SEGURIDAD®
EN AMÉRICA

Especiales:

Seguridad en bancos

Seguridad en eventos masivos

Reporte: Blindaje automotriz

Año 22 / No.128
Septiembre-Octubre

www.seguridadenamerica.com.mx

Multiproseg

A quien valor merece

WWW.MULTIPROSEG.COM.MX

(55)5406 5287 • (55)3455 4375

INFO@MULTIPROSEG.COM.MX

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

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

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

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

CORPORATIVO CDMX

SEGURIDAD EN AMÉRICA

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

Año 22 / No. 128 / septiembre-octubre / 2021

Foto de Portada
SEA

Síguenos por

Seguridad-En-América

@Seguridad_En_Am

@seguridad_en_america

SeguridadEnAmerica

revista-seguridad-en-america

www.seguridadenamerica.com.mx

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

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

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

Coordinación de Diseño
Verónica Romero Contreras
v.romero@seguridadenamerica.com.mx

Arte & Creatividad
Arturo Bobadilla

Diego Idu Julián Sánchez
arte@seguridadenamerica.com.mx

Administración
Oswaldo Roldán
oroldan@seguridadenamerica.com.mx

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

Pilar Erreguerena
perreguerena@seguridadenamerica.com.mx

Reporteros
Mónica Ramos
redaccion1@seguridadenamerica.com.mx

Erick Martínez Camacho
redaccion2@seguridadenamerica.com.mx

Pablo Romero Navor
redaccion3@seguridadenamerica.com.mx

Elizabet Gómez
redaccion4@seguridadenamerica.com.mx

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

Iván Solís Bustos
mdigital2@seguridadenamerica.com.mx

Jesús Chávez García
mdigital3@seguridadenamerica.com.mx

Circulación
Alberto Camacho
acamacho@seguridadenamerica.com.mx

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

María Esther Gálvez Serrato
egalvez@seguridadenamerica.com.mx

Apoyando a:

Socio de:

CÁMARA NACIONAL DE LA INDUSTRIA EDITORIAL MEXICANA

COMPARTE ESTA REVISTA
COMPARTIR ES RECICLAR

Conmutador: 5572.6005
www.seguridadenamerica.com.mx

EDITORIAL

México quiere llevar a juicio a más de una decena de fabricantes y distribuidores de armamento. El Gobierno de Andrés Manuel López Obrador presentó una demanda civil en contra de 11 empresas de producción y distribución de armas en Estados Unidos a quienes acusa de emprender "prácticas comerciales, negligentes e ilícitas, que facilitan el tráfico ilegal de armas a México". La Secretaría de Relaciones Exteriores confirmó que la acción legal fue presentada ante una corte federal en Boston, Massachusetts, con el objetivo de detener el flujo de armamento ilegal que llega al país desde Estados Unidos.

El debate sobre el control de armas es un tema que divide profundamente a los dos países. El canciller, Marcelo Ebrard, señaló que México "no busca interferir en la política de Estados Unidos" sobre armas y que el proceso judicial involucra únicamente a las empresas. La Cancillería dio un aviso a la embajada de Estados Unidos en la Ciudad de México sobre sus intenciones al presentar esta demanda.

De acuerdo con el periódico El País, las sociedades demandadas incluyen a algunos de los fabricantes más poderosos: Smith & Wesson, Barrett Firearms Manufacturing, Beretta, Century International Arms, Colt's Manufacturing Company, Glock, Sturm, Ruger & Co y Witmer Public Safety Group, entre otros. Las ventas anuales de estas firmas a clientes en México, según el Gobierno mexicano, rebasan las 340 mil armas al año, que provocan 17 mil homicidios anuales.

La base de la denuncia es que las empresas armamentísticas incentivan este uso ilícito de las armas a través de su *marketing*, o como mínimo no hacen nada para evitarlo. Ebrard llegó a decir que las compañías llegan a "desarrollar diferentes modelos" de pistolas específicamente "para el narco".

De hecho, la demanda cita que las autoridades mexicanas han detectado el uso de unas Colt de calibre .38 que llegaron al país desde Estados Unidos ilegalmente y que tenían la imagen del revolucionario Emiliano Zapata, un símbolo de estatus entre los cárteles mexicanos.

Según el portal France24, México registró sus dos años más violentos de la historia, precisamente bajo los dos primeros años de Gobierno de López Obrador. Tanto en 2019 como en 2020, murieron por asesinato más de 34 mil 500 personas. Eso significa que la tasa de homicidios es de 29 por cada 100 mil habitantes, un indicador que no ha bajado desde 2018 y que supone la tasa más alta desde que se tiene registro en el país.

¿Usted está a favor o en contra de la indemnización que busca el Gobierno mexicano por daños? ■

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 Ulises Figueroa Hernández, Licenciado en Seguridad Pública del Servicio de Protección Federal, quien en generosas ocasiones ha presentado a nuestro público lector interesantes artículos que atañen a la industria de la seguridad en su conjunto.

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

Si desea conocer más acerca del experto, consulte su currículo:

SEA

ENTREVISTA EXPRÉS CON

Benjamín Barona Coghlan,

director general de Control Seguridad Privada Integral, S.A. de C.V.

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

En mi opinión, será desde dos puntos muy básicos: el primero, que el gobierno no tiene capacidad para cubrir todas las vacantes que podría generar. El segundo, es que se perdería toda la experiencia que la seguridad privada ha adquirido con el paso de los años. Es como querer privatizar un sector sin contar con personal, conocimiento y experiencia. ■

IPS

GRUPO IPS

GARANTÍA EN SEGURIDAD

10 AÑOS

ESR

crese

Síguenos

Tel. (55) 5525 3242

grupoipsmexico.com

VIDEOVIGILANCIA

CONTROL DE ACCESO

TRANSPORTE SEGURO

CONTRA INCENDIOS

CIBERSEGURIDAD Y TI

ESPECIAL

ESPECIAL

SEGURIDAD PRIVADA

CONOCE A TU ASOCIACIÓN

ADMINISTRACIÓN DE LA SEGURIDAD

SEGURIDAD PÚBLICA

EL PROFESIONAL OPINA

FOROS Y EVENTOS

NOVEDADES DE LA INDUSTRIA

TIPS

VIDEOVIGILANCIA EN LOS HOGARES CON LA NUEVA NORMALIDAD

Foto: freepik - Freepik

Foto: Creativeart - Freepik

COSTA RICA | Federico Marín Mora

La tecnología como aliada de los padres de familia

Antes, no mucho tiempo atrás, en El Salvador, cuando no se escuchaba ni se tenía idea de lo que era vivir una pandemia, la prioridad en videovigilancia era la protección en el entorno o perímetro de las viviendas, esto con el objetivo de tratar de minimizar los casos de hurtos y vandalismos hacia las propiedades.

Los retos que en el último año nos ha tocado enfrentar por la pandemia no han sido nada fáciles, pues hemos experimentando circunstancias nunca antes vividas en nuestras generaciones. Esto ha ocasionado cambios radicales en nuestras formas de vida, ya sea, en el entorno laboral, industrial, social y sobre todo el familiar.

Esto lo podemos comprobar en el aumento de solicitudes y requerimientos para la instalación de cámaras dentro de los hogares, en las áreas específicas donde estudian los hijos e hijas, debido a que la modalidad de estudio tuvo que cambiar de presencial a virtual, donde alumnos reciben clases desde sus casas.

SUPERVISIÓN DESDE CUALQUIER LUGAR

Los padres (nuestros clientes), experimentaron una baja en el rendimiento escolar de sus hijos debido a que como ellos salen a trabajar, los menores quedaban sin una supervisión adecuada, porque abandonaban sus clases, jugaban en línea con sus amigos, hacían otras cosas que los distraía de los estudios.

Los padres por esta razón solicitaron, además del video, micrófonos que pudieran ser instalados para estar al tanto de lo que acontecía en el momento que los menores interactuaban en las clases virtuales con los maestros y compañeros y de esta forma, nuestros clientes podían monitorear en vivo, remotamente desde sus dispositivos para estar enterados de lo que sucedía con sus hijos.

Los resultados que se obtuvieron desde la implementación de estos sistemas han sido muy satisfactorios para los padres de familia, ya que sus hijos al sentirse supervisados remotamente tuvieron que comprometerse más con sus estudios y responsabilizarse más, reflejándose ello en el aumento en su desempeño académico.

Una vez más se comprueba que la tecnología, especialmente en videovigilancia, ha contribuido en nuestra nueva forma de vida, no solamente trayendo ventajas de seguridad en los hogares, sino también de monitoreo y supervisión parental que ha logrado prevenir y actuar a tiempo en el entorno académico de los estudiantes. ■

Federico Marín Mora,
gerente de Operaciones en CCTV IMPORT El Salvador.

Más sobre el autor:

SISSA
Monitoring Integral

@sissamx

55.1204.5656 55.1954.2832

SOLUCIONES DE **SEGURIDAD FÍSICA** IMPRESCINDIBLES EN **INSTITUCIONES BANCARIAS**

www.sissamx.com.mx

SOLUCIONES TECNOLÓGICAS QUE REQUIERE UNA SUCURSAL BANCARIA

VIDEOVIGILANCIA

PROTECCIÓN CONTRA INCENDIOS

GESTIÓN DE IDENTIDAD Y CONTROL DE ACCESOS

BIOMETRÍA

En **SISSA MONITORING INTEGRAL** no sólo ofrecemos servicios de integración de soluciones tecnológicas que responden a las necesidades particulares del sistema financiero, sino que también brindamos *consultorías y ofrecemos nuestra experiencia, conocimientos y buenas prácticas* en el mundo de la seguridad electrónica.

¿CÓMO SUS SISTEMAS DE CCTV LE AYUDARÁN A GANAR COMPETITIVIDAD EMPRESARIAL?

Gracias a la información que dispone del área de Seguridad, todas las áreas del banco obtienen rendimiento de los datos procedentes de los sistemas de video, se anticipan a los hechos, les permite mejorar la eficacia y los tiempos de respuesta

ESPAÑA | Alberto Pérez

La Seguridad Bancaria se encuentra inmersa en una etapa muy cambiante donde conceptos como la digitalización e inmediatez forman parte de nuestro día a día.

La banca está transformando su modelo de negocio a través de la reconversión de sus oficinas tradicionales en espacios más abiertos y con capacidad de crear una experiencia de usuario inolvidable para estrechar lazos con sus clientes y donde las nuevas tecnologías, la Inteligencia Artificial (IA), el *Deep Learning* y el *Big Data* convergerán para escribir el futuro.

OFRECER SERVICIOS A LA CARTA

Conozca el tipo de clientes que visitan sus agencias y ofrézcales información relevante a través de pantallas inteligentes para que contraten más servicios.

MINIMIZAR LOS TIEMPOS DE ESPERA

Averigüe en tiempo real si una fila rebasa el número de personas deseado o el tiempo máximo de espera abriendo una caja de cobro automáticamente.

CONTROLAR EL AFORO

Descubra el número de personas que entran y salen, identifique los momentos de mayor afluencia, realice un seguimiento de la ocupación automática y mejore los protocolos de actuación atendiendo a sus necesidades.

COMPETITIVIDAD EMPRESARIAL

A diario, miles de cámaras recogen información sobre el número de personas que entran, su comportamiento, el tiempo medio que permanecen, los espacios más frecuentados.

El *Big Data* permite organizar esos grandes volúmenes de información para identificar preferencias, hábitos, costumbres, horarios, necesidades e incluso predecir el comportamiento de cada cliente en cada momento.

Gracias a la información que dispone del área de Seguridad, todas las áreas del banco obtienen rendimiento de los datos procedentes de los sistemas de video, se anticipan a los hechos, les permite mejorar la eficacia y los tiempos de respuesta.

Y a su vez, son capaces de conocer mejor a sus clientes y ofrecerles servicios que se anticipen a sus necesidades y por tanto maximizar la rentabilidad empresarial de la entidad. ■

Fotos: SCATI

Alberto Pérez,
director de Desarrollo de Negocio para LATAM de SCATI.

Más sobre el autor:

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

EL TORNIQUETE ÓPTICO **MÁS CORTO DE SEGURIDAD**

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

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

BOON EDAM
YOUR **ENTRY** EXPERTS.

COLUMNA ALAS
COMITÉ NACIONAL MÉXICO

Manuel Zamudio

Más sobre el autor:

Industry Associations Manager LATAM&CAR de Axis Communications y presidente de ALAS Internacional Comité Nacional México.

¿BIOMETRÍA? ¡QUÉ MIEDO! PERO... ¿POR QUÉ?

Foto: Creativeart - Freepik

MÉXICO

Como sucede ahora de manera cada vez más frecuente, nos "medio enteramos" por redes sociales y chats de algunas cosas que pueden ser ciertas (en parte o no del todo), pero generalmente damos por sentado que lo que leemos es cierto, sólo porque nos lo compartió alguien de confianza, aunque esa persona no tenga tampoco la información completa.

La mercadotecnia ha hecho su parte también generando altas expectativas sobre el beneficio del uso de la tecnología y recientemente el tema del uso de la biometría ha causado gran revuelo, ya sea por el miedo a tocar superficies o revisar manualmente documentos en medio de una pandemia sumado a temas de legalidad, los derechos de los ciudadanos y las regulaciones. Le dejaré a los abogados, así como a los legisladores los temas "no técnicos", refiriéndome sólo a algunos datos históricos, conceptos generales y algunas tendencias tecnológicas y recomendaciones para su uso en un mundo que exige un presente y futuro más inteligente y seguro.

La biometría llegó para quedarse (también), y la hemos usado de una u otra manera al menos desde el siglo XIV, según cuenta el explorador y escritor portugués João de Barros, describiendo que los chinos estampaban las palmas de las manos en papel con tinta y los comerciantes usaban esa técnica para distinguir a los jóvenes.

Siglos más tarde (s. XIX) se desarrollaron sistemas antropométricos comenzando la historia moderna de la biométrica, registrando medidas de la cabeza y cuerpo, tatuajes y cicatrices a manera de memoria fotográfica, método que presentó fallas en su estandarización hasta que se documentó un proceso científico para identificar por medio de las huellas dactilares, primero a los delincuentes y posteriormente, a todos.

Ya en el siglo pasado (parece que fue ayer) comenzamos a utilizar el iris para identificar a las personas, así como algunas técnicas de detección vascular (venas en dedos y manos), geométricos y más recientemente de voz, de rostro o hasta de ADN (ácido desoxirribonucleico), convirtiendo datos originalmente analógicos en datos digitales que son utilizados en un sinnúmero de maneras.

¿QUÉ BENEFICIOS NOS TRAE LA TECNOLOGÍA BIOMÉTRICA?

Básicamente se trata de comodidad sin esfuerzo (y en algunos casos, por vanidad), automatización de procesos y manejo masivo de información. Uno de los usos más comunes hoy, es para acceder a algunas instalaciones sin necesidad de poner a un guardia que me identifique en la puerta, tener que presentar documentos o de portar llaves, tarjetas o memorizar claves de acceso (que tradicionalmente hay que digitar en un tablero y que, pocos o nadie quiere tocar, algo que haya sido usado por alguien más que no conozco y que podría ser vector de contagio de algún virus o bacteria), agregando o reemplazando básicamente la suma de factores de autenticidad verificando de manera automatizada y existente en una base de datos, algo que yo tengo, algo que yo sé y algo que la organización sabe, con algo que yo soy.

La biometría llegó para quedarse y la hemos usado de una u otra manera al menos desde el siglo XIV, según cuenta el explorador y escritor portugués João de Barros, describiendo que los chinos estampaban las palmas de las manos en papel con tinta y los comerciantes usaban esa técnica para distinguir a los jóvenes

Otro de los usos actuales, es la de poder reconocer a personas de interés sin la necesidad de que éstas se identifiquen voluntariamente. Ya sean clientes frecuentes de algún negocio vinculando su identidad a estadísticas de consumo como a usuarios de servicios en cajeros automáticos o personas no deseadas por algún antecedente, en teoría con la intención de mitigar algún riesgo, agilizar cruces fronterizos, el acceso a algún evento masivo o exclusivo, el abordaje a un avión hasta encontrar entre multitudes a personas presuntamente extraviadas usando los sistemas de videovigilancia, ya sean públicos o privados.

Llevamos años registrando nuestros datos en todos lados, ya sea para realizar trámites bancarios, para adquirir beneficios de los programas de lealtad en los comercios, sacando nuestras cédulas de identificación, licencias para conducir, dar de alta a nuestros hijos en la escuela y poder obtener después sus certificados de estudios y etiquetando a nuestros familiares y amigos en las fotos que subimos a redes sociales, sólo por mencionar algunos sitios y algunas razones y si no queremos ser identificados, pues no usaremos el banco o nos darán descuentos, no tendremos participación en redes sociales, tampoco conduciremos un automóvil, viajaremos al extranjero ni ejerceremos nuestro derecho al voto, es más, no usaríamos el celular para acceder a nuestras aplicaciones más comunes.

Y ENTONCES, ¿DÓNDE ESTÁN LOS RIESGOS?

Por un lado tenemos la preocupación de que la biometría pueda ser utilizada para disminuir las libertades personales de los ciudadanos, tal como hemos visto en algunos reportajes y artículos sobre el concepto del crédito social (y en muchas películas) y que suena aterrador, ya que nadie quiere que el gobierno de donde sea, ni los grupos delincuenciales o particulares sin nuestro conocimiento y autorización, utilicen estas tecnologías que están en todos lados y que tienen el potencial para permitir el acceso a información personal.

Por otro lado, tenemos que toda esta información forma ya parte de alguna o algunas bases de datos y que como ya ha sucedido, pueden ser robados como las contraseñas y tarjetas de crédito de alguna empresa de juegos en línea, los datos de pago de clientes de alguna cadena hotelera o el robo de contraseñas de sitios famosos y necesarios para nuestros nuevos estilos de vida digitales.

Violar el sistema y robar datos no protegidos de manera efectiva es una realidad, pero afortunadamente un buen hábito hablando de bases de datos, puedo (y debo) cambiar NIPs (Número de Identificación Personal), plásticos y contraseñas periódicamente y mantener alguna seguridad en el manejo de mi información, pero… ¿Cómo hago para cambiar mi rostro, mi iris o mis huellas dactilares? ¡No puedo!

Supongamos que mi rostro es utilizado para darle personalidad a alguien más y abusar de mi reputación, o que alguien cambia el nombre asociado a un registro de control de acceso… es decir, que clonen mi identidad y que con ella soliciten fraudulentamente créditos en mi nombre, o que puedan ser "confundidos" conmigo y les permitan el acceso a alguna instalación, cruzar alguna frontera o que me detengan equivocadamente, porque el sistema de identificación arrojó mi nombre como presunto sospechoso de algún crimen.

¿Crees que he leído muchas novelas o visto demasiadas películas de ciencia ficción? Pues no… sin los controles y regulaciones adecuadas y usando tecnologías inseguras, esto y mucho más es posible. Entonces tenemos que la invasión a la privacidad, el robo de información, la suplantación de identidad, la comisión de fraudes, abusos a los derechos humanos por temas de apariencia y discriminación étnica o de género, el control con base en el comportamiento de la población, etc., son amenazas reales, pero ¿puedo detener el cambio? No… ¿Puedo salirme del sistema? Tampoco… ¿Ya les dio miedo? ¿Qué podemos hacer para mitigar los riesgos que estas amenazas representan? El uso de máscaras de privacidad en los sistemas de videovigilancia, la anonimización de metadatos estadísticos, la actualización de la legislación local, el diseño seguro de los equipos conectados a la red para impedir los accesos "por la puerta trasera" a redes, equipos y datos, evitar el envío de información a terceros no autorizados, el resguardo de la integridad del *firmware* de los equipos utilizados, el cifrado de información, políticas adecuadas en el uso de tecnología, la supervisión de usuarios y la capacitación constante, son algunas recomendaciones básicas.

¿Quieres saber más? ¡Nos vemos en ALAS! Aquí convergemos fabricantes, distribuidores, integradores, *resellers*, instaladores, prestadores de servicio, consultores y usuarios de tecnología para la seguridad electrónica y nos reunimos para capacitarnos, debatir sobre las mejores prácticas y compartir experiencias. ■

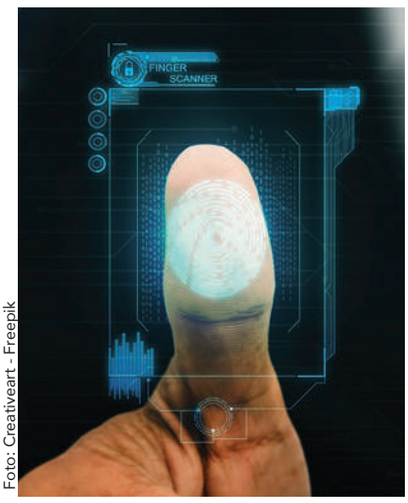


Foto: Creativeart - Freepik

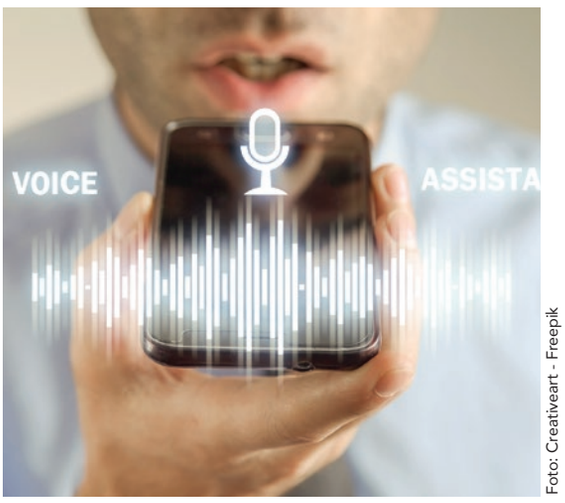


Foto: Creativeart - Freepik

LAS 4 SOLUCIONES DE SEGURIDAD FÍSICA IMPRESCINDIBLES EN INSTITUCIONES BANCARIAS

Los bancos se encuentran en permanente actualización, por lo que apuestan constantemente por la adopción de soluciones tecnológicas que complementen aquellas con las que ya cuentan

MÉXICO | César Arturo Santillán García

La evolución tecnológica de la que hemos sido testigos estos últimos años nos ha brindado múltiples beneficios, especialmente en el entorno bancario. Un claro ejemplo de esto es que hoy en día ya no necesitamos acudir a una sucursal bancaria para realizar operaciones cotidianas, y si necesitamos ir a alguna, podemos hacer transacciones a través de cajeros automáticos que antes sólo se podían realizar con ayuda del personal bancario.

Es por esta razón que, según información de un estudio de la Federación Latinoamericana de Bancos (Felaban), el 98.5% de los riesgos bancarios en América Latina y el Caribe son digitales o informáticos. No obstante, el 1.5% restante que incluye robos en oficinas bancarias y asaltos a mano armada, es un porcentaje de riesgos que deben ser atendidos de manera obligada.

BREVE RECORRIDO HISTÓRICO

Seguramente muchos de ustedes todavía recuerdan cómo era la seguridad bancaria hace algunas décadas; una seguridad enfocada en proteger solamente cajas fuertes y el efectivo que manipulaba el personal de las instituciones bancarias.

En este contexto, al suscitarse algún incidente en el interior de las instalaciones no se podía hacer mucho más que apostar por la eficiencia del personal de seguridad privada para proteger la integridad de las personas. En cuanto al registro de las operaciones bancarias, sólo se podía confiar en la pericia del personal a cargo que realizaba de manera manual los movimientos de retiro y despacho del efectivo.

Sin embargo, con el paso de los años se fueron incorporando nuevos elementos de seguridad en diversas sucursales bancarias, como ventanillas blindadas para la protección del personal y, en menor medida, sistemas de videovigilancia, considerándose pioneras en la industria aquellas instituciones que adoptaron aquellos primeros sistemas analógicos.

Ya en la década de los 90, se sumaron a los sistemas de seguridad bancaria de la época las ahora famosas esclusas, las cuales consisten en un sistema de doble puerta que, al no abrirse de manera simultánea, generaba mayor tranquilidad a los usuarios y mayor resistencia por parte de los delincuentes al intentar ejecutar un atraco.

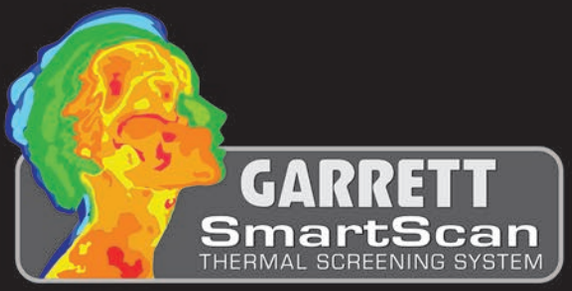
SISTEMA DE SEGURIDAD BANCARIA EN LA ACTUALIDAD

Hoy en día, por la naturaleza de sus operaciones y debido a la gran cantidad de personas que circulan en el interior de sus instalaciones (clientes, personal, proveedores de servicios), estas entidades financieras conforman un sector que exige altos niveles de seguridad y controles de acceso totalmente personalizados y bien definidos, para lo que requieren la implementación de soluciones tecnológicas que se adapten a sus procesos operativos y administrativos,

LA NUEVA

ELECCIÓN INTELIGENTE

PARA DETECCIÓN DE METALES Y CONTROL DE SEGURIDAD SIMULTÁNEOS



Ventajas del SmartScan™

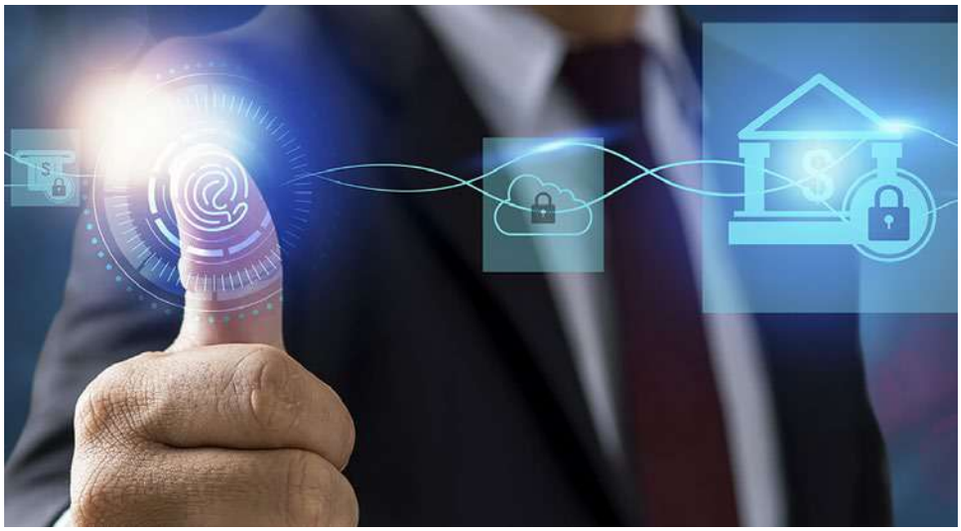
- Detección de temperatura rápida y económica tomada durante la operación de cribado normal
- No ralentiza el proceso de selección existente
- Funciona con pilas para facilitar su uso
- Opciones de alarma visual y audible
- Actualizable en campo para cualquier PD 6500i o MZ 6100 con conexiones simples

GARRETT®
METAL DETECTORS

MADE IN THE USA

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

For more info: https://info.garrett.com/garrett-metal-detectors-smartscan



que respondan a sus necesidades particulares y que garanticen altos niveles de eficacia.

Generalmente, los bancos se encuentran delimitados por zonas específicas:

- **Zona de servicio libre:** espacio donde los clientes acceden de manera individual a los servicios del sistema financiero (cajeros automáticos).
- **Zona de espacio comercial:** espacio donde interactúan los clientes y el personal de la sucursal bancaria (ventanillas y cubículos).
- **Zona de resguardo o suministro de dinero:** espacio donde se almacena, protege y dispone el dinero en efectivo de los clientes (bóvedas).

Las particularidades y propósitos de cada una de estas zonas definen las soluciones de seguridad que requieren. En otras palabras, el diseño, suministro e integración de una solución tecnológica de seguridad debe responder a los objetivos específicos de la zona donde vaya a ser implementada, facilitando y garantizando la continuidad de las operaciones realizadas en el interior de las entidades financieras.

El diseño, suministro e integración de una solución tecnológica de seguridad debe responder a los objetivos específicos de la zona donde vaya a ser implementada, facilitando y garantizando la continuidad de las operaciones realizadas en el interior de las entidades financieras

SOLUCIONES DE SEGURIDAD FÍSICA INDISPENSABLES EN BANCOS

Estas son algunas de las soluciones tecnológicas fundamentales que requiere una sucursal bancaria para proteger la integridad de las personas y bienes que se encuentran en su interior:

- **Videovigilancia:** la implementación de un sistema de CCTV que cubra todas las áreas posibles de una sucursal bancaria permite monitorear, identificar y reaccionar ante diversas situaciones de riesgo que sucedan en su interior. Además, los sistemas con capacidad de analíticos permiten identificar el tipo de personas que ingresan a las instalaciones, la frecuencia con la que lo hacen y los movimientos que realizan.
- **Protección contra incendios:** estos sistemas son obligados en cualquier entidad financiera para la protección de su personal, clientes y bienes, ya que permiten la detección, alertamiento y supresión de conatos de incendio, para lo cual necesitan implementar tanto sistemas activos como sistemas pasivos.
- **Gestión de identidad y control de accesos:** la integración de un sistema de gestión de identidad con un sistema de control de accesos permite mantener mayor control sobre las personas que circulan en el interior de las instalaciones, limitando o concediéndoles acceso a las diferentes áreas de la sucursal a través de un proceso de identificación.
- **Biometría:** aunque su principal finalidad es garantizar la seguridad de los usuarios y de su capital ante intentos de robo de identidad, en tiempos de pandemia la tecnología biométrica sin contacto (*contactless*) ofrece una gran ventaja al reducir los puntos de contacto dentro de un espacio cerrado y al permitir el reconocimiento de personas, incluso cuando porten cubrebocas, para fines de control de accesos. No obstante, las soluciones biométricas son utilizadas con distintos propósitos en el sistema financiero gracias al alto nivel de confiabilidad que ofrecen.

En resumen, las sucursales bancarias han potencializado sus sistemas de seguridad de manera importante al adoptar e implementar soluciones tecnológicas que generan experiencias seguras y satisfactorias para sus usuarios. Así mismo, dichas entidades se encuentran en permanente actualización, por lo que apuestan constantemente por la adopción de soluciones tecnológicas que complementen aquellas con las que ya cuentan.

