatía, es decir ponerse en el lugar del otro.

Existe otro factor que puede ayudar a mejorar la comunicación, que es hágalo simple, hable en términos que sean fáciles de entender.

La comunicación no sólo se basa en el uso de las palabras, ya que las palabras son el primero de los siete lenguajes del hombre, los otros seis pueden fácilmente cambiar el sentido de las mismas.

Estos seis lenguajes son:

4. El tono de voz.
5. Contacto visual o forma de ver.
6. Los gestos que se hacen con las manos.
7. La postura del cuerpo.
8. La expresión de la cara.
9. El acento que se dé a las palabras.

Recuerda que los seis factores anteriores juegan un papel importante en la comunicación. Entonces:

La habilidad para comunicarse no es algo con lo que nacemos, tenemos que aprenderlo.

Cuando hablamos o escribimos acerca de algo, lo que realmente hacemos es manifestar algo que pasa dentro de nosotros, no fuera.

Si encontramos alguna dificultad para entender, o para ser entendidos, es que estamos ignorando alguna de las áreas de comunciacion.

La comunicación en la empresa

Como se muestra en el siguiente esquema, la comunicación en la organización se presenta a nivel horizontal y ascendente / descendente, siendo importante cuidar la retroalimentación en cualquiera de los sentidos, por ejemplo cuando los directivos quieren informar algo a sus colaboradores, es conveniente buscar canales formales y escritos para instruir, delegar, planear y coordinar (comunicación descendente), también es importante generar mecanismos para recibir información del exterior, ya que el intercambio comercial es la razón de ser de la empresa.

Una persona está motivada para hacer un trabajo, cuando sabe exactamente lo que se espera que haga y se da cuenta del por qué debe hacerlo

MOTIVACIÓN, TENER EL DESEO DE HACER ALGO

Una persona está motivada para hacer un trabajo, cuando sabe exactamente lo que se espera que haga y se da cuenta del por qué debe hacerlo.

Al estudiar este material, reforzaré mis conocimientos para desarrollar mejor mi trabajo diario y así voy a desempeñarme mejor.

10. Sugerencias para aprender.
11. Dedicar unos minutos para revisar el trabajo del día anterior, antes de comenzar con el que corresponda al día siguiente.
12. Iniciar el estudio a la misma hora todos los días.
13. Disponer de un lugar particular para estudiar.
14. Tener el propósito de recordar, prestar atención a las cosas.
15. Relacionar las cosas entre sí y asociarlas.
16. Ejercitar la lectura más rápida.
17. Repasar el material unas 12 o 24 horas después, dentro de una semana y finalmente dentro de tres semanas más.

Las tensiones cotidianas, carga de trabajo, exceso de responsabilidad, monotonía y las relaciones interpersonales son, entre otras cosas, factores que alteran el estado emocional de las personas, generando apatía o desinterés que traerá como consecuencia frustración a su vida laboral y personal.

Hoy no basta con un alto coeficiente intelectual para triunfar profesionalmente, se requiere conciencia de nosotros mismos y de nuestro potencial para lograr una mayor pertenencia a la organización y a la sociedad en general para ser exitosos

La superación personal muestra, a nivel humano, que querer es poder y que los límites no están en la realidad sino en la mente.

LIDERAZGO

En la antigüedad el liderazgo era interpretado como una acción en la que un individuo pretendía hacerse jefe de la clase trabajadora o del pueblo en general, con el fin de explotarlos y hacer de tal acción una manera fácil de vivir sin trabajar. Al líder se le atribuía el calificativo de una persona manipuladora e indeseable; idea que, en la actualidad, aunque en menor escala, todavía se asocia con los políticos.

Con el paso del tiempo, esta definición ha venido cambiando de tal forma que el concepto de líder ya no se le da al político, ni al jefe o director de una empresa que toma decisiones y ordena, sino a aquel que además de dirigir a un grupo de personas, los conduce, los inspira, los apoya y los orienta.

Bajo este concepto, ser líder ya no es tan simple. Ser líder implica tener vocación de servicio con la gente y la causa que se persigue.

Existen tres formas genéricas para definir al liderazgo:

r. La **teoría de rasgos**, que se basa en el análisis de rasgos de la personalidad que son comunes a los líderes. Algunas de estas características son: responsabilidad, conocimientos, seguridad, mayor nivel de actividad y participación social, mejor adaptación al ambiente, valores claros y creatividad, entre otros.
s. La **teoría de las funciones**, que enfatiza en la realización de acciones necesarias y la adaptabilidad a situaciones cambiantes.
t. El **liderazgo como posición**, se dice que una persona es líder si mantiene un estatus particular dentro de la organización, aun cuando éste se pudiera haber alcanzado por diferentes formas: elección oficial de la organización, por alguna autoridad superior; por sucesión o por asumir el control del grupo.

Los gerentes que están en el proceso de transición hacia "líderes grupales" no sólo requieren cambiar en forma significativa sus actitudes, sino que también deben modificar sustantivamente la función que desempeñan

Bajo este enfoque el líder puede influir en el grupo por su posición o por su capacidad para ejercer el control. También podemos definir al liderazgo como cualquier acción encaminada a influenciar e impactar la conducta de otras personas; es una actitud personal orientada al desarrollo de una función social con el propósito de dirigir e inspirar los asuntos y actividades de otros seres humanos, para lograr la realización de metas colectivas.

Estilos de liderazgo

- **Liderazgo directivo**: orienta a los empleados sobre qué debería hacerse y cómo debería hacerse, programando el trabajo y manteniendo los estándares de rendimiento.
- **Liderazgo de apoyo**: se preocupa por el bienestar y las necesidades de los empleados, mostrándose amigable y asequible a todos y tratando a los trabajadores como iguales.
- **Liderazgo participativo**: consulta a los empleados y toma en consideración sus ideas al adoptar decisiones.
- **Liderazgo centrado en el logro**: estimula al personal a lograr el máximo rendimiento, estableciendo objetivos estimulantes, realzando la excelencia y demostrando confianza en las capacidades de sus empleados.

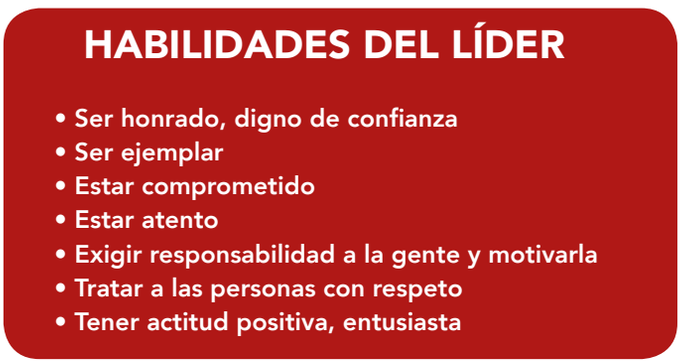
¿Cómo se llega a ser líder?

- Se requiere un pensamiento estratégico. La función más importante y trascendente de un dirigente es visualizar el futuro, estar alerta a los cambios externos, investigar y comprender las tendencias. La estrategia y la manera de organizarse es el primer paso.
- "Pasar del pensamiento a la ejecución", es la fuerza de cambiar el entorno la que nos lleva a influir en los demás y, por tanto, ejercer el liderazgo.
- Por último, hay que inspirar e involucrar a otros, motivando, organizando y trabajando en equipo para sumar esfuerzos y multiplicar resultados.

Para que una organización tenga éxito debe contar con líderes. Los gerentes que están en el proceso de transición hacia "líderes grupales" no sólo requieren cambiar en forma significativa sus actitudes, sino que también deben modificar sustantivamente la función que desempeñan. Se convertirán en facilitadores de trabajo en equipos. Un líder de equipo logra que los individuos trabajen coherentemente en proyectos definidos con marcos de tiempo predeterminados.

El líder reconoce tres áreas de resultados igualmente importantes:

1. **Tareas.** Se trata de lograr resultados específicos, en la cantidad, con la calidad y la oportunidad requeridas. El reto actual es asegurar una mayor productividad y calidad.
2. **Personas.** Donde se requiere ocuparse de los individuos a su cargo para asegurar su capacitación, motivación y progreso. El reto actual es una mayor preparación, involucrarse más y responsabilizarse.
3. **Grupos.** Donde debe asegurarse su integración y desarrollo, así como un clima de comunicación y colaboración. El reto actual es conseguir una mayor participación y trabajo en equipo. ■



Hermelindo Rodríguez Sánchez, CPO, CSSM, DSI, DES, CEO y fundador de la Consultoría en Seguridad y Protección Integral (Cosepri).

Más sobre el autor:

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 las Secretarías de Gobernación y Defensa Nacional para la portación de armas de fuego en todas sus modalidades en todo el territorio nacional.

www.trustgroup.com.mx

Trust Group Trust Group (Seguridad Privada).

Más de quince años brindando servicios profesionales de seguridad

ASIS

CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

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

BLACKTRUST:
GENERADOR DE CONFIANZA

Con más de 8 años de experiencia, BlackTrust ofrece la plataforma de Screening y Background Check más confiable y asertiva de todo México y América Latina

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

Foto: Freepik

BlackTrust es automatización, es confianza, escalabilidad, asertividad y calidad

México tiene uno de los índices de rotación de personal más altos de América Latina (16.7%), siendo uno de los principales problemas para el área de Recursos Humanos y por ende para el desarrollo de las operaciones de cada empresa o empleador. La población económicamente activa oscila entre los 58 millones de personas (59% de la población total mexicana)[1], de estos el 96% tiene algún empleo u ocupación, de los cuales el 40% se desenvuelve en el sector de servicios.

La seguridad privada es una de las industrias que padece de este problema, la rotación de personal no sólo afecta el servicio tan importante que ofrece este sector, sino que desgasta los recursos como capacitación impartida, tiempo y dinero. En una industria donde la confianza es fundamental, así como la credibilidad y la integridad, el personal que desempeña cada posición debe estar contratado bajo la enmienda de ser el adecuado, de brindar seguridad y de generar confianza.

SOLUCIONES QUE TRANSFORMAN LA SEGURIDAD EMPRESARIAL

BlackTrust es una compañía que ofrece a través de su plataforma de *screening* y *background check* (verificador de antecedentes) para México y Latinoamérica, una solución para el control de confianza y la prevención al momento de contratar al personal. A través de herramientas tecnológicas, el proceso de evaluación del personal se vuelve más asertivo y ayuda a tomar la decisión correcta de acuerdo al perfil solicitado.

Algunas de sus ventajas es que a través de la verificación legal de los candidatos, exámenes psicológicos y referencias, reduce el riesgo y los índices de rotación, incrementa la seguridad la cadena operativa de sus clientes, toda la información que se verifica se obtiene de datos precisos, públicos y legales. Uno de sus clientes más reconocidos es la aplicación de transporte privado que todos hemos utilizado.

"BlackTrust es una empresa joven, con poco más de ocho años en el mercado, surge exactamente el 01 de septiembre de 2014 como resultado de un requerimiento muy específico de una empresa que actualmente es multinacional, llamada UBER. El objetivo fue hacer un proceso de *onboarding* de choferes y socios que quisieran trabajar en la plataforma, de ahí se migró a un proceso más ágil, más inteligente, eficiente y que diera como resultado el poder dar confianza a los clientes cuando trabajan con alguien, ya sea cliente, proveedor, representante o socio", explicó en entrevista Bruno Blackmore, director general de BlackTrust.

A través del tiempo la firma ha ido creando una gran base de datos, de información públicamente accesible, 100 por ciento legítima y la cual sirve para contar con antecedentes adversos que puede tener una persona. Este tipo de metodología o actividad en países más desarrollados se llama *screening*.

BlackTrust
Trust in the world

A través del tiempo la firma ha ido creando una gran base de datos, de información públicamente accesible, 100 por ciento legítima y la cual sirve para contar con antecedentes adversos que puede tener una persona. Este tipo de metodología o actividad en países más desarrollados se llama *screening*


Foto: standret - Freepik

"La gran oportunidad y a la vez la carencia que se tiene de esta información en Latinoamérica, es que los registros legales que se tienen en los diferentes países, estados y municipios, no están normalizados, esto dio pie a que BlackTrust pudiera organizar, estructurar y limpiar, de alguna manera, la Data para que se pueda visitar mucho más eficientemente e inteligentemente. Hoy en día puedo decir que somos la plataforma de *Background Check* más grande de México y Latinoamérica, hacemos entre tres mil y cuatro mil evaluaciones diarias", comentó.

CONFIANZA. BASE DE CUALQUIER RELACIÓN

La palabra confianza está ligada directamente a la seguridad, es conocida como el "fundamento de cualquier relación humana", de ahí la importancia tanto de la persona que ejerce una función, como de la empresa que se encarga de seleccionar o brindar las herramientas para seleccionar al personal.

"Nuestra plataforma es multiindustria, ya que tenemos clientes de todos los sectores: logística, financiero, bancario, retail, y a la vez es una plataforma multinivel ya que como vemos al individuo y no a la posición exactamente, puede pasar una evaluación para un puesto muy operacional, muy básico o bien para un CEO, para esto hemos ido incorporando diferentes herramientas".

De acuerdo a Bruno Blackmore, los clientes de BlackTrust se benefician de la plataforma en tres pilares esenciales: uno, para el proceso de selección y reclutamiento de personal; dos, riesgos de seguridad (filtros de personas que no son empleados pero están relacionados con la empresa, por ejemplo proveedores, socios, representantes, clientes), y el tercer punto es el cumplimiento normativo o legal, principalmente por el sector financiero para temas de lavado de dinero, terrorismo, impuestos, corrupción, etc.

"BlackTrust es automatización, es confianza, escalabilidad, asertividad y calidad", compartió Bruno.

La plataforma cumple con diferentes regulaciones y dependiendo el tipo de cliente, el volumen o las necesidades, han desarrollado pequeños aplicativos para poder dar servicio a los diferentes clientes.

Respecto al control de confianza, en BlackTrust realiza evaluaciones y análisis sobre el candidato y brinda información suficiente al cliente para que éste tome la decisión. "Hemos ido integrando diferentes actividades o herramientas a la plataforma para poder sumar información precisa sobre las necesidades de los perfiles que cada cliente necesita de acuerdo a la operación de ese prospecto, para que el cliente tenga la confianza de que esas evaluaciones brindan información precisa sobre si esa persona cumple o no con las aptitudes necesarias para el puesto", explicó.

Estas herramientas van desde pruebas psicométricas, referencias telefónicas, revisión de documentos, comprobación de identidad de la persona, hasta toxicología, entre otras. Lo que hace la plataforma es tener todas estas herramientas en un sólo lugar y dependiendo el perfil, el cliente va decidiendo qué herramientas agregarle a cada uno de acuerdo al nivel de confianza que cada perfil requiere. Los procesos de evaluación de BlackTrust dan confianza en el mundo para decidir si éste candidato es para tal o cual perfil.

LA PREVENCIÓN COMO PIEZA FUNDAMENTAL DE LA SEGURIDAD

La prevención es la mejor herramienta de seguridad para cualquier empresa o sector. La prevención es qué tengo que hacer para que la gente no cometa un robo o fraude, por ejemplo. Y esta parte de la seguridad es la más económica de todas.

"Pese a que las industrias y las empresas no consideran en su mayoría a la prevención, siempre será mucho más efectivo y económico el educar o capacitar a nuestros colaboradores, ciudadanos e hijos sobre la prevención del delito versus detectar e investigar el delito ya cometido. Los seres humanos primero pensamos qué tan probable es que me cachen robado tal o cual cosa, lo segundo es si me cachan, ¿me castigarán o les daría igual? La tercera cosa que pensamos es, ya me cacharon, ¿qué tan severo será mi castigo? La prevención abarca todas esas posibilidades y las evita".

De acuerdo a Bruno Blackmore, los clientes de BlackTrust se benefician de la plataforma en tres pilares esenciales: uno, para el proceso de selección y reclutamiento de personal; dos, riesgos de seguridad; y el tercer punto es el cumplimiento normativo o legal, principalmente por el sector financiero

Foto: Freepik

La plataforma cumple con diferentes regulaciones y dependiendo el tipo de cliente, el volumen o las necesidades, han desarrollado pequeños aplicativos para poder dar servicio a los diferentes clientes.

En años pasados los procesos eran muy manuales, Bruno explica que digitalizar un proceso no es capturar información en una computadora, sino que los procesos se vuelvan automáticos o semiautomáticos quitando toda la parte subjetiva y la parte de error humano y que el resultado sea realmente tangible.

"Lo que estamos intentando es BlackTrust es que la tecnología para el reclutamiento, selección y revisión de antecedentes, sea una tecnología utilizada por todo tipo de empresas. Hoy en día hay muchas soluciones tecnológicas que pueden ser adaptadas ya sea para una empresa de dos empleados o mil, la clave es tener esta apertura a la tecnología, y en BlackTrust tenemos diferentes aplicativos, dependiendo el cliente, el requerimiento, el volumen. Uno de estos aplicativos que recién salió en el 2022, es *SelfTrust*, dirigido a las pymes y a los individuos", señaló Bruno. ■

Bruno Blackmore, director general de BlackTrust

Referencias:

1 "Empleo y mercado laboral en México – Datos estadísticos", Statista, 25 jul 2022 https://es.statista.com/temas/7417/empleo-y-mercado-laboral-en-mexico/#topicHeader__wrapper

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

¿CÓMO PIENSA UN DELINCUENTE?

"Tú tienes algo que yo deseo y te lo voy a quitar"

GUATEMALA | Enrique Jiménez Soza

Se encontró que la mayoría de los criminales homicidas habían recibido en su niñez maltrato infantil, así como abuso psicológico y sexual. También se menciona que el delincuente/criminal, es un sociópata y no un psicópata

Foto: @Freepik

El presente artículo no pretende ser una cátedra magistral ni una tesis doctoral sobre la mente o pensamiento de un delincuente común o un criminal especifico, más bien se trata de aportar los conocimientos básicos para poder reconocer o tratar con personas relacionadas con la delincuencia común o el crimen organizado actual, que se encuentran en todos o casi todos los países de nuestro planeta. Así mismo, para reconocer el perfil y la actuación de los individuos calificados y clasificados como delincuentes o personas que han cometido o cometen ilícitos penales en los distintos entornos que habitan.

La Criminología y la Criminalística son ciencias que estudian y tipifican a los delincuentes y los delitos que cometen indistintamente y desde hace un buen tiempo se han planteado teorías y conceptos de qué, el delincuente, nace o se hace, por lo que las investigaciones sobre uno u otro de los conceptos planteados abundan en distintas bibliografías que se encuentran disponibles para consulta o estudio.

El criminólogo y médico italiano Ezechia Marco Lombroso, (Cesare Lombroso, pseudónimo), del siglo XIX, determinó que "el criminal es nato y que nace con pre disposición hacia el crimen. Presenta reacciones biológicas y genéticas así cómo condiciones económicas precarias y ausencia de paternalismo".

Teorías antropométricas señalan que "el delincuente no nace y que es maleado por ambientes familiares y sociales a los que pertenece". "Es producto de la reacción social".