SOLUCIONES A LA MEDIDA

En SISSA Monitoring Integral no sólo ofrecemos servicios de integración de soluciones tecnológicas que responden a las necesidades particulares del sistema financiero, sino que también brindamos consultorías y ofrecemos nuestra experiencia, conocimientos y buenas prácticas en el mundo de la seguridad electrónica para el desarrollo, uso e implementación de soluciones diseñadas a la medida que cumplan los objetivos específicos de cada cliente. ■

Fotos: SISSA Monitoring Integral

César Arturo Santillán García,
Presales Manager en SISSA Monitoring Integral.

Más sobre el autor:

Lo suficientemente pequeña como para accesar
sus mayores vulnerabilidades.

Es mucho más que solo una llave.

Una llave física es la herramienta de seguridad más utilizada.
Pero sin una manera de administrar y monitorear adecuadamente su uso,
una clave puede convertirse rápidamente en una responsabilidad
que pone en riesgo su instalación, personal y propiedad.

Explore una forma más inteligente de proteger, administrar y auditar
los activos críticos para su negocio enviando
un correo electrónico a nuestros expertos en sales@trakausa.com.

traka

ASSA ABLOY

traka.com | 1-407-681-4001

Las soluciones inteligentes para la gestión de llaves reportan beneficios para las compañías, los empleados y los clientes por igual, pues mejoran la seguridad, fortalecen las políticas de rendición de cuentas y reducen el riesgo de demandas por responsabilidad civil

COMPRENDER EL PAPEL DE LA GESTIÓN DE LLAVES EN LOS NEGOCIOS

EUA | Danny Garrido

Las empresas hacen todo lo posible por incorporar cada vez más niveles de seguridad que les permitan proteger a sus empleados, clientes y organizaciones. De hecho, según informes elaborados por Infosec, las compañías gastan en promedio alrededor de 2.84 dólares por mil dólares en ingresos, o alrededor del 0.03% de su presupuesto anual, en medidas de seguridad para sus negocios. Antes de la pandemia, 62% de las compañías entrevistadas afirmaron que aumentarían su gasto en seguridad en un promedio que oscilaba entre 250 mil y un millón de dólares al año.

Las precauciones en las áreas de control de acceso, videovigilancia, protección contra incendios y ciberseguridad suelen encabezar la lista de prioridades. En contraste, la custodia de las llaves físicas y de los dispositivos utilizados por los empleados a menudo no se tiene en cuenta como un componente fundamental de la seguridad.

Las soluciones inteligentes para la gestión de llaves reducen el riesgo de demandas de responsabilidad civil al proporcionar una cadena de custodia completa para todas las llaves durante las 24 horas del día, los siete días de la semana

Esto se debe a que las organizaciones tratan cosas como las llaves físicas o las tarjetas de acceso como meras llaves. En consecuencia, la mayoría de estas empresas no las incluyen en sus programas de seguridad.

La seguridad de las llaves físicas y la gestión de dispositivos debe ser una prioridad; no necesariamente por el valor de las llaves o los activos en sí mismos, sino porque aquello a lo que la llave o el activo brinda acceso o la acción que permiten realizar es lo más valioso y puede implicar un enorme riesgo para una organización.

AHORRE TIEMPO Y DINERO Y PROTEJA SU REPUTACIÓN

Muchas veces, sólo se dimensiona realmente la importancia de las llaves y los equipos cuando una emergencia hace necesaria una reacción. Un sistema de llaves maestras para cambiar las cerraduras en los puntos de acceso de una instalación podría costar cientos de miles de dólares, además de tiempo y daños a la reputación.

Tomemos como ejemplo la industria de la construcción. Las herramientas a las que no se hace seguimiento y los robos en las obras, sólo en los Estados Unidos, cuestan a las empresas de construcción casi mil millones de dólares al año, según informes del Registro Nacional de Equipos (NER). Además, los trabajadores aseguran haber pasado más del 47% de su tiempo buscando las herramientas adecuadas cada día. Esa

es una ineficiencia significativa que un sistema de gestión de llaves y activos podría fácilmente ayudar a subsanar, al reducir el tiempo de inactividad y aumentar la productividad.

De hecho, los casilleros que forman parte de un sistema de gestión de llaves no sólo permiten hacer seguimiento de activos esenciales —por ejemplo, en el caso de la construcción, las empresas de servicios públicos o la minería—, sino que además pueden conectarse en red para rastrear quién accedió por última vez a los equipos, cuánto tiempo los tuvo en su poder e informar sobre equipos defectuosos.

Esto supone un nivel adicional de prevención de costos por demandas de responsabilidad civil y ofrece mayor seguridad a los usuarios. Además, un sistema de casilleros puede cargar la batería de los equipos y utilizar un proceso de entrega en el que se liberan en principio aquellos que ingresaron primero a los casilleros, garantizando así que sólo se utilicen los equipos que estén mejor acondicionados para una tarea.

¿Qué hay de activos extraviados, como computadores portátiles? Los dispositivos electrónicos, como computadores portátiles o tabletas, contienen información confidencial de las compañías y de los clientes que, en caso de pérdida, robo o daño, va más allá del valor monetario. Las filtraciones de información de las compañías, los datos confidenciales de los clientes y los registros de los empleados no sólo pueden costar miles de millones de dólares en litigios, sino que además pueden acabar con una empresa.

Todo se puede echar por la borda: los empleos de los trabajadores, la confianza de los grupos de interés, la garantía de los consumidores. En el caso de los hospitales, los hoteles y las universidades, una tarjeta de acceso extraviada o mal utilizada puede aumentar el riesgo de una organización de sufrir daños o robos en los inmuebles, e incluso poner a una persona en una situación de mayor riesgo de ser agredida, o incluso de cosas peores.

Las soluciones inteligentes para la gestión de llaves reducen el riesgo de demandas de responsabilidad civil al proporcionar una cadena de custodia completa para todas las llaves durante las 24 horas del día, los siete días de la semana. Las empresas que utilizan sistemas inteligentes de gestión de llaves conocen la ubicación de cada una, la hora en que se utilizó por última vez y la última persona que accedió a ella. Este conocimiento permite responder con confianza y de manera adecuada a diversos problemas frecuentes relacionados con las llaves. Por ejemplo, es frecuente que los gerentes de hoteles interactúen con huéspedes que creen que algo fue robado de su habitación.

En estas situaciones, los huéspedes suelen acusar al personal de limpieza de hurto y quieren que el hotel asuma la responsabilidad de las pérdidas.

Si bien el empleado del hotel puede no ser el culpable, a falta de pruebas contundentes, esta situación puede dar lugar a una estresante batalla jurídica. Los administradores de instalaciones hoteleras que utilizan soluciones de gestión de llaves pueden generar rápidamente informes que ayuden a resolver acusaciones, mantener la confianza de los huéspedes, proteger a los empleados y, al mismo tiempo, obligarlos a rendir cuentas y evitar onerosos costos judiciales.

TRANQUILIDAD PARA LOS ADMINISTRADORES DE INMUEBLES, EMPLEADOS E INQUILINOS

Incorporar e integrar la gestión de llaves y de activos en la red de seguridad de su organización y en los procedimientos de las instalaciones preserva la integridad de las llaves físicas y de los valiosos activos a los que brindan acceso, con cambios mínimos y sin problemas en sus procesos diarios.

De hecho, en la mayoría de los casos su organización puede hacerse más eficiente y usted puede tener más tiempo para concentrarse en otras áreas de sus instalaciones donde pueda generar mayores ingresos. Las soluciones inteligentes de gestión de llaves reportan beneficios para los gerentes comerciales, empleados y clientes por igual, pues mejoran la seguridad, fortalecen las políticas de rendición de cuentas y reducen los costos innecesarios. Estos resultados hacen que aquellas compañías que utilizan soluciones inteligentes para la gestión de llaves sean muy atractivas para la inversión en el competitivo mercado actual. ■

Fotos: Traka

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

Más sobre el autor:

USO DE TECNOLOGÍA EN SEGURIDAD FÍSICA: CAJAS FUERTES

La tecnología puede sustituir a las personas en tareas que son repetitivas y rutinarias sin ningún problema, permitiendo liberar al talento humano de las tareas operativas para enfocarse en otras actividades

Foto: Creativeart - Freepik

PERÚ | Juan Carlos Portilla Gómez

TECNOLOGÍA EN TODAS PARTES

La tecnología ha venido a instalarse en todos los niveles, se han adaptado a los hogares, para controlar tu televisión o lavadora desde tu celular, al mundo laboral, con los controles por reconocimiento facial o acceso a tu PC por huella digital o comandos de voz, a los sectores productivos, con los sistemas SCADA (Supervisory Control And Data Acquisition) que permiten controlar y supervisar procesos industriales a distancia, en el sector de servicios como hacer pedidos a través de aplicaciones o pagar el autobús con una tarjeta, también se han ido incorporando a las instituciones y organismos locales que protegen la seguridad de los ciudadanos, como los sistemas de seguridad y de videovigilancia.

Adicionalmente desde hace un tiempo ya se hablaba de la transformación digital, términos como RPA (Robotic Process Automation), *Inteligencia Artificial (IA), Machine Learning, Chatbots, Big Data*, etc., eran bastante común oírlos o encontrarlos en las redes. ¿Su propósito? Lograr la automatización de los procesos operativos y repetitivos con la finalidad de aumentar la eficiencia en sus servicios, de esta forma mejora la experiencia de sus clientes para que obtengan un provecho de sus ofertas y ventajas competitivas.

UNA PANDEMIA INESPERADA

La llegada de la pandemia por el COVID-19 continúa trayendo nuevos retos para las empresas en todos los sectores, y no sólo al exterior de sus organizaciones como: clientes, proveedores y el mismo mercado; sino también a la interna misma: con nuevas formas de trabajar, coordinar y delegar funciones, entre otras actividades.

Esto ha desencadenado, por ejemplo, que los bancos, aceleren su proceso de transformación digital con la finalidad de encontrar o idear nuevas soluciones que les permitan mantenerse vigentes para lo que hoy llamamos la "nueva normalidad", la cual significa adaptarse de la mejor manera, y por lo tanto, evolucionar en sus áreas y del talento humano que la conforman.

Podemos entonces asegurar que la tecnología se ha convertido en una herramienta importante para la supervivencia de una empresa.

> En nuestro sistema financiero, desde sus inicios y hasta la actualidad aún mantienen el manejo tradicional en la operación con el efectivo en las cajas fuertes, el cual consiste en la dualidad física (dos personas) para su apertura

¿Por qué viajar para trabajar si existe CLOUD?

Los días de estar supeditado a una PC para la programación del sistema de entrada quedaron en el pasado.

Súmate a la vía rápida con el Cloud Account Manager, la programación más avanzada disponible. Ahora el sistema de entrada a tu cuenta se logra desde cualquier computadora, tableta o teléfono inteligente con conexión a Internet— y esto es perfecto para equipos de gestión remota. Disponible con los confiables servicios de conexión digital a Internet y celular de DKS, navegarás por tu control de acceso sin el estrés de los problemas de la PC y las sobreescrituras de datos-- ¡o los traslados!

DKS DOORKING®

HECHO EN EE.UU

ENCUENTRE SU SOLUCIÓN EN
doorking.com/nocommute

BANCOS: PROCESO TRADICIONAL DEL EFECTIVO

En nuestro sistema financiero, desde sus inicios y hasta la actualidad aún mantienen el manejo tradicional en la operación con el efectivo en las cajas fuertes, el cual consiste en la dualidad física (dos personas) para su apertura.

Este es uno de los procesos operativos que aún lo utilizan muchos bancos, los funcionarios que tengan bajo su responsabilidad el manejo de estos elementos, tienen claves asignadas las cuales son personales e intransferibles, ellos son los únicos responsables de administrarlas.

Estas claves son asignadas por la entidad financiera, por lo que cada vez que se requiera la apertura de la caja fuerte o bóveda estas dos personas deben encontrase presentes físicamente.

Esta forma de operar demanda el uso horas/hombre para la apertura de la caja fuerte y los clientes deben esperar entre 10 y 15 minutos en promedio.

APERTURA REMOTA DE CAJAS FUERTES

La problemática del uso horas/hombres para el manejo tradicional del efectivo también es una oportunidad de mejora para lograr una ventaja competitiva, ya que podemos plantearnos implementar un sistema que se encargue de esa operación, con igual o mejores niveles de seguridad y que el recurso humano liberado se enfoque en otros campos del negocio.

La problemática del uso horas/hombres para el manejo tradicional del efectivo también es una oportunidad de mejora para lograr una ventaja competitiva, ya que podemos plantearnos implementar un sistema que se encargue de esa operación, con igual o mejores niveles de seguridad

Con las técnicas de integración de *software* (que se encarga de hacer las validaciones de las credenciales de los usuarios, manejos de los tiempos de retardo, almacenar los *logs* de eventos, etc.) y *hardware* (sistemas de alarmas, cerraduras de alta seguridad, PLC —Programable Logic Controllers—, etc.) se pueden automatizar procesos en el manejo de efectivo dentro del entorno financiero. Este concepto se conoce como Sistema de Dualidad Remota (SDR), y es una forma de valorar el uso de tecnología en el desarrollo de las actividades financieras.

La tecnología puede sustituir a las personas en tareas que son repetitivas y rutinarias sin ningún problema, esto ya no debe causarnos sorpresa, se han ahorrado muchas horas de trabajo manual, permitiendo liberar al talento humano de las tareas operativas para enfocarse en las actividades que son el '*core*' del negocio.

No queda ya ninguna duda de que el uso de la tecnología permite automatizar procesos que eran muy tradicionales y está empezando a reemplazar categóricamente a los sistemas antiguos, impulsado un proceso de transformación necesario, creciente e imparable. ■

Foto: Creativeart - Freepik

Juan Carlos Portilla Gómez,
consultor en Seguridad Electrónica.

Más sobre el autor:

GRUPO EMPRESARIAL CASA

SEGURIDAD PRIVADA

PROFESIONALES DE LA SEGURIDAD A SU SERVICIO

CUSTODIA

INTRAMUROS

CONSULTORÍA

SEGURIDAD PRIVADA | INTRAMUROS

www.gecsa.com.mx

info@gecsa.com.mx

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

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

www.twitter.com/gecsa

www.facebook.com/gecsa

www.youtube.com/gecsa

Columna
WOMEN IN SECURITY

Ingrid Rébsamen Pradillo

Directora general del Consejo Nacional de la Industria de la Balística A.C.

Más sobre la autora:

BLINDAJE, LA MEJOR INVERSIÓN EN PREVENCIÓN

MÉXICO

Foto: Creativeart - Freepik

Cuando compras algún producto siempre ves opciones como calidad, precio, durabilidad, etc., ¿pero qué pasaría si quieres adquirir un producto que prevenga un riesgo, y ese riesgo sea tu vida y la de tu familia?

Las mujeres contamos con intuición, resistencia, resilencia, pero sobre todo tenemos la naturaleza y capacidad de protección, para protegernos a nosotras y a nuestra familia, buscamos prevenir riesgos, pero existen situaciones que no están en nuestras manos, como es la delincuencia, el crimen organizado y la inseguridad.

El blindaje es una opción, pero sobre todo es una solución de protección a nuestros bienes y lo más importante: una protección a nuestra vida contra armas de fuego utilizadas por aquellos delincuentes. Por ello derivado de la conciencia de prevención más que la de reacción, la industria del blindaje crece.

PERO, ¿QUÉ ES EL BLINDAJE?

Lo definimos como el conjunto de materiales balísticos (opacos y transparentes) que cuentan con diversas certificaciones de laboratorios reconocidos y los cuales al instalarse correctamente sirven para impedir la penetración de impactos y/o proyectiles balísticos de diversos calibres.

Es importante que el usuario conozca que dentro del blindaje existen distintas modalidades como son:

- Blindaje automotriz.
- Blindaje táctico.
- Blindaje corporal.
- Blindaje arquitectónico.
- Fabricantes y comercializadores de materiales balísticos.
- Fabricantes de vidrios blindados.

Además de conocer qué es un blindaje, el usuario antes de adquirir un producto blindado tiene que saber cuáles son sus verdaderas necesidades de protección, como lo son: anti asalto urbano, anti secuestro, o si se requiere

para un anti atentado. Con ello la empresa de blindaje te brindará la protección necesaria.

También no ignorar detalles al momento de adquirir un producto blindado de la empresa de su elección, ya que pueden marcar una gran diferencia en nuestra seguridad:

- Visita a la planta para conocer sus procesos.
- Manual de uso.
- Cuidados de sus productos blindados.
- Garantías.
- Caducidad de su blindaje (que las empresas expliquen al usuario cómo funciona el producto que adquiere y cuánto tiempo tiene de vida útil porque también pierden su efectividad con el paso del tiempo y en la industria del blindaje esto no se puede pasar por alto).

La industria del blindaje en México realmente es altamente calificada, no necesitamos forsozamente adquirir productos de otros países pensando que en México no los fabrican, en nuestro país es importante mencionar que nos distinguimos en desarrollo y fabricación de materiales para el blindaje de la más alta calidad, para cumplir con la creciente y exigente demanda a nivel nacional, al igual que de exportación tanto de materiales como de blindajes terminados para diversas partes del mundo.

MENOS ES MÁS

Siempre pensamos que teniendo más producto tenemos mayor calidad, pero es importante conocer que no se necesita un acero tan grueso, o tantas capas de aramida para estar protegidos, ya que existen nuevos materiales más ligeros y resistentes que dan la misma o mayor protección.

Foto: Creativeart - Freepik

Es muy importante quitar el paradigma de que el blindaje es sólo para un sector económico en especial o sólo de uso masculino tanto personal, policial o militar, ya que hay profesionistas, ejecutivas, empresarias, mujeres en las fuerzas policiales y guardias de seguridad que buscan soluciones más femeninas, ergonómicas que se ajustan a su figura y que además les proporcione toda la protección que necesitan, por ello empresas de blindaje hoy en día ya lo ofrecen.

Lamentablemente existen empresas que aprovechando el desconocimiento del cliente no le ofrecen la protección adecuada y necesaria y en algunas ocasiones les realizan trabajos parciales poniendo en riesgo la vida del usuario.

Como expertos y profesionales de seguridad definimos un trabajo parcial como: la falta de protección balística total en el habitáculo del vehículo, por lo que al no estar cubiertas todas las áreas de riesgo tanto en las zonas opacas (parte donde se ve metal), así como en las zonas transparentes (vidrios) ponen en riesgo la vida del usuario ante un siniestro.

En la industria del blindaje nuestro principal interés es que las empresas legalmente establecidas y reguladas por la autoridad, puedan seguir ofreciendo a sus clientes los blindajes de la más alta calidad, innovación y tecnología balística en un entorno de total ética profesional y estricto apego a la normatividad.

> Además de conocer qué es un blindaje, el usuario antes de adquirir un producto blindado tiene que saber cuáles son sus verdaderas necesidades de protección, como lo son: anti asalto urbano, anti secuestro, o si se requiere para un anti atentado

¿CUÁL ES LA AUTORIDAD QUE REGULA A LAS EMPRESAS DE BLINDAJE?

La Dirección General de Seguridad Privada dependiente de la Secretaría de Seguridad y Protección Ciudadana. Es necesario conocer que las empresas de blindaje también ofrecen soluciones y además desarrollan proyectos especiales de acuerdo a las continuas necesidades de protección, por ello es una inversión que tenemos que considerar, ya que estamos expuestos todos los días, tanto en casa, oficina, negocio, en tu propio vehículo, en la calle; porque así como los expertos en seguridad van innovandose y profesionalizandose, con certeza, la delincuencia también.

Es muy gratificante que hoy en día se sumen más mujeres al sector de la seguridad y que además son reconocidas por ser grandes expertas que contribuyen para tener un México más seguro.

Mi objetivo es seguir contribuyendo en pro de la seguridad y del blindaje, y seguir promocionando a las grandes empresas que cumplen al 100% con los requerimientos, además de continuar con la difusión de recomendaciones para el usuario para que elija una empresa confiable, porque lo mas importante para nosotros es “salvaguardar vidas”. ■

BLINDAJE AUTOMOTRIZ: SEGURIDAD PARA EL REGRESO A CASA

Ante el incremento del robo con violencia tanto para el transporte de carga como para el tránsito cotidiano, el blindaje automotriz se ha convertido en una opción para resguardar la seguridad de sus usuarios, sobre todo por la reducción del peso en los vehículos, entre el 27% y 35%, lo que permite diversificar el mercado y ofrecer productos con tecnología a un menor costo

Foto: Creativeart - Freepik

"Tenemos más de 25 años en la industria del blindaje automotriz a nivel mundial, lo cual nos ha enseñado a tener una comunicación muy abierta con nuestros clientes, dependiendo de lo que buscan, su vulnerabilidad y la zona, se recomienda el tipo de vehículo o blindaje",
Mauricio Natale

MÉXICO | Mónica Ramos / *Staff* Seguridad en América

Con la llegada del virus COVID-19, la vida de las personas cambió, se modificaron hábitos, rutinas, empleos, poniendo en riesgo principalmente la salud de millones de personas y la economía del mundo en general. Pero hay acciones que no cambiaron, y una de ellas fue la inseguridad. En el caso de México, el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), informó que tan solo en los primeros cinco meses de este año, se registraron 5 mil 133 robos al transporte de carga, siendo el Estado de México y Veracruz los estados donde se concentraron la mitad de estos incidentes.

El incremento del robo con violencia al transporte de carga y vehículos privados, son los motivos por lo que la ciudadanía se está apoyando de herramientas de la seguridad que antes estaban fuera de su alcance económico y tecnológico, es decir, la industria del blindaje ha diversificado su mercado debido a la demanda de éstos y es por ello que ha adaptado sus soluciones y se encuentra en constante innovación.

De acuerdo a Daniel Portugal, tesorero y asesor del Consejo Nacional de la Industria Balística (CNB), cada vez hay más demanda de blindaje automotriz, por lo que durante la última década se han logrado reducciones de peso de entre el 27 % y el 35 por ciento, haciendo al blindaje más "ergonómico"[1].
Es por ello que **Seguridad en América** (**SEA**) entrevistó a cuatro expertos en el tema y quienes ofrecen distintas soluciones de blindaje para el mercado.

CITYSAFE: LIVIANO Y SEGURO

Mauricio Natale, director general de CitySafe Blindajes, nos compartió una retrospectiva sobre la importancia de la innovación tecnológica para coadyuvar en la diversificación del mercado de esta industria. "Hace 10 años en México no existía el nivel de blindaje antiasalto número II, entonces los clientes tenían que comprar el nivel III invirtiendo en una camioneta y el blindaje, entre un millón y medio de pesos (75 mil dólares) que probablemente no tenía y tampoco necesitaba tanta protección, entonces eso se convertía en una limitante. Hoy en día con menos de un millón de pesos (50 mil dólares), una persona puede comprar un auto con blindaje", comentó.

Continuando con este análisis, el poder ofrecer un blindaje más económico favorece a que más personas puedan acceder hoy en día a un buen blindaje, el cual también puede ser instalado en su coche de uso diario y esto favorece al consumidor final. "Eso lo obtienes con CitySafe, con menos de 20 mil dólares ya obtienes una protección segura, legal y vehículos totalmente funcionales", explicó.

Resaltó que es muy importante subrayar que el blindaje es un trabajo altamente profesional y el cliente debe ser crítico y cuidadoso en la selección de empresas legales y con experiencia, ya que esto

"No es congruente pensar en vehículos blindados sin movilidad, por lo cual los dispositivos *runflat* deben formar parte de cualquier vehículo de seguridad o que transite en zonas de alto riesgo", **Gerardo Corona**

le garantiza obtener productos que lo protejan y le salven la vida.

"Desafortunamente hoy en día hay una subindustria no legal que ofrece productos sustitutos, que no sirven, engañan al cliente y dañan la reputación de las buenas empresas de blindaje que existen en el mercado mexicano", señaló.

Un mito sobre los vehículos blindados es que son muy pesados, costosos y se dañan. "En CitySafe hemos trabajando en estos aspectos, de hecho nuestro lema es 'liviano y seguro', porque entendimos que primero debíamos eliminar la idea de que un automóvil blindado es muy pesado. Lo que hicimos fue investigar en el mundo, la última tecnología de punta: materiales y fibras balísticas diferentes, ingeniería que nos permitiera diseñar vehículos blindados muy livianos. Hoy en día tenemos blindajes antiasalto nivel II, los cuales pesan 140 kilogramos, cubriendo todo el vehículo, es el peso de dos personas, en realidad no es un peso exagerado", explicó.

Actualmente la gente quiere blindar el auto que usa diario, y eso fue lo que CitySafe descubrió. "Nos dedicamos a desarrollar diferentes productos con distintos niveles de blindaje para cubrir todas las necesidades de los diferentes usuarios a los que va dirigido el producto. Tenemos más de 25 años en la industria del blindaje automotriz a nivel mundial, lo cual nos ha enseñado a tener una comunicación muy abierta con nuestros clientes, dependiendo de lo que buscan, su vulnerabilidad y la zona, se recomienda el tipo de vehículo o blindaje, es por eso que tenemos un 98% de satisfacción en nuestras encuestas de calidad a los clientes", señaló.

De acuerdo con el experto, a los vehículos convencionales se les puede instalar muy bien un blindaje nivel II o IIIA y tiene la capacidad motriz suficiente para poder desempeñarse sin ninguna limitante. Pero para los blindajes nivel IV-VI sí se utilizan materiales más pesados, de unos 600 kg o más, para esos casos se les asesora y recomienda que el tipo de vehículo tenga una potencia mecánica suficiente, que sea robusto en transmisión, frenos, etcétera.

Una característica de los servicios de esta firma es que dejó atrás la limitante en los cristales, ya que anteriormente con el blindaje del vehículo, éstos quedaban clausurados con el concepto de que por seguridad tenía que ser así, pero enfrentaba bastantes limitantes para su uso cotidiano que al final vulneraban la seguridad por la necesidad de abrir la puerta. "Es por eso que nuestro departamento de Ingeniería se dedicó a buscar tecnología para vidrios, la cual permitiera blindarlos con apertura al 100 por ciento, pero sí le hacemos la recomendación de mantener el auto cerrado en su totalidad, sin embargo ante una situación como pagar una caseta, o un estacionamiento en un centro comercial, esto es muy útil", puntualizó Mauricio Natale.

Ballistic Protection Levels
Test Summary - NIJ Standard 0108.01

Armor Type	Test Variable: Test Ammunition	Test Variable: Nominal Bullet Mass	Test Variable: Suggested Barrel Length	Performance Requirements: Required Bullet Velocity	Performance Requirements: Required Fair Hits per armor specimen	Performance Requirements: Permitted Penetrations
I	22 LRHV Lead	2.6 g 40 gr	15- 16.5 cm 6 - 6.5 in	320 ± 12 m/s 1050 ± 40 ft/s	5	0
	38 Special RN Lead	10.2 g 158 gr	15- 16.5 cm 6 - 6.5 in	259 ± 15 m/s 850 ± 50 ft/s		
II-A	357 Magnum JSP	102 g 158 gr	10 - 12 cm 4 - 4.75 in	381 ± 15 m/s 1250 ± 50 ft/s	5	0
	9 mm FMJ	2.6 g 40 gr	15- 16.5 cm 6 - 6.5 in	332 ± 12 m/s 1090 ± 40 ft/s		
II	357 Magnum JSP	10.2 g 158 gr	15 - 16.5 cm 6 - 6.5 in	425 ± 15 m/s 1395 ± 50 ft/s	5	0
	9 mm FMJ	8.0 g 124 gr	10 - 12 cm 4 - 4.75 in	358 ± 12 m/s 1175 ± 40 ft/s		
III-A	44 Magnum Lead SWC Gas Checked	15.55 g 240 gr	14 - 16cm 5.5 - 6.25in	426 ± 15 m/s 1400 ± 50 ft/s	5	0
	9 mm FMJ	8.0 g 124 gr	24 - 26 cm 9.5 - 10.25 in	426 ± 15 m/s 1400 ± 50 ft/s		
III	7.62 mm (308 Winchester) FMJ	9.7 g 150 gr	56 cm 22 in	838 ± 15 m/s 2750 ± 50 ft/s	5	0
IV	30-06 AP	10.8 g 166 gr	56 cm 22 in	868 ± 15 m/s 2850 ± 50 ft/s	5	0
Special Requirement	*	*	*	*	*	*

PRORESCUE MX: BLINDAJE AUTOMOTRIZ *PREMIUM*

Otra de las empresas que está inmersa en el mercado del blindaje automotriz es ProRescue MX, "somos un proveedor de insumos *premium* para el blindaje automotriz, el alto desempeño es la bandera de nuestras tres principales líneas: Flats Over®, insertos *runflats* a base del mismo material de las llantas comerciales; Optima Ballistic Glass®, cristales con resistencia balística y atri-

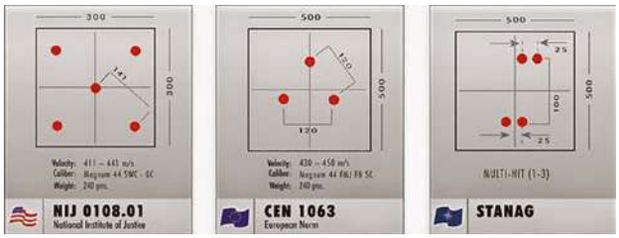


Foto: Creativeart - Freepik

butos ópticos excepcionales, y Kevlar® DuPont™ de Tejidos Especiales, un referente mundial de protección balística. Adicionalmente, tenemos una activa participación en la asesoría sobre los temas Seguridad Vehicular y Protección Ejecutiva", explicó Gerardo Corona, director general de ProRescue MX.

Tan importante es escoger el blindaje adecuado para el vehículo, como la persona que lo va a conducir, si pertenece a una empresa de seguridad privada, es importante que esté capacitado en manejo evasivo, protección ejecutiva, ya que de él dependerá en gran porcentaje la prevención de incidentes o en su caso la reacción inmediata y adecuada ante uno.

"El conductor de seguridad es un especialista de protección competente en el transporte oportuno y seguro de personas o carga valiosa, por lo cual no es ajeno al perfil que deberíamos encontrar en sus compañeros de seguridad ejecutiva; tales como: análisis de riesgos, inteligencia de protección, táctica con armas de fuego, primeros auxilios, control de la violencia, etiqueta y protocolo, entre muchas otras. A nivel preventivo, y además de la obvia actividad de manejo, el conductor de seguridad debe tener concentrada su gestión —por lo menos— en tres tareas: análisis y planificación de rutas, aseguramiento del performance vehicular e inteligencia de protección que a su vez incluye la detección de vigilancia", explicó Gerardo.

ProRescue MX ofrece los dispositivos *runflats*, estos son todos aquellos que permiten la movilidad cuando uno o más neumáticos no cuentan con presión de aire. "Los de mayor difusión y efectividad son los insertos y los neumáticos *runflat*, los primeros son aros ajustados al rin que evitan que las cejas del neumático se desprendan por no tener presión y a la vez brindan altura de rodamiento para evitar que el rin haga contacto con el pavimento, los insertos básicamente son de dos materiales: plásticos o caucho, y son obligatorios en vehículos blindados de niveles superiores (+BR5)", explicó.

Los insertos *runflat*, en especial los de caucho, pueden brindar capacidades de tracción y maniobrabilidad aún sin el neumático. Por otra parte, los fabricantes de llantas han colocado en el mercado sus opciones *runflat*, se trata de neumáticos con el doble o triple de densidad de material en los extremos, esto ayuda a soportar el peso del vehículo ante la ausencia total o parcial de aire al interior de la llanta, son recomendados para pequeñas perfora-

"Nuestro objetivo es expandirnos integrando más empresas que tengan la misma finalidad de 'salvaguardar vidas'", **René Rivera**

"El elemento clave en la validación de los procesos de Isoclima radica en el meticuloso cumplimiento de los estándares de calidad, avalados por certificaciones internacionales", **Jack Farji**

ciones en la banda de rodamiento y en los niveles iniciales de blindaje (-BR4). "No es congruente pensar en vehículos blindados sin movilidad, por lo cual los dispositivos *runflat* deben formar parte de cualquier vehículo de seguridad o que transite en zonas de alto riesgo", señaló Gerardo Corona.

ISOCLIMA: CALIDAD, DISEÑO Y GARANTÍA

En el blindaje automotriz son importantes cada una de las partes que lo conforman, incluyendo los cristales, empresas como Isoclima se han especializado en el desarrollo de vidrio balístico para este sector, el militar, gobierno y arquitectónico, así como soluciones de vidrio especial para el sector aeroespacial, trenes, naval, carros deportivos de lujo y carros de alta velocidad.

"Isoclima se estableció en 1977, en la provincia de Padua en el noreste de Italia. Su negocio principal en ese entonces, era ofrecer soluciones de vidrio para la industria de la construcción. Con la ambición y la innovación recorriendo nuestro ADN, pronto nos convertimos en líderes en el mercado del vidrio aislante y nos lanzamos a la investigación y el desarrollo de nuevas soluciones avanzadas de acristalamiento de alta tecnología que se destacaban por su excelente resistencia balística", comentó Jack Farji, Mexico & Latam *Sales Director*.

A lo largo de esos 40 años, la firma ha desarrollado productos como Omniarmor, Omnilite, Isolite, entre otros, y soluciones avanzadas y certificadas, adoptadas por algunas de las principales empresas del mundo, como Apple, Mercedes-Benz, Audi, Azimut-Benetti, San Lorenzo, BMW, Iveco IDV, Ferrari, Ferretti, McLaren, Leonardo, Airbus y por la policía más condecorada y Fuerzas de Defensa.

"El elemento clave en la validación de los procesos de Isoclima radica en el meticuloso cumplimiento de los estándares de calidad, avalados por certificaciones internacionales. El control minucioso y metódico de nuestros procesos y sistemas de fabricación, además de las inspecciones y pruebas de productos realizadas en nuestros laboratorios, le han otorgado a Isoclima las certificaciones internacionales más prestigiosas, lo que garantiza que nuestro sistema de gestión, diseño, fabricación e instalación es de primer nivel", puntualizó.

Marcas como FCA, Daimler, Mercedes-Benz, BMW, VW-Audi, han recurrido de forma frecuente a los productos de la firma quien tiene planta en Italia, Croacia y México, una de las características de sus productos y por lo cual es muy importante para el blindaje, es que cuentan con el mejor índice de delaminación a nivel mundial. Para las compañías blindadoras esto representa un gran ahorro al no tener producto defectuoso en garantía para cambio. Al cliente final le da una mayor seguridad balística, una mejor visibilidad y un mejor valor de reventa del vehículo.

CNB: LEGALIDAD Y CONFIANZA EN LA INDUSTRIA DEL BLINDAJE

Y como toda industria, el blindaje requiere de un órgano representativo, para ello se creó el Consejo Nacional de la Industria Balística (CNB), quien agrupa a las empresas más importantes de este sector especializadas en las siguientes áreas: blindaje de vehículos de uso civil y táctico, fabricantes de vidrios blindados, blindaje arquitectónico, corporal (chalecos, ropa y placas balísticas), así como también a los principales fabricantes y comercializadores de materiales balísticos.

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Foto: National Institute Justice

"Nuestra industria genera empleos directos e indirectos con mano de obra mexicana altamente capacitada y especializada, ofreciendo a nuestros clientes productos de la más alta calidad y constante desarrollo de efectivas e innovadoras tecnologías balísticas en un entorno de total ética profesional y estricto apego a las leyes vigentes que regulan nuestro sector, contribuyendo orgullosamente a mejorar los niveles de seguridad de nuestro país buscando siempre poner el nombre de México en el más alto nivel internacional", comentó René Fausto Rivera Arózqueta, presidente de la Comisión Ejecutiva del CNB.

Actualmente el CNB se integra por 10 empresas asociadas con participación en toda la república mexicana, así como en Colombia, Venezuela, Brasil, Estados Unidos, Francia, Suecia, entre otros países. "Nuestro objetivo es expandirnos integrando más empresas que tengan la misma finalidad 'salvaguardar vidas'", afirmó René.

Hoy en día con menos de un millón de pesos (50 mil dólares), una persona puede comprar un auto con blindaje

Beneficios de pertenecer al CNB:

- Apoyamos a que las empresas se encuentren legalmente establecidas y reguladas ante la autoridad, que cuenten con certificados y soluciones específicas, para que le ofrezcan a los usuarios siempre la verdad y oferta honesta de sus productos balísticos, y puedan seguir ofreciendo a sus clientes los productos de la más alta calidad para su seguridad.
- Efectuamos intercambio de información y opiniones que ayudan a mejorar la industria.
- Realizamos reuniones mensuales para compartir experiencias e inquietudes.
- Darles mayor fuerza a nuestras empresas asociadas, gestionando colaboraciones en conjunto para beneficio del sector ante instituciones y autoridades.
- Realizamos pruebas balísticas internas para seguir con la calidad que distinguen a nuestras empresas asociadas.
- Posicionamos los productos de nuestras empresas asociadas a través de comunicados y entrevistas con los medios más importantes, así como el fortalecimiento de la industria del blindaje.

Requisitos para afiliarse:

1. Tener su registro vigente ante la Dirección General de Seguridad Privada.
2. Desarrollar las actividades de la modalidad que se tiene registrada.
3. Utilizar siempre materiales certificados bajo la norma balística y que cuenten con estándares de calidad para salvaguardar la integridad de nuestros clientes.
4. No realizar blindajes parciales.
5. Cumplir a cabalidad el Código de Ética.
6. Las que determine el Consejo en beneficio de la industria del blindaje.
7. Contar con más de tres años de experiencia en la industria.
8. Formato de preguntas realizadas por la asociación.
9. Se realiza visita verificadora por parte de los miembros del CNB. ■

REFERENCIAS

[1] *"La industria mexicana del blindaje se diversifica por aumento de la violencia", Agencia EFE, 24/07/2021: https://www.efe.com/efe/usa/mexico/la-industria-mexicana-del-blindaje-se-diversifica-por-aumento-de-violencia/50000100-4593770*

PROGUARDIAS:
CALIDAD, ATENCIÓN Y PROFESIONALISMO

Con 20 años de experiencia en el sector, Proguardias, encabezada por Luis Norberto Barrañón, ofrece servicios de seguridad privada "hechos a la medida", con personal capacitado e integrando la tecnología más innovadora del mercado

MÉXICO

Erick Martínez y Mónica Ramos / *Staff* Seguridad en América

En el año de 1999 surgió la empresa de seguridad privada Protección Generalizada, S.A. de C.V., con sede en Monterrey, Nuevo León, y básicamente con servicios locales. Diez años después (2009), tres empresarios con amplia experiencia en el sector, vieron la oportunidad y adquirieron la empresa para darle continuidad y un mayor crecimiento obteniendo la parte de activos, es decir los guardias y los clientes.

"Al momento de la adquisición no perdimos ni un solo cliente, fue una labor de convencimiento con cada uno de ellos. Para mediados de 2010 hicimos el cambio total de nombre y de imagen. En ese momento teníamos alrededor de 400 guardias, hoy en día estamos arriba de los dos mil. También ampliamos la cobertura, en un principio teníamos presencia sólo en Nuevo León, un poco en Chihuahua y Tamaulipas. Hoy en día tenemos presencia en casi toda la república a excepción de la parte sureste", explicó Luis Norberto Barrañón Castillo, socio y director general de Proguardias.

Pese a la pandemia ocasionada por el virus COVID-19, la compañía siguió brindando los servicios y mantuvo su estabilidad financiera. De acuerdo con Norberto uno de los valores agregados de la empresa es que mantiene descentralizadas las operaciones, dividiendo el país en cuatro regiones activas: centro, noroeste, occidente y noreste.

OPERACIÓN EN 22 ESTADOS, ATENDIDOS POR 12 UNIDADES DE NEGOCIO

Occidente

Jalisco
Aguascalientes
Querétaro
Nayarit
Michoacán
Guanajuato
Colima

Noreste

Nuevo León (3)
Coahuila
Tamaulipas
San Luis Potosí
Durango
Zacatecas

Centro

Ciudad de México
Estado de México
Puebla
Tlaxcala
Veracruz
Morelos
Guerrero
Oaxaca

Noroeste

Chihuahua
Sonora
Tijuana
Baja California
Sinaloa

Protectio

Seguridad Logística

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

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

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

ESR EMPRESA SOCIALMENTE RESPONSABLE

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

COPARMEX CIUDAD DE MÉXICO

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

"La descentralización de las operaciones ha servido para que se tomen decisiones locales sin necesidad de que la dirección de operaciones le tenga que estar consultando a la dirección general. Así cada unidad de negocio sabe perfectamente cuáles son las necesidades de cada uno de nuestros clientes y de su gente, bajo ese esquema el entendimiento con el cliente es exitoso. Esta autonomía propicia cercanía con el cliente, lo cual nos ha mantenido con un buen prestigio a nivel nacional", señaló el empresario.

SERVICIOS PROGUARDIAS

1. Guardias de seguridad:
   - Guardias Patrimoniales.
   - Guardia Elite.
   - Patrullaje Operativo.
   - Custodia.
2. Tecnología:
   - Control de Accesos.
   - Circuito Cerrado de Televisión (CCTV).
   - GPS.
   - Alarmas.
3. Centro de monitoreo.
4. *Benchmarking*.
5. Consultoría e investigación.

Luis Norberto Barrañón

¿POR QUÉ PROGUARDIAS?

- Maneja unidades de negocio descentralizadas.
- Cuenta con un esquema de capacitación básico para el elemento y capacitación personalizada de acuerdo al cliente.
- Certificación BASC.
- Tiene un sistema interno de calidad.
- Elabora evaluaciones de riesgo a todos sus clientes, que a su vez se generan planes y análisis para eliminar esos factores de riesgo.

UNA EMPRESA LOCAL DE CLASE MUNDIAL

Con la experiencia de la Dirección General, la empresa ha adoptado la filosofía CAP: Calidad, Atención y Profesionalismo. Busca las soluciones tecnológicas y las estrategias de seguridad más innovadoras en el mercado y a nivel mundial, siendo la capacitación uno de los pilares para recomendar sus servicios y la constante evaluación no sólo de sus elementos, sino también de los riesgos a los que están expuestos sus clientes.

"Tenemos que estar al día, hacer *benchmarking* en todos los sentidos. Desde sueldos, empresas, cómo estamos posicionados, cuáles son las necesidades del mercado, hay que estar a la vanguardia para saber qué más tenemos qué hacer, qué más podemos hacer para darle un buen resultado al cliente. La tecnología es un complemento vital para el mejor desempeño de sus funciones, que más allá de que pueda sustituir a los guardias de seguridad privada, los va a complementar en sus labores", indicó Norberto.

Proguardias pertenece a la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), lo cual le da una mayor formalidad y alcance, también cuenta con las certificaciones en Business Alliance for Secure Commerce (BASC) y CONOCER (Consejo Nacional de Normalización y Certificación de Competencias Laborales) de la Secretaría de Educación Pública. Y dado que la capacitación es su principal aliado, ésta va desde los guardias, que es su principal activo, hasta el personal administrativo y por supuesto Gerencia y Dirección, todos con conocimientos en seguridad.

"Nuestros supervisores y ejecutivos todos son profesionistas y tienen alguna certificación netamente de seguridad. La capacitación es para todo el *staff*, contamos con diplomados, certificaciones, le invertimos mucho al tema de la capacitación, la tecnología y sobre todo al análisis de las necesidades que requieren nuestros clientes, la cercanía con ellos es lo que ha favorecido al crecimiento y estabilidad de la empresa. Uno de nuestros objetivos es tratar de exceder el requerimiento del cliente para tener un nivel óptimo con él", finalizó el también socio consejero de la AMESP. ■

PEMSA
SISTEMAS DE SEGURIDAD PRIVADA

EVOLUCIONA la SEGURIDAD de tu HOGAR y NEGOCIO al SIGUIENTE NIVEL

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

222 141 12 30

WWW.PEM-SA.COM

gerenciacomer@pem-sa.com

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

No. CERTIFICADO: SG20211485

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD ALAS

SOCIO ACTIVO

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

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

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

RODOLFO CEPEDA, SEGURIDAD INTEGRAL DE COLOMBIA PARA MÉXICO

Egresado de la Maestría en Seguridad Integral impartida por la EPFAC, Rodolfo Cepeda aplica sus conocimientos y experiencia para crear soluciones eficientes y precisas para el transporte de carga a través de la empresa que lidera: REC Servicios Consultores

MÉXICO

Erick Martínez y Mónica Ramos / *Staff* Seguridad en América

Rodolfo Cepeda Rico, presidente de la firma REC Servicios Consultores, es el primer mexicano que cursó y egresó de la Maestría en Dirección y Gestión de la Seguridad Integral impartida por la Escuela de Postgrados de la Fuerza Aérea Colombiana (EPFAC), combinando su profesionalización en el extranjero con las necesidades en materia de seguridad que tienen los diferentes procesos de la cadena de suministro en México.

"La experiencia de cursar la Maestría en la EPFAC ha sido increíble, el llevar estas materias nos permitió conocer de una forma muy diferente la seguridad a nivel integral, estábamos acostumbrados a manejarla (seguridad) desde la iniciativa privada, pero nunca habíamos tenido la experiencia ni la visión de cómo los gobiernos manejan la seguridad, todos los conceptos que toman en cuenta, toda la parte de la visión militar que es una forma muy diferente de ver las cosas en comparación con la seguridad privada", comentó el experto.

Dicha Maestría tiene como objetivo la formación de profesionales capaces de dirigir, gestionar, liderar y comunicar procesos de seguridad integral que minimicen vulnerabilidades, disminuyan factores de riesgo y por lo tanto control de pérdidas, a través de conceptos, teorías, políticas, herramientas y procedimientos desde la visión militar, lo que genera mayor impacto en la calidad de los resultados.

"El aprendizaje adquirido nos abrió un abanico de posibilidades y nuevos panoramas. La visión y la conceptualización con la que un militar ve la seguridad con respecto a una persona o un civil que se dedica a la seguridad privada es muy diferente. Y Colombia se ha convertido en el segundo país más importante en materia de seguridad, sólo debajo de Israel", señaló el empresario.

Soluciones:

- *Assesment* en CS basado en sistemas de gestión.
- Modelos llave en mano para la CS.
- Trazabilidad de activos.
- Monitoreo y Seguimiento de cargas críticas.

Con más de 26 años de experiencia en el mercado de la seguridad, Rodolfo Cepeda lidera la empresa REC Servicios Consultores enfocada en la implementación de estrategias efectivas en prevención, productividad y rentabilidad dentro de la cadena de suministro

De acuerdo con el análisis del ejecutivo, hay muchas diferencias en materia de seguridad integral entre México y Colombia, pero una de las semejanzas más importantes y de las que este país podría aprender del sudamericano, es que Colombia atravesó por una crisis de seguridad hace 20 años muy similar a la que México vive actualmente, cuando Pablo Escobar tenía tomado el país.

El narcotráfico, el crimen organizado y la delincuencia fueron factores que fomentaron la creación de procesos de seguridad efectivos para ese país y por lo que hoy en día "ha podido implementar estrategias efectivas para abatir la delincuencia".

REC SERVICIOS CONSULTORES: RESPONSABILIDAD, EXCELENCIA, COMPROMISO

Con más de 26 años de experiencia en el mercado de la seguridad, Rodolfo Cepeda lidera la empresa REC Servicios Consultores enfocada en la implementación de estrategias efectivas en prevención, productividad y rentabilidad dentro de la cadena de suministro.

"En REC Servicios Consultores estamos conscientes de que tenemos que hacer trajes a la medida en cuestión de seguridad. No podemos establecer una estrategia global, porque no existe. Se debe hacer un *assesment* de seguridad que te arroje un diagnóstico real sobre cuáles son tus fuerzas, tus debilidades y con base en eso establecer un plan de acción que te permita con tecnología, procesos bien definidos y con una adecuada capacitación, llevar a tu negocio al cumplimiento de sus objetivos y misiones", indicó.

Uno de los diferenciadores de REC, es que gracias a la capacitación y profesionalización de sus integrantes, han podido crear una plataforma que da una trazabilidad y un monitoreo activo dejando registro de absolutamente todo y llevando un sistema de gestión muy adecuado a la parte la logística, entrega de mercancía en tiempo y forma. ■

Productos:

- Sistemas de comunicación vía satélite.
- Sistemas de CCTV fijos y móviles.
- Sistemas de control de acceso.
- Sistemas de telemetría y domótica.

Fotos: Erick Martínez / SEA

Foto: Creativeart - Freepik

LA DEFENSA DEL BLINDAJE AUTOMOTRIZ

¿Cómo elegir una empresa blindadora?

MÉXICO | Cap. Joel Espinoza Sosa

¿Defendernos? La defensa, en cualquier ámbito y bajo el enfoque general, consiste en aplicar un conjunto de actividades destinadas a rechazar o reducir el riesgo de una ofensiva, que, por múltiples factores, eventualmente pudieran realizar enemigos, disidentes, contrarios, detractores o simplemente: delincuentes de ocasión. También entran en esta categoría los grupos de poder, simulados movimientos sociales, falsas organizaciones no gubernamentales con fines lucrativos, entre otros.

Uno de los más serios problemas para la ciudadanía es el "cómo vivir alejado de conflictos", es decir, mantenerse al margen de todo efecto dañino directo o colateral. Para ello, si bien se requiere planificar los cursos de acción que garanticen afrontar eventualidades en caso de sufrir un siniestro, que podría poner en riesgo la propia integridad física y la de nuestros seres queridos, también se debe considerar la forma que debemos sujetar nuestro comportamiento durante los momentos de relativa calma y sobre todo, las consideradas acciones disuasivas.

Las actividades habitualmente relacionadas con la defensa son la investigación y el empleo de tecnología, la provisión de implementos estratégicos y el dominio del territorio. El término defensa alude expresamente a la idea de respuesta ante un ataque, contradiciendo la noción misma de "ataque", sin embargo, en ocasiones la propia defensa es utilizada para realizar actos de agresión contra otros, con la excusa de que los mismos fueron ejecutados para prevenir un ataque exterior planeado con anterioridad, acción conocida como un ataque preventivo.

Vital resulta diseñar estrategias de protección de magnitud y potencialidad que garantice la continuidad de los intereses y objetivos personales. Que para el caso considerado sería: preservar la salud y la vida.

En casa (A) y en el lugar de desarrollo laboral (B), por lo regular la seguridad recae en personal profesional y/o implementos que nos resguardan y nos hacen sentir seguros. Pero en gran medida, y en el trayecto de A hacia B, se requiere también transportar esa

GSI
SEGURIDAD PRIVADA

GSI Seguridad Privada SA de CV

Profesionales en Seguridad Privada

Oficiales de Seguridad Armados

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

SOMOS GRUPO GSI, Orgullosamente una empresa Mexicana

www.gsiseguridad.com.mx

atencionaclientes@gsiseguridad.com.mx

Tel. 800 830 5990

CERTIFICADO ISO-9001:2015 GSI SEGURIDAD PRIVADA

ESR EMPRESA SOCIALMENTE RESPONSABLE

redconocer de prestadores de servicios Centro de Evaluación

TYPE OF CERTIFICATION MARK DNV·GL STANDARD

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

EMPRESAS DE GSI GRUPO SEGURIDAD INTEGRAL

sensación de seguridad sin tener que invertir en altos costos o necesariamente en un grupo de escoltas.

PUNTOS A CONSIDERAR

En caso de contar con los recursos necesarios y valorar lo que más importa. Considera mandar a blindar tu vehículo, o adquirir un vehículo blindado de línea o incluso el arrendamiento de un vehículo blindado sólo para las ocasiones que se estime necesario. Para lo cual, es importante: primero, estimar qué es lo que realmente se requiere en nivel de blindaje. Los hay de diversos tipos y naturaleza e independientemente de la norma o nivel que cumplan, los rubros de los vehículos blindados son: anti-asalto, anti-secuestro, anti-atentado y anti-perforante.

Y con la finalidad de obtener mayores elementos de juicio para definir la blindadora automotriz que te puede blindar, vender o arrendar un vehículo blindado, te comparto los principales puntos a calificar:

1. Visita la planta blindadora, si no está en tu ciudad entonces solicita información de su ubicación y verifica que exista físicamente y tenga toda la información en su página web. Realiza una prueba de manejo para evaluar el confort, movilidad, frenado y estabilidad del vehículo.

2. Revisa la **antigüedad de la empresa** que estás eligiendo y la capacidad de producción continua que tiene. Confirma la trayectoria de la empresa y sus ubicaciones (con capacidad y experiencia en exportación).

3. Consulta si cuentan con **garantía mecánica del vehículo** dentro de tu cotización, de dos años o 40 mil km. Además, solicita por escrito, la garantía de materiales balísticos opacos (blindaje en carrocería) utilizados en el vehículo que cuenten con siete años y tres años en transparentes (cristales).

4. Infórmate acerca de la producción que tiene mensualmente y **si tienen entrega inmediata.**

5. Pregunta si tus **datos personales permanecerán en forma confidencial y segura.**

6. Infórmate acerca del personal de la empresa, si tienen ingenieros especializados para el desarrollo del blindaje y **personal capacitado.** Solicita las **certificaciones de la Norma VPAM** (Vereinigung der Prüfstellen für Angriffshemmende Materialien und Konstruktionen - Asociación de Laboratorios de Prueba para Construcciones y Materiales Resistentes a Balas) **en vehículo completo bajo estándar VR4 y NIJ III A y que las certificaciones sean a nombre de la blindadora** que fabrica el vehículo.

1. Solicita que el **certificado de calidad ISO 9001-2015 esté vigente** en el año cotizado y actualizado. Contar con registro ante la Comisión Nacional de Seguridad (CNS) para verificar que es una empresa autorizada y que pertenezca a la Asociación Mexicana de Blindadores Automotrices (AMBA).

2. Consulta que la certificación de materiales balísticos estén realizados por **HP White Laboratory Inc. an Intertek Company (U.S.A) y/o National Institute of Justice NIJ de U.S.A y que las certificaciones tengan vigencia mínima de seis meses** de la empresa que fabrica el blindaje. Revisar que los materiales balísticos, tanto en materiales opaco (acero y Kevlar) como transparentes (cristales), cuenten con la **certificación VPAM.**

3. Consulta que el nivel de blindaje es el adecuado a tus necesidades y **no te quieran vender lo que tengan en inventario de años anteriores.**

4. Que te ofrezcan **certificado de tu vehículo** y te entreguen un documento que avale tu compra (Carta Autenticidad del CNS - Comisión Nacional de Seguridad).

5. Consulta si **incluye en la cotización, un curso básico de inducción y manejo de vehículo blindado.**

Recuerda que estás haciendo una inversión no sólo económica, sino de confiabilidad que protegerá y reducirá los riesgos derivados de un ataque hacia lo que más quieres. ■

Cap. Joel Espinoza Sosa,
coordinador nacional de Seguridad Patrimonial TPS Armoring.

Más sobre el autor:

Vital resulta diseñar estrategias de protección de magnitud y potencialidad que garanticen la continuidad de los intereses y objetivos personales. Que para el caso considerado sería: preservar la salud y la vida

Foto: Creativeart - Freepik

CONTROL®

SEGURIDAD PRIVADA INTEGRAL

20 años

SÚPER EMPRESAS EXPANSIÓN 2021

TOP companies

EMPRESA SOCIALMENTE RESPONSABLE

ISO 9001:2015
Organización Certificada
OC-0080/13

www.seguridadcontrol.com.mx

@segcontrol

Columna de
Jaime A. Moncada
jam@ifsc.us

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

Más sobre el autor:

EUA

NOVEDADES EN SEGURIDAD CONTRA INCENDIOS EN SUBESTACIONES Y CENTRALES DE GENERACIÓN ELÉCTRICA

En los últimos años, a través de esta columna, he tratado el tema de la seguridad contra incendios y las referencias normativas en subestaciones de trasmisión y centrales de generación eléctrica. Quisiera retomar el tema y ponerlos al día sobre la reciente modificación de la NFPA 850, la Práctica Recomendada para la Protección contra Incendios en Plantas de Generación Eléctrica, la cual sufrió una reorganización completa.

Este tema es relevante, porque uno de los sectores de mayor crecimiento e inversión en Latinoamérica es el sector de la generación eléctrica. Por ejemplo, la prensa mundial ha reportado recientemente la decisión del senado Brasilero de permitir la venta del 61% de Electrobras y se espera que esta venta represente entre 5 a 6 mil millones de dólares para el Gobierno brasileño. Como parte de esta venta se va a permitir la construcción de centrales térmicas a gas con generación de 6 GW[1].

De acuerdo con el U.S. *Energy Information Administration*[2], la generación neta de electricidad en Latinoamérica se incrementará en un 60%, entre 2018 y el 2050, de 42 a 67 cuatrillones de BTUs (*British thermal unit*). El crecimiento más importante estará en termoeléctricas utilizando gas natural, seguido por renovables (hidroeléctricas y eólicas), aunque la generación hidroeléctrica es la más prevalente, generando casi la mitad de nuestra electricidad. Termoeléctricas, utilizando carbón o líquidos inflamables, verán una reducción en su capacidad instalada, y en 2050 generarán sólo un 10% de la cantidad neta de electricidad en Latinoamérica. Cada uno de estos métodos de generación tienen riesgos de incendios.

CONFIABILIDAD DEL SERVICIO

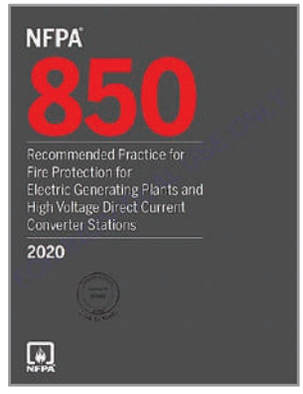
Las instalaciones de generación eléctrica ya sean nuevas o existentes, requieren de confiabilidad y disponibilidad, y su falta de operatividad repercuten sensiblemente en la sociedad en general. Uno de los componentes críticos en nuestro desarrollo económico es la confiabilidad energética y no ha sido raro en nuestra historia regional haber vivido "apagones" por falta de disponibilidad eléctrica. En la mayoría de nuestros países, la generación eléctrica ha estado en manos de entes regionales, y por consecuencia hay diferentes niveles de protección entre una instalación a otra, y de un país a otro. Muchas compañías de seguros están tratando de resolver este problema recomendando el cumplimiento de la normativa NFPA (National Fire Protection Association).

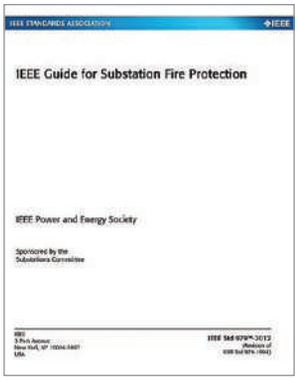
Aunque los incendios en centrales eléctricas no son muy frecuentes, cuando ocurren tienen una repercusión importante. Por ejemplo, un incendio en febrero de 2017 en unos cables de transmisión en el túnel de acceso de una hidroeléctrica en caverna en el centro de Colombia produjo pérdidas de equipos de 23 millones de dólares y lucro cesante de más de 200 millones de dólares, y la ha dejado inoperativa por varios meses. Es común también escuchar sobre cortes de energía en una ciudad debido al incendio de un transformador, túnel de cables o salas de control.

NORMAS INTERNACIONALES

NFPA tiene un documento que establece recomendaciones para la prevención y la protección contra incendios en plantas de generación eléctrica, llamado NFPA 850 – Práctica Recomendada para la Protección contra Incendios en Plantas de Generación Eléctrica. Las subestaciones son reguladas por la IEEE 979 – Guía de Protección Contra Incendios para Subestaciones, que desde el 2012 no ha tenido ninguna revisión.

La NFPA 850 no incluye las plantas de energía nuclear, las cuales están reguladas por la NFPA 805, Norma de Diseño por Desempeño para la Protección contra Incendios para Plantas de Generación Eléctrica por Reactores Eléctricos de Agua Liviana. Tanto FM Global y XL GAPS tienen también guías de control de riesgo de incendios que complementan la NFPA 850.





En mi experiencia, el principal problema ha sido la falta de normatividad local en la materia y la falta de entendimiento de la normativa internacional por parte de los diseñadores de este tipo de instalaciones

Diseño tridimensional de un sistema de aspersión para un transformador de acuerdo con la NFPA 15

La NFPA 850, en su última revisión de 2020, tuvo una reorganización completa. Aunque los primeros capítulos siguen unos lineamientos parecidos a los que se encuentran en ediciones anteriores, el nuevo capítulo 9 establece criterios para los sistemas de protección contra incendios básicos, como la bomba contra incendios, equipos comunes como equipos oleo hidráulicos y bodegas, y el manejo de combustibles dentro de una central. Los capítulos 11 al 20 establecen criterios de protección para diferentes tipos de centrales como por ejemplo turbinas de viento, hidroeléctricas, plantas solares y de generación geotérmica.