DEFINICIONES DE DELINCUENCIA

Revisando publicaciones relacionadas con el tema[1], encontramos que John Douglas, miembro del FBI (Buró Federal de Investigaciones), en los años setenta (70) y quien trabajó en esa oficina federal de los Estados Unidos de América veinticinco años, fue uno de los pioneros en analizar el perfil de criminales de esa época en su país, por medio de entrevistas y análisis sobre: edad, sexo, raza, nivel social y económico, estudios y otras actividades de los entrevistados con el fin de obtener un perfil criminal de ellos como punto de partida de las diferentes investigaciones de delitos y crímenes cometidos.

Otros estudios se encargaron también de analizar el perfil de los homicidas, sus características y enfoques psicológicos en sus hechos delictivos. Se encontró que la mayoría de los criminales homicidas habían recibido en su niñez maltrato infantil, así como abuso psicológico y sexual. También se menciona que el delincuente/criminal, es un sociópata y no un psicópata.

Tomando en cuenta el análisis previamente realizado y aunque el delincuente pareciera ser y actuar como una "persona normal", socialmente hablando, sus acciones están basadas en ideas e impulsos mentales y psicológicos diferentes a la mayoría de personas comunes

PERFIL DELINCUENCIAL

Basados en lo anterior, se plantea que un delincuente/criminal puede tener el siguiente perfil delincuencial:

- Egoísta, pues por lo general actúa en solitario.
- Tiene un nivel y estilo de vida diferente a las personas con las que habita o se relaciona.
- Vive en un núcleo familiar problemático y desintegrado.
- Tiene bajos ingresos económicos.
- Patrones de conducta anti sociales y rebeldes.
- No tiene límites para las acciones que comete.
- Sus delitos siguen un mismo patrón por lo que "deja huella" al cometerlos.
- Muestra conductas psicológicas inestables.
- Busca el placer y la evasión de la realidad.

Diferencia entre delincuente y criminal:

Bibliografía jurídica consultada determinó que al delincuente se le determina así por el número de delitos en los procesos legales que ha enfrentado. El criminal ha recibido una sentencia por proceso judicial realizado en su contra.

La delincuencia juvenil es el "fenómeno de la sociedad actual" (SciElo – México). Estudios antropológicos, genéticos, endocrinólogos y psicológicos, han determinado que "la niñez nos marca para siempre": conflictos sin resolver, relaciones interpersonales inadecuadas, vida sexual indefinida.

Niño culpable = niño mentiroso.
Infancia que nunca tuve = conducta anti-social y familiar.

"El delincuente es producto de la reacción social", Silvia Dahiana Pita Torres, Universidad Psicológica y Tecnológica de Colombia.


Foto: @Freepik


Foto: @Freepik

TIPOS DE DELINCUENTE:

- **Criminal nato:** desde su niñez.
- **Ocasional:** actúa cuando tiene la oportunidad o se le presenta la "tentación" de robar, como sucede con el cleptómano a quien se le considera un enfermo.
- **Personal:** actúa solo y va directamente a la víctima u objeto codiciado sin importarle que lo identifiquen.
- **Profesional:** se dedica a cometer los delitos que practica como forma de vida y se especializa en ellos, buscan objetos de mayor valor y seleccionan víctimas de alto nivel económico.
- **Especialistas:** desde el ladrón callejero o "ratero de mercado", hasta roba vehículos, carteristas, asaltantes, clonadores de tarjetas, roba teléfonos celulares y un largo etcétera.
- **Dependiente de adicciones:** roba dinero u objetos de fácil venta para mantener su adicción a drogas y sustancias adictivas, realmente es un enfermo física y mentalmente.
- **Delincuente de cuello blanco:** se le menciona en altas élites económicas y financieras actuando casi siempre en el anonimato personal o relacionado con sociedades mercantiles de capitales importantes.
- **Otros:** la corrupción política y gubernamental que, lamentablemente, se señala en algunos países y gobiernos estatales, ha dado lugar a que algunos funcionarios resulten involucrados en "negocios públicos", donde se manejan fondos voluminosos con dudas y señalamientos en cuanto a la administración de ellos.
- **Bandas criminales:** se considera una banda delincuencial cuando se involucran o "asocian" dos o más delincuentes con fines determinados; cada uno de ellos tiene una función específica al momento de un robo, asalto u otro hecho delictivo. En el caso de los secuestradores, éstos requieren de una logística profesional más extensa como vehículos, residencias de resguardo, líneas de comunicación, negociadores de rescate, formas de pago, alimentos y medicinas para las víctimas y vías de escape. Casi siempre en un secuestro está involucrado un familiar cercano, empleado de confianza o persona que conozca las actividades rutinarias del secuestrado, vida familiar, rutinas diarias y potencial económico.


Foto: Freepik

Aprovecha situaciones como la ausencia de autoridades, nocturnidad, victima débil (niños, ancianos, mujeres)

¿CÓMO PIENSA EL DELINCUENTE?

Tomando en cuenta el análisis previamente realizado y aunque el delincuente pareciera ser y actuar como una "persona normal", socialmente hablando, sus acciones están basadas en ideas e impulsos mentales y psicológicos diferentes a la mayoría de personas comunes. Previamente a su acción delictiva el delincuente, sea cual sea su accionar, sigue un proceso mental y analítico previo a cometer un ilícito:

Selecciona a su víctima: puede ser anticipadamente o rápidamente, en la calle, antes de proceder al robo, asalto o daño a cometer.

Valora el objeto o bien que busca obtener: lo hace para saber cuánto puede obtener al "negociar" lo robado o simplemente para satisfacción personal de tener un bien de alto valor (vehículos, dinero en efectivo, relojes, casas, teléfonos, etc.); casi nunca se quedan con los objetos obtenidos.

Analiza los riegos que pueda tener: considera los pros y contras que va a enfrentar y decide el plan de acción adecuado: qué, cómo, cuándo, dónde y por qué. Aprovecha situaciones como la ausencia de autoridades, nocturnidad, victima débil (niños, ancianos, mujeres). Y evita a cualquier costo el ser apresado por la policía y quedar detenido un tiempo en la cárcel sin poder seguir delinquiendo.

Conoce leyes y limitaciones policiales: sabe de las penas que puede tener por los ilícitos que comete y el tiempo que purgará por ellos, así como las limitaciones o "beneficios" que tiene una aprehensión policial en el momento de ser detenido.

Se actualiza en su modus operandi: esto se refiere a la forma o mecanismo para cometer nuevos delitos considerando los avances tecnológicos de actualidad como teléfonos celulares, GPS, WhatsApp, cajeros automáticos, acceso a Internet, cámaras de vigilancia, alarmas electrónicas, distorsionadores de voz y otros más. Sabemos que constantemente se presentan nuevas formas de delinquir y de extorsionar que no habían sido usadas anteriormente y éstas tienen también un tiempo de "vigencia" antes que se presenten nuevas, (referencia: redes sociales, prensa y avisos preventivos).

PREVENCIÓN

La prevención y actualización sobre la delincuencia y crimen organizado es la forma adecuada para estar libre de riegos, personales, familiares, económicos, laborales, callejeros y otros que se presentan inesperadamente, por lo que esperamos que esta publicación sirva al lector como una información básica, pero útil para su seguridad personal. ■

Referencias

[1] *Forma de inadaptación social y desafío a la sociedad y a las normas de convivencia y La delincuencia tiene un origen poli forme. (Jiménez 2005, 215-261).*

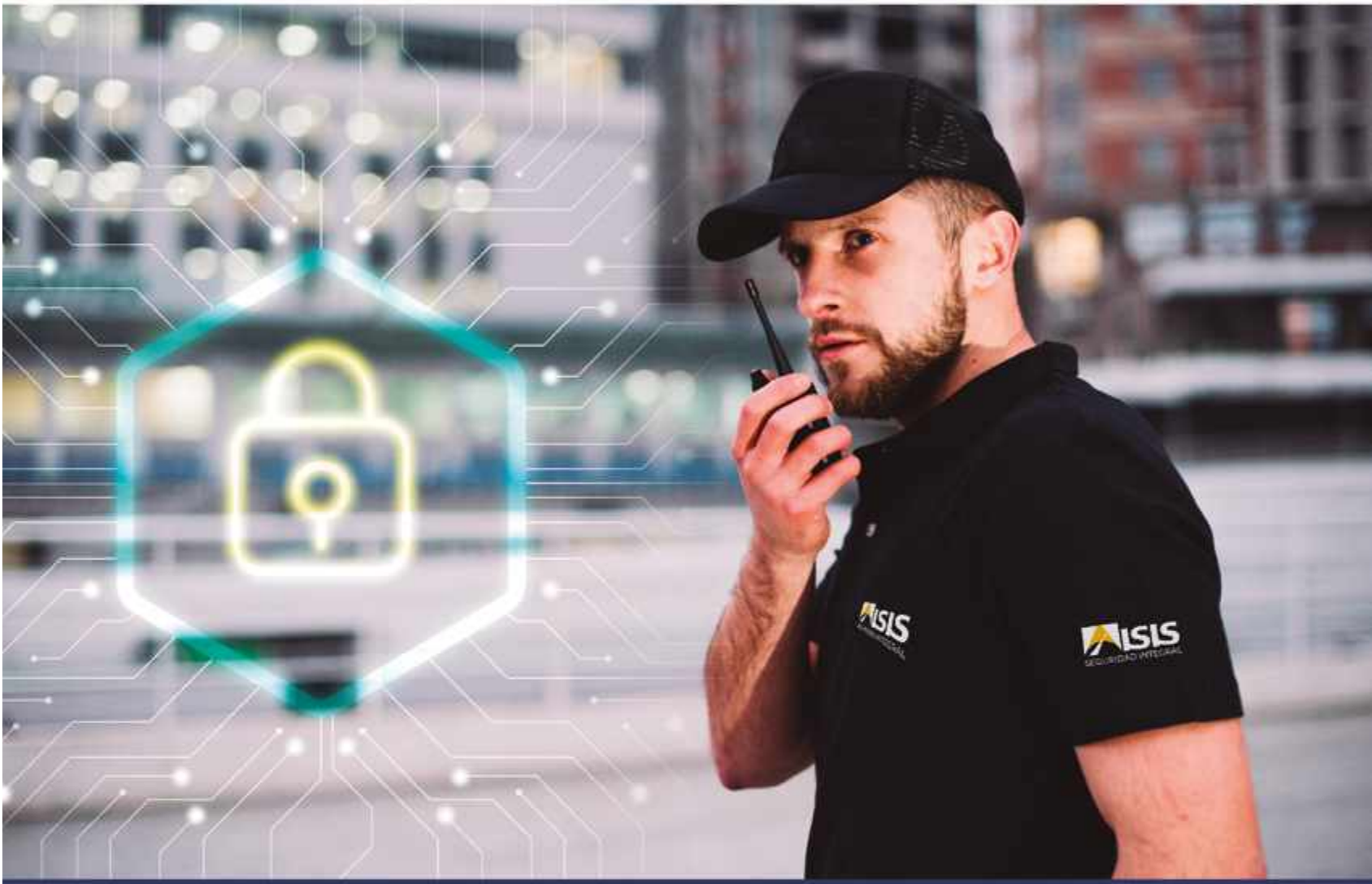

Foto: @Freepik

Enrique Jiménez Soza, asesor profesional de seguridad

Más sobre el autor:

ISIS SEGURIDAD INTEGRAL

Creamos entornos seguros



Servicios:

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

55 1089 1089

55 5762 6630

ventas@isis-seguridad.com.mx

www.isis-seguridad.com.mx

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

iuvity, SEGURIDAD FINANCIERA

Foto: Creativeart - Freepik

Amigable, ágil, segura, así es la solución que iuvity ofrece para el sector financiero con asesoría y apoyo personalizado sin importar la distancia y ubicación de sus clientes; primero las personas, después la tecnología

MÉXICO | Mónica Ramos / *Staff* Seguridad en América

¿Cuántos de ustedes han desistido de un trámite bancario y/o financiero por el exceso de gente y las largas filas en las sucursales? O bien, ¿cuántos han sufrido de robo de identidad o cargos desconocidos en su tarjeta de crédito? Actualmente el principal problema de la banca es el fraude digital, la tecnología es una herramienta increíble para facilitar y mejorar la vida de las personas, pero hay que saber cómo utilizarla y sobre todo, tener el respaldo de una institución o empresa que nos oriente y resuelva problemas de este tipo.

iuvity es una empresa que tiene sus orígenes en el año 2000 con el nombre TODO1, actualmente desarrolla soluciones para la banca en línea para diferentes e importantes bancos, así como plataforma de pago, y soluciones de prevención de fraude digital, que dan seguridad a la herramienta de compra del día a día, el *e-commerce*.

Para iuvity, primero están las personas y después la tecnología, ya que con la llegada del *open banking*, es decir, esa apertura financiera en donde otras marcas ofrecen sus soluciones a través de estos entes financieros, para cubrir todas las necesidades de las personas facilitando el acceso masivo, abierto y sin fricción al dinero y a oportunidades financieras.

"Lo que hacemos en iuvity es entender dónde están nuestros clientes, hacia dónde van y qué quieren hacer; adecuamos la solución hacia lo que ellos necesitan. Protegemos su inversión aprovechando los recursos que ya tienen y atendiendo los retos del mercado. Por ejemplo, en México, uno de los grandes retos es la inclusión

"Lo que hacemos en iuvity es entender dónde están nuestros clientes, hacia dónde van y qué quieren hacer; adecuamos la solución hacia lo que ellos necesitan. Protegemos su inversión aprovechando los recursos que ya tienen y atendiendo los retos del mercado"

Foto: Freepik

El cliente puede colocar factores de doble autenticación para mejorar aún más la seguridad del usuario, con un *soft token o one time password*, que cambia continuamente, además se verifica que las transacciones las haga siempre desde su mismo dispositivo

Foto: thicha2707 - Freepik

financiera. Y esto es importante no sólo para los clientes de la banca, sino también para los pequeños comercios, las pymes e incluso los comerciantes individuales; nosotros ofrecemos una solución amigable, ágil, segura", comentó en entrevista Salomon Arrache, director comercial de iuvity.

Y agregó que esta solución puede conectar a sus usuarios con sociedades de préstamos y créditos o con una FinTech (Tecnología Financiera), eso les abre la puerta para participar en el sistema financiero, crear un historial crediticio y avanzar en temas financieros y personales contribuyendo con México y su economía.

El corporativo de la firma se encuentra en Miami, Florida (Estados Unidos), sin embargo tiene una larga trayectoria atendiendo bancos de Latinoamérica y Estados Unidos, y nació justamente dando un servicio de consultoría para hacer la transformación digital de bancos en esta región. Estos bancos siguen siendo sus clientes y actualmente iuvity está creciendo ya que ofrece soluciones de seguridad contra fraude, de oficina virtual y de canal digital para las instituciones de servicios financieros.

PRIMERO LAS PERSONAS

La transformación digital en todos los sectores vino a facilitar la vida de las personas, pero requiere de cuidado y prevención sobre todo si se tratan temas financieros. A continuación describimos las soluciones que iuvity ofrece y cómo es que ayudan a lidiar con la seguridad financiera:

• **iuviPROFILER.** Predice y gestiona el fraude en tiempo real y con muy alta precisión, es fácil de implementar, simplifica las actividades del *back office*, mejora la experiencia del usuario y por ende incrementa la adopcion de sus canales digitales.

• **iuviBANKING.** Es una plataforma omnicanal, APIficada, flexible y modular; una banca digital integral para el uso y operaciones cotidianas de sus usuarios. Además ofrece soporte experto para el mantenimiento, la operación y la renovación tecnológica.

• **iuviNOW.** Y la más anhelada por los usuarios de la banca y servicios financieros, ya que es el medio por el cual los usuarios pueden tener una comunicación ágil, directa, sin importar dónde se encuentren físicamente, para atender, resolver y generar los servicios de la banca o la institución financiera. Puede ser desde atención al cliente hasta el escaneo en vivo de documentos para algún trámite.

PROTECCIÓN FINANCIERA

La ciberseguridad es una herramienta que por supuesto iuvity tiene presente. "En la actualidad hay dos tipos de empresas: las que han sido atacadas y las que no saben que han sido atacadas", señaló Salomon, quien además explicó que desde el punto de vista de la ciberseguridad, en Iuvity construyeron una solución que atiende diferentes necesidades de los usuarios que requieren extrema prevención y seguridad.

"Lo que necesitamos como seres humanos es tener la cercanía con la institución financiera que nos ofrece un servicio y como personas, la agilidad para poder hacer el trámite desde el teléfono móvil sin tener que acudir a la sucursal a hacer fila y eso se puede conciliar con una solución que a través de tu dispositivo móvil puedas tener calendario para agendar una cita con tu asesor, dentro de la cita tener una teleconferencia para tener esa visión y contacto con el otro, y que además con esa misma cita me puedas ayudar a llenar los formatos, lo pueda firmar electrónicamente y si necesitas documentación adicional pueda ahí mismo escanearlo y enviarlo y que todo eso quede grabado para que tenga soporte tanto la institución financiera como el cliente y con esto sentirse seguro de contratar o adquirir un servicio financiero de forma ágil, sencilla y segura", explicó.

"Lo que necesitamos como seres humanos es tener la cercanía con la institución financiera que nos ofrece un servicio y como personas, la agilidad para poder hacer el trámite desde el teléfono móvil sin tener que acudir a la sucursal a hacer fila"

Una vez que el cliente ya domina y se autogestiona a través de esta aplicación con la institución financiera, lo que quiere evitar es un hackeo, las soluciones de iuvity están basadas en el *machine learning* e Inteligencia Artificial, por lo que entiende cuál es el comportamiento habitual de sus usuarios y si la solución detecta una actividad inusual, lanza alertas para verificar o comprobar que alguien está usufructuando su identidad.

Además puede colocar factores de doble autenticación para mejorar aún más la seguridad del usuario, con un *soft token o one time password,* que cambia continuamente además se verifica que las transacciones las haga siempre desde su mismo dispositivo y comprobar con métodos de autenticación si es o no el usuario quien está realizando esa actividad. Ante una emergencia puede hablar con su asesor cara a cara y lo ayudará a resolver la emergencia sin tener que ir a la sucursal, sin tener que hacer fila entendiendo perfectamente la situación humana y apremiante que está viviendo ahí.

Foto: Freepik


Salomon Arrache, director comercial de iuvity

TIPS PARA LA BANCA VIRTUAL

A continuación, Salomon Arrache nos compartió algunos tips para el usuario final, al momento de usar la banca digital:

1. Desconfíe de todo. Los riesgos de seguridad están presentes en cualquier actividad, en cuanto a medios y herramientas digitales, es importante verificar cualquier tipo de solicitud que llegue supuestamente de la institución financiera y que solicite información confidencial, ya sea a través de correos electrónicos, mensajes SMS. Primero, cerciórese llamando directamente al banco.

2. Cuidado con el *phishing*. Este es el tipo de ciberataque más común y vigente, porque siguen teniendo éxito. Revise la URL, que el nombre del banco esté bien escrito y de dónde proviene.

3. Cuidado con códigos QR con *malware*. Existen códigos QR que al momento de descargarlos pueden estar descargando algún *malware*.

4. Ante la duda, verifique la información las veces que sean necesarias.

Siéntase seguro y cómodo con iuvity. ■

NUESTRO VALOR, SU SEGURIDAD

TIMUR Latinoamérica

GALEAM

SERVICIOS

- PROTECCIÓN EJECUTIVA
- GUARDIAS INTRAMUROS
- CONSULTORÍA

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

info@galeam.mx | info@timurlatinoamerica.com

55 6840 1036 / 56 3048 9610 / 56 3700 0133

ecaptureDtech: TECNOLOGÍA 3D PARA LA SEGURIDAD

MÉXICO | Mónica Ramos / *Staff* Seguridad en América

Gracias a eyesCloud3d se puede tener una recreación más acertada de la escena de un accidente, un crimen y la cadena de custodia.

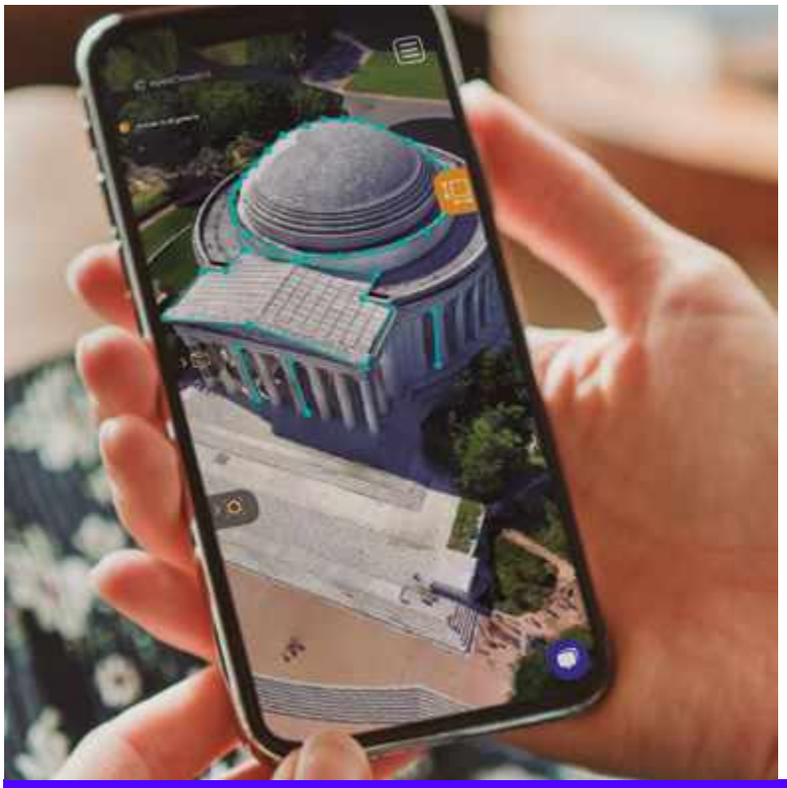
SOLUCIONES 3D PARA LA SEGURIDAD

El principal objetivo de la empresa es el tratamiento de imágenes procedentes de cualquier dispositivo, aplicado a dos soluciones:

- **eyesCloud3D** es una plataforma en la nube multidispositivo que permite la generación automática de modelos 3D, a través de fotos o vídeos de cualquier dispositivo ya sea teléfono móvil, cámara réflex o digital, GoPro o dron; por parte de cualquier usuario de manera rápida, fácil y siencilla, sin tener conocimientos previos ni ser expertos en *software*.

  Esta herramienta es utilizada principalmente por las fuerzas policiales. "Hemos simplificado todos los procesos que se hacían actualmente para la generación de modelos 3D a tan solo 3 pasos: uno, grabar el vídeo o capturar las fotos; dos, subirlo a la plataforma; y tres, esperar a que se genere el modelo 3D. Es un proceso sencillo y rápido, que facilita a las fuerzas policiales, por ejemplo, la documentación 3D de los escenarios criminalísticas, ya que cualquier elemento policial puede datar la escena y obtener el modelo 3D en entre tres y treinta minutos, dependiendo de las imágenes", comentó en entrevista Miguel González Cuétara, CEO de ecaptureDtech.

Con una trayectoria de más de 10 años en el mercado, la empresa especializada en el análisis y tratamiento de imágenes, ecaptureDtech, se suma a las soluciones tecnológicas para el área de seguridad. La firma con sede en España genera contenido 3D con cualquier tipo de dispositivo con cámara, incluidos teléfonos móviles y cámaras hiperespectrales, que posibilitan la generación de modelos 3D hiperespectrales; además de realizar el reconocimiento objetos y personas sobre imágenes 2D a través de Inteligencia Artificial.



"Hemos simplificado todos los procesos que se hacían actualmente para la generación de modelos 3D a tan solo 3 pasos: uno, grabar el vídeo o capturar las fotos; dos, subirlo a la plataforma; y tres, esperar a que se genere el modelo 3D."

ecaptureDtech se distingue por la innovación en sus soluciones, que ya son utilizadas principalmente por fuerzas policiales para sus labores de documentación de escenarios criminalísticos y análisis de sucesos. Labores que se ven facilitadas a partir de la documentación 3D de los hechos en la plataforma eyesCloud3D que cuenta con más de 40 herramientas que agilizan labores como el cálculo de velocidad, distancia, fuerza de impacto entre otras.

Entre las funcionalidades de la plataforma eyesCloud3d, se encuentran la posibilidad de ver los modelos 3D generados en realidad virtual obteniendo así una imagen más detallada de lo sucedido. La facilidad de uso de la plataforma permite, por ejemplo, que un patrullero que llega a un accidente de tráfico o un crimen, o a cualquier otra

"La idea de eyesNroad es que, a partir de una cámara colocada en el salpicadero de tu coche, seas capaz de hacer un inventario de la carretera donde veas todas las señales de tráfico verticales y horizontales, clasificadas e identificadas, así como todos los desperfectos que haya en la carretera, así como toda la ausencia de líneas, todo georreferenciado y datado."

situación donde sea necesario documentar en 3D el escenario y, sin necesidad de llamar a la Central o esperar a otro equipo de agentes. Él mismo, directamente puede grabar la escena, subirla a la plataforma y obtener el modelo. Así, además de no perder tiempo, la escena no se daña con el paso del resto de cuerpos de rescate o auxilio.

Una de las más recientes innovaciones de la plataforma es el desarrollo de una herramienta para el cálculo de la energía de deformación la cual ayuda, por ejemplo, en la investigación de accidentes si un auto impacta contra otro. Para ello, primero se crea el modelo 3D deformado del vehículo, se agrega el plano original de éste y en automático esta herramienta calcula la energía de deformación.

Otra herramienta es la Proyección 3D. Con ella, si una cámara de seguridad tomara imágenes de un vehículo implicado en un accidente en un cruce, con esta herramienta se puede hacer el modelado del cruce y obtener y calcular la velocidad a la que pasó el vehículo en tan sólo dos minutos. En la plataforma encontramos, además, la herramienta de cálculo de trayectoria de bala, cálculo de trayectoria de sangre, entre otras útiles para el Área de Seguridad.

- En su búsqueda de soluciones para el sector seguridad, ecaptureDtech desarrolla eyesNroad, plataforma web que detecta y crea inventarios de señales de tráfico horizontales y verticales, pórticos, baches y deterioros en la calle o avenida; mediante el análisis de imágenes de vídeo obtenidos con una cámara estándar colocada en un coche, empleando Inteligencia Artificial y *Machine Learning*.

  "La idea de eyesNroad es que, a partir de una cámara colocada en el salpicadero de tu coche, seas capaz de hacer un inventario de la carretera donde veas todas las señales de tráfico verticales y horizontales, clasificadas e identificadas, así como todos los desperfectos que haya en la carretera, así como toda la ausencia de líneas, todo georreferenciado y datado. Que te permita hacer comparaciones de un momento a otro del tiempo, con lo que puedes hacer una observación adecuada de la carretera para la seguridad, y además se puede adaptar a otros campos como la ingeniería" explicó Miguel González Cuétara.

Esta solución es útil también para la cadena de custodia, ya que permite tener un controlo unívoco del proceso y sin problemas de trazabilidad, desde que se suben las imágenes, hasta que se obtienen los resultados, teniendo validez desde el punto de vista judicial.

DE EUROPA A AMÉRICA

ecaptureDtech es ya reconocida en España por la mayoría de las fuerzas policías del país en su prestación de servicios que van desde la información hasta la reconstrucción de accidentes de tráfico a la conservación de carreteras a través de ingeniería. A nivel internacional, cuenta ya con más de 20 mil usuarios tanto de la criminalística como la policía; y actualmente ya se encuentra implementando sus soluciones en Centroamérica y Sudamérica.

"Las ventajas de ecaptureDtech es que funcionamos totalmente online. Nuestras soluciones son accesibles a nivel mundial y no hace falta los productos estén instalados en ningún sitio, se pueden utilizar desde cualquier país. Dentro de los planes a corto plazo, está introducir la marca en Norteamérica y que seamos reconocido para que cada vez más usuarios se beneficien de nuestras soluciones, que son accesibles y de gran utilidad para el sector seguridad".

LA COMPAÑÍA TRAS LAS SOLUCIONES A PARTIR DE MODELOS 3D

Miguel González Cuétara es un empresario con más de 20 años de experiencia acumulada en el mundo de los negocios, que tomó la decisión junto a otros socios de tomar y reestructurar ecaptureDtech en su búsqueda por hacer que la tecnología desarrollada, estuviera al alcance de cualquier usuario. ■

Fotos: ecaptureDtech

¿QUÉ VENTAJAS TIENE EL **SERVICIO DE VIGILANCIA FÍSICA** EN UN CENTRO HOSPITALARIO?

VENEZUELA | Mario Fernando Cabrera García

Las organizaciones prestadoras de servicio de seguridad privada deben estar a la vanguardia y siempre en busca de nuevas alternativas que permitan minimizar el accionar de las organizaciones criminales al margen de la ley para salvaguardar los bienes muebles e inmuebles encargados y/o encomendados a la seguridad privada

Foto: @Freepik

Hoy en día el personal de vigilancia es capacitado constantemente en temas de atención al usuario, amenazas potenciales, la agresividad del usuario y que tanto el cliente como el guardia es objetivo de las bandas delincuenciales, por lo que todo esfuerzo debe ser canalizado al mismo objetivo

La importancia que tienen nuestros hombres de seguridad en la prestación del servicio de vigilancia sin armas de fuego en un centro hospitalario, en donde están expuestos en todo momento a diversos riesgos, durante el ejercicio de su labor. El guardia, individuo que pasan por circunstancias críticas, para aportar todo su conocimiento y capacidad en pro de la actividad encomendada para contribuir al cumplimiento de un excelente servicio y al final de la larga jornada estar tranquilo por el deber cumplido.

Cuando se presenta servicio de vigilancia privada, el cliente siempre está a la expectativa en donde el hombre de seguridad cometerá errores y no se preocupa por fomentar una cultura de seguridad, sino que por lo contrario en vez de ser un facilitador, que canalice todo esfuerzo hacia un mismo objetivo y que se complemente los conocimientos en el área de la seguridad, realizando alianzas estratégicas, basadas en las experiencias vividas, para evitar que se sigan repitiendo situaciones que afectan notablemente el buen desempeño de nuestro hombre de seguridad y es entonces cuando nuestro cliente, al cual consideramos como nuestro aliado, se ha convertido en un obstáculo para ejercer nuestra función primordial la de custodiar y velar por el bienestar de sus bienes muebles e inmuebles que han sido dejados bajo custodia de la seguridad y en aras de establecer unos buenos procedimientos de seguridad, la cual afecta a toda la organización de alguna manera y en algunos casos puede hasta generar el cierre definitivo de la institución.

LAZOS DE COOPERACIÓN

¿Entonces por qué no establecer parámetros definidos que permitan que la seguridad desarrolle su actividad con la ayuda de toda la organización? Fortaleciendo los lazos de cooperación mutua, en beneficio de la misma sociedad, ya que es sabido que la seguridad la hacemos todos y todos somos responsables por los acontecimientos al margen de la normalidad, en virtud de lo anteriormente expuesto no se justifica que el usuario maltrate ya sea de forma verbal o por sus actos a un individuo, que lo único que hace, es brindar un ambiente de tranquilidad y armonía, bajo condiciones adversas a las circunstancias.

Foto: @Freepik

DISTRIBUCIONES E IMPORTACIONES DEL PEDREGAL, S.A DE C.V.

Ventas de materiales Balísticos Certificados

Blindaje Arquitectónico para:

·Casas ·Joyerías
·Oficinas ·Instalaciones estratégicas

(55) 5216-0050

www.blindaje007.com

Blindaje@prodigy.net.mx
ReneRivera@Deipedregal.com


Foto: @Freepik

Por lo tanto, hoy en día el personal de vigilancia es capacitado constantemente en temas de atención al usuario, amenazas potenciales, la agresividad del usuario y que tanto el cliente como el guardia es objetivo de las bandas delincuenciales, por lo que todo esfuerzo debe ser canalizado al mismo objetivo, realizando trabajos mancomunadamente, logrando la minimización de los riesgos potenciales a los que se está expuesto.

Considerando que en la actividad se ha generado una cultura encaminada a la protección de personas, bienes, es necesario establecer las pautas básicas, conociendo cuál es el servicio que deseamos para nuestras organizaciones con el ánimo de no afectar el desarrollo de nuestra actividad, por lo tanto el tema de la seguridad privada acapara toda la atención en las diferentes organizaciones permitiendo desarrollar servicios acorde a las necesidades del cliente garantizando un ambiente de tranquilidad soportado por una entidad que brinda el servicio con personal capacitado e idóneo para ejercer funciones de vigilancia.

Es entonces cuando surgen una serie de interrogantes en pro y encontrar de la seguridad privada y más aún, si la prestación del servicio se realiza en instituciones hospitalarias, donde se dan un sinnúmero de escenarios que facilitan o dificultan el buen desempeño de las funciones ejercidas por nuestros guardias, quienes a la hora de actuar realizan maniobras sorprendentes para garantizar la protección adecuada de las personas, bienes, dejados bajo su custodia y no es fácil determinar en un momento crítico las funciones a desarrollar, puesto que la atención sobrepasa los límites y se convierte en una herramienta encaminada a generar malestar dentro de la población que recurre a solicitar los servicios hospitalarios.

Si bien es cierto que el guardia está preparado para asumir todo tipo de situaciones, relacionadas con su actividad en muchas de ellas, apenas puede dar aviso a su jefe inmediato, estas situaciones debido a la falta o poco conocimiento por parte de la población que visita el centro médico, con relación al verdadero servicio que presta la seguridad privada, convirtiendo el sitio de trabajo para el hombre de seguridad en un verdadero campo de batalla, donde el resultado final es sin duda una mala imagen para la seguridad privada, sin darle la importancia necesaria a los hechos que realmente ocurren y por las peripecias por las cuales debió pasar nuestro hombre de seguridad.

Es interesante plantearnos el por qué en los centros hospitalarios el servicio de seguridad privada ha ganado adictos desde el momento en cual se reglamentó el no uso de armas de fuego, por parte del personal de seguridad, estos escenarios han contribuido a determinar que el señor de seguridad, en momentos de situaciones críticas puede optar por emplear mecanismos de control basados en la utilización de armas no letales que garantizan el desarrollo efectivo de su labor permitiendo que el cliente este satisfecho por su actividad y que no es un riesgo para la comunidad, sino por lo contrario hace parte de una imagen corporativa basada en los buenos principios institucionales, estableciendo dentro de la población un clima de tranquilidad y armonía que permitirá fortalecer y canalizar los esfuerzos en contra de la delincuencia, obteniendo resultados favorables.

No obstante, vale la pena aclarar que se presentan situaciones ajenas que discriminan o ponen en tela de juicio la buena labor ejecutada por la seguridad privada debido a que la mayoría de la población, considera que si un guardia no porta un arma de fuego, no representa ningún tipo de autoridad y por lo tanto se podrán hacer actividades en contra de las políticas del bien a cuidar, alguna de ellas son: ingresar a las instalaciones sin la debida autorización del cliente y el respectivo control por parte del personal de vigilancia, realizar hurtos, cometer actos vandálicos, etc.

HOMBRES DE SEGURIDAD

La seguridad privada ha tomado un papel primordial y esencial dentro de las organizaciones, por lo que hoy en día, pensar en que no se tiene algún tipo de seguridad privada es algo inaudito, puesto que todo gira en el entorno de la seguridad, basado en los principios de tranquilidad y armonía, es entonces cuando el hombre de seguridad entra a ejercer un papel primordial y de vital importancia para desarrollar una serie de funciones encaminadas a minimizar los riesgos a los que están expuestos los clientes, ya que su función primordial es la de brindar todo el apoyo necesario para establecer mecanismos de protección adecuados garantizando un ambiente de tranquilidad y armonía tanto al personal interno como externo convirtiendo su sitio de trabajo en un lugar que realza un estado de seguridad.

La mayoría de la población, considera que si un guardia no porta un arma de fuego, no representa ningún tipo de autoridad y por lo tanto se podrán hacer actividades en contra de las políticas del bien a cuidar


Foto: @Freepik

FACEit

PLATAFORMA TECNOLÓGICA EN LA NUBE PARA COMPAÑIAS DE SEGURIDAD

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

GRUPO SALUS
SEGURIDAD Y BIENESTAR

SOLUCIONES SIMPLES A PROBLEMAS COMPLEJOS

Dirección:

- Control integral de la operación de la empresa
- Visión en tiempo real de la operación
- KPI's y reportes automatizados
- Automatización y eficiencia en la operación con contribución al margen

Comercial:

- Registro de clientes nuevos, servicios solicitados
- Documentación digital del contrato con el cliente, comentarios, indicaciones, etc
- Reporte de cumplimiento para facturación
- Diferenciador tecnológico para la captación de nuevos clientes

Recursos Humanos:

- Control de personal con tipos de empleados
- Documentación digital de identificación, antecedentes no penales, seguro social, etc.
- Control de vacantes y reclutamiento
- Enrolamiento de personal con fotografía
- Control de vacaciones e incapacidades

Operaciones:

- Control y detalle de Contratos, Servicios, Puestos y Turnos
- Estado de fuerza en tiempo real
- Asignación de guardias a los diferentes servicios
- Control de Asistencia de guardias con reconocimiento facial y geocercas
- Operación de custodias: Registro de viajes, unidades, custodios, custodiados, etc
- Visitas de Supervisores y Rondines
- Bitácora electrónica de eventos con fotografía
- Cumplimiento histórico de contratos

Contabilidad:

- Reporte de horas trabajadas y turnos realizados para el pago de nómina
- Reporte de clientes y servicios para facturación

Cliente:

- Visibilidad y transparencia en el control de asistencia
- Recepción de incidencias y bitácoras electrónicas con fotografía en tiempo real
- Solicitud de nuevos servicios o guardias
- Control de cumplimiento de contrato

Guardia:

- Transparencia en su registro de asistencia, horas trabajadas, turnos extras
- Envío de bitácoras electrónicas con fotografía
- Reporte de incidencias en tiempo real
- Solicitud de equipamiento, uniforme, radio, etc

INTELIGENCIA ARTIFICIAL Y RECONOCIMIENTO FACIAL.