EL RIESGO DE INCENDIO

La problemática de la seguridad contra incendios en una instalación de generación eléctrica o en una subestación es casi idéntica de planta a planta, no importa donde esté localizada en el mundo. Esto quiere decir que los retos para controlar un incendio, en una instalación de este tipo es el mismo, ya sea que esté instalación en los Estados Unidos, Europa o Latinoamérica.

En la elaboración de la NFPA 850, la NFPA revisó la experiencia mundial en seguridad contra incendios en plantas de generación eléctrica y utilizó esta información como la base de la filosofía en seguridad contra incendios contenida en estas prácticas recomendadas[3].

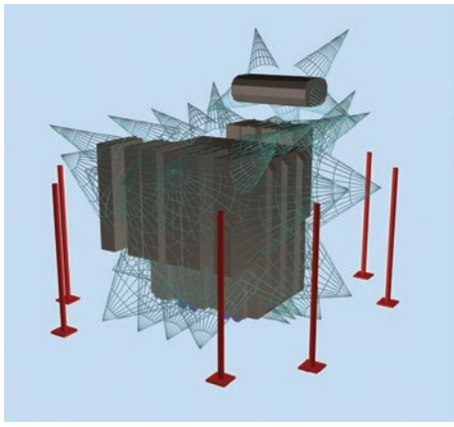
Estas prácticas son utilizadas a nivel internacional como la base técnica para el diseño, construcción y operación de proyectos de generación eléctrica, y

me consta que un creciente número de instalaciones de generación eléctrica en Colombia, Chile, Ecuador, México, Perú, la República Dominicana y Uruguay han tomado la decisión de cumplir los criterios de diseño encontrados en estos documentos.

INGENIERO CONSULTOR

La NFPA 850 reconoce que el proceso de evaluación y diseño es muy especializado e indica que "el proceso de diseño de protección contra incendios de una planta de generación debe iniciarse bajo la dirección de alguien experimentado en el área de ingeniería de protección contra incendios y que tenga amplios conocimientos y experiencia en la operación de una planta de energía" (NFPA 850: Art. 4.1.1).

Es decir, la NFPA asume que quien interpreta esta guía, no sólo tiene experiencia en ingeniería de incendios, sino que conoce la problemática de una planta de generación eléctrica. Esto es importante, porque la NFPA 850 da lineamientos generales y en muchos casos no da una solución prescriptiva. Es por consecuencia relativamente fácil "perder el norte", y por falta de experiencia, establecer soluciones que no son adecuadas o equivalentes a lo que se establece para instalaciones similares en otras partes del mundo.



Pruebas hidráulicas quinquenales, de acuerdo con la NFPA 291, en una red contra incendios en una subestación eléctrica

> La problemática de la seguridad contra incendios en una instalación de generación eléctrica o en una subestación es casi idéntica de planta a planta, no importa donde esté localizada en el mundo

PLAN MAESTRO DE SEGURIDAD CONTRA INCENDIOS

El Capítulo 4 de la NFPA 850 establece el proceso de diseño de la protección contra incendios, el cual busca establecer las bases de diseño lo más temprano posible en el diseño de la instalación. Estas bases de diseño se llaman tradicionalmente el Plan Maestro de Seguridad Contra incendios, el cual tiene como propósito proveer un registro del proceso de decisiones durante la determinación de las protecciones a los riesgos de incendios presentes en la instalación y establecer la estrategia de protección.

Este documento no solamente se revisa, mejora y modifica a medida que se refina el diseño de la central, sino que debe ser continuamente revisado y mantenido durante la vida de la instalación. Actualmente es común que instalaciones existentes en Latinoamérica contraten a firmas de ingeniería de protección contra incendios con el interés de conocer cómo están y que deben hacer para eventualmente obtener un nivel aceptable de seguridad contra incendios.

OPCIONES DE CAPACITACIÓN

Yo he tenido la oportunidad de trabajar en la ingeniería contra incendios de decenas de centrales de generación eléctrica, así como en muchas instalaciones de trasmisión eléctrica en toda Latinoamérica. He también inspeccionado instalaciones después de un incendio. Durante más de 15 años me han dado la responsabilidad de dictar cursos sobre seguridad contra incendios para instalaciones de generación y transmisión eléctrica. En mi experiencia, el principal problema ha sido la falta de normatividad local en la materia y la falta de entendimiento de la normativa internacional por parte de los diseñadores de este tipo de instalaciones.

En este sentido, un grupo de profesionales nos hemos dado a la tarea a desarrollar programas de formación, en este caso virtuales, tanto para centrales de generación eléctrica como subestaciones de transmisión. Por ejemplo, con el apoyo del Fire Protection Institute (FPI), la Organización Iberoamericana Protección Contra Incendios (OPCI) ofrecerá a partir de 2 de noviembre hasta el 18 de diciembre de 2021, un programa certificado de protección contra incendios para la industria de generación eléctrica, el cual tendrá 56 horas de formación (*www.tiendaopci.org*).

Por otro lado, la Cámara Boliviana de Hidrocarburos y Energía (CBHE), también con el apoyo del FPI, ofrecerá un programa avanzado de protección contra incendios para subestaciones de 24 horas de formación, del 7 de septiembre al 5 de octubre de 2021 (*www.cbhe.org.bo*). Estas dos opciones de capacitación buscan actualizar el conocimiento y ofrecer un mejor entendimiento de los criterios de protección a las autoridades competentes, aseguradores, diseñadores e instaladores de sistemas contra incendios. ■

Fotos: Cortesía IFSC

REFERENCIAS

[1] *Brazil's Senate Approves Electrobras Privatization Bill, Junio 17, 2021, Reuters.com.*

[2] *International Energy Outlook 2019, Septiembre 24, 2019.*

[3] *La NFPA 850 es una "Práctica Recomendada", o sea un documento que es similar en contenido y estructura a una norma, pero que no es mandatario, pues su objetivo es que sea adoptado por entidades de generación y transmisión eléctrica como sus guías corporativas.*

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

SISSA INFRAESTRUCTURA DESARROLLA PROYECTO DE PROTECCIÓN CONTRA INCENDIOS EN LA TORRE SCOTIABANK

El reto que enfrentaron al implementar sus soluciones en este caso de éxito

MÉXICO

Elías Valencia Trejo

En SISSA Infraestructura, empresa dedicada al diseño, implementación y desarrollo de proyectos llave en mano, nos encontramos desarrollando un proyecto de Sistema de Protección Contra Incendios (SPCI) para la modernización de la Torre Scotiabank en la Ciudad de México.

Luego de que este proyecto nos fuera asignado a finales de 2019 por la constructora GIA, comenzamos operaciones a partir de febrero de 2020. Es importante mencionar que, aunque la pandemia de COVID-19 provocó un retraso en las operaciones de aproximadamente cinco meses, logramos sortear el desarrollo de este proyecto con gran éxito.

¿CUÁL ES EL PAPEL DE SISSA INFRAESTRUCTURA EN ESTE PROYECTO?

Podemos señalar que es un gran reto, ya que además de tratarse de una edificación de alrededor de 55 mil m² de construcción, se está trabajando en sus cuatro sótanos, planta baja, 21 niveles, azotea y helipuerto sin inhabilitar sus espacios, es decir, estamos trabajando en un edificio "vivo" donde actualmente se encuentra personal laborando.

En SISSA Infraestructura procuramos las mejores prácticas de ingeniería y planeación, nos adaptamos a los procesos y protocolos de seguridad que se manejan en todos los proyectos y nuestras operaciones están orientadas a la integración de los mejores sistemas de detección y supresión del mercado. Todo esto se puede comprobar en nuestra participación dentro del proyecto de modernización de la Torre Scotiabank.

> En SISSA Infraestructura trabajamos bajo las especificaciones del sistema de certificaciones *Leadership in Energy & Environmental Design* (LEED), orientadas a la sostenibilidad y protección del medio ambiente

NUESTRO EQUIPO Y CERTIFICACIONES

Este proyecto ha estado a cargo de un equipo de trabajo multidisciplinario, desde su ejecución operativa hasta la administración de sus diferentes procesos, ya que también es necesario cumplir al 100% las solicitudes del cliente. Es por ello que diferentes áreas de SISSA como Compras, Recursos Humanos, Finanzas y Contabilidad han sido clave para sacar adelante este proyecto al brindar soporte a la interacción que se tiene con las contrapartes de GIA.

Además, los profesionales que realizan el suministro de equipos en el área de trabajo garantizan que dichos equipos estén apegados a las normas de seguridad mundial al contar con su respectiva certificación. De igual forma, se garantiza la calidad y certificación por parte de la mano de obra utilizada, medidas a través de las cuales se busca asegurar el éxito de este importante proyecto.

Al respecto, cabe destacar que contamos con un equipo de profesionales altamente capacitados y certificados ante entidades nacionales e internacionales aprobadas, como la NFPA (National Fire Protection Association)

de la Torre Scotiabank:

- Tendido del *raiser* para 25 pisos.
- Instalación de diversas tuberías, desde el sótano 4 hasta el piso 6.
- Instalación de las bombas, diésel y eléctrica en el cuarto de máquinas.
- Instalación de rociadores.
- Instalación de sistema de pre-acción.
- Instalación de sistema de espuma.
- Colocación de hidrantes.

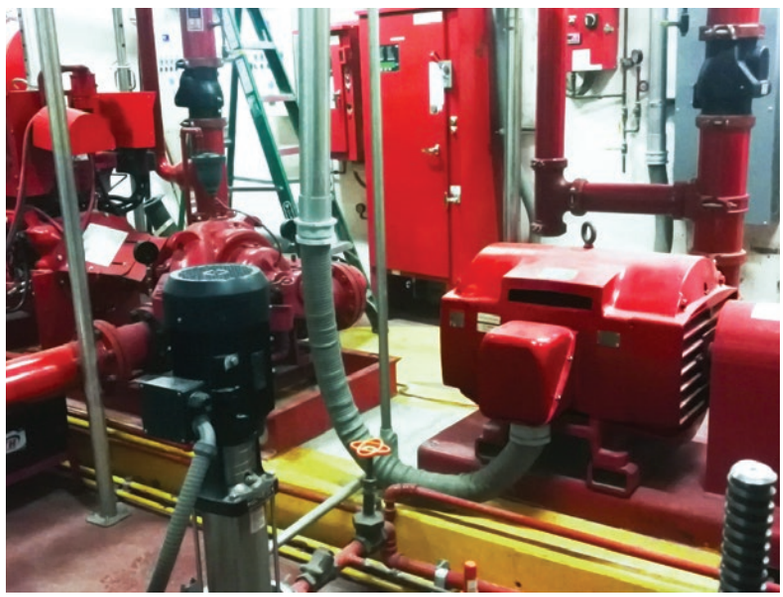
Es un gran orgullo para SISSA estar desarrollando un proyecto de esta magnitud, un proyecto de gran envergadura que nos permite ofrecer nuestros conocimientos y experiencia para el desarrollo de nueva infraestructura en nuestro país. ■

Fotos: SISSA Infraestructura

y UL/FM (Underwriters Laboratories / Factory Mutual), certificaciones con las que buscamos garantizar la satisfacción de nuestros clientes.

Así mismo, en SISSA Infraestructura trabajamos bajo las especificaciones del sistema de certificaciones *Leadership in Energy & Environmental Design* (LEED), orientadas a la sostenibilidad y protección del medio ambiente.

También es importante resaltar las labores de nuestros residentes de obra, quienes, al igual que todo el equipo de trabajo de SISSA Infraestructura, han destacado por su esfuerzo, compromiso y profesionalismo, trabajando más allá de su horario establecido (incluso en horarios nocturnos y fines de semana) debido a la demanda del mismo proyecto.



AVANCES DEL PROYECTO DE MODERNIZACIÓN

Un proyecto de Sistema de Protección Contra Incendios implica una gran responsabilidad para cualquier empresa, razón por la cual imprimimos todo nuestro profesionalismo y calidad de servicio en cada operación realizada en dicho proyecto.

A continuación, se enlistan los temas más relevantes que hasta el momento hemos desarrollado en el proyecto del Sistema de Protección Contra Incendios para la modernización

> Cabe destacar que contamos con un equipo de profesionales altamente capacitados y certificados ante entidades nacionales e internacionales aprobadas, como la NFPA y UL/FM, certificaciones con las que buscamos garantizar la satisfacción de nuestros clientes

Elías Valencia Trejo,
director comercial en SISSA Infraestructura.

Más sobre el autor:

Foto: Creativeart - Freepik

ANÁLISIS DE VULNERABILIDADES Y SU IMPORTANCIA EN EL MARCO DE CIBERSEGURIDAD

MÉXICO | Víctor Díaz Bañales

Consiste en definir, identificar, clasificar y priorizar las debilidades de las aplicaciones para proporcionar una evaluación de las amenazas previsibles y reaccionar de manera apropiada

¿QUÉ ES UN ANÁLISIS DE VULNERABILIDADES?

Con la llegada de la pandemia, se expusieron muchas aplicaciones y sistemas a los que normalmente se accedía a través de intranet o de forma interna y que no estaban expuestas a Internet, por lo cual en muchas organizaciones ha cambiado y se han visto en la necesidad de exponer aplicaciones a Internet o liberar aplicaciones móviles que debido a la premura y las necesidades de la operación, pueden ser liberadas sin ningún protocolo de seguridad o no haber pasado por una metodología correcta de SDLC (*Software Development Life Cycle*) Desarrollo Seguro de *Software* para poder mitigar riesgos asociados a vulnerabilidades conocidas o emergentes.

¿QUÉ TIPOS DE ANÁLISIS DE VULNERABILIDADES EXISTEN?

En el mercado existen diversas herramientas, pero básicamente se dividen en ejecutar dos tipos de análisis: DAST (*Dynamic Application Security Testing*) y SAST (*Static Application Security Testing*), lo ideal claramente es generar una mezcla de ambos esquemas de protección, cada uno de ellos cuenta con ventajas y desventajas que iremos desglosando, lo interesante es aclarar el concepto y hacerlo digerible de forma sencilla.

Los análisis dinámicos están orientados para aplicaciones que ya fueron liberadas a su versión final, es decir aplicaciones ya compiladas y listas para su uso, por el otro lado las aplicaciones estáticas se utilizan en una fase más temprana del desarrollo y es cuando el código aún está siendo escrito y en desarrollo, los análisis dinámicos suelen tener un costo menor que las estáticas a nivel económico.

La recomendación es que si la empresa tiene un marco de desarrollo de aplicaciones debería integrar alguno de estos dos mecanismos de análisis de vulnerabilidades.

¿POR QUÉ IMPLEMENTARLO LO ANTES POSIBLE?

Las aplicaciones tanto expuestas en Internet como puede ser un portal de comercio electrónico, plataformas digitales, aplicaciones móviles, etc., pueden estar a merced de diversos ataques que buscan explotar vulnerabilidades conocidas como SQL Injection, Cross-Site Scripting (XSS), etc.

Es por ello que se debe implementar y escanear las aplicaciones para que tengamos la seguridad de que no pueden ser vulneradas por la explotación de dichas debilidades, la recomendación es escanear, remediar y volver a escanear, siendo un proceso iterativo, debido a que una vulnerabilidad remediada puede generar otras vulnerabilidades, normalmente remediar una vulnerabilidad implica varias cosas y elementos que deben corregirse, tales como código, sistema operativo, parches de seguridad, etc. Por lo que no es una labor meramente rápida y sencilla lo cual debe ser tomado en cuenta para generar un plan adecuado de remediación con puntos de retorno y sus respectivos controles de cambios para evitar pérdida de funcionalidad y tener control de las modificaciones realizadas.

VENTAJAS DE UN DAST

- El análisis permite a los desarrolladores detectar los problemas durante la ejecución del código.
- Pueden ser fallas de autenticación y configuración de red o problemas que surgen después del inicio de sesión.
- Hay menor número de falsos positivos.
- Admite lenguajes y marcos de programación personalizados y disponibles en el mercado.
- Presenta una alternativa menos costosa y compleja a SAST.

DESVENTAJAS DE UN DAST

- Las herramientas DAST no proporcionan información sobre las causas subyacentes de las vulnerabilidades.
- Tienen dificultades para mantener los estándares de codificación.
- El análisis no es adecuado para etapas iniciales del desarrollo.
- Sólo se puede realizar en una aplicación en ejecución.
- No simularán a la perfección ataques potenciales.
- Los *exploits* son ejecutados, por una parte, con una base de conocimiento interna sobre la aplicación.

VENTAJAS DE UN SAST

- Las herramientas SAST descubren vulnerabilidades altamente complejas durante las primeras etapas de desarrollo de un *software*, ayudando a resolverlas rápidamente.
- Tiene amplia compatibilidad con diferentes lenguajes de programación.
- Permite que pueda integrarse en entornos existentes en diferentes puntos del desarrollo de *software*.
- Dado que establece los detalles de un problema, incluida la línea de código, simplifica la reparación.
- Se necesita poco tiempo para examinar el código y se compara favorablemente con las auditorías manuales.

Los análisis dinámicos están orientados para aplicaciones que ya fueron liberadas a su versión final, es decir aplicaciones ya compiladas y listas para su uso, por el otro lado las aplicaciones estáticas se utilizan en una fase más temprana del desarrollo y es cuando el código aún está siendo escrito y en desarrollo

DESVENTAJAS DE UN SAST

- No se puede probar la aplicación en el entorno real.
- Las vulnerabilidades en la lógica de la aplicación o la configuración insegura no son detectables.
- Tiende a modelar el comportamiento del código de manera inexacta.
- El 53% de los problemas detectados no existen.
- Los desarrolladores tienen que lidiar con muchos falsos positivos y falsos negativos.
- El resultado es un informe estático que rápidamente se vuelve obsoleto. Implementar la tecnología a escala puede ser un desafío, el proceso puede ser lento y las pruebas no son aplicables a sistemas en etapa de producción.
- No todas las empresas o personas están dispuestas a proporcionar datos para el análisis de código binario y código fuente. ■

Foto: Creativeart - Freepik

Víctor Díaz Bañales,
socio director de Ramdia.

Más sobre el autor:

LA SEGURIDAD EN LAS REDES SOCIALES

Los 6 principales consejos que debes poner en práctica

MÉXICO | Miguel Ángel Champo Espinosa

Hoy en día estamos inmersos en una sociedad que vive y se comunica por medio de las redes sociales, en muchas ocasiones éstas son utilizadas para un bien común como, por ejemplo: comunicación rápida y sin fronteras, denuncias sociales, a su vez mayor información junto con una fuente mucho más amplia y alcance de un clic, entre otros, pero también estas mismas redes sociales que pudiesen parecer inofensivas pueden tornarse peligrosas.

LA PELIGROSIDAD DE LAS REDES SOCIALES

Las redes sociales, como lo mencionaba en el párrafo anterior, nos permiten estar cerca de nuestros seres queridos y aquellas personas que no están cerca de nuestra comunidad, pero ¿qué pasa con aquellas personas que no conocemos y aceptamos? ¿Qué pasa con aquella información como: ubicación, fotografías, con cuántas personas te encuentras, edad, gustos… y así un listado infinito? Es aquí donde debemos tener énfasis y cuidado con el tipo de información que tenemos en nuestras redes sociales.

Aquí te daremos una lista de aquellas cosas que puedes hacer para tener más cuidado:

1. **Si el contenido es privado o información personal,** piensa si realmente vale la pena compartirlo, que las redes sociales sirvan como herramienta para estar cerca de nuestros seres queridos no es sinónimo de dar dirección ya sea de oficina o de tu propia casa, esa información debes de tenerla sólo para ti y aquellas personas de las cuales estas seguro de que te puedes fiar.

2. **No aceptar solicitud de personas que no conozcas.** En ocasiones las redes sociales han servido como método de creación de relaciones interpersonales, pero repito, al final no sabes quién es la verdadera persona que esta detrás de esa pantalla.

3. **Ser precavido al utilizar un ordenador compartido.** Esto es importante, ya que si en tu oficina (de no ser prohibido) o en algún café Internet los utilizas y por error dejas tus cuentas abiertas, la siguiente persona tendrá acceso a mensajes e inclusive información bloqueada sólo para ti.

4. **Usar herramientas para administrar la seguridad y preferencias.** Tú puedes tomar el control de quién puede visitar tu perfil, también quién puede mandarte solicitud e inclusive dentro de tus amigos quiénes tienen acceso a cierta información.

5. **Si tienes hijos en casa o algún familiar de una edad pequeña,** recomendable controlar el uso de estas, siempre tener en poder la administración de sus redes sociales.

6. **Leer bien los términos de privacidad de cada red social.** Es importante saber cómo utilizarán desde fotos, publicaciones y en realidad todo tu perfil está en redes sociales a las cuales estas entregando información.

Las redes sociales tienen como intención facilitarnos la comunicación y un acceso a cierto tipo de información, pero como profesionales de seguridad tenemos la responsabilidad de cuidarnos y cuidar a la gente que haga uso de ellas, en estos tiempos la delincuencia esta cada vez más cerca de nosotros, no le demos un acceso fácil a nuestra privacidad. ■

Miguel Ángel Champo Espinosa,
Co-Founder de la empresa de seguridad privada BRIMA.

Más sobre el autor:

ASI SEGURIDAD PRIVADA

UNA COMPAÑÍA DE SEGURIDAD PRIVADA CON MÁS DE 10 AÑOS DE EXPERIENCIA.

Somos una compañía de seguridad privada, conformada por un equipo de profesionales con certificaciones en diversas especialidades de la seguridad.

Conoce nuestros servicios:

- Protección y Vigilancia
- Custodia a transporte
- Patrullaje al comercio e industria
- Rastreo y monitoreo
- Consultoría
- Contratación Segura
- Seguridad Electrónica
- Protección Ejecutiva
- Y mucho más...

En ASI Seguridad Privada es importante destacar que formamos a nuestro personal a través de un proceso continuo de capacitación en las funciones y competencias que su posición requiere.

REPSE
Registro de Prestadoras de Servicios Especializados u Obras Especializadas

BASC

ISO 9001:2015

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

TEL: 55 5719 0072 ventas@asiseguridadprivada.com www.asiseguridadprivada.com

/ASI Seguridad @ASIseguridad ASI Seguridad Privada /asiseguridadprivada

EL ENEMIGO OCULTO DE NUESTRAS BILLETERAS

Foto: Creativeart - Freepik

Fraude y robo de las tarjetas de crédito y débito

URUGUAY | Héctor Nessi

¿Qué nos imaginamos cuando vemos un título como el que he puesto a este artículo? Sí, es correcto, seguramente es alguien que desde las sombras, se encuentra buscando nuevas formas y modalidades de tomar nuestro dinero.

Obviamente, muchas son estas formas, muchos son los engaños que hacen que gente inescrupulosa se haga del dinero que tanto nos cuesta ganar y que simplemente con algunas ingeniosas "artimañas", nos dejan nuestros bolsillos o nuestras cuentas bancarias sin un centavo.

Hoy voy a intentar llevarles a ustedes mi experiencia desde la década de los años 90 a la actualidad, de la forma que han ido cambiando las modalidades de estafas con tarjetas de crédito y débito en el Uruguay, aunque tal vez mi relato difiera de la situación en otros países.

Uruguay, ubicado en América del Sur, es un pequeño país de 176 mil 215 km^2, siendo el segundo país más pequeño de la región, luego de Surinam. Hoy en día, su población asciende a un poco más de tres millones de habitantes, estando la mayor concentración en Montevideo, su capital, con más de 1 millón 500 mil de ellos.

Al ser un país tan pequeño, la mayoría de las veces, los adelantos tecnológicos demoran más en llegar que a otros más desarrollados o con mayor poder adquisitivo. Es así que por los años 90, comenzamos a hacer nuestras primeras experiencias en materia de personas damnificadas por estafas cometidas contra sus tarjetas de crédito.

Aclaremos que en ese entonces Uruguay no procesaba las tarjetas de sus tarjetahabientes, sino que las mismas se recibían ya emitidas desde el exterior, normalmente de Argentina, Emisores Europeos o de Estados Unidos, por intermedio del Correo Postal Uruguayo.

BREVE HISTORIA

Tomemos como primer punto de partida, que en el año 1949 se inventa y sale al mercado de Estados Unidos de América, la primera tarjeta de crédito en el mundo. Creada hasta por un hecho fortuito, durante una cena entre dos importantes empresarios y el abogado de uno de ellos, al momento de pagar la cena, el anfitrión, se da cuenta que había olvidado su billetera. Llama a su esposa para que se la traiga para poder pagar y en ese preciso momento, los tres comienzan a idear la forma

Foto: Creativeart - Freepik

de inventar un medio de pago que no necesitara utilizar el dinero efectivo, dando el comienzo a la creación de la primera tarjeta de crédito en el mundo "Diners Club" (Club de cenadores).

Esta tarjeta fue evolucionando con dificultad durante su primer año, pero luego fue un elemento que a las personas de muy buen poder adquisitivo, les iba perfecto y hasta daba un sobre estatus, ya que no todos accedían a tener una de ellas en esos momentos.

Luego, otras marcas comenzaron a lanzar sus tarjetas, siendo competidoras de la primera e intentando llegar a mercados nacionales e internacionales. A medida que se fue expandiendo internamente y luego a otros países, como en todos los casos donde se manejan valores, comienzan a aparecer quienes intentan hacerse de ellos de forma ilegal, por lo que los delincuentes, se toman sus tiempos, para idear formas de vulnerar las seguridades de estas tarjetas y obtener sus ganancias de forma ilícita.

Volviendo a Uruguay y tomando que la primera tarjeta nace en 1949, no es hasta finales de los años 70 cuando comienzan los primeros desembarcos de ellas en nuestro país. Diners y American Express llegan a Uruguay, pero las mismas no eran procesadas aquí, por lo que venían ya procesadas desde el exterior.

En 1980 dos empresas, Argencard y Mastercharge, comienzan sus procesos de emisión en Argentina y envían vía correo postal, las tarjetas ya emitidas hacia sus clientes de Uruguay. Posteriormente, tres bancos de Uruguay comienzan sus procesos de emisión propia y aparece una primera tarjeta de crédito local.

COMIENZO Y EVOLUCIÓN DE LOS FRAUDES

Con la llegada de estos nuevos medios de pago, también comenzaron a proliferar pequeñas organizaciones de delincuentes que buscaban la forma de realizar compras, que fueran pagadas por los verdaderos titulares de esas tarjetas. Es así que una de las primeras modalidades detectadas en nuestro país, fueron los robos de tarjetas que venían en las sacas del correo postal. En aquellos momentos, no había una lectura electrónica de la banda magnética, y se realizaba la venta en los comercios, solicitando telefónicamente un número de autorización al *call center* de la marca, imprimiendo el cupón con unos POS (*point of sale*) manuales (de carro), que imprimían en un comprobante que luego era firmado por el comprador, al que se le agregaba manualmente por parte del comercio, el número de autorización recibido de forma telefónica del *call* de la marca. Con el hurto de las tarjetas de las sacas del correo, los delincuentes tenían dos formas de hacer las maniobras delictivas, una, teniendo comercios que se asociaban a las maniobras y que hacían sus ventas sabiendo y en contacto con los delincuentes (no solamente vendían sus mercaderías, sino que luego solicitaban el reintegro del dinero, ya que ellos habían obtenido de la marca, la autorización telefónica y por lo tanto, la marca debía en muchas ocasiones devolver el dinero de la estafa al propio comercio), la otra forma, falsificaban un documento de identidad con el nombre que venía impreso en relieve en la tarjeta, con el fin de que todo coincidiera cuando el comercio solicitaba el documento.

Foto: Creativeart - Freepik

> Metodologías como el "lazo libanés" (en su forma antigua de colocación de traba dentro de la boquilla de acceso a la tarjeta, manteniéndola retenida), mientras un delincuente ofrece su ayuda al usuario a fin de observar su número de PIN y en horarios donde los bancos se encuentran cerrados

Obviamente, a medida que esto ocurría, se hacía experiencia por los grupos dedicados a la seguridad de las marcas, y también por quienes teníamos a cargo las investigaciones de estas estafas a nivel policial. Cada nueva medida que íbamos implementando y que permitía detener la modalidad del fraude anterior, ideaban otra buscando una nueva vulnerabilidad (hasta nuestros días y siendo ya todo de forma electrónica, esa carrera del gato y el ratón, continúa de la misma forma).

Fueron pasando los tiempos, y se empezaron a sumar integrantes de organizaciones dedicadas a estas estafas, procedentes de Argentina y Brasil. Obviamente, en estos países, ya más adelantados en la operativa de emisión de tarjetas y formas de control de fraudes, venían e instruían a delincuentes locales y comercios que se prestaban a estas maniobras, en las nuevas modalidades que tal vez en los países de origen ya estaban siendo detectadas por los equipos antifraudes de las marcas, pero que aquí podrían funcionar por ser un mercado más chico y por venir atrasados en esas "nuevas modalidades".

Es así que se van conformando organizaciones mixtas, entre argentinos y uruguayos o brasileños y uruguayos. Tuvimos que ponernos a trabajar muy duro para poder minimizar daños a las empresas y clientes, además instruir personal policial para poder hacer las investigaciones de acuerdo a cada nueva modalidad que se presentaba, instruir a los comercios en las posibles formas y nuevos requisitos a exigir para minimizar estafas, hasta instruir a jueces penales, ya que eran nuevos delitos que simplemente entraban

en un delito menor dentro del Marco Jurídico Uruguayo, lo que hacía que sus penas eran muy pequeñas (cuando se lograba procesar al delincuente), no siendo un escarmiento que intimidara a los mismos a no volver a intentarlo cada vez que podían.

Con todo este trabajo por delante, las marcas, sellos y emisores de tarjetas, la policía y la justicia, tuvimos que mancomunar esfuerzos para poder lograr en unos años diezmar a estas organizaciones y permitir un normal funcionamiento del producto tarjeta de crédito, con los menos riesgos y vulnerabilidades posibles y los menores daños económicos y de prestigio hacia esa industria y producto.

Todo va cambiando, hoy el medio de pago electrónico es el medio de pago por excelencia. Las tecnologías van avanzando día a día, así como las formas de estafas y fraudes hacia estos medios de pago. Si bien nuestro resumen histórico va dirigido a que aunque hoy la gran cantidad de estas estafas pasen por lo tecnológico, se siguen viendo casos de formas anteriores, más artesanales, menos tecnificadas, que cada tanto tiempo continúan apareciendo (al menos en nuestro país).

Por lo que el proceso de nuestro aprendizaje y el haber pasado por cada una de esas etapas, nos favorece a poder distinguir si ante lo que nos encontramos, es una nueva o vieja modalidad y poder ver si aún tenemos vulnerabilidades a corregir que sea por ello que estos delincuentes las vuelven a intentar y ahora no sólo a lo que es fraude de crédito, sino también a lo que es el fraude de débito, fundamentalmente en los ATM (cajeros automáticos).

Metodologías como el "lazo libanés" (en su forma antigua de colocación de traba dentro de la boquilla de acceso a la tarjeta, manteniéndola retenida), mientras un delincuente ofrece su ayuda al usuario a fin de observar su número de PIN (generalmente personas mayores) y en horarios donde los bancos se encuentran cerrados, o la misma forma, pero en su versión moderna, donde varios delincuentes operan a la vez contra un cliente mientras este opera en un ATM (uno le observa el momento cuando introduce su tarjeta al cajero y coloca su PIN, otro tira algo al piso con la finalidad de distraer a la víctima diciéndole que algo se le cayó y en momentos que ésta se agacha, un tercero da cancelar al sistema del cajero automático y retira la tarjeta de la persona, llevándose entonces la tarjeta física y el primer delincuente el número de PIN), pudiendo realizar los retiros hasta su tope mientras la titular no puede realizar la denuncia de bloqueo ante el banco hasta que éste no abra sus puertas en horario de atención al público.

Foto: jcomp - Freepik

Bloqueadores falsos de dispensadores de dinero, que cuando el usuario realiza su operación de extracción de dinero, ésta se realiza normalmente, pero el dinero no sale y luego de varios intentos, el usuario estima que puede ser una falla del sistema del ATM y decide retirarse del lugar, siendo ahí que ingresa el delincuente y retira la tapa falsa que es similar a la original que cubre la salida de extracción del dinero y acondicionada con elementos que dejan pegados los billetes, se lleva el dinero que intentaba retirar el verdadero cliente.

Muchas antiguas modalidades, siguen funcionando y siguen siendo intentadas por los delincuentes, por lo que nunca debemos descartar que por antiguas, ya no se utilicen. Hoy los fraudes con tarjetas, mayoritariamente, se realizan a través de medios de búsqueda de hurto de información y suplantación de identidad.

Métodos como el *skimming*; el *phishing*; o la copia de información de tarjeta y código de seguridad (para compras por Internet); robos de tarjetas y uso de ellas mientras los titulares no se dan cuenta; engaños telefónicos induciendo al titular (por lo general personas mayores) a concurrir a un ATM y mediante procedimientos dirigidos por el delincuente de forma telefónica, aduciendo que será beneficiario de un subsidio del Gobierno (modalidad muy común en este año de pandemia y crisis económica en el mundo) y que mediante ingeniería social luego se adueñan de su cuenta o hacen que el usuario termine realizando una transferencia a una cuenta del delincuente, etc.

Cientos de modalidades delictivas existen hoy en este sector de la delincuencia, desde estas estafas de diversas formas, hasta las explosiones de cajeros automáticos que han tenido y aún tienen a muchos países sin poder solucionar totalmente esas situaciones.

Las organizaciones ya dejaron de ser pequeños grupos para pasar a ser organizaciones trasnacionales que operan y se mueven a nivel mundial, que lavan sus ganancias tal cual lo hace cualquier otra forma de crimen organizado.

Mantienen alianzas con otras formas de delitos e interactúan entre ellas. Adiestran gente dentro de las cárceles que por ser del lugar, les pueden proporcionar insumos y logística

> Con la llegada de estos nuevos medios de pago, también comenzaron a proliferar pequeñas organizaciones de delincuentes que buscaban la forma de realizar compras, que fueran pagadas por los verdaderos titulares de esas tarjetas

que para quienes son extranjeros, a veces se les hace más difícil de conseguir.

CONCLUSIONES

Obviamente, estas modalidades, mientras existan los medios de pago tal como las tarjetas de crédito, débito, prepagos, o cualquiera de sus formas, serán una tentación y un permanente desafío para la delincuencia en la búsqueda de vulnerabilidades y para las marcas, sellos y emisores, la implementación de nuevas medidas de seguridad que permitan la continuidad del negocio, la confianza de los clientes y la mejora de los servicios que se ofrezcan.

En cuanto a quienes trabajamos en la prevención e investigación de estos ilícitos, considero que la continua capacitación, no solamente personal o de los equipos abocados a estas tareas, sino de fuerzas policiales y fuerzas de seguridad que se encuentren en puntos estratégicos de ingreso, seguimiento de información vinculada a las organizaciones trasnacionales (muchas veces nos conformamos con realizar el procedimiento que nos estaba dañando en nuestro país), pero no se buscan canales para compartir información hacia otros países (perdemos muchas veces la óptica, de que quienes operan en nuestro país hoy, mañana seguramente lo harán en un país vecino o lejano, pero seguro lo harán).

Unir esfuerzos a nivel internacional de aquellos que a nivel particular nos dedicamos a investigar y prevenir estas modalidades, estructurando redes de contactos donde podemos compartir las experiencias de nuestros países, posibilitar dentro de lo que legalmente se pueda, bases de información de delincuentes que han sido procesados en cada país y que mediante sistemas de autorizaciones en organizaciones dedicadas a esta temática, se pudiese consultar desde diferentes países, logrando con esto muchas veces, poder dar nombre a imágenes que tenemos de videovigilancia de comercios o ATM y que es un tiempo fundamental para el esclarecimiento y detención de estos delincuentes.

Las operaciones de ellos, no son normalmente durante muchos días, por lo que la celeridad de la investigación, puede dar beneficios a la pronta identificación, a la minimización del daño económico a empresas y particulares y a la colaboración con la justicia al instruirla que dicho delincuente, ya ha sido detenido en tal o cual país por delitos similares (aunque con esta información, la autoridad correspondiente que esté a cargo oficialmente de la investigación, pueda solicitar por los medios legales los antecedentes de estas personas en ese país).

Considero que hay mucho por hacer, que este tipo de delitos va a continuar su accionar y que el mismo nos afecta a todos y cada uno de los países (tal vez de diferente forma, pero seguro que a todos nos daña y mucho) y que todos aquellos profesionales que tienen y pueden aportar experiencia en el tema, debemos sumarnos y mancomunar esfuerzos que seguramente harán que cada uno de nosotros mejoremos nuestra gestión, implementemos o adecuemos procesos o formas de operar de otros países, que nos permitan mantenernos actualizados y prevenir factores de riesgo y vulnerabilidades que podemos aún tener en nuestros sistemas.

> Todo va cambiando, hoy el medio de pago electrónico es el medio de pago por excelencia. Las tecnologías van avanzando día a día, así como las formas de estafas y fraudes hacia estos medios de pago

Foto: DCStudio - Freepik

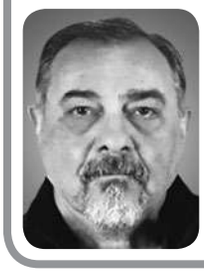
AGRADECIMIENTOS

Agradezco especialmente al señor Samuel Ortiz Coleman, ex presidente de ASIS México, quien gentilmente me invitó a participar en esta revista, para la cual, llevo a ustedes mi aporte.

No puedo dejar de agradecer a mi mentor en esta tarea de la investigación de fraudes con tarjetas, quien ha sido y continúa siendo mi guía, mi apoyo permanente y la persona que me ha enseñado el camino en esta dura lucha contra estas organizaciones delictivas en estas modalidades.

A quien mi profesión como policía me dio la oportunidad de conocer y gracias a su forma de ser, enseñándome y actualizándome permanentemente, llegar a ser excelentes amigos hasta la actualidad y quien despertara en mí la pasión de seguir aprendiendo día a día sobre este tema y hacer de cada caso un nuevo desafío, agradezco profundamente a Héctor Dante Cabano Etchebarne, gerente de Riesgo y Operaciones en varias empresas multinacionales del sector referido. A él, mi eterno agradecimiento. ■

Héctor Nessi,
director de HN Asesoramiento en Seguridad – Uruguay.



Más sobre el autor:

EL CRECIMIENTO DE *LOS E-COMMERCE* Y EL PAPEL DE LA SEGURIDAD

Cómo reducir el riesgo ante un posible fraude u otro ciberataque en el comercio electrónico

Foto: Creativeart - Freepik

MÉXICO | Ana Julieta Alvarado Aldama

El comercio electrónico ha presentado un crecimiento exponencial en el último año, debido a las circunstancias impulsadas por la emergencia sanitaria COVID-19, la IDC (International Data Corp.) reporta que se ha dado un crecimiento del 60%. Sabemos que esta "nueva normalidad" ha obligado a la sociedad a cambiar sus hábitos de consumo permitiendo que las empresas restructuraran sus modelos de negocios para abarcar más mercado.

A pesar de esto debemos considerar que existe una barrera de desconfianza que impide que este nuevo modelo de negocio se desarrolle completamente, ya que dentro de este miedo se encuentran los fraudes, que pueden representarse desde no recibir un producto, no adquirir lo que se mostraba en la página *web*, hasta publicar datos personales.

Foto: Creativeart - Freepik

TIPS

El papel de la seguridad dentro de los *e-commerce* es de suma importancia, ya que por medio de ésta podemos proteger nuestra información, puesto que a pesar de que las plataformas más famosas como Amazon, Mercado Libre y Liverpool, cuenten con métodos de pago seguros debemos tomar en cuenta las siguientes recomendaciones:

1. Utiliza una conexión segura; evita comprar artículos haciendo uso de wifi gratuitos o públicos, ya que no garantizan la seguridad de los datos ingresados en tu navegador.

2. Investiga acerca del producto o marca; busca información en redes sociales y buscadores para saber las opiniones de los usuarios, las tiendas *online* deben empezar su dirección por HTTPS para garantizar que la información que proporciones esté cifrada.

3. Ser precavido al momento de brindar datos personales; realizar las transacciones por medio de plataformas como PayPal y Google Wallet para garantizar que tu pago sea seguro, si no cuenta con estos métodos de pago investiga sus políticas de privacidad.

4. Si tienes duda acerca de la credibilidad de la tienda *online*, descártala y busca diferentes alternativas.

Tomando en cuenta estos consejos podemos asegurar nuestra información e incluir a nuestras vidas las nuevas tecnologías, que pronto eliminarán los métodos de compra tradicionales sin temor a la desconfianza que hoy existe. ■

Ana Julieta Alvarado Aldama,
socia directora de la empresa de mercadotecnia y publicidad JUMI-MKT.

Más sobre el autor:

JR

CONOCE NUESTRA GAMA DE EQUIPOS DE UNIFORMES O CREA TU PROPIA IMAGEN

CORTE Y CONFECCIÓN
BORDADOS
DISEÑO DE UNIFORMES

www.uniformesjr.com.mx

Palmira #14
Col. Francisco Villa
C.P. 54059, Tlalnepantla,
Estado de México.

ventas@uniformesjr.com.mx

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

CARACTERÍSTICAS DE UN PROGRAMA DE **SEGURIDAD INFORMÁTICA**

Conoce cuáles son los elementos que debe combinar un programa exitoso

Foto: Creativeart - Freepik

COLOMBIA | Javier Nery Rojas Benjumea

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

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

CONFIDENCIALIDAD

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

- **Aplicación de políticas de seguridad:** las políticas son los lineamientos generales, dictados desde la alta dirección, que formulan los parámetros que debe cumplir la organización para el logro de los objetivos formulados en la estrategia empresarial.

- **Clasificación de la información:** hace referencia a que todo documento realizado en la organización, debe tener asignado un parámetro de divulgación, en tanto su contenido sea más o menos sensible para la empresa.

> Los lugares donde la información es almacenada, ya sea en medios físicos o electrónicos, deben ser protegidos físicamente, para evitar el acceso fraudulento, o sustracción deliberada, así como los daños producidos por riesgos naturales, accidentales o provocados

- **Almacenamiento seguro de documentos:** los lugares donde la información es almacenada, ya sea en medios físicos o electrónicos, deben ser protegidos físicamente, para evitar el acceso fraudulento, o sustracción deliberada, así como los daños producidos por riesgos naturales, accidentales o provocados.

- **Criptografía:** es el arte de cifrar o codificar la información, en general la información más sensible debe estar protegida bajo este parámetro.

DISPONIBILIDAD

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

PRIVACIDAD

La definición de privacidad no se enfoca sobre la libertad de observación o acceso a la información, se debería enfocar sobre el uso de la información en formas conocidas para la persona que la provee. Es ahora posible recolectar y combinar información desde diferentes fuentes, las cuales han producido detalladas bases de datos cuyos componentes podrían ser usados de manera no correcta, o sin la debida autorización del dueño de la información.

Existen varios métodos técnicos para proteger las bases de datos y documentos con información sensible, en este sentido, es también importante proteger la información durante su transmisión por las redes internas y externas.

IDENTIFICACIÓN

Un sistema de información posee las características de identificación cuando es capaz de reconocer usuarios individuales. La identificación es el primer paso en conseguir el acceso para el material seguro, y sirve como soporte para las subsiguientes autenticación y autorización.

La autenticación e identificación son esenciales para estandarizar el nivel de acceso o autorización que se le concede a un individuo. Por lo general el nivel de identificación es dado mediante un nombre de usuario o ID; su manejo confidencial, así como su permanente actualización son claves a la hora de la implementación.

AUTENTICACIÓN

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

La autenticación e identificación son esenciales para estandarizar el nivel de acceso o autorización que se le concede a un individuo

AUTORIZACIÓN

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

Un programa de seguridad exitoso en información, combina estos y otros elementos. El arte de reducir y administrar el riesgo requiere comunicación y cooperación entre todos los niveles de la organización. En otras palabras el aseguramiento de los activos de información puede ser alcanzado sólo a través de la administración cuidadosa y la concientizacion de todos los funcionarios, lo cual genera cultura en torno al tema de la seguridad. ■

Foto: Creativeart - Freepik

REFERENCIAS

- *Management Of Information Security, Michael Whitman y Herbert Mattord.*

Javier Nery Rojas Benjumea, CPP,
jefe nacional de Seguridad en RANSA Colombia.

Más sobre el autor:

RESILIENCIA Y CIBERSEGURIDAD:

ENTRE LA COMPLEJIDAD, LAS TECNOLOGÍAS DIGITALES Y LOS SISTEMAS SOCIO-TÉCNICOS

Es necesaria la transformación de la cultura de las organizaciones a una donde los procesos no lineales, abiertos y discontinuos son parte fundamental de la respuesta a lo incierto y la creación de propuestas de valor innovadoras

Foto: Creativeart - Freepik

COLOMBIA | Jeimy Cano

INTRODUCCIÓN

Las organizaciones de la actualidad viven en un escenario cada vez más inestable y de situaciones complejas, las cuales obligan a actualizar su lectura estratégica y táctica de la realidad para renovar sus estrategias competitivas y tratar de identificar un lugar privilegiado desde donde movilizar su promesa de valor. En este ejercicio, las tecnologías de información y comunicaciones (TICS) juegan un papel fundamental para acelerar sus procesos, cambiar la manera como leen los intereses de sus clientes y cómo crean experiencias distintas en sus grupos de interés.

Las tecnologías emergentes (Day & Schoemaker, 2000) y aquellas disruptivas (McKinsey, 2013) aparecen en el escenario con su atractivo de novedad y transformación que, cautivando a los ejecutivos de alto nivel, logran generar la suficiente atención para movilizar los recursos requeridos con el fin de concretar ideas innovadoras que terminan en productos y servicios digitalmente modificados que en la mayoría de las veces logran conectar con las expectativas del cliente, haciendo de esta apuesta un nuevo punto de inflexión para la práctica de su sector negocio.

Si lo anterior es correcto, estamos asistiendo a un desarrollo acelerado en un entorno socio-técnico que combina comportamientos, datos, servicios, aplicaciones e infraestructura para crear un entramado de relaciones digitales que configuren una nueva relación entre las personas, así como en la dinámica social que se lleva a cabo (Cano, 2021). En consecuencia, se advierte un aumento de la complejidad de las nuevas conexiones entre los componente antes mencionados, que hace más exigente distinguir aquello que es exclusivamente un logro de lo digital y eso que es eminentemente parte de la esencia humana.

La primera dimensión dice que la resiliencia es dinámica, esto es: un proceso cíclico y acumulativo casi permanente en el que las organizaciones se preparan para afrontar una variedad de riesgos que varían en gravedad y frecuencia (antes), despliegan políticas de protección que pueden reducir su exposición a estos riesgos

ENTENDIENDO LA COMPLEJIDAD EN LAS TECNOLOGÍAS DIGITALES

El aumento de la complejidad previamente anunciado en palabras de Benbya *et al*. (2020) responde a características propias de las tecnologías digitales como son:

- **Integración:** pueden codificar y automatizar procesos cognitivos abstractos para convertir la nueva información en cambios adaptativos de los objetos.
- **Conexión:** con otras redes sociotécnicas y con actores sociales que se vuelven mutuamente dependientes.
- **Edición:** introduce procesos cognitivos cada vez más diversos en las redes de relaciones sociotécnicas.
- **Reprogramación:** el mismo *hardware* puede realizar diferentes funciones dependiendo del *software* que se ejecute en el dispositivo.
- **Comunicación:** las tecnologías digitales se comunican entre sí siguiendo un conjunto de protocolos acordados.
- **Identificación:** todos y cada uno de los dispositivos conectados a la infraestructura digital son identificables a través de una dirección única.
- **Asociación:** los objetos digitales son asociables a través de rasgos compartidos, que permiten identificar patrones emergentes.

Lograr un despliegue en profundidad de la ciberseguridad en una organización no está sujeto a qué tanta difusión, entrenamiento o *marketing* se haya efectuado, sino al proceso de transformación de una cultura basada en respuestas conocidas, a una que privilegia la experimentación y el error como ocasión de aprendizaje

Así las cosas, en un mundo cada vez más interconectado y de abundantes tecnologías digitales, las prácticas de seguridad y control deberán salir de su perspectiva exclusiva de regulación basado en estándares y buenas prácticas, para crear escenarios enriquecidos que respondan a la realidad de los inciertos que plantean los sistemas socio-técnicos y así, revertir el ejercicio actual de crear entornos confiables, sobre la base de las certezas que pueden ofrecer los marcos de trabajo conocidos (Dupont, 2013).

Entender la complejidad creciente de las propuestas de los productos y servicios digital y tecnológicamente modificados, es reconocer al menos cuatro elementos inherentes a su dinámica, que definen en sí mismos, las características de imprevisibilidad, influencia mutua, efectos cascada y fallas sistémicas (Benbya *et al*., 2020).

El primer elemento es la emergencia, como una propiedad de que tiene el sistema socio-técnico de crear estructuras o comportamientos que no son inherentes a sus componentes básicos, sino que surgen como parte de la interacción entre ellos. Esto implica que las tensiones e interacciones pueden tener efectos positivos o negativos que influencian de manera general la dinámica de la propuesta que se genere (Benbya *et al*., 2020). Tener la perspectiva de la emergencia es comprender la imprevisibilidad de fenómenos sociotécnicos a nivel de cada uno de sus componentes con impactos que pueden trascender al nivel de la sociedad en general.

El segundo elemento es la coevolución que implica la noción de interdependencia y adaptación mutua de los diferentes componentes del sistema socio-técnico, las cuales se hacen evidentes en relación con el entorno de ejecución y su evolución. Muchos de los sistemas podrán funcionar de forma adecuada o no en conexión con los retos del ambiente de operación. De igual forma, la presencia del sistema y su dinámica, podrá terminar influenciando y alterando el medio donde este desarrolla sus actividades (Benbya *et al*., 2020). Revisar esta perspectiva de coevolución es entender la influencia mutua que tienen tanto entorno como sistema socio-técnico para advertir posibles mutaciones o transformaciones que pueden ser esperadas o inesperadas.

El tercer elemento es el caos, como ese elemento que reconoce una realidad más probabilística que cierta, y más orientada en las desviaciones que en la linealidad y el determinismo. Es entender que la estabilidad de un sistema, no se alcanza cuando éste se detiene o no cambia, sino precisamente cuando es capaz de reconocer y balancear sus situaciones de no equilibrio, donde el aprendizaje juega un papel fundamental para crear las estructuras sistémicas que lo lleven a su estabilidad (Benbya *et al*., 2020). Explorar esta perspectiva de caos es tomar nota de las condiciones iniciales del sistema y revisar cómo escalan las causales de las inestabilidades que puedan llegar a comprometer toda la operación.

Foto: Creativeart - Freepik

El cuarto elemento habla de la dinámica escalable, aquella que identifica patrones similares subyacentes en diferentes niveles de análisis, que se convierten en un principio básico de la ciencia de la complejidad y da lugar a diversas teorías para caracterizar cómo una sola causa puede escalar en eventos extremos positivos o negativos y conducir a resultados similares en otras categorías (Benbya *et al*., 2020). Esta perspectiva de dinámica escalable advierte la repetición de patrones interconectados que pueden generar resultados positivos o negativos, esto es, fallas sistémicas según la dinámica del sistema y variaciones identificadas.

COMPRENDIENDO LA RESILIENCIA DIGITAL

Basado en esta revisión conceptual sobre las tecnologías digitales, los sistemas socio-técnicos y los elementos que crean y aceleran la complejidad de las innovaciones propias de la cuarta revolución industrial, es posible explicar por qué una organización puede tener ciberseguridad (basada en estándares y prácticas) y no ser resiliente, pero no viceversa (Dupont, 2019). Esto implica que la resiliencia reconoce la presencia de la inestabilidad como fundamento de su actuar y en ese sentido, exige una lectura sistémica de la realidad con los efectos que esto supone.

En este sentido, investigaciones recientes concluyen que la resiliencia, como disciplina que surge de la ciencia de los materiales que denota una propiedad de un material que absorbe energía cuando se somete a una tensión bien para mantener o retomar su forma o posición original después de ser doblada, estirada o comprimida, se articula en cinco dimensiones que hacen posible conectar los retos en diferentes niveles de comprensión como los demandan los sistemas socio-técnicos (Dupont, 2019).

La primera dimensión dice que la resiliencia es dinámica, esto es: un proceso cíclico y acumulativo casi permanente en el que las organizaciones se preparan para afrontar una variedad de riesgos que varían en gravedad y frecuencia (antes), despliegan tecnologías y políticas de protección que pueden reducir su exposición a estos riesgos, implementan protocolos de detección y respuesta que pueden facilitar la continuidad de sus operaciones, y mitigar los impactos negativos de los eventos adversos (durante), y, por último, adaptar sus sistemas y procedimientos para absorber las lecciones aprendidas (después) (Dupont, 2020, p.6).

Foto: Creativeart - Freepik

La cuarta dimensión declara que la resiliencia es adaptativa, lo que supone flexibilidad, esto es: reasignar rápidamente los recursos disponibles y desarrollar una cultura favorable a la improvisación y a la delegación de la toma de decisiones para hacer frente a peligros inesperados

La segunda dimensión afirma que la resiliencia está conectada en red, lo que significa: la integración de las organizaciones modernas y sus sistemas socio-técnicos en complejas redes de interdependencias que las habilitan y las limitan simultáneamente. Esto sugiere la presencia de una densa red de vínculos intra e interorganizacionales que se basan en una fuerte confianza y que pueden activarse con poca antelación para proporcionar recursos y conocimientos adicionales en caso de emergencia (Dupont, 2020, p.6).

La tercera dimensión insiste en que la resiliencia se practica, lo que demanda: ensayar escenarios de crisis que provoquen respuestas cognitivas que reten los saberes previos de los diferentes participantes del ejercicio e impacten el desempeño de la organización ante la adversidad. Estos ejercicios de entrenamientos regulares y bien calibrados —no demasiado predecibles pero sí manejables— contribuyen a la creación de un repertorio más amplio de respuesta a incidentes que esté disponible cuando se necesite (Dupont, 2020, p.7).

La cuarta dimensión declara que la resiliencia es adaptativa, lo que supone flexibilidad, esto es: reasignar rápidamente los recursos disponibles y desarrollar una cultura favorable a la improvisación y a la delegación de la toma de decisiones para hacer frente a peligros inesperados. La flexibilidad y la capacidad de respuesta necesarias para hacer frente a condiciones nuevas y difíciles pueden lograrse mediante la redundancia y la diversidad.

Las organizaciones resilientes no sólo muestran capacidades de adaptación durante durante una crisis, sino que, una vez restablecidas las operaciones básicas, son capaces de aprender de su experiencia e identificar mejoras en sus sistemas y procedimientos para mejorar su nivel de preparación contra futuros peligros (Dupont, 2020, p.7).

La quinta dimensión detalla que la resiliencia es controvertida, una afirmación que implica: enfrentar las tensiones existentes entre una racionalidad orientada al rendimiento que busca mejorar la productividad por encima de todo y una mentalidad orientada a la resiliencia que requiere compromisos entre la eficiencia y la adaptabilidad. Esto supone evaluar y aceptar adecuadamente su nivel de incertidumbre e ignorancia

para desarrollar estrategias metodológicas que les permitan sondear lo desconocido y diseñar planes de respuesta, sin sobrestimar sus capacidades de pronóstico (Dupont, 2020, p.7).

REFLEXIONES FINALES

Entrar en el paradigma de la ciberseguridad es conectarse con el ejercicio de la resiliencia. Un ejercicio que considerando las prácticas vigentes, es capaz de conectar y aprovechar la complejidad de las tecnologías digitales para crear oportunidades antes ignoradas, para lo cual se hace necesario darle vida a las cinco dimensiones revisadas previamente.

Lograr un despliegue en profundidad de la ciberseguridad en una organización no está sujeto a qué tanta difusión, entrenamiento o *marketing* se haya efectuado, sino al proceso de transformación de una cultura basada en respuestas conocidas, a una que privilegia la experimentación, el error como ocasión de aprendizaje y la incertidumbre como fundamento de sus acciones. En este sentido, la ciberseguridad sale de su visión técnica para ubicarse en un imaginario de construcción colectiva, que va más allá de la implementación tecnológica.

Cuando la ciberseguridad tiene como objetivo final asegurar la resiliencia digital de la empresa, comienza su exigente camino de evolución, crisis y renovación que transita entre mapas de riesgos, diseño de escenarios, simulaciones, responsabilidades compartidas, seguros y respuesta a incidentes que habla de un concepto clave para las organizaciones modernas, que muchas veces resulta ambigüo y contradictorio frente a las decisiones que los ejecutivos deben tomar, donde la diversidad y la redundancia son parte de las inversiones que se deberán priorizar y valorar para dar cuenta con la capacidades absorción y rebote previstas por la empresa.

El cambio en los sistemas sociotécnicos está tan instalado y embebido en la dinámica de sus componentes que la respuesta más acertada deberá ser aprovechar y entender su complejidad e incertidumbre, simplemente porque sus certezas son cada vez son menos ciertas. En este contexto, se hace necesaria la transformación de la cultura de las organizaciones de silos y desencuentros entre áreas, a una donde los procesos no lineales, abiertos y discontinuos son parte fundamental de la respuesta a lo incierto y la creación de propuestas de valor innovadoras.

Entender la complejidad creciente de las propuestas de los productos y servicios digital y tecnológicamente modificados, es reconocer al menos cuatro elementos inherentes a su dinámica, que definen en sí mismos, las características de imprevisibilidad, influencia mutua, efectos cascada y fallas sistémicas

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Así las cosas, la ciberseguridad, bajo esta perspectiva, y parafraseando a Ballester y Colom (2017) se configura como una capacidad adaptada al futuro, a la complejidad y al cambio, donde la información, los riesgos (conocidos y emergentes) y la creatividad son capaces de estimular un debate sobre la incertidumbre que termine deconstruyendo y retando sus saberes e imaginarios actuales y construyendo nuevas distinciones que no sólo demoren a los adversarios, sino que lo anticipen en su propio terreno. ■

REFERENCIAS

- *Ballester, L. & Colom, A. (2017) Epistemología de la complejidad y educación. Barcelona, España: Octaedro.*
- *Benbya, H., Nan, N., Tanriverdi, H. & Yoo, Y. (2020). Complexity and information systems research in the emerging digital world. MIS Quarterly. 44(1). 1-17. DOI: 10.25300/MISQ/2020/13304.*
- *Cano, J. (2021) Modelos formales de seguridad y control. Una reflexión no convencional de estrategias y prácticas probadas para un contexto digital. Global Strategy. Global Strategy Report No.17. https://global-strategy.org/modelos-formales-de-seguridad-y-control-una-reflexion-no-convencional-de-estrategias-y-practicas-probadas-para-un-contexto-digital/*
- *Day, G. S. & Schoemaker, P. (2000). Avoiding the pitfalls of emerging technologies. California Management Review, 42(2). 8–33.*
- *Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks? Technology Innovation Management Review. 3(7): 6-11. http://doi.org/10.22215/timreview/700*
- *Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity. 1-17. doi: 10.1093/cybsec/tyz013.*
- *Mckinsey (2013) Disruptive technologies: Advances that will transform life, business, and the global economy. - Mckinsey Global Institute. https://mck.co/3moDm3F.*

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

Más sobre el autor:

Foto: marymarkevich - Freepik

Foto: our-team - Freepik

LA SEGURIDAD Y SU EVOLUCIÓN AL CIBERTRABAJO

Los pros, contras y retos que conlleva el home office

VENEZUELA | Riomer José Castro Fernández

Con el arribo de la pandemia del COVID-19, las organizaciones alrededor del mundo han experimentado una serie de cambios en los procesos del negocio, obligándolas a adoptar medidas emergentes para así garantizar la continuidad de las operaciones comerciales.

La administración de la seguridad en las corporaciones no escapa de percibir estos cambios derivados de la pandemia, escenario que ha incitado a acelerar la adaptación y convergencia de todos los procesos tradicionales asociados a la protección de activos, con el uso de los medios de tecnología de información disponibles para conservar la rentabilidad y el aporte de valor, migrando a la mayoría de las organizaciones al cibertrabajo.

VENTAJAS Y DESVENTAJAS

Entre las ventajas obtenidas en este proceso de adaptación, podemos destacar la optimización de recursos tangibles dedicados a la protección de las instalaciones tal y como lo son el personal, infraestructura y equipos, lo que se ha traducido en la reducción de gastos operativos asociados a estas actividades dentro de las organizaciones; adicionalmente, con el empleo de los dispositivos tecnológicos de comunicación, se ha hecho posible que los profesionales de la seguridad puedan mantenerse conectados desde cualquier lugar con acceso a los servicios de la web.