¡MODERNIZATE Y DIGITALIZA TU EMPRESA YA!

Tel. 55 2560 7642

WWW

WWW.GRUPOSALUS.COM.MX/FACEIT

CONTÁCTANOS Y SOLICITA TU DEMO

Poco a poco los servicios de seguridad hospitalarios van desarrollándose, en generar sin planificación, como queda dicho, y habitualmente por agregación

Probablemente no exista mejor puesto de observación que un hospital respecto de la sociedad a la que acoge. Un centro hospitalario es un microcosmos en sí mismo. Lo es en cualquier país, ciudad, lugar, y lo es más si cabe, en las naciones industrializadas y socialmente avanzadas. Un gran centro sanitario acoge permanentemente a un número muy elevado de trabajadores, razón por la cual es indispensable, que nuestro hombre de seguridad esté capacitado y entrenado en el tema de las seguridad privada, con el fin de que el cliente se sienta satisfecho y forme parte primordial en los diversos esquemas de seguridad con vertiéndose en un eslabón más de la cadena de la seguridad, al determinar la ventaja se logra con la prestación de un servicio físico sin armas de fuego, es establecer una serie de parámetros en los cuales, se determinan los factores de riesgos a los cuales está expuesto el hombre de seguridad y por ende se puedan contrarrestar y minimizar al máximo mediante la utilización de técnicas disuasivas, con la contribución del guardia.

Actualmente existe tecnología basada en la utilización de armas no letales que mediante una capacitación consciente nos permite inmovilizar al perpetrador en cuestión sin provocarle daños permanentes ni la muerte, razón por la cual es ideal su utilización en centros hospitalarios donde la población flotante es alta y provienen de varios estratos sociales. Esta tecnología es ideal para que el guardia tenga control frente a los disturbios dentro de los mismos hospitales y para defensa del hombre de seguridad.

Los hombres de seguridad estarán mejor preparados para atender situaciones que afectan el buen funcionamiento del establecimiento y además para defenderse. En el mejor de los casos, el uso de estas armas podría salvarle la vida a un criminal y no compromete al personal encargado de la seguridad a procesos judiciales que perjudican a dicho personal y que afectan el desarrollo de la organización, ya que esto genera la capacitación y entrenamiento de un nuevo guardia.

Es esencial buscar mecanismos y utilizar herramientas que eviten causar confrontaciones que van en contra de una buena prestación del servicio tanto al cliente interno como al externo, situación por la cual en la actualidad las organizaciones dedicadas a la prestación de un servicio de seguridad privada han establecido una serie de procedimientos encaminados en fortalecer los esquemas de seguridad dándole como prioridad el respeto a la vida y las buenas relaciones interpersonales mejorando los ambientes donde la seguridad privada desarrolla su papel: Poco a poco los servicios de seguridad hospitalarios van desarrollándose, en generar sin planificación, como queda dicho, y habitualmente por agregación.

Se incorporan más guardias y se les dotan de más funciones, o simplemente realizan al completo algunas que desde siempre deberían haber realizado: por ejemplo realizar rondas y no sólo estar de puesto. Este desarrollo un tanto irregular no guarda relación con el que ya se ha dado en otras empresas en las que empieza, o ya se ha alcanzado, un concepto mucho más global técnico y avanzado de la seguridad patrimonial.

ANÁLISIS DE RIESGOS

Para nadie es un secreto que las organizaciones prestadoras de los servicios de seguridad privada ejercen su actividad en muchas ocasiones sin desarrollar un análisis confiable del sinnúmero de siniestros o situaciones, por las cuales debe pasar o participar el hombre de seguridad y simplemente es enviado a ejercer su labor en cualquier sitio, sin capacitarlo de los posibles riesgos a los cuales se va a exponer y que pondrá en tela de juicio hasta la misma organización en el manejo de procesos y procedimientos seguros realizando una matriz de riesgos potenciales mediante su evolución y pasos a ser tenidos en cuenta, se parte del principio de quien realiza unos cursos de seguridad ya está en condiciones de ejercer la labor como hombre de seguridad.

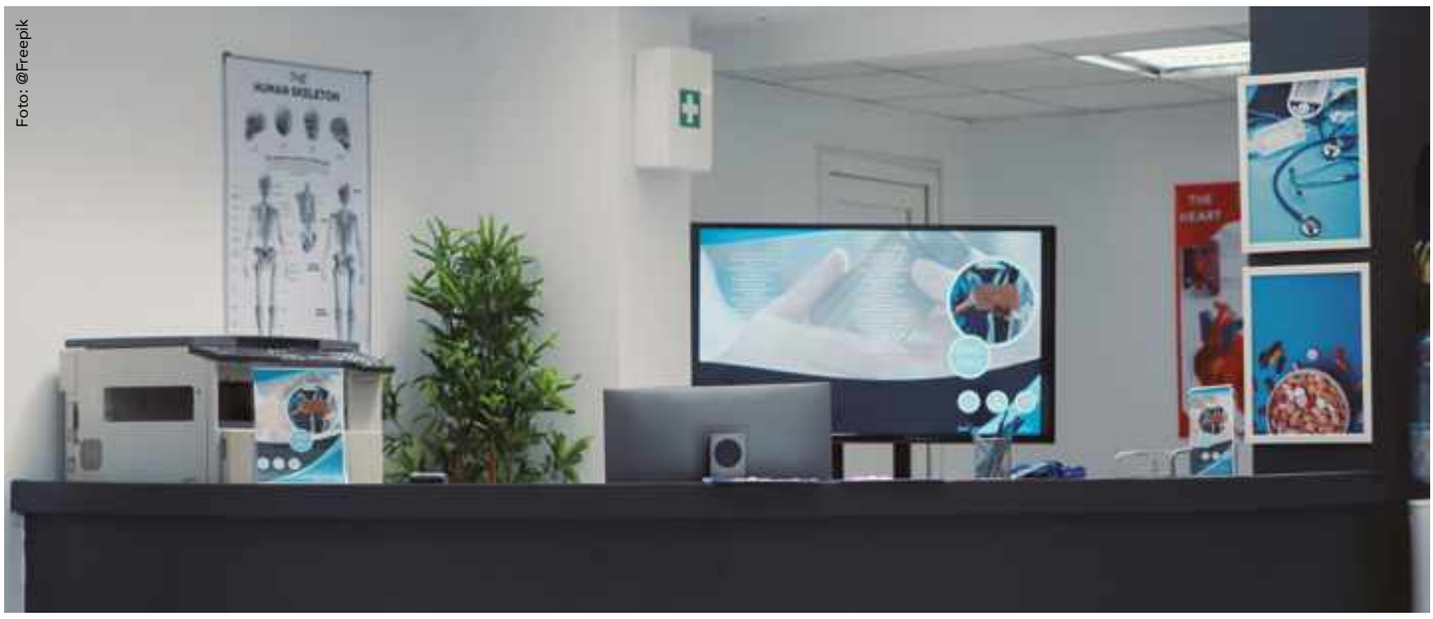


Foto: @Freepik

El cliente debe tener en cuenta que es importante mantener unos lazos de comunicación mutuos entre la empresa y el personal de seguridad mediante mecanismos debidamente establecidos generando una cultura de integración encaminada a prevalecer sistemas de seguridad enfocados a un mismo propósito


Foto: @Freepik

No se tiene en cuenta que cada sitio de trabajo es diferente y por lo tanto se debe contar con personal capacitado y entrenado en el desarrollo de consignas particulares acordes a la actividad del cliente. Es entonces cuando se presenta choques frontales en las actividades ejecutadas por el personal de vigilancia, pues dicho personal simplemente realiza una serie de funciones que desde su punto de vista son las requeridas para brindar seguridad.

Por lo tanto, dicha problemática se debe analizar desde una óptica que permita vislumbrar la realidad y establecer procedimientos de control encaminados a elegir hombres de seguridad con cualidades y habilidades que permitan cumplir con tareas especificas y más aún si su labor va a ser ejercida en un centro hospitalario en donde mantener niveles aceptables de seguridad es uno de los temas más complejos en los denominados espacios públicos, así no queramos aceptarlo la seguridad se ha convertido en un elemento primario para el buen funcionamiento de cualquier organización moderna.

De aquí se colige que quienes en ella labore entienda que su actividad no es un trabajo aislado; sino que forma parte del engranaje de toda la organización de lo contrario los objetivos empresariales no se cumplen; pues la seguridad no es más que un servicio. El cliente que recibe en su organización un servicio de vigilancia debe tener en cuenta que es importante mantener unos lazos de comunicación mutuos entre la empresa y el personal de seguridad mediante mecanismos debidamente establecidos generando una cultura de integración encaminada a prevalecer sistemas de seguridad enfocados a un mismo propósito.

Uno que permita un mutuo beneficio mediante la cooperación de los empleados con el guardia, logrando establecer eslabones en la cadena que comprende la seguridad, mitigando los riesgos a los que están expuestos dentro de una sociedad, en donde los índices de inseguridad se incrementan cada día, y los maleantes utilizan modus operandi avanzados, basados en la utilización de tecnologías avanzadas, estando siempre un paso adelante de los esquemas de seguridad aprovechando las vulnerabilidades que se dan en el ejercicio de la seguridad.

Por lo consiguiente, las organizaciones prestadoras de servicio de seguridad privada deben estar a la vanguardia y siempre en busca de nuevas alternativas que permitan minimizar el accionar de las organizaciones criminales al margen de la ley para salvaguardar los bienes muebles e inmuebles encargados y/o encomendados a la seguridad privada.

Por lo tanto, el hombre de seguridad debe ser consciente de la función que desarrolla en su diaria labor para evitar que situaciones que frente a los ojos del cliente resultan poco importante, son fundamentales para contrarrestar la acometida emprendida por el delincuente que busca las situaciones o escenarios más vulnerables para desplegar su accionar delincuencial, obteniendo sin duda su propio beneficio con el más mínimo síntoma de ser atrapado por la seguridad privada, se puede determinar que la seguridad juega un papel importante dentro del desarrollo de las actividades de toda organización. ■


Foto: @Freepik

Mario Fernando Cabrera García,
gerente nacional de Sucursales de Grupo Sistealarmas.

Más sobre el autor:

¿EN QUÉ MOMENTO CAMBIÓ LA SEGURIDAD?

La pandemia ha expuesto el alcance de las vulnerabilidades en las cadenas de suministro modernas y cómo múltiples eventos pueden unirse para crear interrupciones

Foto: Freepik

PERÚ

Herbert Calderón

La actividad o proceso denominado seguridad o protección patrimonial: antes se encontraba en las manos de unos pocos especialistas o directos responsables ha venido cambiado e incorporándose a la mentalidad, responsabilidad de las otras personas que laboran en una empresa y ¿de qué modo?

La situación inició cuando los pocos responsables de la seguridad patrimonial administraban un sistema de seguridad física, el cual estaba basado en accesos, cámaras y agentes. Sin embargo, este sistema no era el proporcional a los múltiples problemas que enfrentaba una empresa desde los desastres naturales hasta temas de fraudes incluyendo los accidentes. Pero, ¿por qué debería ser de competencia del responsable de seguridad patrimonial todos estos hechos?

La respuesta es muy sencilla, primero que la denominación del proceso es seguridad patrimonial, el cual se refiere al patrimonio. ¿Y qué es el patrimonio?

El patrimonio de una empresa está formado por sus bienes, derechos y sus obligaciones. Como patrimonio se denomina el conjunto de los bienes y derechos de una persona. La palabra, como tal, proviene del latín patrimon□um, que se refiere a aquello que se ha recibido por línea paterna.

En este sentido, el patrimonio es también la hacienda que alguien hereda de sus ascendientes. Por lo tanto, la definición del patrimonio ya involucra activos nuevos y que se desconocían, porque sólo eran de dominio del encargado de cada proceso dentro de la empresa.

¿EN QUÉ CONSISTE ESE PATRIMONIO?

De acuerdo con la definición antes expuesta, tenemos que es todo recurso, proceso que permite la operación de la empresa, puede ser como en una empresa de limpieza, el recurso más importante son las personas, herramientas, maquinarias, insumos, información, computadoras, documentos, instalaciones, oficinas, etc.

¿Cuál sería la mejor forma de entender el valor de cada uno de ellos? La mejor manera sería a través de la medición de cada proceso, por ejemplo, en la empresa de limpieza tenemos: clientes, compras, almacenes, programación, RRHH, mantenimiento.

Foto: Freepik

De acuerdo con el reporte 2022 de Allianz Risk Barometer 2022, los ataques cibernéticos son el mayor riesgo, la interrupción del negocio e interrupción de la cadena de suministro es el segundo riesgo y se generan como consecuencia de las catástrofes cibernéticas y naturales

Foto: Freepik

La definición del patrimonio ya involucra activos nuevos y que se desconocían, porque sólo eran de dominio del encargado de cada proceso dentro de la empresa

- En el proceso del cliente tenemos a las personas, equipos de comunicación, base de datos.
- En el de compras tenemos: personas, base de datos, equipos informáticos, comunicación.
- En el de almacenes tenemos: repuestos, maquinarias, insumos, uniformes, EPP.
- En el de RRHH tenemos: personas, base de datos, documentos confidenciales, equipos informáticos, comunicación.
- En el de mantenimiento tenemos: personas, base de datos, equipos informáticos, combustible, repuestos, lubricantes.

Entendemos por el valor o la severidad, cuando nos hacemos la siguiente pregunta: ¿cómo nos afecta el proceso con el daño al activo?

- En el proceso del cliente puede ser la base de datos, si está es dañada se para el proceso.
- En el de almacenes pueden ser los repuestos, sin ellos no hay proceso.
- En el de RRHH puede ser los documentos o base de datos, sin ellos se para el proceso.
- En el de mantenimiento puede ser el combustible, sin ello se para el proceso.
- Habiendo algunos activos comunes como: las personas, la base de datos, la red informática.

Esto va a permitir ser mas acucioso a partir de ahora con esta nueva responsabilidad patrimonial tanto en el tema del levantamiento de la información de activos, como en la responsabilidad a cada dueño de proceso y evitar la interrupción de la operación.

De acuerdo con el reporte 2022 de Allianz Risk Barometer 2022, los ataques cibernéticos son el mayor riesgo, la interrupción del negocio e interrupción de la cadena de suministro son el segundo riesgo y se generan como consecuencia de las catástrofes cibernéticas y naturales, es una preocupación perenne para las empresas de todo el mundo. Mientras tanto, la pandemia ha expuesto el alcance de las vulnerabilidades en las cadenas de suministro modernas y cómo múltiples eventos pueden unirse para crear interrupciones, el tercero es de catástrofes naturales.

Finalmente, esto nos permite concluir sobre la integración de los riesgos como el cyber, seguridad y salud de las personas e involucramiento de la organización en estos procesos. ■

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

Más sobre el autor:

Omar A. Ballesteros, director general y CEO de Ballesteros y Barrera Servicios de Protección.
ballesteros.barrera@hotmail.com

Más sobre el autor:

Foto: tonodiaz - Freepik

CONSCIENTE, INCONSCIENTE Y SUBCONSCIENTE

MÉXICO

En el mundo existen diversas expresiones corporales que pueden tener significados diferentes, por lo que es necesario tomarlas en cuenta para que cuando vayas a analizar la conducta y expresión corporal de una persona tengas un acierto del 97%, nadie tiene un acierto del 100%

¡Amigos! Hoy comienzo una nueva columna que gracias al apoyo de los amigos de la revista Seguridad en América, es una realidad.

Soy un apasionado del estudio del crimen y más específicamente en el tema de la conducta humana, me considero un conductista criminalista, en el estudio del lenguaje corporal o lenguaje no verbal o kinésica, es un tema que, en mi red de LinkedIn, publico en el apartado de mis artículos, además de videos de ejemplo y de ejercicio.

Esta columna más específicamente la llamo "EL SILENCIO HABLA", porque expresamos más con el cuerpo, que con palabras.

¿No te gustaría saber si tus hijos, tu esposa, familiares, amigos, socios, empleados, abogados, doctores, y cualquier persona con la que tengas contacto, están siendo honestos o te están mintiendo para una toma de decisiones rápida?

¿Puede que alguien te invite alguna vez a un negocio "jugoso" con grandes ganancias, y no quisieras saber si en "verdad" hay ganancias antes de meterle dinero? He tenido la fortuna de participar con este tema y su practica con varias empresas que han tenido temor de saber si un inversionista con un negocio "muy bueno" y que se "ve muy generoso", está siendo honesto, o empleados robando, aunque lo nieguen, y más.

Como bien saben me especializo más en criminología, porque es mi segunda carrera, maestría y especialidad y dentro de eso contexto me dedique a la conducta humana y actitud criminal; y entre las conferencias y talleres en este tema busco que creen interés y habilidades más que conocimiento, 100% práctico.

Por lo anterior en mi red de LinkedIn: https://www.linkedin.com/in/omar-ballesteros-criminologo/, puedes encontrar videos e información de este tema que en lo consecutivo saldrá también en esta columna.

Lo primero antes de entrar en este tema, es necesario tomar en cuenta que todos los libros que hablan del tema, artículos de revistas, y más literatura del tema, no son 100% concluyentes, es decir, no los tomes como biblias y que lo que dicen es así y sólo así, he podido comprobar que no es así debido a lo complejo que es el comportamiento y psicología del ser humano, desde la concepción en el seno familiar hasta la cultura de la zona, poblado, país y raza, etc. En el mundo existen diversas expresiones corporales que pueden tener significados diferentes, por lo que es necesario tomarlas en cuenta para que cuando vayas a analizar la conducta y expresión corporal de una persona tengas un acierto del 97%, nadie tiene un acierto del 100%, pero con mis artículos y videos de mi red que te invito a ver, puedes llegar al 97%, quien te diga lo contrario está mal.

La conducta humana es muy difícil de entender y más de predecir, pero una vez que ya conoces las bases, las sabes identificar, e intepretar, puedes aventurarte de dar una predicción de la siguiente reacción de una persona

Para comenzar es necesario ver al ser humano como un ente lleno de emociones que son expresadas a través de lo sentimientos, y son reflejados en las tres partes del cuerpo que debes ver siempre que son: cara, extremidades y tronco, dos ellas deben estar en sincronía para que una emoción sea genuina, no puedes basarte en sólo ver la cara a la persona o las manos para dar una conclusión de una emoción o aventurarte a dar un fallo de mentira o verdad.

ESTADOS PSÍQUICOS DEL HUMANO

De la misma manera, pasa que debemos tomar en cuenta los estados psíquicos del humano que desde los estudios de Freud son tres principalmente: consciente, inconsciente y subconsciente, y también tomar en cuenta tres elementos mentales que son: ello, yo y superyo.