Sin embargo, no sólo podemos resaltar las fortalezas de este tiempo evolutivo, también es necesario identificar una serie de desventajas que afectan el cumplimiento de las tareas inherentes a la protección, que como profesionales de seguridad no podemos perder de vista; por ejemplo, es potencialmente posible que el recurso humano dedicado al servicio de protección de instalaciones pueda verse familiarizado con la ausencia de supervisión directa o indirecta, generando como tendencia la disminución del esfuerzo dedicado con lo que respecta a los servicios de guarda y custodia.

De igual manera, los ejecutivos y oficiales de protección que no poseen competencias en el manejo de las herramientas de tecnología de la información, pueden impactar la eficiencia de los controles implementados, retrasando los procesos de registro y control de las actividades asociadas a las funciones

Foto: prostooleh - Freepik

de protección de activos; y por último, los oficiales de protección patrimonial, han adoptado funciones adicionales referentes al *safety* que han surgido de los protocolos definidos por las áreas de salud ocupacional para combatir las potenciales fuentes de contagio del COVID-19, sumando al personal de seguridad física tareas que no estaban previstas dentro de su contratación.

CALIDAD DE LOS SERVICIOS

Otra variable que ha impactado significativamente la continuidad de las operaciones en la mayoría de los países en Latinoamérica, ha sido la calidad de los servicios básicos requeridos para garantizar la comunicación y el enlace remoto con todos los procesos neurales del negocio; la electricidad y el Internet han tenido un funcionamiento intermitente, debido a que la infraestructura actual en nuestra región dedicada a soportar estos recursos no es suficiente para mantener la demanda de los ciudadanos que intentan mantenerse conectados a los servidores de las empresas desde sus residencias.

Estas desventajas pueden ocasionar una serie de inconvenientes que pudiesen incrementar el nivel de exposición de las instalaciones custodiadas, por lo tanto, es necesario tomar medidas preventivas que garanticen el cumplimiento de los objetivos definidos para la protección de los activos, pudiendo mencionar:

1. Definir un acuerdo contractual ajustado a la prestación de servicios adicionales a las funciones tradicionales prestadas por el personal de seguridad.
2. Ajustar los diversos manuales, normas y procedimientos en los puestos de servicio donde se vea reflejado el alcance de las funciones del personal de seguridad.
3. Mantener constante comunicación con los equipos de protección de las instalaciones a través de medios de tecnología de información y comunicación disponibles.

Foto: rawpixel-com - Freepik

Foto: teksomolika - Freepik

4. Contar con la disponibilidad de sistemas de videovigilancia inteligente, que permita implementar controles digitales adicionales para la supervisión de las tareas del personal.
5. Capacitar a los oficiales en las aplicaciones y sistemas de tecnología de seguridad antes de ser asignados a los servicios, estableciendo el paso a paso de estas herramientas en normas técnicas de uso.
6. Ajustar descripciones de cargo de los oficiales de seguridad incluyendo las actividades de *safety* que se están desarrollando en las organizaciones.
7. Contar con sistemas redundantes de electricidad e Internet que garanticen la no interrupción de las telecomunicaciones en el cumplimiento de las funciones operativas.

El cibertrabajo se ha convertido en el principal medio de gestión de actividades en las organizaciones a nivel mundial, en consecuencia, los profesionales de seguridad, como socios en la rentabilidad del negocio, deben acelerar el paso ante esta pujante realidad

> Los ejecutivos y oficiales de protección que no poseen competencias en el manejo de las herramientas de tecnología de la información, pueden impactar la eficiencia de los controles implementados, retrasando los procesos de registro y control de las actividades asociadas a las funciones de protección de activos

que obliga a adaptarse y proyectarse en el futuro como recursos competitivos y de valor agregado en la consecución del éxito organizacional, de lo contrario, será muy difícil mantenerse vivo dentro del sistema evolutivo en el cual nos encontramos.

Para finalizar, cito a Charles Darwin, naturalista inglés reconocido como uno de los científicos más influyentes en el planteamiento de la idea de la evolución y que resume el compromiso que como líderes de seguridad debemos asumir para garantizar nuestro aporte dentro de las organizaciones: "No es la más fuerte de las especies la que sobrevive, tampoco es la más inteligente la que sobrevive, es aquella que se adapta mejor al cambio". ■

Riomer José Castro Fernández, *Security Supervisor* en Cardon IV (ENI / REPSOL).

Más sobre el autor:

Nuevo grupo | Añadir participantes | Añadir asunto | ✓ | Administrador creó el grupo | Administrador te añadió

Foto: Creativeart - Freepik

MENSAJERÍA INSTANTÁNEA MÓVIL,

LA ÚLTIMA LÍNEA DE DEFENSA COMUNITARIA

ECUADOR | Esteban J. Acosta

Lo que hace apenas algunos años no podíamos concebir, actualmente forma parte de nuestro día a día; con infinidad de objetivos, sean sociales, culturales, deportivos, religiosos, etc., familia y amigos, o absolutamente desconocidos entre sí, están juntos, aún distantes.

Con más de dos mil millones de usuarios en el año 2021 y muy cerca a Facebook, WhatsApp se ha convertido en el segundo canal de comunicación digital interpersonal, casi la cuarta parte de los habitantes del mundo lo utilizan al menos una vez por mes.

Comunicar una idea, participar en un plan, invitar a un evento, motivos sobran para que las personas saquen el mayor provecho a la funcionalidad de grupo en WA.

A nivel local y presumiendo sucede exactamente en la región y por qué no globalmente, bajo un pensamiento un tanto apolítico, con el cual se identifica la mayoría de integrantes en las sociedades, por antecedentes y circunstancias que no ameritaría sean

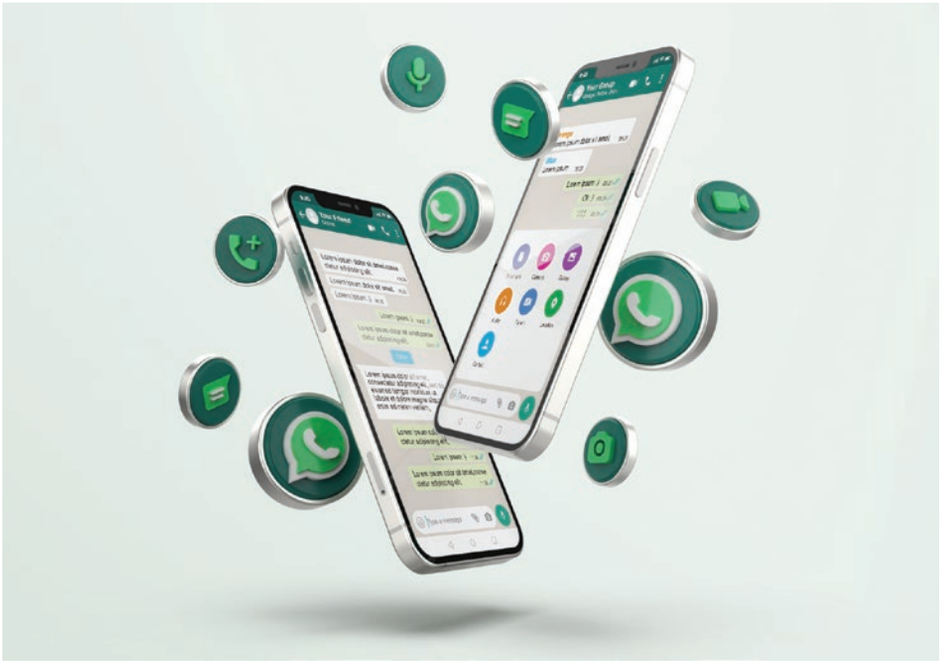


Foto: Creativeart - Freepik

mencionados, la gente, aspirando tiempos mejores, motivados por sus propios derechos, deseos, necesidades y aspiraciones, ha buscado impulsar iniciativas, propósitos y proyectos de estabilidad, mejora, superación, entre otros, para alcanzar lo que aparentemente la gran mayoría aspira: bienestar y tranquilidad.

Es una certeza que por la densidad poblacional y relacionados, ciudades y estados no se encuentran preparados para satisfacer las necesidades básicas de sus integrantes, entre ellas encabezando la seguridad.

Uno de los aspectos precisamente, porque los proyectos inmobiliarios de vivienda se conceptualizan cada vez más como Gated Community, buscando disponer condiciones para que individuos, familias y sociedad en general, puedan a través de la autogestión, contar con factores como la privacidad y seguridad, en definitiva, la paz relativa; se ha optado por establecer vías de comunicación directa entre sí, integrando a instituciones indispensables, como la fuerza pública local, por ejemplo.

Foto: Creativeart - Freepik

HERRAMIENTA PARA LA SEGURIDAD

Calles, conjuntos, urbanizaciones y barrios, han formado grupos WA, sus integrantes los residentes, coordinadores y directivos, seguridad privada y en ocasiones seguridad pública, a veces todos juntos, otras de modo independiente.

Reportar un sospechoso, alertar sobre un ilícito, notificar un incidente de servicios básicos, así como recomendar medidas de prevención y protección o incentivar a buenas prácticas de seguridad personal, se han vuelto los asuntos diarios constantes de los grupos, a través de los cuales noticias, videos, audios e imágenes, captan nuestra atención y motivan inmediatamente una reacción.

La seguridad privada igualmente, además de los medios tradicionales de comunicación con su personal y clientes, ha podido aprovechar las funcionalidades de los *smartphones*, principalmente a través de WA, para su operación permanente, como una vía oficial de contacto o una alternativa de contingencia; mejorar los tiempos de respuesta, reforzar el control, presentar reportes e informes, todo se ha facilitado gracias a esta *app*, para la cual, de alguna manera, sugerimos e invitamos a su uso.

Con más de dos mil millones de usuarios en el año 2021 y muy de cerca a Facebook, WhatsApp se ha convertido en el segundo canal de comunicación digital interpersonal, casi la cuarta parte de los habitantes del mundo lo utilizan al menos una vez por mes

La policía recibe constantemente reportes de parte de los ciudadanos, con ubicaciones de posibles delincuentes, características de personas y vehículos, detalles sobre modos de operación, antecedentes y hábitos, lo que ha podido ser un valioso aporte para que su gestión sea más eficiente y visible.

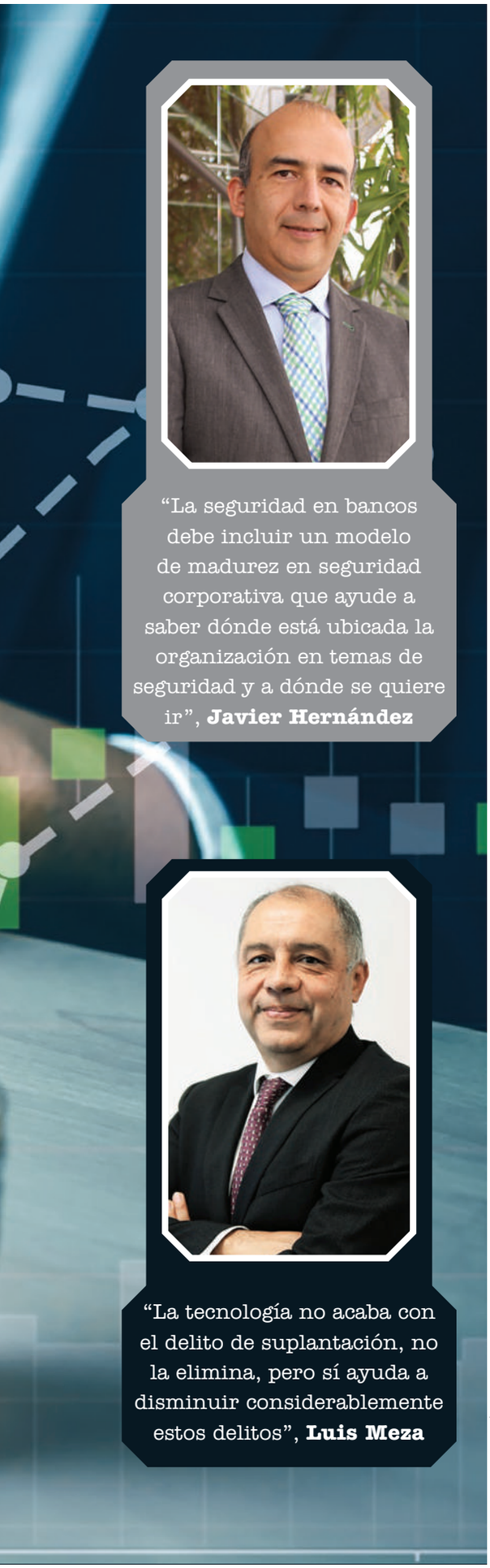
La coyuntura generada por WhatsApp es difícilmente comparable, ha permitido como en pocos casos, que la sociedad civil y la fuerza pública interactúen como verdadera comunidad, con un fin común, mantener el orden y la convivencia general, como buenos vecinos. ■

Esteban J. Acosta,
gerente general en Grupo Fractal.

Más sobre el autor:

SEGURIDAD EN BANCOS

Los riesgos y amenazas a la seguridad bancaria varían y se adaptan continuamente, afectando a miles de usuarios y entidades financieras a diario. Para prevenir esos riesgos y amenazas a la seguridad financiera y mantener tus cuentas bancarias seguras, es necesario estar actualizado y conocer los modus operandi de los cibercriminales



"La seguridad en bancos debe incluir un modelo de madurez en seguridad corporativa que ayude a saber dónde está ubicada la organización en temas de seguridad y a dónde se quiere ir", **Javier Hernández**

"La tecnología no acaba con el delito de suplantación, no la elimina, pero sí ayuda a disminuir considerablemente estos delitos", **Luis Meza**

Foto: Creativeart - Freepik

MÉXICO | Erick Martínez / *Staff* Seguridad en América

La seguridad en bancos a través de los años ha ido evolucionando constante y fuertemente, antes la seguridad en bancos era considerada sólo como un elemento de reacción en caso de algún siniestro o evento delictivo, sin embargo, hoy en día la seguridad bancaria forma parte de la seguridad corporativa, además de que tiene muchas aplicaciones más allá de prevenir incidentes, a través de los sistemas de videovigilancia grabar asaltos, reaccionar, etc.

La tecnología sin lugar a dudas ha sido un elemento crucial para que la seguridad bancaria hoy pueda apoyar incluso en áreas como *Marketing*, Ventas, etc. En términos generales, la seguridad bancaria se refiere a todos los métodos, herramientas, procedimientos y protocolos aplicados por una institución financiera para salvaguardar el patrimonio, información y demás activos de sus clientes y colaboradores.

A continuación, se presentarán perspectivas y métodos de aplicación vistas desde diferentes expertos en seguridad bancaria, con los que **SEA** pudo conversar.

"Hoy en día los datos biométricos también son susceptibles a suplantación", **Pedro Villanueva**

Para Javier Hernández Vargas, director de Continuidad de Negocio y Seguridad Física para Latinoamérica en Grupo Financiero Banorte, la seguridad en bancos debe incluir un modelo de madurez en seguridad corporativa que ayude a saber dónde está ubicada la organización en temas de seguridad y a dónde se quiere ir, basados en estándares internacionales, 12 dominios agrupados en tres familias:

A) Liderazgo y cultura:

1. Compromiso de alta dirección y cómo apoya las iniciativas.
2. Estructura de gestión de roles y responsabilidades.
3. Seguimiento y aseguramiento.
4. Cultura y comportamiento.
5. Educación y comunicación.

B) Planeación, políticas y procesos:

6. Estrategia y planeación.
7. Políticas, procesos y procedimientos.
8. Gestión de riesgos.
9. Administración de incidentes.

C) Dominio de seguridad:

10. Seguridad personal.
11. Seguridad de la información.
12. Seguridad física.

Esos 12 dominios tocan diversos puntos de seguridad en cuatro niveles: informal, básico, administrado y mejora. El informal es el menos recomendable, pero donde empiezan las empresas de seguridad con sus primeras actividades. El básico es el cumplimiento parcial, cuentan con algún requerimiento de autoridades y es un sistema que sigue desarrollándose.

El administrado ya cumple con los requerimientos mandatorios de las autoridades, del sector y de la industria, de mejores estándares, cuentan con recursos dedicados y se hace lo que se necesite para administrar un riesgo. El de mejora reacciona a los riesgos que se van presentando y se llevan a otro nivel, se selecciona, maneja y se mide, tienen la capacidad de reacción por agilidad en estructura que lo permite. Es

"La ciberseguridad es el área más joven o nueva, pero hoy en día es la más poderosa y juega el rol más importante en la estrategia de un modelo de seguridad integral", **Hugo Montes**

importante que los gerentes de Seguridad se pregunten a qué nivel quieren llegar y para ello hay que identificar el nivel en el que se encuentran.

USURPACIÓN DE IDENTIDAD

Luis Meza, director regional de Proyectos de Seguridad en Citibanamex, junto con Pedro Villanueva Melendez, director de Seguridad en INBURSA, platicaron un tema que preocupa a muchos directores de Seguridad de un banco, que es la usurpación y robo de identidad, la apropiación de la identidad de la persona y asumirse frente a otras personas, el objetivo es acceder a recursos o información a nombre del titular.

La banca para prevenir la usurpación de identidad comenzó a monitoreo de números telefónicos, direcciones, referencias, correos electrónicos, hasta evolucionar a la validación de datos biométricos, identificación oficial (INE), para verificar datos de los clientes. "Hay que trabajar en la prevención, las redes sociales son una puerta grande para la usurpación de identidad", mencionó Luis Meza.

La tecnología no acaba con el delito de suplantación, no la elimina, pero sí ayuda a disminuir considerablemente estos delitos, aún hay muchas situaciones donde se depende de un tercero para la validación de datos, incluso los biométricos. Ninguna tecnología es 100% eficaz, y la delincuencia siempre está innovando. El reto principal es la estandarización, hay muchos recursos tecnológicos avanzados, al guardar y proteger datos biométricos convertirlos en algoritmos, mas no el dato como tal.

Pedro Villanueva comentó que en México el robo de identidad ocupa el número ocho en materia de legislación. En la Ciudad de México, Estado de México y Baja California, se tipifica como delito y se da entre uno a cinco años de prisión. Se recomienda que una vez afectados o son víctimas hay que ejercer la denuncia, ratificar a las autoridades que perdieron documentos o que llegó un estado de cuenta no reconocido, también acudir a la tienda comercial, banco, para manifestar que no realizó el trámite, para evitar daños económicos y reputacional.

La denuncia es importante, porque la institución la va a solicitar para dar seguimiento y poder deslindar la responsabilidad. Es importante tener el sistema de buró de crédito activado, pues éste notifica cualquier movimiento al titular por cualquier consulta. Hoy en día los datos biométricos también son susceptibles a suplantación.

El uso de tecnología en la parte presencial, se mitiga bastante con medidas de identificación biométrica, por ello hay que actualizarlo constantemente y crear herramientas de validación cada vez más sofisticados.

MODELO INTEGRAL DE SEGURIDAD CORPORATIVA Y CIBERSEGURIDAD

Gracias a la transformación digital se incorporan muchas nuevas tecnologías que han cambiado la forma de ver y hacer la vida, entre ellas la banca, por ejemplo, las transacciones digitales entre otras actividades, han reducido las visitas a las sucursales considerablemente, abriendo otros canales de posibles vulnerabilidades para usuarios, clientes y la propia institución.

"La seguridad ahora tiene que adaptarse acorde a las nuevas necesidades de las instituciones financieras, y el perfil del director de Seguridad en un

Foto: Creativeart - Freepik

nuevo modelo de seguridad corporativa no debe dejar de lado estas funciones", comentó Fernando Martín Gómez Villarreal, director de Seguridad en Compartamos Banco.

Hugo Raúl Montes Campos, director de Seguridad y Prevención de CI BANCO, coincidió en que hoy los riesgos se están mudando al mundo digital, por lo tanto, el principal cambio que debe haber en un director de Seguridad, está en la forma de evaluar los riesgos, éstos se miden a través de cómo se guarda la confidencialidad, disponibilidad, y la

"La seguridad ahora tiene que adaptarse acorde a las nuevas necesidades de las instituciones financieras", **Fernando Gómez**

CONSULTORES INTERNACIONALES DE SEGURIDAD ASOCIADOS

CONSULTORES EN SEGURIDAD INTEGRAL

Guardias Armados

- Custodia de Vehículos
- Protección a Ejecutivos
- Guardias Intramuros
- Rastreo Satelital
- Central de Monitoreo
- Evaluación de Riesgos

37 Años

Gracias a tu confianza

www.consultoresenseguridad.com

Sinaloa 33, Col. Roma Norte,
C.P. 06700, CDMX.
Tels.: 5525 6847 / 5525 6850

integridad de la información. "Cómo se custodian las joyas de la corona, que es la información", señaló.

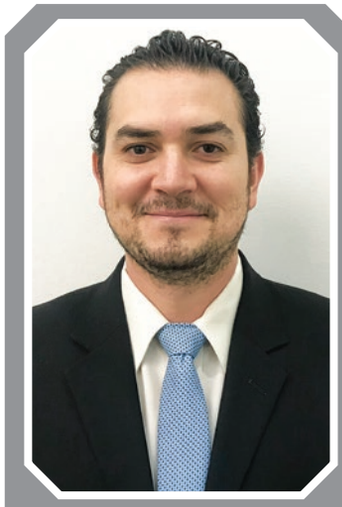
Como seguridad necesariamente hay que evolucionar hacia las nuevas capacidades y competencias que demanda hoy el sistema financiero en todo el mundo.

La ciberseguridad se ha convertido en la nueva punta de lanza del área de Seguridad, se tiene que proteger con un plan integral de ciberseguridad, el cual representa un gran esfuerzo para las empresas, inicialmente bancos.

"La ciberseguridad es el área más joven o nueva, pero hoy en día es la más poderosa y juega el rol más importante en la estrategia de un modelo de seguridad integral. Hoy existe la Nube, donde la información está en cualquier parte del mundo, sin embargo, en la Nube también se tiene que cuidar la información", comentó Hugo Montes.

Por ello hay que cumplir con regulaciones gubernamentales en cuanto a las herramientas que se ocupan en la infraestructura, el manejo de información y la privacidad de los datos. "Por otra parte, se tiene que estar inmersos en todos los procesos relevantes en los cuales se utiliza la tecnología:

"Las nuevas medidas implementadas ayuden a mitigar los delitos y que a su vez sean medidas no violentas", **José Antelmo Cuellar**



"Como banco internamente hay que reforzar muchas cosas y la principal forma de prevenir de manera interna es con la capacitación del personal", **Diego de la Torre**

dentro de los procesos que aseguren que la herramienta tecnológica está puesta de acuerdo a los parámetros programados evite que la información salga, la arquitectura de seguridad para que toda la tecnología este integrada en uno mismo, tener el área técnica capaz de implementar las herramientas tecnológicas, una estrategia muy clara y una inversión de recursos que obligan a estar regulados", mencionó Fernando Gómez.

Añadió que "la evolución del modelo de prevención de fraudes por su parte debe proteger productos, canales y servicios, todas las transacciones, pagos, manejo de fondos, es pensarlos a través de la digitalización", lo que ha orillado a actualizar certificaciones específicas para la prevención de fraudes, pues ésta también evoluciona.

LOCALIZACIÓN SATELITAL EN LA BANCA

José Antelmo Cuellar Retama, gerente nacional de Seguridad Patrimonial en Bancoppel, habló acerca de las medidas de seguridad que ayudan a mitigar los delitos. La evolución en los sistemas y estrategias de seguridad ha empujado hacia soluciones más profesionales con plataforma de sistemas de alarmas donde se tenga a muchas personas conectadas a la vez, centrales de monitoreo, etc.

Desde su perspectiva y práctica, José Antelmo Cuellar mencionó que siempre se están buscando que las nuevas medidas implementadas ayuden a mitigar los delitos y que a su vez sean medidas no violentas, como es el caso de la localización satelital. "Lo que buscamos es que el delincuente tome el dinero, se vaya, y lo atrapemos fuera del banco, a través de las herramientas tecnológicas, apoyado también de las autoridades, como con el Centro de Comando, Control, Cómputo, Comunicaciones y Contacto (C5), para no poner en riesgo a los usuarios, al personal y los bienes".

La localización satelital es una gran herramienta que ha ayudado a detener a diferentes grupos delictivos, logrando bajar el índice delictivo. Funciona por muchos puntos principalmente la tecnológica, la parte operativa, el contar con protocolos de actuación muy precisos y personal bien capacitado, además de la coordinación con las autoridades mu-

Foto: Creativeart - Freepik

nicipales, estatales y las fiscalías, para poder gestionar cateos y aseguramientos.

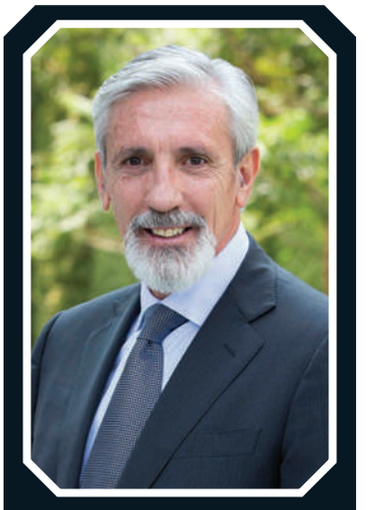
FRAUDES CON CHEQUES

Diego de la Torre, gerente ejecutivo de Seguridad en Banco del Bajío, habló de cómo evitar fraudes con cheques, y lo que están haciendo los expertos para disminuir los delitos. Éste se comete comúnmente cuando se realiza una compra de algún bien, puede ser la venta de un auto o un inmueble, el defraudador emite un cheque sin fondos o que sabe que va a rebotar. En la actualidad las transacciones digitales han alcanzado mucho terreno, por ello es que este tipo de delito ha perdido fuerza, además de que las áreas de Seguridad han implementado una serie de medidas y contramedidas para salvaguardar el patrimonio de los usuarios y clientes.

"Como área de Seguridad nos preocupamos por identificar fuga de información o documentos, así como posible coalición con trabajadores", mencionó Diego de la Torre.

La falsificación de cheques y firmas se alteran o modifican la banda magnética, el nombre del cliente, la cuenta, el monto, o la falsificación del papel mismo. Los delincuentes no siempre buscan personas con altos recursos, hay un alto índice de fraude a personas de bajos recursos económicos.

"Como banco, internamente hay que reforzar muchas cosas y la principal forma de prevenir de manera interna es con la capacitación del personal, donde puedan validar las medidas de seguridad que nuestros documentos tienen, los cheques propios y los de otros bancos", puntualizó Diego de la Torre.



"Necesitamos modelos de cooperación interinstitucional apegados a la ley que permitan fortalecer la comunicación entre sectores públicos y privados", **Carlos Sanroma**

"Los avances tecnológicos en dispositivos para sucursales han ido evolucionando constantemente haciendo cada vez sistemas más robustos", **Víctor Manuel Durán**

ALARMAS EN SUCURSALES

Manuel Ferrer, gerente de Seguridad de Actinver Banco; y Víctor Manuel Durán González, director de Seguridad de la misma empresa, explicaron que la seguridad en la actualidad está dividida en dos: seguridad operativa y ciberseguridad, los avances tecnológicos en dispositivos para sucursales han ido evolucionando constantemente haciendo sistemas cada vez más robustos.

Víctor Durán mencionó que los antecedentes más importantes y todos los pasos, etapas y años que pasó la seguridad en los bancos contra la intrusión, para llegar a los grandes avances tecnológicos hoy en día, son a través de la Nube, IoT (Internet of Things), etc. La tecnología de sistemas de alarmas, los centros de trabajo y operación y su relación con los centros de monitoreo, la infraestructura con cámaras su evolución, y como las imágenes hoy son esenciales para verificar las alarmas, dar seguimiento a un robo, y sobre todo prevenir.

Es importante resaltar el apego a las políticas y procedimientos, por ello es fundamental la capacitación a empleados de todos los niveles en sucursales y en centros de monitoreo, para poder mandar alarmas verídicas.

COORDINACIÓN DE SEGURIDAD BANCARIA CON AUTORIDADES

Sin duda alguna los delitos hacia la banca pueden llegar a tener un alto impacto en las instituciones financieras, pero no sólo a los bancos, sino también a los clientes y usuarios, la coordinación con autoridades para poder hacerle frente a este tipo de delitos es sumamente necesaria.

Epigmenio Treto Martínez, subdirector de Infraestructura Crítica y Tecnología en Banorte, comentó que debe existir una coordinación y relación con altos mandos, de los diferentes niveles de Gobierno y autoridades, esto puede dar resultados muy positivos para la

"La información de inteligencia, se recolecta gracias a la coordinación con autoridades, se intercambia información para generar estrategias, cursos de capacitación, acciones coordinadas en vinculación y coordinación con áreas jurídicas", **Ciro Ortiz**

"Trabajar desde diferentes instancias para poder tipificar los delitos bancarios en la legislación mexicana y así facilitar la persecución de los delitos", **Epigmenio Treto**

atención de delitos bancarios. Así como trabajar desde diferentes instancias para poder tipificar los delitos bancarios en la legislación mexicana, así facilitar la persecución de los delitos.

"El éxito también depende de que la banca pueda capacitar a las autoridades en esta materia, por lo tanto, los especialistas técnicos se convierten en una persona clave para la resolución de delitos", señaló.

Epigmenio expuso que la Ley Federal de Seguridad Privada (modificada en abril de 2020), obliga a las empresas de este rubro, a mantener registrados a sus elementos. No el 100% de las empresas de seguridad privada cumplen con esa reglamentación, esto obliga a las empresas que dan servicios a que estén debidamente establecidos, capacitados y alineados a los requerimientos de la ley al igual que los especializados deben estar en norma. Se estima que sólo el 65% de las empresas están debidamente constituidas. "La seguridad bancaria tiene que cambiar, ser más estratégica y analítica, alineada al negocio", puntualizó.

Por su parte, Ciro Ortiz Estrada, director de Seguridad en SEPROBAN, habló acerca de la colaboración y coordinación con las autoridades, y en el papel que desarrolla SEPROBAN ha logrado el generar convenios de colaboración con los cuerpos de seguridad y procuración de justicia. A través de los apoyos que solicitan las instituciones bancarias, ya sea mediante el centro de monitoreo o llamada de emergencia, llegan al centro de coordinación para atención de incidentes bancarios, reciben solicitud de emergencia y se coordinan el evento con apoyo de las autoridades.

De igual manera la información de inteligencia, se recolecta gracias a la coordinación con autoridades, se intercambia información para generar estrategias, cursos de capacitación, acciones coordinadas en vinculación y coordinación con áreas jurídicas. La coordinación con el SECAE es un modelo perfectible que ayuda a mitigar actos delictivos y fortaleciendo prácticas en módulos del C5.

Carlos Sanroma Sánchez, director de Seguridad en BBVA, mencionó que en México existe la necesidad de colaboración para combatir cualquier delito, en esa línea se enfrenta una complejidad muy importante, principalmente por cómo está compuesto geográficamente y políticamente. "Necesitamos modelos de cooperación interinstitucional apegados a la ley que permitan fortalecer la comunicación entre sectores públicos y privados".

Declaró sobre la necesidad de disponer de fiscalías especializadas donde concentrar todas las denuncias por ilícitos bancarios y así tener mayor trazabilidad y seguimiento de los casos, con objeto de asegurar la persecución y el combate del delito que nos lleve a neutralizar y minimizar su impacto sobre la personas y sus bienes. "Tenemos que buscar formas de facilitar al ciudadano la presentación de denuncias que permita el acercamiento del mismo a los órganos de procuración de justicia, generando confianza entre el ciudadano, sujeto pasivo de un hecho delictivo y el sistema de seguridad pública", agregó. ■

Foto: Creativeart - Freepik

"Es importante resaltar el apego a las políticas y procedimientos, por ello es fundamental la capacitación a empleados de todos los niveles en sucursales y en centros de monitoreo", **Manuel Ferrer**

EXECUTIVE PROTECTION SUMMIT 2021

2021

19 Y 20 OCTUBRE

PINK PANTHER

Olivera Ćirković

Greg Williams

Brian Marren

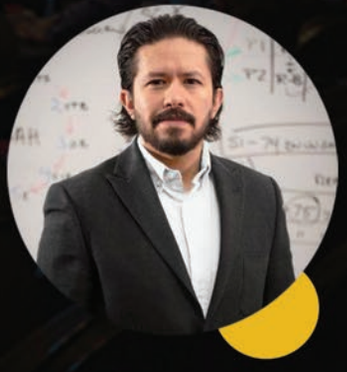
Byron Rodgers

REGÍSTRATE

CON EL CÓDIGO

#SEA

Y RECIBE UNA TARIFA PREFERENCIAL



Isaac del Bosque

Ivan Ivanovich

Gonzalo Senosiain

Christian West

¡Y muchos más!...

CUPO LIMITADO

REGÍSTRATE AHORA www.epsummit.com.mx

SEGURIDAD EN EVENTOS MASIVOS: GEL, SANITIZANTE, ACCIÓN

Con una pérdida económica de más de 38 mil millones de pesos (mil 902 millones de dólares), la industria del entretenimiento ha tenido que adaptarse y encontrar nuevos escenarios para que el COVID-19 no la lleve a la quiebra, pero lo más importante: para que no afecte la seguridad de los asistentes y personal del medio

Foto: Creativeart - Freepik

MÉXICO

Mónica Ramos / *Staff* Seguridad en América

La música, el teatro, el cine y los festivales, todos esos eventos al aire libre y en recintos con filas y filas de asientos esperando a sus ocupantes, quedaron vacíos cuando fue anunciada la emergencia sanitaria por COVID-19 en México en marzo de 2020. El famoso Vive Latino se llevó a cabo entre incertidumbre y temeridad, y fue notoria la disminución no sólo del número de asistentes, sino también del ambiente que entre ellos había.

Se puede decir que fue uno de los últimos eventos masivos de la vieja normalidad, pero no para siempre, ya que la industria del entretenimiento tiene una derrama económica muy importante para el país, con el 7.4% del Producto Interno Bruto (PIB)[1]. Sin embargo la Asociación de Permisionarios, Operadores y Proveedores de la Industria del Entretenimiento y Juego de Apuesta en México (AIEJA), quien aglomera a cines, teatros y casinos, estimó las pérdidas del sector en más de 38 mil millones de pesos (mil 902 millones de dólares).

A eso le faltan las pérdidas de organizadores de eventos en vivo como OCESA, operada por Corporación Interamericana de Entretenimiento (CIE), quien reportó que en el tercer trimestre de 2020 tuvo un 82% menos de ingresos que lo registrado en igual periodo del año pasado.

Alrededor de 600 conciertos masivos fueron suspendidos, evidentemente por el riesgo de salud y seguridad que eso implicaba, afectando no sólo a las empresas y sus empleados, sino también a los músicos, artistas, *staff*, todo el personal que labora en el medio del espectáculo y por supuesto a los espectadores, porque este tipo de eventos son parte de la vida de las personas, de la diversión y el goce.

Es por eso que conforme fue avanzando el confinamiento, los procesos de seguridad y las indicaciones de las autoridades, así como los estudios del virus, el medio del espectáculo generó nuevos espacios para esta nueva normalidad. El 7 de agosto de 2020 se dio el primer autoconcierto en México. El Foro Pegaso, ubicado en el Aeropuerto de Toluca (Estado de México), recibió a los vehículos y sus no más de cinco ocupantes en cada uno, con cuatro filtros de seguridad y un kit de sanidad. Pero ante la euforia de los espectadores, hubo varios que se bajaron del auto para corear al aire libre las canciones de Moderatto.

El *streaming* a nivel mundial también fue otra opción para esta industria, conciertos en línea en diferentes plataformas, unas con mejor o menor calidad, con un chat en vivo en el que los participantes pueden mandar saludos, escribir sus opiniones o como en México, hasta las frases célebres de los conciertos como "ahí va el agua". Esto le dejó a CIE el año pasado, 222 millones de pesos (11 millones de dólares)[2].

DE VUELTA AL ESCENARIO

Gracias al desarrollo de diferentes vacunas contra el COVID-19, se puede ver la luz en el camino, todavía al final del túnel no, porque aún falta tiempo para adaptarse y aceptar esta nueva normalidad, así como un mejor control de los contagios, sin embargo a raíz de la vacunación, en México comenzaron a efectuarse eventos masivos, aunque sólo con el número de asistentes permitidos por las autoridades sanitarias, y las adecuaciones de acuerdo al semáforo epidemiológico, pero ya se han realizado conciertos, reabrieron teatros, cines, y hay fechas para festivales como el Pa'l Norte (Monterrey, Nuevo León), entre otros.

Es por ello que **Seguridad en América** (**SEA**) realizó entrevistas a expertos en el tema para ahondar más sobre las medidas, estrategias y riesgos de seguridad en esta nueva normalidad para eventos masivos. Carlos Seoane Noroña, socio director de Seoane Consulting Group; Violeta Edith Arellano Ocaña, gerente de Seguridad Integral en Corporación Interamericana de Entretenimiento (CIE); C.T.A. Carlos Sainz Luna, coordinador de gestión de riesgos, servicios de navegación en el espacio aéreo mexicano; y Arnaldo Lovera, gerente de Canales para Motorola Solutions México, quienes nos compartieron su análisis sobre el tema y su experiencia en la industria de la seguridad.

Foto: Creativeart - Freepik

CARLOS SEOANE NOROÑA, SOCIO DIRECTOR DE SEOANE CONSULTING GROUP

SEA: De acuerdo con su análisis, experiencia y en dado caso de que con semáforo verde se reactiven los eventos masivos, ¿cuáles considera que serán las características de éstos en materia de seguridad o cómo cambiarán los eventos masivos en la pospandemia? (Número de asistentes, medidas de seguridad, bioseguridad, delincuencia, etc.).

"Los eventos masivos, ante todo, son un negocio y deben generar ganancias. No veo un concierto de los Rolling Stones en el Foro Sol con una capacidad de 50 a 55 mil espectadores con solamente la tercera parte de su aforo tratando de disminuir el riesgo de contagios. Ningún promotor arriesga su capital si no tiene la esperanza de vender todos los boletos. El reto será convencer al público adulto (no los jóvenes) para que decida encerrarse con miles de personas y el riesgo que ello conlleva, así sea al aire libre.

La delincuencia ha retornado a sus niveles prepandemia, el bono COVID-19 dio resultados en descensos marcados durante cuatro meses del año 2020. Este no es un factor que agrave o atenúe los eventos masivos. Asumo que todo lo que hemos visto y vivido en materia de protocolos de limpieza y sanidad serán llevados a cabo al 100%. Pero el que la sala, plaza, arena o estadio estén perfectamente desinfectados, no impedirá los gritos, cantos y porras de los asistentes que —involuntariamente— esparcirán sus gotículas de saliva. ¿Podrás convencer a 10 mil personas de permanecer con tapabocas mientras ven a su artista favorito? ¿Y cómo revisar a los asistentes a la hora del acceso al inmueble para evitar que entren armados o con objetos prohibidos? Este es un proceso establecido desde hace décadas que se va a tener que dejar de lado por lo pronto. La industria de la música en vivo y del entretenimiento ha sufrido grandes pérdidas y lo seguirá haciendo hasta que la vacunación y la inmunidad de rebaño cumplan su objetivo".

PROTEGE.MX

GRUPO CORPORATIVO DE PREVENCIÓN

XV años

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

Armados para el traslado de valores
Armados Intramuros.

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

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

manuelgm@grupogcp.mx / www.grupogcp.mx

55 79316739

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

ACERCA DE...

Carlos Seoane egresó de la Universidad Iberoamericana de la Ciudad de México, con un enfoque publicitario. Actualmente cuenta con dos certificaciones internacionales en seguridad, seis diplomados y una maestría en Psicología Forense e Investigación Criminal de la Universidad de Liverpool. También imparte clases para varios diplomados en diferentes universidades y en la primera maestría de Seguridad en México.

¿Cómo llegó al área de seguridad? Por coincidencia. En 1987 con algunos amigos de la universidad conformó un grupo de seguridad para fiestas y bodas. Al inicio no eran más de 20 personas, y ese modesto grupo creció y evolucionó hasta convertirse en Organización Lobo, la empresa líder de seguridad privada en eventos masivos como conciertos, partidos de futbol, exposiciones, carreras automovilísticas y torneos deportivos.

Organización Lobo le dejó 14 años de experiencia, el cual considera "el mejor de los empleos", esto porque le permitió viajar por todo el país y el continente americano.

Artistas como Bon Jovi, Sting, Guns and Roses, Scorpions y Elton John, entre muchos otros, estuvieron bajo el resguardo de Seoane, de ahí el gusto y pasión por ese grupo de seguridad. Posteriormente, el experto colaboró en Securitas, como director de Servicios de Seguridad para la región centro del país y más adelante dirigió Pinkerton Consultoría e Investigaciones en México. Actualmente dirige su propia firma y participa en algunos foros de seguridad dictando diferentes ponencias y análisis sobre la seguridad en distintos sectores.

Seguridad:	Mi pasión.
México:	Mi casa.
COVID-19:	Maldito sea.
Pospandemia:	Aprendizaje.
Seoane Consulting Group:	Profesionalismo y experiencia.
Gobierno:	Sin palabras.

"Ningún promotor arriesga su capital si no tiene la esperanza de vender todos los boletos. El reto será convencer al público adulto para que decida encerrarse con miles de personas y el riesgo que ello conlleva", **Carlos Seoane**

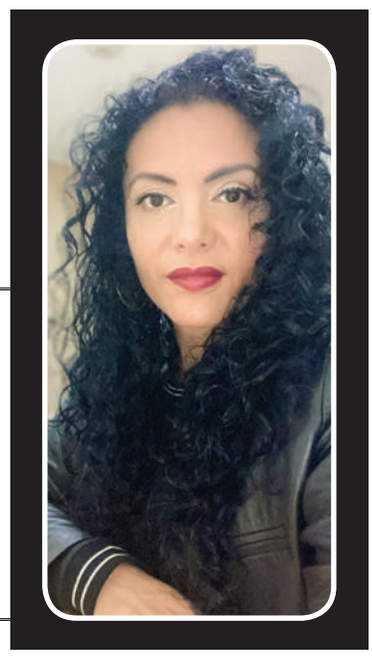
VIOLETA EDITH ARELLANO OCAÑA, GERENTE DE SEGURIDAD INTEGRAL EN CIE

SEA: Además de los riesgos por COVID-19, al reactivar los eventos masivos en México, ¿cuáles son los riesgos de seguridad? y ¿cuáles son las estrategias para mitigarlos?

"Derivado de la crisis económica mundial, es muy probable que se incremente la actividad delictiva dentro y fuera de nuestras instalaciones. Dentro de ellas, la seguridad de los asistentes, siempre ha sido uno de nuestros principales objetivos, por lo que, incluso con aforos reducidos, se siguen manteniendo los mismos dispositivos de seguridad junto con campañas de comunicación para invitar al público asistente a cuidar en todo momento sus pertenencias.

Por otra parte se le dará mucho más peso a los sistemas '*cashless*' para reducir el flujo de efectivo. Con respecto a las inmediaciones de los inmuebles, existe una constante comunicación con las autoridades para contar con dispositivos de seguridad pública y mantener en óptimas condiciones el sistema de alumbrado público, flujo peatonal y vehicular.

La empresa (CIE) ha sido muy cautelosa en la manera de ir retomando actividades, siempre en apego de los lineamientos dictados por nuestras autoridades y siendo muy rigurosa en el cumplimiento de los mismos, tanto por el *staff* como por el público asistente, tomando en cuenta las mejores prácticas con empresas globales y líderes en el mercado mundial del entretenimiento, ya que somos muy conscientes del daño a la imagen de la empresa que podría ocasionar una nota en la que se le involucrara como fuente de contagios por incumplimiento. La seguridad reputacional es de suma importancia para mantener la confianza de nuestro público en este camino de regreso a nuestras actividades".



"La seguridad reputacional es de suma importancia para mantener la confianza de nuestro público en este camino de regreso a nuestras actividades", **Violeta Arellano**

ACERCA DE...

Violeta Arellano es Licenciada en Protección Civil, cuenta con un diplomado en Desarrollo de Habilidades para el Directivo de la Seguridad Integral (DSI) y es la primera mujer brigadista en México certificada como bombero industrial ante CONOCER (Consejo Nacional de Normalización y Certificación de Competencias Laborales). Laboró en el área de Seguridad Ocupacional en la Base de Mantenimiento de Aeroméxico y posteriormente, ingresó a CIE como Coordinadora en la recién creada Gerencia de Seguridad e Higiene. Si bien su formación está más enfocada a *Safety*, en CIE se involucró primero en Protección Civil y más adelante en *Security*, con la finalidad de desarrollarse más en el área y contribuir a la empresa. Actualmente es la gerente de Seguridad Integral.

Adicionalmente, ha tenido la oportunidad de impartir clases en universidades y ser ponente para empresas, asociaciones, congresos, nacionales e internacionales.

Seguridad:	Certeza.
México:	Hogar.
COVID-19:	Pérdidas.
Pospandemia:	Reto.
CIE:	Pasión.
Gobierno:	Compromiso.

C.T.A. CARLOS SAINZ LUNA, COORDINADOR DE GESTIÓN DE RIESGOS Y PROTECCIÓN CIVIL EN SENEAM/SCT

SEA: ¿Cuáles son los requisitos del gobierno para la reactivación de eventos masivos? "Después de este tiempo de *impasse* se tendrán que rehacer o verificar los programas internos y programas especiales de Protección Civil de los inmuebles, así como incluir nuevos requisitos como el de la sanitización para las personas que accedan en los programas internos y programas especiales de cada uno de los eventos. También habrá que estar verificando los aforos, aunque todavía es remoto en que tengamos el semáforo en verde, pero ya se están realizando eventos masivos por lo que habrá que tomar en cuenta la concientización de los asistentes a estos eventos para que guarden las medidas de higiene y seguridad que estará demandando el virus.

Aunque estemos vacunados no hay que bajar la guardia, sobre todo por civismo y respeto a nuestros compañeros, aunque puede resultar complicado, ya que después de estar en resguardos año y medio, lo primero que los jóvenes y las personas en general estaremos demandando nuevas condiciones para disfrutar el derecho de ocio y entretenimiento, sin embargo hay que estar muy atentos en la vigilancia de los inmuebles porque mucha gente y lo hemos visto en los festejos de la Eurocopa y la Concacaf, esa proximidad natural e inconsciente se deberá tener en cuenta para la reapertura.

Esa normalidad que conocemos ya no va a regresar, será una nueva realidad en la que debemos tomar en cuenta puntos muy importantes, en los requisitos tanto de los inmuebles como de los talentos que participan en esos eventos, y que se quedarán de forma permanente serán las medidas que alguna vez se instauraron en 2009 para mantener la seguridad e higiene, la aplicación de gel al 70% de alcohol, la distancia, el estornudo de etiqueta, y ahora la sanitización, los cuales ya son términos usados muy comúnmente. En todos los inmuebles deberá haber agua corriente y jabón adecuado para mantener esa higiene.

Estos requisitos deberán ser revisados de manera interna por el equipo de Protección Civil, así como los recintos o espacios eventuales e inmuebles que no son dedicados al entretenimiento. Será bueno revisar la propuesta de una cartilla de vacunación contra el COVID-19. Que sea un requisito tener esa cartilla de vacunación como respeto a los otros asistentes en una muestra cívica".

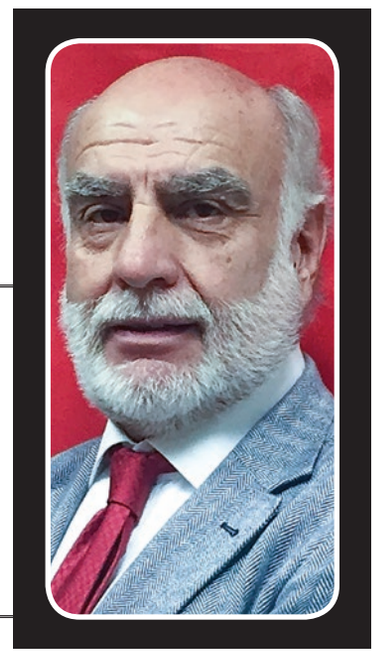
> "Será bueno revisar la propuesta de una cartilla de vacunación contra el COVID-19. Que sea un requisito tenerla como respeto a los otros asistentes en una muestra cívica", **C.T.A. Carlos Sainz Luna**

ACERCA DE...

C.T.A. Carlos Sainz Luna es Controlador de Tránsito Aéreo (CTA) egresado (1969) del Centro Internacional de Adiestramiento de Aviación Civil, en ese momento patrocinado por la ONU (Organización de las Naciones Unidas) y la Secretaría de Comunicaciones y Transportes (SCT), para capacitar al personal técnico aeronáutico en esas materias al menos desde México hasta Colombia.

Posteriormente, ingresó al gobierno de la Ciudad de México como asesor del jefe de gobierno, Manuel Camacho, en asuntos de aviación y principalmente por el tema de Guadalajara (Jalisco, México) en donde hubo un estallamiento de ductos que contenían hidrocarburos y gasolina, donde lamentablemente hubo muchos fallecidos, en ese momento el regente los mandó a capacitar en materia de Protección Civil en la Ciudad de México, que estaba en materia incipiente después del terremoto de 1985.

Tiene cursos en la Asociación Internacional de Manejadores de Inmuebles para Eventos (IAM), en ASIS, en el Centro Nacional de Prevención de Desastres (CENAPRED) y otras instancias dedicadas a la gestión de riesgos. Y ha tenido diferentes cargos en el gobierno de la Ciudad de México en materia de Protección Civil.



Seguridad:	Requisito de la vida cotidiana.
México:	Lo más grande que existe.
COVID-19:	Amenaza latente.
Pospandemia:	Realidad vigente.
Ciudad de México:	En crecimiento.
Gobierno:	Bien, gracias.


Foto: Creativeart - Freepik

COMUNICACIÓN SEGURA Y EFICIENTE PARA EVENTOS MASIVOS

La tecnología como herramienta indispensable para la seguridad se ha adaptado a los nuevos retos que la pandemia por COVID-19 trajo consigo, sin dejar de lado los riesgos que anteriormente ya existían.

En el caso de los eventos masivos, y como lo comentó Arnaldo Lovera, gerente *senior* de Canales región noreste de México en Motorola Solutions, la comunicación eficiente y rápida forma parte de los requerimientos para que se lleven a cabo con éxito dichos eventos, pero además debe ser una comunicación segura, es por ello que Motorola Solutions ofrece ecosistemas de radiocomunicación con esas tres cualidades.

"Desde la parte de radiocomunicación hay muchas soluciones para este tipo de eventos, soluciones, primero de comunicación y luego de seguridad, para mantener un entorno seguro; el sistema de radiocomunicaciones va a generar una comunicación efectiva, rápida y segura, por ejemplo puedo tener controladas las puertas de acceso, o al personal de seguridad e inclusive grupos de trabajo: seguridad, sonido, alimentos, todo puede estar conectado en un sistema de radiocomunicaciones. Las ventajas son privacidad al momento de realizar el evento, pues sólo el personal va a estar escuchando las indicaciones, sin que el ruido externo interfiera, ya que el sistema de comunicaciones lo va a filtrar, y así obtendrás una comunicación instantánea y rápida que se va a traducir en respuestas efectivas ante determinada situación y regularlas durante el evento masivo", señaló.

Para mantener la seguridad en estos eventos, un punto importante es que sólo el personal de éstos conozca cierta información, entonces contar con un sistema de radiocomunicación evitará que un tercero interfiera en la comunicación y lleve acciones en contra del evento. Una de las soluciones que ofrece esta marca para los eventos masivos es la radio inteligente MOTOTRBO™ Ion, un equipo que pueda calzar en cualquier vertical, sea misión crítica o no, va a depender de las necesidades del cliente. Así como las cámaras de Avigilon que pueden ayudar al tema de temperatura para los riesgos por COVID-19 o para detectar situaciones irregulares.

Dado el constante cambio en las indicaciones de las autoridades por el alza o disminución de los contagios, los eventos masivos y el medio del espectáculo tendrán que aumentar sus estrategias de seguridad para así poder operar en esta nueva normalidad. ■

"El sistema de radiocomunicaciones va a generar una comunicación efectiva, rápida y segura", **Arnaldo Lovera**

REFERENCIAS

[1] y [2] *"El show ya no está aquí... a un año sin conciertos ni eventos masivos, ¿el futuro es el streaming?", Eduardo Bautista, El Financiero 06/05/2021. https://www.elfinanciero.com.mx/bloomberg-businessweek/2021/05/06/el-show-ya-no-esta-aqui-a-un-ano-sin-conciertos-ni-eventos-masivos-el-futuro-es-el-streaming/*

Promoción 50% de descuento

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

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

Renta de blindados

Nivel III

20 Aniversario COLEMAN

www.rentadeblindados.com.mx

Tel. 55 5572 6005 Cel. 55 7672 4992

krauda@seguridadenamerica.com.mx

RENTA DE BLINDADOS

COLEMAN

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

Socio Director, Altair Security Consulting &Training.

Más sobre el autor:

LOS DELITOS CIBERNÉTICOS, IDENTIFICACIÓN Y PREVENCIÓN

Foto: Creativeart - Freepik

LATINOAMÉRICA

Con el arraigo durante la pandemia, en la nueva realidad han crecido exponencialmente diversos delitos, entre ellos los delitos cibernéticos, los cuales ya de por si venían creciendo a tres dígitos porcentuales por año. Según la ONU, estos delitos crecieron en un 600% durante la pandemia sólo en 2020.

¿QUÉ ES EL DELITO CIBERNÉTICO Y CÓMO SE DIGIERE?

El delito cibernético es una forma emergente de la delincuencia nacional y/o transnacional y uno de los de más rápido crecimiento en la ultima década. Con los cambios tecnológicos y a medida que el Internet se ha convertido prácticamente esencial en nuestras vidas, al cambiar la forma en la que nos relacionamos y muy de la mano con un mundo digital, las amenazas a la seguridad en la *web* se dispararon de forma exponencial, y el delito cibernético afecta ahora a cientos de millones de víctimas a nivel global.

Según la División Cibernética de la Guardia Nacional en México, han enlistado una serie de delitos que emanan del ciberespacio, que van desde acciones básicas de robo de información hasta delitos de gran impacto como la trata de personas, extorsiones y secuestros entre otros. Semana tras semana se deshabilitan decenas de páginas de Internet apócrifas, pero al puro estilo medusa, eliminan una y aparecen cinco nuevas. En México, la CONDUSEF (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros) recibe más de un millón de quejas por semestre derivadas de estos delitos, desde:

- Clonación de tarjetas bancarias.
- Transferencias electrónicas no reconocidas.
- Robos de identidad.
- Falsificación.
- Prácticas engañosas para obtener información.

> Acciones como permanecer atento, escéptico, tener sentido común e intuición, no ser un blanco fácil, es permanecer seguro

Al creciente mundo digital, al no haber una solución pronta por parte de los gobiernos locales e internacionales, con una impunidad altísima, debido principalmente a la falta de regulaciones claras y al anonimato que ofrece el ciberespacio, lo más recomendable es la autoprotección, esto es, educar a la sociedad, al personal de las oficinas, a que aprendan a identificar, prevenir y reaccionar eficientemente ante estos delitos para que eviten ser sorprendidos.

¿CÓMO IDENTIFICARLOS Y PREVENIRLOS?

Para identificar los delitos cibernéticos y evitarlos, se requiere de una buena dosis de conocimiento, sentido común y entendimiento del modo de operación de los ciberdelincuentes. Algunas modalidades de ataque son:

- ***Phising*:** engañar a los usuarios de Internet para que compartan sus datos personales. Es la forma más sencilla de ciberataque, la más riesgosa y efectiva.
- ***Pharming*:** engañar a los usuarios para descargar contenido.
- ***Vishing*:** realizar llamadas simulando ser entidades principalmente bancarias para confirmar compras y actualización de datos, cuando en realidad son delincuentes.
- ***Phreaking*:** realizar actividades ilícitas a través de los teléfonos, interceptando y hasta ejecutando llamadas de móviles sin que el usuario lo detecte.
- ***Smishing*:** estafa por medio de mensajes SMS, solicitando datos o pidiendo llamar a un número o entrar a un sitio *web* desde el móvil.
- ***Ransomware*:** infectar tu computadora e incluso bloquear la pantalla o cifrar archivos, mostrando mensajes que exigen el pago de dinero para restablecer el funcionamiento.

Foto: Creativeart - Freepik

Acciones como permanecer atento, escéptico, tener sentido común e intuición, no ser un blanco fácil, es permanecer seguro. Pareciera fácil, pero muchas veces no lo es, más cuando estamos apurados, desentendidos o jugando al *multitasking* y no enfocados, centrados en una cosa a la vez. Algunas observaciones en las comunicaciones que recibes digitalmente y que identifican un posible engaño son:

1. Errores de "dedo", ortográficos y/o de redacción o donde no te hablan por tu nombre.
2. Negocios u ofrecimientos que suenan demasiado buenos para ser ciertos.
3. Solicitudes de donaciones a organizaciones después de una catástrofe.
4. Mensajes alarmistas y/o amenazantes para hacer accionar de inmediato.
5. Solicitándote tus datos personales y/o confidenciales.

Foto: Cortesía Enrique Tapia

Semana tras semana se deshabilitan decenas de páginas de Internet apócrifas, pero al puro estilo medusa, eliminan una y aparecen cinco nuevas

Hay infinidad de medidas de prevención y reacción, de hecho esta información forma parte de un entrenamiento en autoprotección que realizamos frecuentemente en las organizaciones, pero les compartimos estos cinco principios básicos de seguridad para que difundan en sus oficinas y con sus familias:

1. En correos publicitarios, revisar la dirección del remitente y nunca responderlos, ni a través de las ligas.
2. Usar antivirus y mantenerlo actualizado, así como el sistema operativo; accionar los filtros de privacidad.
3. Las aplicaciones tienen acceso a tu información, la decisión de descargarlas es tuya. Por cierto, sugerimos ver la película Social Dilemma.
4. Considerar de dominio público todo lo que subas a Internet, piensa dos veces antes de compartir algo.
5. En redes sociales, filtros de privacidad y doble filtro a quien no conoces, tendrá acceso a tu vida.

Como verás, mucho de la prevención está en nuestras manos, educarnos y hacer la parte que nos corresponde es indispensable para tener vidas más tranquilas y más seguras. ■

Foto: Creativeart - Freepik

EXPECTATIVAS ACTUALES DE LA RELACIÓN CLIENTE-PROVEEDOR EN UN SERVICIO DE SEGURIDAD

Como proveedor se tiene la obligación de conocer al cliente, su gente, sus instalaciones y sus procesos críticos

MÉXICO

Diana Lorena de la Garza Vizcaya

En este tiempo imprevisible, cambiante, competitivo y complejo, cuando las empresas buscan optimizar el uso de sus recursos, ¿cómo podemos establecer una relación de negocios cliente-proveedor de largo plazo en un mercado de servicios de seguridad privada, que históricamente se ha regido por el precio?

Hoy más que nunca los clientes, por la escasez de recursos derivada de la recesión y la contingencia sanitaria que están enfrentando, quieren pagar menos, asegurándose que el servicio que reciban sea de calidad y cumpla con sus necesidades, de acuerdo a lo que se quiere proteger, brindando certidumbre, confianza y atención oportuna a cualquier situación de riesgo que se presente.

El proveedor actual debe enfocar su servicio en la diferenciación, ofreciendo soluciones de seguridad, basadas en un análisis de riesgos específico para el cliente, integradas por: capital humano, infraestructura/tecnología y protocolos/procedimientos.

¿QUÉ CONSIDERAR EN UN ANÁLISIS DE RIESGOS?

Para realizar un análisis de riesgos, además de los factores externos, se requiere que el proveedor conozca los procesos críticos del negocio del cliente a fin de que pueda diseñar y proponer una solución de seguridad que contribuya a la continuidad operativa del negocio.

Los recursos que el cliente asigne a un servicio de seguridad con este enfoque, serán justificables al estar alineados con el negocio. Si el cliente sigue con la costumbre de contratar guardias bajo el esquema de precio más bajo y sin soluciones de seguridad alineadas al negocio, los recursos serían desperdiciados y la continuidad del negocio no estaría soportada debidamente.

Cuando un cliente decide cambiar al proveedor es necesario ponderar los riesgos que puede enfrentar (conocimiento del servicio, curva de aprendizaje, requerimientos especiales, etc.).

En la selección del proveedor hay que tomar en consideración aspectos tales como: clientes actuales, tiempo de respuesta para casos de emergencia, capacidad para responder ante incidencias. Verificando que sea una empresa legalmente constituida, registrada en la SSP (Secretaría de Seguridad y Protección Ciudadana), que cumpla con las obligaciones que establecen las leyes, con personal capacitado, bien atendido, enfocada a la atención del cliente.

Como proveedor se tiene la obligación de conocer al cliente, su gente, sus instalaciones y sus procesos críticos. Contando con sistemas de calidad y de mejora continua, con estrategias que generen valor como una de las principales ventajas competitivas, ofreciendo un servicio integral de seguridad, con el propósito de que el cliente vea a su proveedor como un socio de negocio para cubrir requerimientos de seguridad. ■

Diana Lorena de la Garza Vizcaya,
gerente regional noreste de GSI.