- **Consciente:** estado del presente, reconocer el entorno, saber quién soy yo.
- **Inconcsiente:** reacción del cuerpo no deseada y controlada por el subconsciente.
- **Subconsciente:** estado de la mente que no es controlado, donde la reacciones son manejadas por la parte animal del ser humano de cuando nace y que a través de los sentidos reacciona a los estímulos del ambiente (ejemplo, ver el peligro de un animal que te va a morder y correr muy rápido, es una reacción inconsciente en la mayoría de los casos).

Los elementos:

- **Yo:** en coordinación con el consciente es reconocerme (soy yo Omar).
- **Ello:** reacción de placer principalmente del cuerpo, la mente no quiere estar presionada o estresada y buscara el placer siempre.
- **Superyo:** la moral del hombre controlada por el lóbulo frontal del cerebro, este se desarrolla cuando vamos creciendo.

¿Y LO ANTERIOR PARA QUE ME SIRVE?

Si sabes lo anterior y ves que una persona expresa un sentimiento de "dolor", que se supone en cierta forma es una respuesta inconsciente, porque las lágrimas no las controlamos lo que vemos, principalmente, y oímos tiene evocaciones a los recuerdos y hacen que lloremos, porque si quieres llorar de manera consciente no se puede, tienes que entrar a los recuerdos para encontrar un evento triste que te saque las lágrimas.

Si la persona analizar le ponemos videos de personas abrazándose, besándose, y drama, una persona con dolor deberá llorar fácilmente, si la persona menciona que tiene dolor por la muerte de su mamá y al mencionarle que tu mamá también murió y lloras y la persona no "te copia" significa que no tiene dolor, por lo que el sentimiento que menciona no es verdad. Por eso debemos saber qué es: el ello, yo y superyo, el consciente, subsconsciente e inconsciente.


Foto: ASDFpik - Freepik

Antes de sugerirte libros primero lee cualquier documento de Freud que encuentres en las bibliotecas y librerías, cuidado con videos de redes sociales: Fase, Kwai, TikTok, y más porque las personas que suben eso muchas veces ni saben de que hablan, lo mejor es que busques artículos o revistas de ciencia y personas serias como Freud y Allan Pearce y también de Paul Ekman, de quienes hablaré en las siguientes ediciones.

Por lo pronto hablando del tema de interés, es sumamente útil para el reclutamiento de personal, ya que te permite saber si el candidato puede ser honesto o no más que sus habilidades, dentro de mi organización busco personas en quién confiar, tener aliados, con los cuales hacer fuerte la operación del negocio más que sus habilidades, esas se pueden desarrollar, pero la confianza es más difícil de conseguir.

Para terminar, te comento finalmente: la conducta humana es muy difícil de entender y más de predecir, pero una vez que ya conoces las bases, las sabes identificar, e intepretar, puedes aventurarte de dar una predicción de la siguiente reacción de una persona, ya sea para probar un empleado, cliente, socio, proveedor, o el abogado que te esta diciendo que si se puede ganar un juicio cuando no se puede.

Un fuerte abrazo a todos y sígueme en mis redes. ■


Foto: gpointstudio - Freepik

ASOESPA
Asociación de Expertos en Seguridad Privada de Aguascalientes A.C.

Carmen Dena Escalera

presidenta de la Asociación de Expertos en Seguridad Privada de Aguascalientes (ASOESPA)

Seguridad en América (SEA): ¿Cómo surge ASOESPA y cuáles son sus objetivos?

Carmen Dena Escalera (CDE): ASOESPA nace el 21 de julio de 2021, como una necesidad de dignificar y profesionalizar el gremio de la seguridad privada, así como de mejorar las condiciones de nuestros colaboradores y la de sus familias. Fomentamos los valores de: honestidad e integridad, profesionalismo y calidad en el servicio, responsabilidad, confidencialidad, solidaridad, legalidad y justicia.

Dentro de nuestros principales objetivos están:

1) Impulsar el desarrollo competitivo, profesional y de calidad de las empresas de seguridad privada afiliadas, así como la de sus colaboradores.
2) Fomentar la partición gremial de las empresas de seguridad privada en el estado de Aguascalientes.
3) Buscar la mejora en la calidad de vida de los integrantes del gremio tanto de empresarios como de sus colaboradores mediante la profesionalización.
4) Interactuar con todas las cámaras empresariales del estado de Aguascalientes para promover los servicios de las empresas afiliadas.

SEA: ¿Quiénes integran la actual mesa directiva y qué se necesita para afiliarse?

Presidenta: Mtra. Carmen G. Dena Escalera
Tesorero: Lic. Rosa Marcela Arteaga De Luna
Secretario: Lic. Noé Rodarte Salgado

Comisiones:

de Inducción: Lic. Jorge Espinoza Torres
de Capacitación: Cmdte. Adrián Esparza López
de Difusión Interna: C. Alejandro Carrillo De Luna

Consejo de Honor y Justicia:

- Lic. Alicia Judith Villalobos Alvares
- Cmdte. Víctor Manuel Pérez
- C. Alejandro Ariza Núñez

Para afiliarse es necesario presentar todos los permisos que solicita el estado de Aguascalientes en perfecto orden, así como las opiniones de cumplimiento del SAT, IMSS, INFONAVIT y Finanzas del Estado, permiso estatal de la SSP y federal, en caso de contar con él, registro REPSE, último pago de la liquidación del IMSS e INFONAVIT, solicitud de ingreso y curricular de la empresa y pagar las cuotas de adhesión.

SEA: ¿Cuáles son los beneficios de pertenecer a la ASOESPA?

CDE: Sólo por mencionar algunos como:

- Ser representados ante las autoridades del estado para promover y defender sus intereses.
- Crecimiento profesional de los empresarios del gremio a través de la capacitación en temas relevantes y necesarios para la dirección de sus empresas.
- Capacitación para sus colaboradores.
- Orientación y atención en contabilidad, asesoría legal, laboral y fiscal.
- Sesiones de networking para promover sus empresas.
- Alianzas con las cámaras y asociaciones para beneficio de ellos y de sus colaboradores.
- Compras conjuntas y en volumen de uniformes y equipos de protección.
- Eventos recreativos para sus colaboradores que permitan la adhesión de los mismos hacia sus empresas.

SEA: ¿Cómo contribuye ASOESPA al sector de la seguridad?

CDE: Con campañas de concientización hacia el empresario para invertir en la profesionalización de sus colaboradores lo que permite una mejoría en su estilo de vida. Así como ampliando el horizonte de actuación de la seguridad privada en el estado de Aguascalientes, y promoviendo las buenas prácticas entre las empresas de seguridad privada. También promovemos la legalidad y transparencia entre los actores de la seguridad privada, y así combatir la competencia desleal.

SEA: ¿Cuáles son los planes para 2023?

CDE: Entre muchas acciones, están las de impartir un diplomado en seguridad privada para los colaboradores de los agremiados. Conformarnos como un órgano supervisor del cumplimiento de nuestros agremiados con la SSP del estado, participar a través de convenios con otras asociaciones de seguridad privada del resto del país, con la finalidad de intercambiar buenas prácticas, compartir experiencias y apoyar a sus asociados que tengan sucursales en el estado de Aguascalientes. Además de adherirnos como miembros del CCE de Aguascalientes y de Coparmex (para participar activamente en las comisiones de seguridad). Tenemos convenios con otros estados, con AMESP desde hace un año y planeamos integrarnos a otras asociaciones como ASUME y ASIS.

¿QUIÉN ES CARMEN?

Carmen Dena Escalera es licenciada en Contaduría Pública egresada de la Facultad de Contaduría de la Universidad Nacional Autónoma de México (UNAM), cuenta con las maestrías de Impuestos, y Gestión de la Competitividad, con una especialidad en Finanzas, y en Liderazgo. Así como los Diplomados en Desarrollo de Habilidades Gerenciales, e Innovación Exponencial y Moderación 4.0.

Desde 1990 participó en la conformación de su empresa de seguridad privada, SIPSA, donde ha desarrollado todos los puestos, tanto operativos como administrativos. He impartido cursos de análisis y evaluación de riesgo, seguridad electrónica, seguridad para eventos, entre otros. ■

APLICACIÓN DEL BAJO PERFIL EN LA PROTECCIÓN DE PERSONAS (D.R.A.)

COLOMBIA | Javier Nery Rojas Benjumea

El bajo perfil puede hacer que el personaje literalmente "desaparezca" de la vista del público y de los delincuentes, imposibilitando el desarrollo de las primeras fases del secuestro


Foto: @Freepik

Los métodos de protección "dura" están encaminados a reaccionar efectivamente ante un ataque y no siempre tienen éxito, debido a que hay infinidad de detalles que pueden presentarse, y que no están bajo el control del equipo de protección

El bajo perfil es el conjunto de acciones que desarrolla un personaje y su sistema de protección, para pasar lo más desapercibidos posible, ante la mirada investigadora de delincuentes organizados y curiosos en general, con el fin de negar toda la información posible a todo aquel que no tenga poderosas razones para poseerla.

El bajo perfil es una de las más efectivas medidas de seguridad pasiva, por cuanto se basa en el principio lógico de que quien no existe, no tiene riesgos, y el bajo perfil es, literalmente, una tendencia a "desaparecer" de la vista, las preguntas y las investigaciones de los intrusos; sin embargo, como cualquier medida de seguridad, tiene un efecto positivo sólo como parte de un sistema complejo de seguridad.

La Protección de Bajo Perfil es aquella en la cual las medidas protectoras no llaman la atención del común de las personas, si bien, puede ser detectada por un experto. La cobertura es completamente discreta y la falta del "muro" protector, típico de un sistema de protección de alto perfil, se compensa con un sistema de manejo de información alimentado por contravigilancia efectiva y de medidas de engaño, de manera que el riesgo y el costo de custodiar a una posible víctima, se salgan de las manos, del presupuesto y de la paciencia de los delincuentes.

Los métodos de protección "dura" están encaminados a reaccionar efectivamente ante un ataque y no siempre tienen éxito, debido a que hay infinidad de detalles que pueden presentarse, y que no están bajo el control del equipo de protección. Desde luego, es más complicado secuestrar que asesinar, pero en todos los casos exitosos, todo el problema para los delincuentes, consiste en neutralizar la protección humana de la víctima, por medio de obstáculos, de engaños, de ataques etc.; logrado eso, la víctima está en manos de sus captores o asesinos.

El alto costo de los equipos de protección técnica y humana para personas, que muchas veces no tienen análisis detallados de los riesgos, hacen que el bajo perfil, como medida central del sistema protectivo, cobre más relevancia y efectividad. En este caso, la seguridad del personaje está fundamentada en su capacidad de ocultarse de la mirada de cualquier intruso, lo cual le facilitará, a la vez, descubrir oportunamente sus amenazas, ya que la intrusión será obvia en un ambiente de bajo perfil.


Foto: @Freepik

RECOMENDACIONES

Para realizar un sistema de seguridad fundamentado en el bajo perfil, se sugiere seguir los siguientes pasos:

- Hacer una lista de las formas, personas, lugares, documentos, donde un delincuente o terrorista podría levantar información sobre la víctima.
- Diseñar las medidas para ocultar, cambiar, desviar o suprimir la información disponible para el intruso, tales como códigos de comunicación, desinformación, secreto, cambios de identidad en documentos, delegación de autoridad en la empresa y cualquiera otra que las condiciones y el contexto permitan.
- Desarrollar las siguientes acciones:
  - Recolectar, mediante personas propias, una información completa de las áreas que el protegido frecuenta.
  - No permitir o propiciar que le personaje se mueva con un grupo de escoltas rodeándolo y "llevando un maletín".
  - Los hombres de seguridad deben llevar ropa que pase desapercibida y encontrarse a una distancia del personaje que no llame la atención, pero que permita cubrir el área de seguridad.
  - Los miembros de seguridad que van cerca del personaje deben vestir en forma similar y tener apariencia de su misma condición y categoría para desviar la atención.
  - Cuando el riesgo de atentado está presente, las medidas de seguridad deben mantener alejados a los delincuentes.
  - El análisis de riesgo personal, detallado, permitirá conocer las posibilidades de un ataque con fines de secuestro y determinará las vulnerabilidades que deben ser cerradas para bajar las posibilidades. Recuerde que la capacidad de reaccionar deben mantenerse por bajo que sea el perfil del personaje.
  - Con el fin de mantener el perfil bajo, la protección puede instalarse fija en los puntos críticos, en lugar de que se mueva con el personaje.
  - Las motos deben permanecer a distancias prudenciales que impidan ser identificados como parte de la seguridad de un personaje.

Las medidas de engaño son el complemento básico del bajo perfil. En este sentido puede tomar las siguientes medidas:

- Cambiar de lugar al personaje en el vehículo y si está entrenado, permitirle que conduzca él mismo.
- Se pueden hacer movimientos sin el personaje a sitios que frecuenta y a sitios que no frecuenta, con el fin de saturar la capacidad de vigilancia de los delincuentes.
- Cuando hay varios vehículos disponibles, se pueden hacer entrar y salir innecesariamente de las instalaciones para saturar de información a los observadores e impedir que puedan determinar cuándo sí sale y cuándo no.
- Es necesario establecer, probar y usar permanentemente los códigos de seguridad y señales para indicar peligro o normalidad y cambiarlos por lo menos cada seis meses.

El alto costo de los equipos de protección técnica y humana para personas, que muchas veces no tienen análisis detallados de los riesgos, hacen que el bajo perfil, como medida central del sistema protectivo, cobre más relevancia y efectividad

Hay muchas otras acciones que pueden ser inventadas por la creatividad de un jefe de seguridad inteligente y diligente. También hay que mantener bajo perfil, desinformación y engaño, en otras actividades y actividades: cuentas, reuniones públicas, relaciones con otros personajes, etc.

El bajo perfil puede hacer que el personaje literalmente "desaparezca" de la vista del público y de los delincuentes, imposibilitando el desarrollo de las primeras fases del secuestro: la selección del blanco dentro de un universo de probabilidades y el planeamiento de la acción delincuencial.

La enorme dificultad para detectar y vigilar a una posible víctima, cuyo equipo de seguridad maneja profesionalmente el bajo perfil como fundamento del sistema de protección, la pondrá fuera del alcance de sus intenciones. ■

Si desea contactar al autor:
Página web: www.riesgos-gestion.com
Correo: javier@riesgos-gestion.com

Foto: @Freepik

Adrián Prieto Olivares, CPP, consultor en seguridad.

Más sobre el autor:

"El ansia de seguridad ha sido el motor del progreso de la humanidad. Fue el propulsor de la agricultura y asegurar alimento. Fue propulsor de la formación de tribus, aldeas, ciudades para protegerse ante los enemigos exteriores", Mallet

EL GERENTE DE SEGURIDAD COMO SER PROMOTOR DEL DESARROLLO

MÉXICO | Mónica Rodríguez

Foto: @Freepik

Un gerente de EHS&SS podría tener a su cargo un promotor del desarrollo humano quien se especializa y tiene como meta permear y transformar toda la actividad humana hacia la conciencia, convivencia, congruencia, responsabilidad, actualización y auto-realización de cada ser humano

Me ha tocado acompañar a los gerentes de Seguridad en la búsqueda respuestas, en el intento de encontrar soluciones y elegir decisiones adecuadas ante situaciones paradójicas donde se consideran inseguras y poco apropiadas para el ambiente laboral.

Situaciones como cuando algún empleado operativo pone en riesgo su vida brincando reglas de procedimientos (aunque su intención sea resolver un problema), cuando un empleado de confianza de la empresa se lleva material por saber que será desechado (pensando que tiene el derecho a no pedir autorización de sacarlo); cuando se accidentan los empleados, mutilándose una parte de su cuerpo, por no seguir los procedimientos adecuados de protección, etc.

La frustración y desilusión en la humanidad surge en los responsables de dicha gerencia. No encuentran la responsabilidad en lo que la empresa los responsabiliza.

Como resultado veo, con asombro, que la línea aprendida de toma de decisiones para resolver estas situaciones está marcada hacia el rechazo, el castigo, el regaño y el despido junto con la tendencia a querer sustituir la labor humana por tecnología para evitar los errores, malos entendidos y este tipo de accidentes como si ahí estuviera la respuesta hacia la seguridad.

Sin embargo, veo que se ignora por completo al proceso de crecimiento y desarrollo de la responsabilidad del individuo convirtiéndolo en víctima de la misma situación que generó en el trabajo.

ELEMENTO ESTRATÉGICO

El gerente o el director de Seguridad de una empresa es un elemento estratégico en toda misión de prevención y seguridad de cualquier organización, y debe ir acumulando una serie de cualidades para que su labor profesional se desarrolle de forma congruente y satisfactoria.

Una de las cualidades primordiales del responsable de la seguridad es tener el correcto concepto y definición de lo que es seguridad, entender de donde viene el sentido y cómo se ha desarrollado la seguridad humana, así como, generar y proteger la meta genuina del valor de la seguridad.

La seguridad se ha definido de diferentes formas. Entre ellas esta la de la definición de "Ausencia de peligros y de condiciones que puedan provocar daño físico, psicológico o material en los individuos y en la sociedad en general". Pero, ¿qué tal si la definimos a la seguridad como la necesidad básica de estado de bienestar que nos impulsa a generar conexión, comunidad, desarrollo y crecimiento? ¿Cambiarían nuestros objetivos en Seguridad?

GRUPO PAPRISA

SEGURIDAD • PROTECCIÓN • CONFIANZA

ALARSEGM UNA DECISIÓN SEGURA

B&A Transporte • Seguridad • Puntualidad

UNIFORMAL UNIFORMES A&E

ασφάλεια asfáleia

CUSTODIOS

OEMPSA

Jivabe

Una Decisión Segura

ASIS INTERNATIONAL CAPÍTULO MÉXICO 217

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

ANERPV®
Asociación Nacional de Empresas de Rastreo y Protección Vehicular

JUAN RACINE 112-PISO 3, POLANCO, POLANCO I SECC, MIGUEL HIDALGO, 11510 CIUDAD DE MÉXICO, CDMX

55 8438 2340

GRUPOPAPRISA.COM

REDES SOCIALES

Foto: @Freepik

Desde los tiempos remotos el hombre se ha enfrentado al mundo que no entiende y que le agrede constantemente. Vivir en la Tierra inhóspita y acoso de los fenómenos naturales lo ha hecho sentir inseguro por lo que ha tenido que aprender a satisfacer por instinto sus necesidades elementales:

a) Aprendió a elaborar plan de contingencias:

- Guardar alimentos para la escasez.
- Domesticar animales, convirtiéndose en cazador y pastor.
- Generó refugios y viviendas para su protección.

b) Consideró y manejó los riesgos de contingencia sociales:

- Superar la enfermedad y prevenirla.
- Manejar la vejez, la invalidez y subsistir por sus propios medios.
- Aceptar y lidiar con la muerte misma.

Por razones naturales, llega a formar el núcleo básico social que es la familia, desarrolló su sentimiento de solidaridad, y evolucionó a formas más complejas de organización social, hasta llegar, con el transcurso de los siglos, al concepto de Estado y comunidad internacional.

"El ansia de seguridad ha sido el motor del progreso de la humanidad. Fue el propulsor de la agricultura y asegurar alimento. Fue propulsor de la formación de tribus, aldeas, ciudades para protegerse ante los enemigos exteriores", Mallet.

A lo largo de la historia de la humanidad podemos constatar que la seguridad ha sido un tema a resolver desde diferentes perspectivas y expectativas particulares de cada cultura. Mencionemos a los mayas, egipcios, Babilonia, Grecia y Roma con sus ideas de ayuda mutua, instituciones de defensa, servicio de salud pública, capacitación y ayuda a los vulnerables: pobres, viejos, enfermos, desempleados y huérfanos cuando no contaban con ayuda familiar; generando una especie de responsabilidad de la comunidad a través de la solidaridad, compasión y empatía.

El pilar de la seguridad se refiere a la seguridad física de las personas y bienes e incluye la reputación e imagen de todas las partes involucradas, activos tangibles e intangibles

Son estas culturas antiguas las que dejaron evidencia de que es a través de la solidaridad, la conexión y la comunidad que se genera desarrollo y evolución en la raza humana.

La necesidad de defender y proteger de los peligros, enfocarse a estudiar, evaluar y manejar los riesgos a los que se encuentra sometida una persona o grupo es inminente e insustituible. Sin embargo, creo que lo que se ha olvidado en la estrategia de seguridad es el generar la interacción necesaria de los integrantes de la comunidad, crear una red de protección entre ellos y desarrollar las virtudes individuales de aprendizaje, responsabilidad y confianza para crear ambientes saludables que generen conexión, compromiso y que ayude a aumentar la seguridad.

David Isaacs Jones, estudioso de las virtudes y fortalezas del ser humano, menciona que tanto la ausencia de un valor como la práctica extrema y desbalanceada del mismo puede llevar a tener una consecuencia negativa en el ser humano y en la comunidad. Es así como la ausencia de la creatividad nos lleva a la conformidad y su exceso nos lleva a la excentricidad, la ausencia de bondad nos lleva a la indiferencia y su exceso a la intrusión, y la ausencia de protección nos lleva a la inseguridad y la seguridad extrema nos ha llevado a las guerras.

Nuevamente habrá que buscar formas nuevas para evitar caer en desequilibrio en la seguridad. Hay que tomar consciencia que el mismo desarrollo tecnológico la modernidad y el ritmo acelerado que se vive actualmente nos ha ido llevando al fatalismo, individualismo, la distracción y perder el enfoque del origen y la dirección de la seguridad, con desequilibrio.

Desde su nacimiento el individuo va desarrollando la imagen de sí mismo y debido a su necesidad de pertenecer, ser aceptado y amado por su núcleo social va desarrollando conductas adaptativas o destructivas emanadas de las expectativas y demandas de los demás, como también de la satisfacción o de la frustración de sus propias necesidades.

El individuo, con su capacidad de interactuar, comunicar, aprender y de adaptarse va modificando su comportamiento con su entorno y su entorno con su comportamiento. Es un proceso natural que toma su tiempo.

En este mundo moderno, modificado por el ser humano, el estilo de vida se ha vuelto acelerado rompiendo el ritmo del proceso de crecimiento del ser humano. El desarrollo tecnológico crece a pasos agigantados y el manejo de los medios de comunicación y redes sociales generan obstáculos para tener espacios de desarrollo personal, reflexión, auto-conocimiento y vínculo.

Todo esto genera carencias en los procesos de maduración y de auto-realización de las personas. Personas que desde sus carencias generan, inconscientemente, ambientes carentes de visión, valores y seguridad. Y es así como llegan las personas a pedir empleo y trabajar en las empresas.

Esto no significa que ya esta determinado el ambiente carente y el ser humano estancado, los factores de riesgo no determinan a la persona sin proceso de crecimiento. Simplemente existe el reto de aceptación y redirigir de re-direccionar para generar un equilibrio.

ASIS INTERNATIONAL
CAPÍTULO MÉXICO 217

AFILIACIÓN

¡ÚNETE A LA RED DE PROFESIONALES DE SEGURIDAD MÁS GRANDE DEL MUNDO!

ASIS
CAPÍTULO MÉXICO

$5,650.00 MXN

ASIS
INTERNACIONAL

$120.00 USD

Beneficios

- Reuniones mensuales.
- Webinars
- Cuatro cursos **(1 cada trimestre).**
- Taller de asesoría en la elaboración del "Plan de Emergencia Familiar".
- Bolsa de trabajo.
- Networking.
- Comunidades Temáticas.
- Newsletter semanal.
- Chat privado de socios.
- Convenios de descuento para diversos productos y servicios.
- Acceso a las Guías & estándares de ASIS Internacional.
- Acceso a la base de datos de más de 34 mil profesionales.

MAYOR INFORMACIÓN

(55 3437 6890

info@asis.org.mx

Se va formando objetivos que ayudan a lograr su meta general, entre los cuales es ayudar a la comunidad a desarrollar habilidades sociales que generen desarrollo en la comunidad

¿QUIÉN SERÍA RESPONSABLE DE ESTO?

La gestión de EHS&S (*Environment, Health and Safety & Sustainibility*) tiene cuatro pilares: medioambiente, salud, seguridad y sustentabilidad. El pilar ambiental (*E enviroment*) de la gestión de EHS incluye procesos para reducir las afecciones a la naturaleza y el planeta cuidando al medio ambiente. El pilar de salud (*H health*) abarca sistemas para proteger a los trabajadores, los clientes y las comunidades circundantes frente a la exposición de riesgos contra su salud: patógenos, radiación o químicos peligrosos.

El pilar de seguridad laboral (*S safety*) implica procedimientos para mantener a los trabajadores a salvo de lesiones físicas causadas por la maquinaria o la exposición a sustancias peligrosas en el trabajo. El pilar de la seguridad (segunda *S security*) se refiere a la seguridad física de las personas y bienes e incluye la reputación e imagen de todas las partes involucradas, activos tangibles e intangibles.

Mi propuesta sería adicionar una S (EHS&SS) representando la tercera "S" la sustentabilidad la cual es un indicador del cambio en la gestión de EHS, de un enfoque reactivo a una perspectiva proactiva y a largo plazo.

Es aquí donde podria entrar la visión del trabajo en el ser humano para redirigir y redireccionar para generar personas responsables con la comunidad y la seguridad de la misma.

Este doble trabajo tanto interno como externo, la naturaleza nos lo ejemplifica de muchas maneras: podríamos mencionar el movimiento de rotación y de traslación de la tierra.

El ser humano tiene que girar en su propio eje al mismo tiempo que se mueve alrededor de su núcleo social en pro de seguir su trayectoria. No hay que perder la trayectoria sin perder el trabajo interno de cada persona (fuerza de gravedad).

Es a través de la búsqueda de la satisfacción de nuestras necesidades de seguridad que hemos crecido, generado comunidad; evolucionado, desarrollado y logrado ambientes cada vez más seguros y saludables.

¿Es el responsable de la Seguridad generar ambientes seguros? ¿Qué tipo de ambiente necesitamos generar como responsables de seguridad para evitar tal fenómeno?

Un gerente de EHS&SS podría tener a su cargo un promotor del desarrollo humano quien se especializa y tiene como meta permear y transformar toda la actividad humana hacia la conciencia, convivencia, congruencia, responsabilidad, actualización y autorealización de cada ser humano.

Se va formando objetivos que ayudan a lograr su meta general, entre los cuales es ayudar a la comunidad a desarrollar habilidades sociales que generen desarrollo en la comunidad:

1. Generar confianza en el grupo y observar el proceso grupal y sus interacciones con las personas.
2. Tomar consciencia de actitudes que podrían resultar autodestructivas en la relación para después generar un vínculo productivo.
3. Ofrecer experiencias profundas y significativas.
4. Orientarse hacia el desarrollo personal, al aumento y mejoramiento de la comunicación y relaciones interpersonales y promover de opciones responsables hacia la salud y el crecimiento.
5. Estar en un proceso de desarrollo constante de habilidades sociales como la empatía, actitud positiva incondicional, escucha, congruencia, comunicación expresiva y asertiva, inteligencia emocional y manejo de conflictos.
6. Utilización de valores como la apertura a la experiencia y al conocimiento desde una perspectiva plural, el amor, el afecto no condicionado, la honradez y transparencia en la comunicación, y un máximo respeto a la dignidad de cada persona y a sus libres decisiones.
7. Ver la comunidad como parte de un todo y no fragmentada.
8. Crear las condiciones necesarias para que en el encuentro todos aprendan.
9. Comprender vs. estar de acuerdo.
10. Intervenir guiando hacia los objetivos del grupo, entre muchos más.

Sólo queda imaginar como sería trabajar en una empresa donde no sólo hay movimiento de traslación y sinergia sino que también pone atención en el movimiento de rotación y la fuerza de gravedad del individuo. ■

"Existen acciones que desarrollan congruencia: Pensar lo que deseamos, decir lo que pensamos, hacer lo que decimos y desear lo que esta en nuestro potencial"

Mónica Rodríguez, *Coach* de Seguridad en Universidad de las Américas Puebla (UDLAP) y Tec de Monterrey, facilitadora del desarrollo del potencial humano a través de la congruencia.

Más sobre el autor:

amesis MR

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

FORTALECIENDO LA INDUSTRIA DE SEGURIDAD Y TECNOLOGÍA SATELITAL EN MÉXICO

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

NUESTROS SOCIOS

Tracking Systems · si4tel Seguridad Satelital · Holkan · skyguardian · ADS LOGIC Telematics · INFO TRAX · TECNO LOGISTIK · GLOBAL MIT · RAINDE · skymeduza · GEOTRACKING · SEGURIDAD 360 .com · SECURE WITNESS · ATLANTIDA · Centro GPS · DUMAY · ISIS · MAGNI Tracking · GRUPO ALCA · TTC · gps · SOLUCIONES · GEOTRUCKS · GRUPO ALFIL

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

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

COMUNÍCATE
55 3334 4707

ACONTECIMIENTOS DE LA INDUSTRIA
DE LA SEGURIDAD PRIVADA

Fecha: 12 de octubre de 2022.

Lugar: Ciudad de México.

Asistentes: más de 150 cibernautas.

Seguridad en América
realiza *Roadshow* enfocado en el Blindaje Automotriz

Seguridad en América (SEA) llevó a cabo el *Roadshow* virtual enfocado en el tema de Blindaje Automotriz, el cual fue coordinado por Samuel Ortiz Coleman, director general de dicha casa editorial, y Alex Parker, gerente de Ventas, también de SEA.

En esta ocasión, la conferencia magistral fue impartida por René Fausto Rivera Arózqueta, director general de Distribuciones e Importaciones del Pedregal, quien también es Enlace con autoridades y asociaciones, y presidente de la Comisión de Blindaje Arquitectónico del Consejo Nacional de la Industria Balística (CNB). El experto hizo un recorrido por la historia y evolución del secuestro en México para analizar y comprender la importancia del blindaje automotriz en materia de prevención y seguridad.

"La industria del blindaje inicia en México en la década de los años 70 del siglo pasado, cuando a finales de los años 60, se empiezan a formar diversos grupos guerrilleros como La liga Comunista 23 de septiembre, quienes para obtener recursos económicos a fin de financiar sus actividades, empiezan a secuestrar personas y pedir rescate por ellas", comentó.

CONFERENCIAS COMERCIALES

La segunda conferencia la brindó Juan Carlos Casas Rincón, gerente de Ingeniería e Industrialización en AGP, quien habló sobre la experiencia y trayectoria que tiene AGP diseñando y fabricando vidrios especializados para los mercados automotriz, marítimo y de seguridad. Juan Carlos explicó que un vidrio blindado es una composición multilaminada formada por capas de vidrio y polímeros que combinados tienen propiedades de resistencia balística. AGP es reconocida a nivel mundial por la innovación tecnológica en este sector y por comprobar la eficacia de sus productos, un vidrio blindado salva vidas.

La última conferencia del *Roadshow* estuvo a cargo de Pablo Ortiz-Monasterio, CEO de AS3 Driver Training, con el tema "El conductor como eje de la seguridad", siendo el conductor de seguridad quien requiere la mejor capacitación y entrenamiento para la prevención de incidentes, secuestros, asaltos, y sobre todo la mejor reacción posible, contemplando el tipo de vehículo que maneja, si es blindado, etc.

En AS3 Driver Training utilizan ciencia y tecnología para el desarrollo de cursos evasivos de manejo con estrategias comprobables, con expertos en la materia, en instalaciones que implican retos reales.

COLEMAN

Jetlife

EL PODER DE VOLAR

RENTA DE AVIONES PRIVADOS Y HELICÓPTEROS

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

Powered by:
SEGURIDAD EN AMÉRICA

IS-BAO

REGISTERED OPERATOR
verify with wyvern

AEROPUERTO INTERNACIONAL DE TOLUCA

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

Tel. 55.7672.4992

Fecha: 18 y 19 de octubre de 2022.

Lugar: Jardín de Eventos Santa Fe, Ciudad de México.

Asistentes: más de 200 invitados.

EP SUMMIT
2022

La cuarta edición del EP SUMMIT 2022 (Executive Protection Summit) dio inicio durante la Reunión Mensual de ASIS Capítulo México el 18 de octubre. Los tres ya conocidos organizadores de dicho evento, Gonzalo Senosiain (GRIP), Pablo Ortiz-Monasterio (AS3 Driver Training), e Ivan Ivanovich (Executive Protection Institute), arrancaron el EP con la conferencia de Michael Julian, CPI, PPS, CSP, titulada "El perfil del tirador activo. Causas y detonantes históricos".

Este año fueron 13 los conferencistas magistrales que participaron con temas como los mitos y el cine en la protección ejecutiva, protección de personas en zonas de alto riesgo, el lado humano de la protección de personas, entre otros. Durante el desayuno inaugural, estuvo presente Midori Llanes Gaytán, presidenta del Capítulo ASIS México, y los patrocinadores del evento.

Ivan Ivanovich (Executive Protection Institute), Gonzalo Senosiain (GRIP), y Pablo Ortiz-Monasterio (AS3 Driver Training)

Fecha:
del 23 al 25 de octubre de 2022.

Lugar:
Cancún, Quintana Roo (México).

Asistentes:
más de 500 visitantes de todo el mundo.

ASIS Internacional
realiza el Primer Congreso Latinoamericano

Con el lema "Seguridad más allá de cualquier frontera", ASIS Internacional llevó a cabo el Primer Congreso Latinoamericano en el que participaron más de 20 conferencistas de talla internacional, logrando el éxito esperado, reuniendo a expertos en la materia de 25 países de América.

Los encargados de la organización del Congreso fueron los Capítulos de México, Centroamérica, Sudamérica y el Caribe; algunos de los ponentes que participaron fueron: Christian Bernard, CEO de BS Consulting y presidente de ASIS Perú; Carlos Eduardo Veiga, RSOM Latin America de Twitter; Mercedes Escudero Carmona, CPTED LATAM, y vicepresidenta de ASIS Capítulo Yucatán; Jeffrey Slotnick, CEO de Setracon, entre otros.

"El Congreso Latinoamericano es una iniciativa de las Regiones 7 y 8 de ASIS, donde se compitió con todos los Capítulos de Latinoamérica, Centroamérica, Sudamérica y el Caribe para decidir quién sería la sede, fue un concurso a nivel internacional de todos los que formamos ASIS y se escogió a México, una vez que se ganó, todos los Capítulos de la Región competimos a su vez, presentamos una propuesta para llevar a cabo ahí el Congreso", comentó en entrevista para SEA Carlos Contreras, socio-fundador y Comisario de ASIS Capítulo 311 Península de Yucatán.

"Tuve el gran honor de ser conferencista en el Congreso ASIS LATAM 2022, en donde compartí escenario con otros grandes colegas hablando sobre temas de interés para esta industria, el cómo ayudarnos a mirar qué es lo que viene y sobre todo a saber cómo estamos gestionando nuestros riesgos de seguridad; lograr esa visión 360 y la unión entre todas y cada una de las áreas de seguridad que buscamos el mismo objetivo. Haber formado parte del Congreso, fue una experiencia totalmente enriquecedora", Gigi Agassini, CPP

El Capítulo 311 ganó por votación unánime, siendo Cancún la sede final. El Congreso de ASIS es un evento que se ha venido realizando en Estados Unidos y Europa, y gracias al trabajo y esfuerzo de sus representantes en Latinoamérica, por primera vez se logró llevarlo a cabo en esta región.

"Latinoamérica ya está en el mismo nivel que cualquier otro país en temas de organización como asociación y se lograron reunir a ponentes de alta referencia, con un gran curriculum que hablaran sobre temas regionales, para ello el Comité Académico escogió cuatro ejes temáticos: el primero, situación geopolítica y seguridad en Latinoamérica; dos, factor humano; tres, seguridad estratégica, y cuatro, ciberseguridad y transformación digital. Esto nos permitió tener un enfoque holístico de cómo se está abordando la seguridad en toda Latinoamérica", comentó Carlos.

El Congreso recibió más de 500 visitantes, con la presencia de los más altos representantes de todo el mundo de ASIS International, así como los presidentes regionales de la Zona 7 y 8. Se tiene pensado que a partir de este primer evento, cada año se realicen, siendo Perú la sede del año 2023.

"ASIS a diferencia de otras asociaciones, afiliamos personas, no empresas, y lo que busca es tener un estándar global, es decir, contar con las mismas capacidades y capacitaciones que requiere la industria de la seguridad, además de profesionalizar al sector y dignificarlo, con estándares de competencia a nivel mundial, brindamos networking y contamos con diferentes certificaciones", puntualizó.

ORGULLOSOS CONFERENCISTAS

ASIS Internacional es un organización integrada por profesionales de seguridad y que actualmente cuenta con más de 38 mil miembros de todo el mundo, tiene presencia en los cinco continentes y cuenta con más de 250 capítulos. Fue fundada en 1955, con el objetivo de brindar las herramientas necesarias para la profesionalización de sus agremiados y de la propia industria de la seguridad, a través de programas de desarrollo educacional, materiales y recursos enfocados a seguridad.

"Haber podido participar como conferencista en el primer Congreso de ASIS LATAM, fue una gran oportunidad, no solamente por el honor de compartir el escenario con excelentes profesionales, sino el también haber podido aprender de ellos, compartir los conocimientos y los puntos de vista que cada uno tenemos sobre los desafíos a los que nos estaremos enfrentando en los próximos años, así como las oportunidades que tenemos en el rubro de la Seguridad, ya que es muy importante tener en cuenta cuáles son los riesgos a los que nos enfrentamos y poder darle continuidad al negocio, darle la posibilidad a cada uno de los líderes de enfrentar de forma exitosa estos riesgos", Alvar Orellana McBride, CPP, ASIS RVP Region 8C

"Tuve la suerte de participar en el primer Congreso LATAM de ASIS dentro de un panel con colegas de América Latina en el que comentamos sobre los retos y las oportunidades que existen en nuestra región. Escogimos un marco metodológico situado en diferentes cuadrantes, reconociendo el mundo tan complejo en el que vivimos hoy en día. Por ejemplo uno de ellos considera las amenazas tradicionales, que son las que ya conocíamos del siglo XX, grupos armados, delincuencia organizada, desastres naturales; otro de ellos, considera las amenazas catastróficas, como crisis financiera, crisis energética, declive masivo del turismo, de importaciones; otro habla de amenazas desconocidas como las nuevas enfermedades, el camblio climático; y otras amenazas que desconocemos como el impacto que tendrá la delincuencia organizada a nivel internacional, o los ataques cibernéticos. Fue una experiencia muy enriquecedora", Mario Arroyo Juárez, director del Instituto Iberoamericano de Liderazgo en Seguridad SC

"En tiempos de crisis la gente giró hacia nosotros y los protocolos que tuvimos que desarrollar. La hermandad que formamos previamente nos permitió actuar con rapidez, y dejó en evidencia de que debemos de tener un trabajo constante en fortalecer nuestros lazos en todo el continente", comentó Peter J. O'Neil, CEO de ASIS Internacional.

Para Latinoamérica es un evento de gran relevancia en donde además del aprendizaje, el *networking* e intercambio de buenas prácticas y tecnología en seguridad, es un reconocimiento a nivel internacional, de todo el trabajo y desarrollo realizado en este lado del hemisferio. A continuación compartimos algunos comentarios de los conferencistas que participaron en el Congreso.

"Estoy muy honrada de haber sido conferencista en el primer Congreso Latinoamericano de ASIS LATAM 2022, en donde pude compartir con muchos colegas y expertos profesionales en el sector dea seguridad, sobre la visión y el expertice con el que trabajo, desde una perspectiva humana de reconciliación social para ciudades seguras y smarts citys , estructuras físicas seguras porque la seguridad para poderla tener, se debe diseñar, y esa es la base de la seguridad por diseño, CPTED, es una metodología que funciona para tener soluciones integrales y holísticas, y la visión de mis colegas en el Congreso, complementó todo lo que es un diseño de seguridad y gestión, cómo analizamos nuestros riesgos, cómo los tratamos y qué soluciones proponemos", Mercedes Escudero, especialista en análisis y gestión de riesgos sociourbanos con la metodología CPTED

Fecha: del 24 al 26 de octubre de 2022.

Lugar: Hotel Hyatt Regency, Minneapolis (Estados Unidos).

Asistentes: más de 200 invitados.

Milestone Partner Summit 2022:
Tecnología e innovación

Milestone Systems, proveedor líder de software de video basado en datos dentro y más allá de la seguridad, llevó a cabo el Milestone Partner Summit (MIPS 2022), evento que reunió a los principales socios de la marca para presentarles las nuevas soluciones tecnológicas de la firma acompañados por diferentes conferencias magistrales. Uno de los objetivos de Milestone es Convertise en el líder mundial en *data-drive*, en *software* de tecnología de video, dentro de la seguridad, y más allá de ésta, de acuerdo con Thomas Jensen, CEO de Milestone Systems.

Milestone Systems continúa expandiendo su oferta de soluciones de tecnología de video basadas en datos, con instalación local, de nube híbrida y nativa. El nuevo servicio VSaaS (videovigilancia como servicio) Milestone Kite™ presentado en el MIPS, complementa la implementación de XProtect en AWS (Amazon Web Services). Milestone Kite™, es una solución fácil de implementar, segura y escalable para la gestión de video (VMS) en la nube, orientada a pequeñas y medianas empresas. En este servicio la implementación de XProtect en AWS ha sido optimizada para el mercado empresarial.

Fecha: 26 de octubre de 2022.

Lugar: Ciudad de México.

Asistentes: más de 200 invitados.

Seguridad en América efectúa *Roadshow* "Soluciones de Seguridad en *Data Centers*"

Seguridad en América (SEA) llevó a cabo el *Roadshow* orientado a las Soluciones de Seguridad en *Data Centers* con presentaciones de diferentes expertos en el tema. El Roadshow fue coordinado por Samuel Ortiz Coleman, director de SEA; y por Alex Parker, *Sales Manager* de la misma casa editorial.

CONFERENCIA MAGISTRAL

La conferencia magistral fue impartida por Alejandro Valdez, director del Centro de Comandos Regionales de Seguridad para México y Latinoamérica en CITIBANK, quien nos comentó sobre la Seguridad del Futuro en *Data Centers* y como está conformada la Seguridad del ayer y la Seguridad del hoy.

Alex Valdez expresó que hay cinco capas de protección en un *Data Center*, las cuales son: Perimetral exterior, Perimetral interior, Control de acceso, Monitoreo Interior y Protección de *Data;* que nos presentan un antes y un después de la Seguridad en *Data Centers*. Por último, mencionó: "Todo gerente de seguridad en un *Data Centers* o centro de procesamiento de datos debe de estar involucrado en las siguientes áreas o actividades adicionales, ya que la seguridad puede ser vulnerada: Brigadas de Emergencia/Protección Civil, Sistemas de Supresión de Incendio y Sistemas de Administración de Edificios (BMS)".

PATROCINADORES

En cuanto a las conferencias de los patrocinadores, se contó con la presencia de Jonathan Ávila Sánchez, Country Manager México y Centroamérica de EVERBRIDGE, con la conferencia "La importancia de la gestión de eventos críticos para *Data Centers*". Señaló que la marca que representa tiene el propósito de incrementar la resiliencia dentro de las organizaciones unificando la inteligencia de riesgos, la seguridad física y las comunicaciones críticas.

Por su parte, Guadalupe Arroyo, gerente *Senior* de Desarrollo de Negocios para México y Latinoamérica de la empresa Atalait. Explicó que la marca "ofrece una solución única en el mercado que integra de manera amplia y robusta la tecnología de punta en cuanto a seguridad física y lógica como parte de la gestión de riesgos de manera preventiva y dar respuesta, recuperar y lograr la continuidad de su negocio, ante cualquier incidente o contingencia mayor".

Alejandro Valdez, director del Centro de Comandos Regionales de Seguridad para México y Latinoamérica en CITIBANK

Finalmente, nos acompañó Isidro Tamariz Fossas, gerente de Soporte Técnico y Comercial de STID (Electronic Identification), quien platicó sobre el tema de "Realiza tu propia encripción y asegura tus datos", en donde presentó las diferencias de la Seguridad Física y la Seguridad Electrónica.

Mencionó que existen dos tipos principales de seguridad en control de accesos de un *Data Center,* los cuales son: la seguridad física, que es aquella que está representada por elementos que impiden que una persona u objeto sin permisos, ingrese al espacio del *Data Center* (puertas controladas, cerraduras, lectoras, biométricas, etc.); y la seguridad electrónica, que es aquella que está representada por los elementos no visibles en un sistema de control de accesos (protocolos de comunicación, encripción, tecnologías de identificación, etc.).

Fecha: 27 de octubre de 2022.

Lugar: Restaurante Loma Linda en Plaza Carso (Ciudad de México).

Asistentes: más de 100 invitados.

UNV presenta las tendencias de la videovigilancia IP

Uniview (UNV), fabricante líder mundial en videovigilancia IP, de la mano de Tecnosinergia, mayorista reconocido en el mercado, ofrecieron un desayuno VIP para sus socios de mercado y prensa, en donde presentaron las tendencias de la videovigilancia y las soluciones que UNV ofrece, además de casos de éxito y nuevas funcionalidades.

"Una de ellas es que venimos directamente del mundo de la IP (Internet Protocol) es decir, no convergimos del análogo al IP, sino directamente de la tecnología IP, contamos con 3 mil 200 patentes establecidas en cualquiera de nuestros productos, somos una empresa que tiene cinco certificaciones ISO a través de estás y que contamos con certificaciones internacionales muy importantes que prácticamente empresas de otros países no las pueden tener", comentó Osvaldo Ordaz Reyes, *Business Development Manager* de UNV México.

Osvaldo Ordaz Reyes, *Business Development Manager* de UNV México

Fecha: 03 de noviembre de 2022.

Lugar: Escuela de Cadetes General Santander en Bogotá (Colombia).

Asistentes: más de 500 concurrentes.

La Dirección de Investigación Criminal y la INTERPOL realizan nueva edición del "Frente de Seguridad Empresarial"

Se llevó a cabo el XVIII Encuentro Anual del "Frente de Seguridad Empresarial" de la mano de la Policía Nacional de Colombia y la INTERPOL, el cual contó con una asistencia de 516 invitados presenciales y más de mil 700 asistentes de manera virtual, todo esto con el fin de fortalecer la unión entre empresarios y autoridades en contra de la criminalidad que perjudica a las empresas del país.

Uno de los principales ponentes del evento fue el Fiscal General Francisco Barbosa Delgado, quien recalcó la importancia de mantener e impulsar la paz y comparó los gobiernos actuales de Colombia con los de hace 30 años, resaltando el avance que se ha logrado en materia de seguridad e igual señalando la importancia de seguir progresando en beneficio de la ciudadanía. El fiscal resaltó el rol que juegan la inseguridad y la delincuencia en la circulación del delito, algo que él denomina como "Corredores Regionales de Criminalidad".

Fiscal General Francisco Barbosa Delgado

Fecha: 07 de noviembre de 2022.

Lugar: Hacienda de Los Morales, Ciudad de México.

Asistentes: más de 150 miembros de la AMESP.

La AMESP elige a su nueva Mesa Directiva 2022-2024

Los miembros de la Asociación Mexicana de Empresas de Seguridad Privada, A. C. (AMESP) se reunieron para llevar a cabo la Asamblea General Extraordinaria del mes de noviembre y a su vez las elecciones para nombrar al nuevo presidente del periodo 2022–2024 y la nueva Mesa Directiva de la asociación. El Cap. Salvador López Contreras, tomó el micrófono para otorgar unas palabras de bienvenida, así como también reflexionó sobre el final de su presidencia y expresó sus buenos deseos a los futuros ganadores de la elección.

Finalmente se anunció el resultado, el cual pronunció como ganadores, con una diferencia de dos votos, a los miembros de la planilla Azul y Negro. Con gran emoción, Gabriel Mauricio Bernal Gómez otorgó unas palabras a los presentes, donde agradeció el apoyo a su equipo y a los miembros que le brindaron su voto, mencionando su deseo de superar las adversidades y hacer crecer a la asociación como grupo.

Fecha: 08 de noviembre de 2022.

Lugar: Hotel Sheraton María Isabel, Ciudad de México.

Asistentes: más de 150 invitados.

Braulio Arsuaga presente como conferencista en la Reunión Mensual de ASIS

Braulio Arsuaga Losada, presidente del Consejo Nacional Empresarial Turístico

Los miembros de ASIS Capítulo Ciudad de México, tuvieron su reunión mensual con la participación de Braulio Arsuaga Losada, presidente del Consejo Nacional Empresarial Turístico y CEO de Grupo Presidente, quien habló sobre la "Ruta crítica de competitividad turística en México". Braulio comenzó su ponencia hablando de cifras en cuanto al turismo en México, comparando los índices con otros países. De igual manera, mencionó la importancia de aumentar la seguridad a la par del turismo para tener un mejor alcance a nivel internacional y combatir la imagen negativa que se pueda percibir en el área de nuestro país.

También reconoció la falta de apoyo en cuanto presupuesto por parte del gobierno hacia este sector, haciendo énfasis en que el sector debería ser de los de principal importancia para el país, incluso señaló el ejemplo de la pandemia, situación en la que México fue una de las pocas naciones en mantener sus fronteras abiertas con el fin de prolongar el turismo.

SEGURIDAD EN AMÉRICA

SÍGUENOS EN NUESTRAS REDES SOCIALES Y MANTENTE INFORMADO DE LAS ÚLTIMAS TENDENCIAS DE SEGURIDAD

www.seguridadenamerica.com.mx

Fecha: 17 de noviembre de 2022.

Lugar: Seproban
Coyoacán, Ciudad de México.

Asistentes: más de 50 participantes.

SEPROBAN festeja su 35° aniversario e inaugura su nueva sede

La empresa Seguridad y Protección Bancarias S. A. de C. V. "SEPROBAN", realizó la celebración de su 35° aniversario, así como también aprovecharon la ceremonia para inaugurar la nueva sede de sus instalaciones ubicada en la av. Coyoacán Eje 3 Poniente No. 1622 en la colonia Del Valle en la alcaldía Benito Juárez de la Ciudad de México. Ciro Ortiz, director general de SEPROBAN, agradeció el apoyo y los buenos deseos de los presentes, así como a los miembros de su equipo con los que en conjunto han logrado 35 años creciendo y fortaleciendo su organización.

También se llevó a cabo la presentación de un proyecto de innovación denominado ABM digital, una herramienta tecnológica desarrollada por la misma asociación que tiene como objetivo agilizar los procesos en cuanto a toma de decisiones en la administración y la gestión en los comités de la ABM. "Esto es ABM digital, una herramienta que quiere fomentar el autoservicio, pero donde vamos a fomentar el incremento de la comunicación hacia ustedes." comenta Rodrigo Pineda, titular del área de Tecnologías de la Información, Sistemas y Logística de la ABM.

COLEMAN

RENTA DE BLINDADOS

Ya contamos con *Suburban 2023* – Nivel V

557672.4992

www.rentadeblindados.com.mx

krauda@seguridadenamerica.com.mx

Fecha: 23 de noviembre de 2022.

Lugar: Ciudad de México.

Asistentes: más de 150 espectadores.

Seguridad en América lleva a cabo el *Roadshow* "Seguridad en Supermercados y tiendas de conveniencia"

Seguridad en América, llevó a cabo el *Roadshow online* titulado "Seguridad en Supermercados y tiendas de conveniencia" presentado y dirigido por Samuel Ortiz Coleman, director general de SEA; y Alex Parker, *Sales Manager* de la misma casa editorial. Julieta Muñoz Cornejo, gerente de Riesgos de Chedraui, fue la conferencista magistral con la ponencia denominada "Replanteamiento de la Seguridad en *Retail*".

Julieta Muñoz Cornejo, gerente de Riesgos de Chedraui, Samuel Ortiz Coleman, director general de SEA; y Alex Parker, *Sales Manager* de la misma casa editorial

PATROCINADORES

Jonathan Ávila Sánchez, *Coach Manager* de México y Centroamérica de EVERBRIDGE, también dirigió su ponencia hacia el área de *retail*, titulada "Transformación digital a los procesos de seguridad en supermercados". El experto señaló que los eventos de riesgo ocurren todos los días, por lo cual el tiempo de resolución es de suma importancia. Con el objetivo de crear soluciones diseñadas para mantener a la gente a salvo en un mundo cada vez menos seguro, Jonathan ofrece la plataforma digital de EVERBRIDGE.

Esta plataforma busca implementar la resiliencia dentro de las organizaciones unificando la inteligencia de riesgos, la seguridad física y las comunicaciones críticas. Contando con el proceso de evaluar, localizar, actuar y analizar, la plataforma busca impulsar la mejora contínua dentro de las organizaciones utilizando prácticamente cualquier modelo o dispositivo de tecnología, e igual cuenta con la capacidad de identificar los riesgos externos y realizar la cobertura de monitoreo de medios y redes sociales, siempre teniendo como objetivo la proactividad.

Posteriormente se presentó José de Jesús Arellano, *Account Manager* de GENETEC México, con la ponencia titulada "¿Cómo impactar positivamente la operación invirtiendo en seguridad?" en la que busca señalar los desafíos y necesidades que presenta el área de retail y qué soluciones se pueden presentar para hacerla más eficiente. Él señala que en el área de seguridad siempre están surgiendo nuevas amenazas, por lo cual la seguridad física ahora debe estar entrelazada con la seguridad cibernética.

En GENETEC se enfocan en la seguridad, la inteligencia y las operaciones con el fin de ofrecer eficacia en cuanto a resultados, de una manera híbrida que engloba la tecnología y la seguridad física, menciona José de Jesús. Implementando distintas herramientas que actúen de manera continua con el fin de mejorar los procesos de la organización de manera proactiva expandendiendo de manera segura las partes tecnológicas con el uso de su plataforma llamada Security Center.

Victor Calderón, *Sales Manager* de NVT México junto con ADISES, habló sobre las "Mejores prácticas para el diseño de una infraestructura de red para los sistemas de seguridad física en *retail*", él menciona que todos los dispositivos tecnológicos que usa el área de *retail* tienen un punto en común que es la infraestructura, la cual debe de ser capaz de transmitir bastante información. También resalta cómo la innovación tecnológica ya permiten a uno actuar de manera independiente.

Resaltó la importancia de la infraestructura en cuanto al *software* u otras herramientas, Víctor mencionó la tecnología de NVT, la cual esta enfocada a dar una solución efectiva no solamente al sector retail, sino a cualquiera de las verticales del negocio de la empresa, teniendo como desafío la actualización de IP (Internet protocol). Ofreciendo un cambio de cables analógicos con el fin de actualizarlos a una nueva etapa digital, fortaleciendo así la infraestructura del cableado, maximizando los recursos para permitir entrar a una era de tecnología avanzada.

Finalmente, se presentó Arturo Flores, director comercial de OMNICLOUD, con la ponencia titulada "Transformando la seguridad del retail con servicios *cloud*". OMNICLOUD se dedica al desarrollo de sistemas de seguridad 100% cloud donde se puede integrar diferentes soluciones de video o alarma, o cualquier requerimiento del cliente. Manteniendo la importancia de las tecnologías cloud en las áreas de *retail*, Arturo comenta la oferta de cámaras o servicios de comunicación y alarma pertenecientes a su plataforma.

SEGURIDAD®
EN AMÉRICA

Visita nuestro portal desde tu tablet o móvil

https://www.seguridadenamerica.com.mx

Roadshows online 2023

	40 Minutos de Presentación	Base de Datos	Promoción de la Marca en Medios	Transmisión de Video Corporativo de 2 Minutos (4 Veces)	Costo Unitario
Patrocinio Plata		✓	✓	✓	$25,000
Patrocinio Oro	✓	✓	✓		$45,000

ENERO

Seguridad en Telecomunicaciones
Miércoles 25

FEBRERO

Seguridad en Puertos Marítimos
Miércoles 8

Técnicas en Pruebas de Confianza e Investigaciones
Miércoles 22

MARZO

Seguridad en la Industria Manufacturera
Miércoles 8

Seguridad en Logística y Custodia de Mercancía
Miércoles 22

ABRIL

Seguridad en Parques Industriales
Miércoles 5

Centrales de Monitoreo y GPS
Miércoles 26

MAYO

Supermercados y Tiendas de Conveniencia
Miércoles 9

Seguridad en Centros Educativos
Miércoles 24

JUNIO

Seguridad en la Industria Farmacéutica
Miércoles 7

Seguridad en Bancos
Martes 27 y Miércoles 28

SEGURIDAD EN AMERICA

SEA

JULIO

Nuevo perfil de protección ejecutiva
Miércoles 12

Soluciones contra Incendio
Miércoles 26

AGOSTO

Seguridad en Plantas Automotrices
Miércoles 09

Seguridad en Maquiladoras
Miércoles 23

Cumbre de Seguridad Corporativa
(evento prescencial, solicitar cotización a su ejecutivo)
Martes 29 y Miércoles 30

SEPTIEMBRE

Seguridad en la Industria Alimentaria
Miércoles 6

Seguridad en Petróleo y Energía
Miércoles 20

OCTUBRE

Seguridad en la Industria Hotelera
(Evento presencial)

Soluciones de Seguridad en *Data Centers* & *TI*
Miércoles 26 de octubre

NOVIEMBRE

Seguridad en Hospitales
Miércoles 8

Blindaje para la protección de mercancía
Miércoles 22

Seguridad en Casinos y Centros de Entretenimiento
Miércoles 29

DICIEMBRE

Seguridad en grandes superficies con el uso de Drones
Miércoles 6

Reunimos a los tomadores de decisiones de la seguridad en distintos sectores para que usted ofrezca sus productos y/o servicios por medio de conferencias dinámicas.

BENEFICIOS

- Usted podrá impartir su conferencia a más de 500 profesionales de la seguridad.
- Interactuar directamente con tomadores de decisiones.
- Promocionar sus productos y servicios.

EL PATROCINIO INCLUYE

- Base de datos de los asistentes.
- Reporte analítico de la estrategia de publicidad.
- Presentación de 30 minutos.

telemarketing@seguridadenamerica.com.mx
www.seguridadenamerica.com.mx
(55) 5572 6005

SISSA
Monitoring Integral

Isaac VALENCIA TREJO,

fundador y director general
en SISSA Monitoring Integral

Foto: Freepik

Seguridad en América (SEA): ¿Cómo llegó al sector de la seguridad y cómo inició SISSA?

Isaac Valencia Trejo (IVT): tengo 21 años de trayectoria en el ámbito de la seguridad, durante los cuales he desarrollado diversas actividades que van desde el diseño e implementación de soluciones hasta servicios posventa, tales como acciones de soporte (mantenimiento preventivo y correctivo) para diferentes tipos de implementaciones.

SISSA es una empresa que fundé hace casi 12 años. En un inicio nos dedicamos a desarrollar software para otros integradores de seguridad; sin embargo, con el paso de los años logramos tener presencia directa con los usuarios finales y comenzamos a tener acceso a diferentes tipos de proyectos, especialmente en las denominadas instalaciones críticas.

SEA: Como experto, ¿cuáles considera que son los principales problemas de seguridad en el país?

IVT: existen muchos problemas de seguridad en el país; sin embargo, creo que la raíz de todos ellos radica principalmente en la falta de continuidad que se le da a las cosas. Es decir, cuando se desarrollan proyectos interesantes, sobre todo a nivel gubernamental, no se les da un debido seguimiento, lo que hace que todo resulte en esfuerzos aislados ejecutados en diferentes periodos de tiempo (equivalentes a lo que dura un gobierno en el poder, por ejemplo).

En este sentido, considero que gran parte de los problemas que tenemos en México -no sólo en materia de seguridad, sino en muchos ámbitos- se deben a tres factores principales: la irregularidad, la mediocridad y la falta de seguimiento a proyectos importantes para el país.

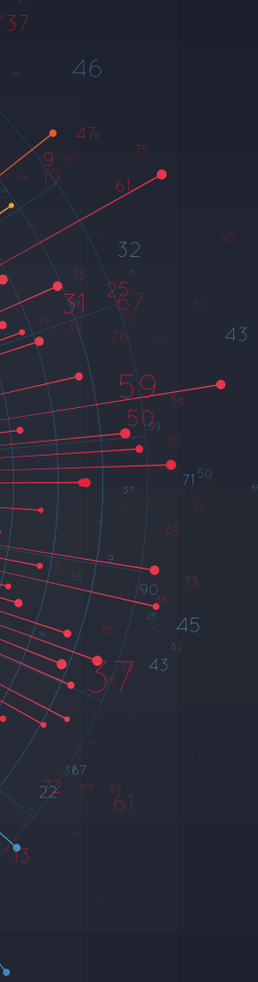
SEA: ¿Cuáles son los servicios que ofrece SISSA?

IVT: dado que no somos solamente unos instaladores de tecnología -como la mayoría de las propuestas en el mercado actual-, sino que somos integradores de soluciones tecnológicas llave en mano, en SISSA nos entusiasma participar en los proyectos desde su concepción, por lo que llevamos a cabo análisis de vulnerabilidades, estudios de mitigación de riesgos y análisis de riesgos.

En SISSA no nos gusta trabajar en partes, por lo que nuestra principal oferta de valor son los proyectos de integración basados en soluciones que realmente resuelven los problemas de nuestros clientes, y no proyectos que generan problemas a largo plazo.

SEA: En específico, ¿qué soluciones tecnológicas ofrece SISSA para los sectores de e-commerce y hospitales?

IVT: Al ser integradores de soluciones tecnológicas llave en mano, no nos limitamos únicamente al campo de la seguridad, sino que también ofrecemos soluciones enfocadas al



Los cinco aspectos que Isaac Valencia recomienda al usuario final, al momento de contratar el servicio de Seguridad Privada:

1. Asegúrese de estar contratando una empresa reconocida en el medio.
2. Valide que cumpla al 100 % con todas las regulaciones del gobierno, desde las relacionadas con la seguridad hasta cuestiones fiscales y laborales.
3. Valide que su equipo esté conformado por personal debidamente capacitado, es decir, que cuente con una capacitación seria y formal.
4. Verifique que ofrezca una propuesta seria. Para ello, debe contar con un soporte técnico sólido.
5. Por último, considero que también nuestros clientes y prospectos deben comprender que la elaboración de un proyecto serio lleva tiempo y no se logra de un día para otro, ya que éste implica ingenierías previas que nos permiten presentar una propuesta técnica de valor a un costo adecuado.

ámbito de las tecnologías de la información (TI) y destinadas a dar soporte a temas de infraestructura.

El abanico de posibilidades que ofrecen los proyectos de SISSA es bastante interesante. No obstante, la más destacable es la referente a la integración de proyectos: nosotros difícilmente participamos en proyectos aislados (con instalaciones aisladas); nuestra principal propuesta de valor es la integración de sistemas para la creación de soluciones únicas y personalizadas.

A propósito, uno de nuestros productos estrella es VSS: plataforma de integración de sistemas ideal para el entorno hospitalario, e-commerce y muchos otros.

SEA: ¿Por qué elegir a SISSA?

IVT: SISSA participa muy activamente en instalaciones críticas, siendo éstos los principales proyectos en los que nos desarrollamos. No trabajamos directamente con el gobierno, sino a través de diversas concesionarias o constructoras, las cuales sí están contratadas por instancias federales y estatales.

No obstante, desde hace unos años también nos estamos abriendo brecha en sectores más corporativos que industriales (como el sector inmobiliario y educativo).

Hoy día contamos con dos oficinas en la Ciudad de México y una en Guadalajara, al igual que tenemos cobertura en algunos países de Centroamérica e incursiones en EE. UU. Cabe mencionar que contamos con despliegue administrativo-técnico en todos los lugares donde tenemos operaciones.

En lo referente a alianzas estratégicas, en SISSA creemos y apostamos por la profesionalización del sector de la seguridad, razón por la cual formamos parte de diversas organizaciones y asociaciones del sector como ASIS, ALAS y ASUME, con las cuales sumamos esfuerzos para lograr objetivos en común, entre ellos hacer que el sector de la seguridad tenga leyes que le den más solidez.

SEA: ¿Cuáles son los diferenciadores de SISSA?

IVT: En SISSA tenemos tres principales diferenciadores:

1) Nosotros sí entendemos la problemática del prospecto o cliente gracias a que realizamos un análisis serio del problema que se busca resolver. Partiendo de esto, procedemos a realizar un proyecto ejecutivo e ingenierías con una verdadera propuesta de valor.
2) Nuestra capacidad de integración nos permite ofrecer al prospecto o cliente la opción de no cambiar forzosamente todo su equipamiento. Analizamos en conjunto la posibilidad de aprovechar al máximo el rendimiento de las instalaciones con las que ya cuenta y la manera de integrar, paralelamente, nuevos sistemas.
3) Tenemos la capacidad de desarrollar nuestros propios sistemas de integración y diversas soluciones gracias a que contamos con nuestra propia fábrica de *software*: SISSA Digital. ■

MILESTONE SYSTEMS ANUNCIA EL LANZAMIENTO DEL XPROTECT 2022 R3

La nueva actualización del software de gestión de video (VMS) XProtect 2022 R3 está basada en innovaciones anteriores y ofrece una experiencia de usuario ágil, integrada y fácil de usar, pero muy potente. Con esta última actualización de producto, Milestone Systems continúa avanzando en la tecnología de video empresarial para satisfacer la demanda cada vez mayor que hay en el mercado de soluciones de tecnología de video integrales y de primera categoría. La actualización de producto R3 refina y mejora aquello que más necesitan los usuarios del VMS: las soluciones de plataforma abierta confiables, potentes, fáciles de usar y administrar que ofrecen la flexibilidad y seguridad necesarias para satisfacer cualquier requerimiento de administración de video. El 2022 R3 es una actualización de software muy recomendada para todos los usuarios de XProtect. ■

PROSEGUR MÉXICO GESTIONA EL USO EFICIENTE DE EFECTIVO CON CASH TODAY

El efectivo continúa siendo el medio de pago más utilizado en el país tanto para compras menores de 500 pesos, como para compras de mayor monto, es por ello que Prosegur ofrece Cash Today, una solución integral que permite la transformación de los procesos de administración del efectivo para pequeñas, medianas y grandes empresas. Además, el conjunto de herramientas y sistemas que proporciona permite la simplificación de procesos, mejora la administración de recursos humanos, reduce drásticamente pérdidas de efectivo, mejora la conciliación de ventas y de tesorería e incrementa la liquidez financiera, entre otros. Prosegur Cash Today ayuda a empresas de todo tipo y tamaño en la automatización de procesos y proporciona información en línea para que la empresa pueda realizar las conciliaciones y cuadres de venta y de tesorería de forma rápida y sencilla. ■

PALO ALTO NETWORKS ANUNCIA LA EXPANSIÓN DEL PROGRAMA NEXTWAVE

Con el objetivo de impulsar los servicios administrados, Palo Alto Networks (NASDAQ: PANW) anunció la expansión del programa NextWave para fortalecer a sus socios para contener y remediar rápidamente las ciber amenazas, al permitirles brindar servicios de respuesta a incidentes (IR, por sus siglas en inglés) impulsados por Cortex XDR®, líder en la industria. El programa para respuesta a amenazas ofrece a los socios: Tecnología IR XDR líder, construida utilizando casos de uso proactivos y reactivos para reducir el tiempo y los recursos gastados en la prestación de servicios; soporte técnico experto y de implementación las 24 horas del día, los 7 días de la semana, para acceso en línea a los arrendatarios de XDR en cuestión de minutos y soporte técnico las 24 horas, y rutas ampliadas al mercado. ■

AVASANT NOMBRA A **UNISYS** LÍDER EN SERVICIOS DE ESPACIOS DE TRABAJO DIGITAL 2022

Avasant reconoció a Unisys Corporation como pionera, en su informe Digital Workplace Services 2022 RadarView™, el cual identifica y analiza las capacidades de los proveedores de servicios en materia de tecnología y soporte para que las organizaciones puedan seleccionar los socios estratégicos adecuados. “Las compañías han sufrido un tremendo cambio en los últimos años y ahora están obligadas a incorporar modelos de trabajo remotos e híbridos en sus estrategias de negocio para seguir siendo relevantes y competitivas", dijo Leon Gilbert, vicepresidente senior y director general de Digital Workplace Solutions de Unisys. "Este reconocimiento de Avasant valida la importancia de las soluciones de lugar de trabajo digital que no sólo permiten mejorar las experiencias de los empleados, sino también mejorar la productividad y la colaboración”. ■

FORTINET LANZA EN LATAM SERVICIO GRATUITO DE EVALUACIÓN DE SEGURIDAD OT

Fortinet® anunció el relanzamiento para toda América Latina de un servicio gratuito para que las organizaciones industriales puedan evaluar el nivel de madurez de ciberseguridad de sus ambientes de tecnología operacional (OT, por sus siglas en inglés). Disponible en español, inglés y portugués, la evaluación de seguridad de ambientes operacionales e infraestructura crítica se realiza de forma rápida y objetiva a través de una serie de preguntas simples. Una vez enviadas las respuestas, la empresa recibe un reporte personalizado con recomendaciones para elevar el nivel de ciberseguridad de su organización. A partir de esta evaluación, Fortinet puede proveer una consultoría individual de forma gratuita para identificar los riesgos y mejores prácticas para elevar el nivel de protección de los entornos de OT. ■

HONEYWELL LANZA UNA NUEVA SUITE PARA AYUDAR A OPTIMIZAR TIEMPO Y PRODUCTIVIDAD DE CENTRO DE DATOS

Honeywell lanzó su Suite de Centros de Datos, una cartera de soluciones de *software* que ayuda a los administradores y propietarios de centros de datos a optimizar el tiempo de actividad, la productividad de los trabajadores, la salud de los activos críticos y los gastos operativos, al tiempo que proporcionan una mejor visibilidad de los KPI de sostenibilidad. Los centros de datos desempeñan un papel cada vez más importante para mantener la productividad de la economía mundial; en el hogar, por ejemplo, brinda comodidades de la vida diaria, así como en el trabajo a distancia y las compras en línea. Al digitalizar, agregar y analizar sistemas críticos dispares en un banco de datos unificado, la analítica producida por la *suite* de Honeywell proporciona a los operadores información más integral y procesable para ayudar a aumentar la eficiencia y reducir los costos. ■

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.

POR PRIMERA VEZ CELEBRAN EN MÉXICO EL DÍA NACIONAL DE LA PREVENCIÓN DE INCENDIOS

Por su iniciativa de la "Campaña Nacional de Prevención Contra Incendios", que cumplió, del 3 al 7 de octubre, su 8ª edición, empresarios asistentes a la Reunión Anual de Industriales (RAI) 2022, que se llevó a cabo en León, Guanajuato, entregaron el premio "Ética y Valores" a la AMRACI (Asociación Mexicana de Rociadores Automáticos Contra Incendios) y CONAPCI (Consejo Nacional de Protección Contra Incendios). Este reconocimiento pone de manifiesto la importancia de la labor que llevan a cabo en todo el país las instituciones que reúnen a las empresas más importantes del sector contra incendio en México preocupadas por la creación de una cultura de prevención más robusta y participativa. La RAI es el evento industrial más importante de México, que reúne a más de mil líderes empresariales. ■

Juan José Camacho Gómez, presidente de la AMRACI

DELL TECHNOLOGIES OFRECE INNOVACIONES EN EL SECTOR CON VMWARE

Dell Technologies (NYSE: DELL) presentó nuevas soluciones de infraestructura, diseñadas conjuntamente con VMware, las cuales ofrecen mayor automatización y rendimiento para las organizaciones que adoptan estrategias de multicloud y de Edge. "Los clientes nos dicen que quieren ayuda para simplificar sus estrategias de multicloud y de Edge al buscar impulsar una eficiencia y un rendimiento mayores de su TI", explicó Jeff Boudreau, presidente de Dell Technologies Infrastructure Solutions Group. "Dell Technologies y VMware tienen una gran cantidad de iniciativas de ingeniería conjuntas que abarcan áreas centrales de TI, como multicloud, Edge y seguridad, para ayudar a nuestros clientes a administrar y obtener valor de sus datos más fácilmente". Los datos y las aplicaciones de negocios continúan creciendo en ambientes de multicloud compuestos por ubicaciones en el Edge, *multicloud.* ■

TIPS PARA ACUDIR A UNA CASA DE EMPEÑO Y OBTENER CON ÉXITO EL PRÉSTAMO SOLICITADO

A través de los años, enero se ha convertido en el mes en el que más usuarios acuden a las Casas de Empeño, sin embargo estos lugares no están exentos a de robo o fraudes, es por ello que a continuación, extraídos del Blog "Manual de Seguridad" de David Lee, les compartimos algunos tips para empeñar con seguridad sus bienes.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1. **Busque otras opciones**. Empeñar uno o más bienes personales, no es una decisión sencilla, antes de realizarlo, agote otras opciones como familiares, empleador, amigos o instituciones bancarias que puedan facilitarle el crédito o préstamo que requiere.

2. **Conozca el proceso de empeño**. Asegúrese de conocer todo el procedimiento de la casa de empeño que eligió, los formatos, contratos, tiempos, intereses, y verifique que el negocio cuente con el número de registro otorgado por la PROFECO; pida consejos y ayuda a familiares o amigos que ya hayan empeñado alguna vez.

3. **Analice el costo total anual.** Visite al menos tres casas de empeño para comparar y evaluar la opción que más le convenga. Analice el costo anual que le ofrecen y evalúe todos los costos: tasas de interés, comisiones, avalúo, gastos de almacenaje, entre otros.

4. **Empeño.** Ya que haya revisado todo lo anterior y esté listo para empeñar, tome fotografías de su artículo, en las que se aprecien características como estado, número de serie, etc. Si es oro, usted mismo pese el objeto para que esté seguro al momento de realizar el empeño y avalúo por el negocio.

5. **Al acudir a empeñar.** Acuda al negocio a primera hora evitando las famosas "horas pico", vaya acompañado y oculte bien su prenda u objeto. Cuando el valuador le dé el monto del préstamo, puede aceptar o no, en dado caso de aceptar revise bien los datos de la boleta de empeño, nombre, descripción de la prenda, costo, y los datos para recuperarla. Cuídese de los famosos "coyotes" que están alrededor de esos lugares y lo pueden engañar y hasta robar su prenda.

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

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

incluye gastos de envío

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. **(Marque así X)**

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA 2022	☐ $ 550 MN	☐ $ 120 dólares

FORMAS DE PAGO:

☐ Depósito en banco HSBC a nombre de Editorial Seguridad en América, S.A. de C.V. Cuenta 04016012049

☐ Cargo a tarjeta de crédito o débito.

No. de cuenta: _____ Fecha de vencimiento: _____ Código: _____

☐ Transferencia bancaria: Clabe 021180040160120491

_____
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 via: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2023

SEGURIDAD EN AMÉRICA

Suscripción Anual (6 ejemplares)

México: **$650 pesos**

Extranjero: **$270 dls.**

(incluye gastos de envío)

¡SUSCRÍBETE YA!

Cel. 55 5965 4582 (55) 5572 6005

telemarketing@seguridadenamerica.com.mx

www.seguridadenamerica.com.mx

"SEPSISA se ha transformado en SER grande"

Facility Services

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.

- Guardias
- Comercializadora
- Limpieza
- Consultoría
- Custodia
- Seguridad Electrónica
- GPS / Monitoreo

REPSE

Registro de Prestadoras de Servicios Especializados u Obras Especializadas

EMPRESA SOCIALMENTE RESPONSABLE · ISO · ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD · CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C. · AMESP · BAC · COPARMEX®

CDMX, Estado de México, Monterrey, Guadalajara, San Luis Potosí, Aguascalientes, Hermosillo, Querétaro, Guanajuato, Pachuca, Puebla, Cuernavaca, Acapulco, Veracruz, Villahermosa, Mérida, Cancún, Mexicali, Chihuahua, Tijuana, Ensenada.

www.sepsisa.com.mx ventas@sepsisa.com.mx 55 5351 0402