Más sobre el autor:

SEGURIDAD EN AMÉRICA

2021

Roadshows & Eventos ONLINE

Seguridad en Casas de Empeño y Servicios Prendarios
13 de enero

Videovigilancia en Zonas Urbanas
27 de enero

Gestión de Seguridad en Aeropuertos
10 de febrero

Seguridad en Pruebas de Confianza
24 de febrero

Seguridad en la Industria Manufacturera
10 de marzo

Administración de Flotillas
24 de marzo

Seguridad en Plataformas Marítimas
7 de abril

Centrales de Monitoreo
28 de abril

Seguridad en Parques Industriales
12 de mayo

Seguridad en Centros Educativos
26 de mayo

Seguridad en la Industria Farmacéutica
9 de junio

Seguridad en Bancos
22, 23 y 24 de junio

Cumbre Latinoamericana de Seguridad
14 y 15 de julio

Seguridad en Plantas Automotrices
11 y 12 de agosto

Seguridad en la Industria Hotelera
25 y 26 de agosto

Seguridad en la Industria Alimentaria
8 de septiembre

Seguridad en Aduanas y Recintos Fiscales
29 de septiembre

Blindaje Automotriz
13 de octubre

Soluciones de Seguridad en *Data Centers*
27 de octubre

Seguridad en Hospitales
10 de noviembre

Seguridad para Supermercados y Tiendas de Conveniencia
24 de noviembre

Seguridad en Casinos y Centros de Entretenimiento
1 de diciembre

Seguridad en Maquiladoras
15 de diciembre

100 Más Influyentes de la Seguridad Privada (Presencial)
28 de enero 2022

Reunimos a los tomadores de decisiones de la seguridad en distintos sectores para que usted ofrezca sus productos y/o servicios por medio de conferencias dinámicas.

Beneficios:

- Usted podrá impartir su conferencia a más de 500 profesionales de la seguridad.
- Interactuar directamente con tomadores de decisiones.
- Promocionar sus productos y servicios.

El patrocinio incluye:

- Base de datos de los asistentes.
- Reporte analítico de la estrategia de publicidad.
- Presentación de 30 minutos.

telemarketing@seguridadenamerica.com.mx
www.seguridadenamerica.com.mx
(55) 5572 6005

Foto: Cortesía Javier Fernández

JAVIER FERNÁNDEZ, SEGURIDAD ELECTRÓNICA EN TENDENCIA

Con más de 30 años en el sector de la seguridad, Javier Fernández, CEO de Seccomm, se integra a la dirección de Tecnología de BlackIND, empresa especializada en seguridad corporativa y en la que implementará la cultura de seguridad en todos los niveles de la empresa, socios y en el entorno social de ésta

MÉXICO

Erick Martínez y Mónica Ramos / *Staff* Seguridad en América

Ingeniero en electrónica de profesión, DSE (Dirección de Seguridad en Empresas en la Universidad Pontificia Comillas), Diplomado en Liderazgo Gerencial (UDELAP), Diplomado en Empresas de Seguridad Exitosas y Sustentables, Javier Fernández emprende un nuevo proyecto impulsando la cultura de la seguridad no sólo a nivel dirección, sino para todo el personal y el entorno global de BlackInd, empresa especializada en seguridad corporativa que, "garantiza" la continuidad de negocios, a través de gestión de riesgos. Javier Fernández se integra a la Dirección de Tecnología y, además, como responsable de la región Occidente (Colima, Nayarit, Michoacán y Jalisco).

"Debido a la pandemia tomé diferentes decisiones, además de cambiarme de residencia a Guadalajara (México), inicié con este reto en Jalisco que me da la oportunidad de gestionar mi responsabilidad en BlackInd desde uno de los puntos estratégicos de desarrollo tecnológico del país. Las tendencias en tecnología y en seguridad electrónica surgen de la región occidente y como empresa, pretendemos explotar éstas, en su totalidad. Ya no sólo se requiere en la industria de conocer videovigilancia, control de accesos, detección de incendios, protección perimetral, es importante hacer conciencia en el mercado, de que todos estos sistemas están inmersos en la ciberseguridad. Todos los sistemas modernos se comunican a través de redes de comunicación, están en la Nube y hoy día, sólo por estas condiciones, se convierten en vulnerables, entonces ese es mi reto ahora, fomentar la cultura de la seguridad corporativa y participativa", comentó Javier.

BLACKIND, SERVICIOS Y DIFERENCIADORES:

- Gestión de riesgos.
- Inteligencia para la seguridad.
- Vigilancia activa y prevención de pérdidas.
- Centro de Inteligencia y Control de Seguridad ISCC.
- Herramientas de contramedidas.
- Manejo de crisis.
- Barridos electrónicos.
- Unidades de ciberinteligencia.
- Capacitación.
- Protección Civil.
- Seguridad tecnológica.
- Presencia en Estados Unidos, España, Colombia y México.

Foto: Cortesia Javier Fernández

PLANES A MEDIANO Y LARGO PLAZO:

- Crear la cultura de seguridad, enfocando ésta hacia el servicio.
- Satisfacción del cliente de al menos un 90% de nuestros servicios.
- Incrementar ventas en los próximos cinco años, cuando menos el 50%.
- Estabilizar los márgenes de ventas a un porcentaje estándar y adecuado para ser una empresa socialmente responsable y que sus colaboradores desarrollen el arraigo a participar en BlackInd.

La comercialización de una alarma ultrasónica proveniente de Francia, fue el inicio de Javier en la seguridad (1987), justo a unos meses de terminar la ingeniería en la Universidad La Salle, Banamex apoyó con su servicio social y posteriormente contrató y financió con al menos 100 mil dólares, el proyecto de tesis del ahora socio de BlackInd. Además del DSE, Javier cuenta con un Diplomado en Calidad Total (ITESM), el cual le sirvió para incursionar en la manufactura y en la dirección de bancos, en el año de 1996 se incorpora a Johnson Controls desarrollando el mercado emergente de los edificios inteligentes, automatización y control, con importante relevancia en los equipos de seguridad.

En el año 2002, se incorpora como gerente general en Telefónica Ingeniería de Seguridad (TIS) y donde se especializa en soluciones de seguridad, en 2006, se integra como director general de Human Factor, y para el 2008, Schneider Electric lo contrata para del desarrollo de negocios de Building Automation, en el área de Servicio.

Con Seccomm (Seguridad y Comunicaciones) en 2010, Javier Fernández se lanza como empresario independiente, y esto hasta el día de hoy.

Ligado siempre a las asociaciones de seguridad, la profesionalización es para Javier de suma importancia, contemplando a todos los niveles de la empresa la certificación en su ámbito de trabajo y el promover la cultura de seguridad en la empresa, con los colaboradores, con los clientes, amigos y con la ciudadanía en general su entorno.

Es vicepresidente de Seguridad por México, secretario ejecutivo de la NFPA Capítulo México, fue presidente de la Asociación Latinoamericana de Seguridad Comité México (ALAS), vicepresidente de Especiales en la Asociación Mexicana de Empresas del Ramo de Instalaciones para la Construcción (AMERIC), y es socio fundador de Agrupaciones de Seguridad Unidas por México (ASUME), además de ser socio de ASIS Capítulo México, de la Asociación Mexicana de Especialistas en Seguridad Integral (AMEXSI) y como parte de BlackInd, ahora de AMESP (Asociación Mexicana de Empresas de Seguridad Privada).

> "Los socios en BlackInd somos profesionales con más de 30 años en el sector de la seguridad, siempre a la vanguardia en la profesionalización y empujando a que esto permeé hacia todo el sector, a todos los niveles para con ello contribuir a un México más seguro promoviendo la cultura de la seguridad"

SEGURIDAD ELECTRÓNICA: NECESARIA Y EN TENDENCIA

El equipo que conforma BlackInd se caracteriza por tener amplia experiencia en temas de inteligencia, ciberseguridad y gestión de riesgos, ahora con la llegada de Javier se complementa el portafolio de servicios al atender la seguridad en tecnología, que es una de las partes que le faltaba al portafolio de servicios de BlackInd.

"Los socios y directores somos profesionales que contamos con más de 30 años en los diferentes sectores de la seguridad, buscamos la mejora continua y la profesionalización del sector, pero que no sólo quede ahí, sino que esa experiencia se permeé y abarque de ser posible como seguridad corporativa en todos los niveles con nuestros clientes, colaboradores y asociados", explicó.

Javier Fernández comentó la importancia de transmitir la cultura de la seguridad no sólo en la empresa, sino también a los socios de negocios y al ciudadano común. BlackInd es una puerta para desarrollar sus conocimientos desde el punto de vista de la seguridad corporativa, ofreciendo las soluciones reales que sus clientes necesitan, diferenciándose por ofrecer la solución con base en un análisis de riesgos y la gestión de éstos. "No es lo mismo sentirte seguro que estar seguro", señaló. ■

CONTROL®
SEGURIDAD PRIVADA INTEGRAL

20 AÑOS GENERANDO CONFIANZA

A lo largo de los años, la empresa ha trabajado para consolidarse como líder en el ramo de la seguridad privada y ha dedicado todos sus esfuerzos para que el nombre de Grupo Control Seguridad Privada Integral sea sinónimo de confianza y protección.

Control es una empresa que cuenta con una trayectoria de 20 años en el giro. Surge por la visión emprendedora del fundador Santiago Barona.

Desde su creación, Control surge con una misión y visión, enfocadas a convertirse en la empresa líder en el ramo de la seguridad privada, ofreciendo soluciones integrales que, no sólo satisfacen las necesidades de sus clientes y usuarios, sino que las cumplen y las superan con creces. El perfeccionamiento constante, es uno de sus principales objetivos. El capital humano de Control se mantiene siempre a la vanguardia, obteniendo nuevas certificaciones como resultado de su labor y buscando la mejora continua.

El 5 de junio de 2021, Grupo Control celebró su 20 aniversario lleno de satisfacción, aprendizaje y agradecimiento a tantos clientes que han confiado en Control en estas primeras dos décadas de su existencia. Los socios comerciales son parte esencial del crecimiento de Control en todos los sentidos: las necesidades y exigencias de seguridad requerida en las distintas industrias en las que ofrece servicios, han fomentado la creación de nuevas áreas de negocio que puedan atender a cada uno de manera personalizada y óptima. Y sobre todo la confianza y tantas experiencias vividas en conjunto que impulsan a Control y a todos sus colaboradores a dar siempre lo mejor de sí.

Este año Control se incorporó al Ranking Súper Empresas de Top Companies. Este distintivo los certifica como una empresa innovadora y enfocada en su capital humano, siguiendo los más altos estándares de calidad y servicio, consolidándose como una de las empresas culturalmente poderosas. Control se ha convertido en un lugar en el que todos desean trabajar, una empresa que garantiza el bienestar de cada colaborador y su familia, una organización con un ambiente sano que propone e innova, para reafirmar la confianza que le tienen sus clientes.

Ahora, miran hacia el futuro bajo el liderazgo de su CEO, Benjamín Barona que, junto a la pasión de cada colaborador, seguirán creciendo y creando nuevas áreas de negocio con un entendimiento profundo de la realidad actual y con la visión de las tendencias futuras. Continuarán trabajando por la seguridad de cada uno de los que han confiado y confiarán en Control.

Estos son sus primeros veinte años, pero van por muchos, muchos más.

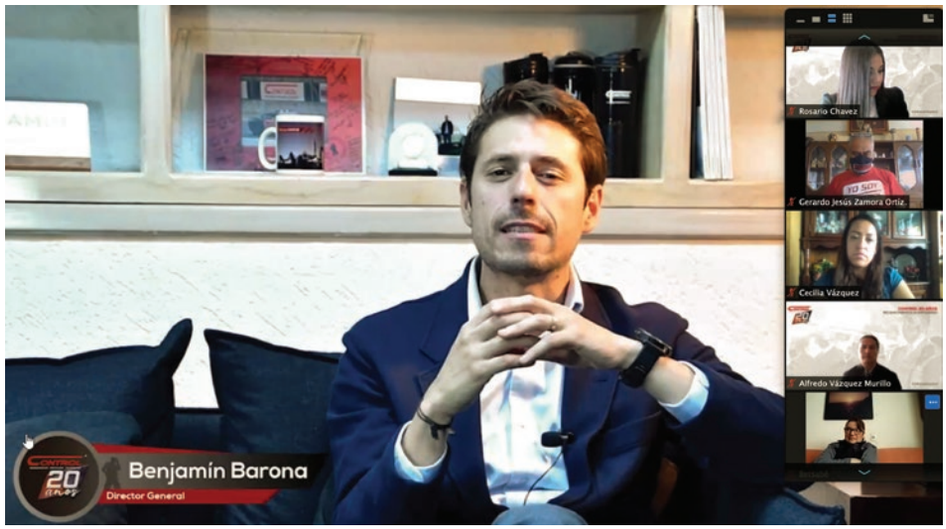
EVENTO 20 AÑOS DE CONTROL

El día de la celebración llegó, juntos disfrutamos del aniversario número 20 de Control. Los primeros veinte años de existencia de una empresa que se ha convertido en un referente para la seguridad privada en el país.

Este evento tuvo un enfoque especial, uno sin precedentes que nos marcó una clara tendencia: la construcción de un camino hacia el futuro. Tres fueron los principales ejes que se pudieron apreciar en la ceremonia solemne. En primer lugar, el pasado. De dónde venimos, lo que nos constituyó en primer lugar, los motivos, sueños y metas con los que la empresa surgió; esto de la mano de un discurso de nuestro director de Capital Humano, Adrián Barona.

En segundo lugar, Ernesto Guerrero, director de Operaciones, habló sobre nuestro presente, lo que hoy en día constituye a Control, las metas que estamos alcanzado, el estatus de líder que poseemos, todas las acciones que nos certifican como una empresa de calidad y socialmente responsable que mira sin miedo al futuro. Finalmente llegó el tiempo de hablar sobre el futuro, la visión de un Control que apunta a la vanguardia en seguridad, que piensa en tecnología y que se visualiza como la empresa líder en el ramo de la seguridad privada; esto desde la voz de nuestro director general el Ingeniero Benjamín Barona.

Además de la visión de todas las fases de nuestra historia, este evento nos sirvió para brindar reconocimiento a todos nuestros colaboradores que han contribuido para la escritura de esta historia. Los reconocimientos de antigüedad se otorgaron a quienes cumplieron tres, cinco, diez, quince y veinte años de trayectoria en Control.



Nuestros compañeros de tres años recibieron nuestro clásico reloj conmemorativo y nuestros compañeros con mayor antigüedad recibieron respectivamente la estatuilla especial de reconocimiento. Gris, Plateado, Dorado y Rojo, fueron los colores que vistieron a los galardones que recibirán nuestros colaboradores ejemplares, además del reconocimiento impreso. Para las personas que han estado desde que este sueño inició, aquellos que durante los 20 años han estado al pie del cañón, se les proporcionó además una réplica a escala del Camaro, un emblema de Control.

Veinte años se dicen fáciles, pero pocos tienen la fortuna de vivirlos como lo hemos hecho en Control. Son las primeras dos décadas y vamos por muchas más, porque en Control sabemos que no existen límites, nuestro combustible es la pasión, para continuar hoy y siempre teniendo claro que el "Cielo es el límite". ■

Fuente y fotos: Control Seguridad Privada Integral

Foto: Cortesía Dagoberto Santiago

Dagoberto Santiago Toledo,

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

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

1. ¿Cuáles son los objetivos de GEMARC para este 2021?

El plan de trabajo está contemplado para un periodo de dos años (mayo de 2021 - mayo de 2023), siendo prioridad la parte interna de la asociación. Empezando por la creación de seis Comités de Trabajo:

- **Ética.** Es muy importante el cumplimiento del código de ética, ya que somos un área que nos toca investigar desviaciones al código de conducta y deberemos ser ejemplos de cumplimiento.
- **Admisiones o Membresía.** Éste verificará y analizará que los nuevos integrantes de la asociación cumplan los requisitos para pertenecer a GEMARC.
- **Alertas Tempranas.** El cual buscará toda la información publicada en medios de comunicación, redes sociales, o a través de nuestros contactos, que esté relacionada con seguridad y que pueda anticiparnos o apoyarnos si hay bloqueos, algún tipo de evento, afectaciones naturales como inundaciones, incendios, cualquier evento que pueda afectar en primer lugar a la seguridad de los empleados, miembros de GEMARC y la operación de los negocios. Para que a su vez el área de seguridad y la empresa apliquen los protocolos necesarios.
- **Comité de actualización profesional.** Tiene que ver con fundar un área de actualización profesional que sirva para mantener al día a todos los miembros de GEMARC o bien para los grupos que están bajo nuestro cargo, impartiendo cursos a la medida de los profesionales de seguridad corporativa, riesgos y buenas prácticas.
- **Comité MES (Mujeres en Seguridad).** Lo que buscamos es ampliar el panorama, no sólo para mujeres en seguridad, sino que sea un comité enfocado en la diversidad e inclusión.
- **Comité de información y contenidos.** Se encargará de crear los canales adecuados de comunicación para los integrantes de GEMARC y así poder transmitir todo lo que compete de seguridad e información que pueda serles útil. Se va a encargar de darle más profesionalidad a cualquier tipo de encuesta que queramos hacer. Se realizará un sondeo a los integrantes sobre cierta temática de interés, se analiza

y entrega como un estudio profesional sobre el tema con información de utilidad.

Además de continuar enriqueciendo las relaciones con las demás asociaciones hermanas.

2. ¿Cómo beneficia GEMARC a sus afiliados?

GEMARC es un foro en el que estamos aproximadamente 150 líderes, los primeros beneficios están enfocados a nuestros agremiados, con el aprendizaje de las buenas prácticas entre unos y otros. Es muy interesante escuchar las distintas formas de pensar de una empresa mexicana, una americana, española o de cualquier parte del mundo, porque hay empresas prácticamente de todo el planeta y el compartir estas experiencias nos ayuda a tener un parámetro en el que cada uno de nosotros toma lo que mejor le parezca y dependiendo de la filosofía de cada empresa.

3. ¿Cómo o cuáles son los requisitos para pertenecer a GEMARC?

El primero y más importante es que tenga la máxima autoridad de seguridad corporativa en la institución que representa, sólo podrá integrarse una persona por empresa. Y segundo, que cumpla en su totalidad con el Código de Ética.

4. Cuéntenos un poco sobre su trayectoria profesional en el sector de la seguridad

Llevo 32 años de trabajo ininterrumpido, soy Ingeniero en Aeronáutica, por lo tanto empecé a trabajar en la aviación, exactamente en el servicio a la navegación en el espacio aéreo, diseño de rutas aéreas, procedimientos de aproximación, publicación de información aeronáutica. Estuve en el área de investigación, y comencé a participar en el área de accidentes aéreos y a partir de ahí me empecé a involucrar más en temas de seguridad aérea y aeroportuaria.

Realicé protocolos sobre qué hacer en casos de secuestro aéreo, de amenaza de bomba en avión, en tierra, y como en los aeropuertos ocurre de todo, robo de maletas, tráfico de drogas, de personas, es un mundo y son tan importantes las cosas que pasan por su carácter nacional e internacional. Comencé a involucrarme no sólo en seguridad aérea y aeropuertos, sino también en temas de accidentes de personas, y los temas relacionados a *security* y *safety*.

Después de algunos años, me invitó una farmacéutica inglesa a trabajar con ellos y me fui prácticamente llorando de la aviación, extrañando el olor a turbosina, el sonido de los aviones, pero también me enganché en una nueva industria desconocida por mí. La industria farmacéutica es muy organizada, precisa, colaboran científicos, fórmulas de productos y tienen la tecnología más nueva en cuestión de investigaciones.

Como seguridad me tocó conocer los centros de investigación en Carolina del Norte (Estados Unidos), en Londres (Inglaterra), me tocó ver la parte de protección a la propiedad intelectual y me gustó, porque también eran productos buscados por el narcotráfico, sustancias como la pseudofedrina, que fue retirada del mercado, porque es un precursor de drogas y protegerla era también un reto.

Foto: Cortesía Dagoberto Santiago

De ahí me invitaron a trabajar en PepsiCo y sigo siendo hasta la fecha, director del área de Seguridad México, con otro reto más grande por el volumen de la compañía y encantado de trabajar en este desafío, y a la vez ahora llevo tres meses como presidente de GEMARC con el gusto de colaborar y trabajar para que esta asociación se conozca.

5. ¿Por qué decidió formar parte de GEMARC?

Es el mejor foro para compartir experiencias y para impulsar la profesionalización de todos los que trabajamos en seguridad corporativa. Tenemos un chat que se creó el 3 de mayo de 2016, aunque hace 15 años hubo un primer intento para juntarnos en Grupo Ejecutivos de Seguridad Corporativa (GESC), en realidad hace cinco años es cuando se formaliza la idea y se crea GEMARC, única en México de Seguridad Corporativa.

6. Como presidente de GEMARC, ¿cuál es el mensaje que quiere darle a sus afiliados?

La seguridad corporativa se ha ido transformando de tal forma que hoy en día se ha vuelto un área mucho más estratégica, trabaja más de cerca con la organización para la creación de programas específicos como continuidad del negocio, en la seguridad de ejecutivos, en la seguridad de los empleados y no tengo ninguna duda que sobre todo ahora con la pandemia nos hemos vuelto mucho más visibles.

Hemos pasado del *back office* al *front office*, lidiando con este tipo de temas, con las áreas de salud ocupacional, con el Comité de Crisis de las empresas y la importancia del área ha quedado claramente visible. Es por ello la importancia de pertenecer a un grupo de profesionales para la continua capacitación y profesionalización, además y muy importante, el de compartir aprendizajes para un mejor desarrollo del área. ■

¿QUÉ SE REQUIERE AL HACER UN ANÁLISIS DE RIESGOS?

Foto: Creativeart - Freepik

Aunque un análisis de riesgos no impedirá que algo salga mal, sí será útil para que se tenga un panorama realista que considere tanto lo positivo como lo negativo y, por lo tanto, para que fomente mayor confianza entre los involucrados frente a la certeza de que las decisiones que van a tomarse están bien sustentadas

MÉXICO | Omar Ballesteros

Cuando realizo un análisis de riesgo de robo, busco que los clientes se den tiempo para participar en la auditoría que tengo que hacer primero, el recorrido que permita reconocer los peligros, riesgos y vulnerabilidades de la empresa o negocio, y casi ningún cliente, de la dirección general tiene tiempo, o no quieren dárselo, pero deben estar ahí, porque al final el análisis busca evitar la fuga de dinero. Comencemos primero entonces en la forma en que tenemos que hacer este análisis, muchos expertos en seguridad, que merecen todo mi respeto, han aprendido hacer estudios de manera empírica, pero hay más que tenemos que tomar en cuenta además de la experiencia.

A TOMARSE EN CUENTA

El estudio se tiene que hacer en tres niveles, en tres áreas y dos ambientes:

3 NIVELES:
- Abajo.
- En medio.
- Arriba.

3 ÁREAS:
- Infraestructura.
- Tecnología.
- Personal.

2 AMBIENTES:
- Afuera.
- Adentro.

Cuando mencionamos "abajo" tiene que ver desde alcantarillas, pisos, terrenos, pavimento, tierra donde está construida o montada la empresa, la forma fácil de ingresar por abajo. "En medio", significa factores que puedan permitir el ingreso de alguien a la altura del pecho de una persona promedio de la zona. "Arriba", tiene que ver con la facilidad de ingresar por encima de todo, arboles tan altos que permiten subir al techo y meterse, entre otros. En las áreas, comentamos lo siguiente:

- **Infraestructura:** mallas, bardas, puertas, ventanas, portones, luces exteriores, luces interiores, etc.

- **Tecnología:** cámaras de todo tipo, drones, chapas biométricas o inteligentes, detectores de humo, relojes checadores de estaciones, computadoras de supervisión; en este punto también se debe considerar manuales, reglamentos, consignas, instructivos, hojas descriptivas de puesto, hojas de actividades, *record score card*; políticas de prevención, políticas que interactúan con las actividades de seguridad, certificaciones de la empresa, P.R.E., etc.

- **Personal:** supervisores, guardias o agentes de seguridad, perfiles de éstos, entrenamiento, capacitación de los mismos, actualizaciones, etc.

En los dos ambientes, se debe revisar en cada uno los tres niveles y las tres áreas que hay en ellos, de igual manera se debe tomar en cuenta el clima, parece que no es necesario, pero una zona donde llueve mucho, es difícil que las personas ingresen saltando la malla perimetral, porque lo que puedan extraer se les echará a perder o se les caerá de las manos por el agua.

Se debe registrar en la auditoría el clima variable y principal de la zona, así como también el índice de crimen que tienen registradas las autoridades de la localidad. Hay que preguntar los incidentes de robos de los últimos dos años.

Cuando estamos realizando una auditoría debemos tener la capacitación requerida para denotar y entender lo que se está buscando, podemos usar un formato para ello, pero lo que sí no puede faltar es que el informe final debe estar estructurado con base en lo anterior.

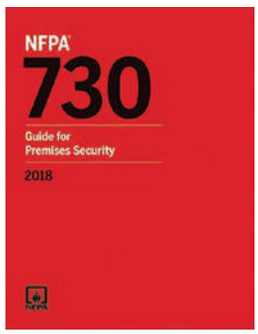
Todo auditor de protección, se sugiere que tenga un curso o si se puede, una certificación en auditorías de calidad, esto le permitirá hacer preguntas más específicas y razonadas.

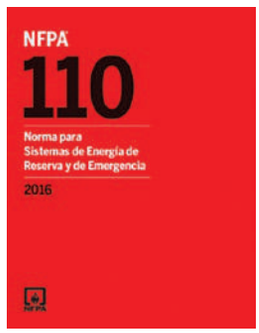
Algunos pueden pensar que como sus empresas no están exportando y que no requieren el C-TPAT, sin embargo, los tópicos que maneja aplican a cualquier empresa, exporte o no y se deberían de considerar

NORMAS INTERNACIONALES

Casi nadie toma en cuenta las siguientes normas internacionales en materia de protección planta, prevención de pérdidas, etc.:

- **C-TPAT:** Customs-Trade Partnership Against Terrorism.
- **NFPA 110:** (Asociación Nacional de Protección Contra el Fuego). Norma para sistemas de energía de reserva y de emergencia.
- **NFPA 730:** Guía para Seguridad Física de Establecimientos.
- **NFPA 1600:** Norma sobre Administración de Emergencias/Desastres y Programas para la Continuidad del Negocio/Continuidad de Operaciones.





Algunos pueden pensar que como sus empresas no están exportando y que no requieren el C-TPAT, sin embargo, los tópicos que maneja aplican a cualquier empresa, exporte o no y se deberían de considerar.

Conocer las normas NFPA, tomadas en cuenta en todo el mundo, es prioritario, así como el C-TPAT para mejorar y actualizar la forma de realizar auditorías de prevención de robos o pérdidas. El tiempo de la auditoría o revisión puede ser tan largo o corto conforme a la participación de la empresa y sus ejecutivos, y la pericia del auditor.

Finalmente, podemos concluir que la necesidad de una auditoría en prevención de pérdidas es necesario y que ésta se debe realizar con la participación de la persona de mayor rango dentro de la organización, si se puede claro; debe ser realizada por una persona con experiencia en lo anterior y con preparación en auditorías de calidad, y obviamente con estudios en análisis del crimen y delincuencia. ■

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

Más sobre el autor:

Los esquemas mentales determinan la forma en que las personas ven la realidad

Foto: Creativeart - Freepik

LA ENTREVISTA LABORAL COMO MÉTODO PREVENTIVO DE **LA VIOLENCIA LABORAL**

ARGENTINA | Juan Manuel Iglesias

En los últimos dos artículos hemos explicado como la violencia en el trabajo se relacionaba con las experiencias de apego y el aprendizaje emocional que realizaban las personas mediante la reproducción de las conductas que observaban de sus figuras cuidadoras. Estos aprendizajes formaban parte de las estrategias de afrontamiento que utilizaban para resolver los problemas en el ámbito laboral.

A su vez los individuos, siguiendo la "teoría de los cosntructos personales de George Kelly, construyen "esquemas mentales", estructuras de pensamiento que nos permiten recabar información sobre la realidad y estructurar estrategias para anticiparnos a los eventos. Son la forma en que habitualmente visualizamos las cosas. Con esto la persona intenta desarrollar conceptos que hagan más predecible su vida personal en el campo de las relaciones.

Las experiencias tempranas de maltrato y de apegos inseguros generan la construcción de esquemas mentales rígidos y pobres. Como dice Robert Leahy, la ansiedad, que es una propiedad del Síndrome de Cronos[1], es característica de esquemas sobre amenazas o miedo al fracaso, y la ira, emoción que acompaña a este síndrome, por esquemas sobre la humillación, insultos y maltrato. Todos estos esquemas se aprenden en la infancia y se tornan "permeables" cuando ese aprendizaje se generaliza. ¿Qué quiere decir esto? Que aprendemos una estrategia en la infancia, por ejemplo generar desconfianza hacia el otro, esa práctica la generalizamos y aplicamos a otras situaciones en la vida adulta, esto sucede cuando de un aprendizaje se forma un esquema o constructo que puedo aplicar a nuevas situaciones.

Los esquemas mentales determinan la forma en que las personas ven la realidad. Cuando nos vemos a nosotros mismos y a los demás aplicamos los esquemas que surgen de los constuctos personales: por ello, es importante conocer los constructos que los futuros directores tienen sobre el éxito, el dinero, la solidaridad y el liderazgo. Por ejemplo con respecto a esto último si la persona maltratada, aprendió a "ir contra las personas" para impedir la pérdida del control dispone de pocos constructos y muy rígidos y es muy factible que define el liderazgo como autoritarismo y aplique terrorismo laboral a todas las situaciones.

Es por ello que esta propuesta es incorporar algunas preguntas a la entrevista laboral de ingreso para detectar posibles esquemas rígidos que evidencien en futuros directores el Síndrome de Cronos.

¿CUÁLES SON LOS ESQUEMAS QUE APARECEN EN EL SÍNDROME DE CRONOS?

- Suelen considerar al otro como un oponente que compite con su puesto.
- Se mueve con gran desconfianza hacia el ambiente.
- Cree que si no controla todo el tiempo la situación y a las personas todo sucumbirá.
- Suele desarrollar sesgos cognitivos como la "lectura de mente": "Seguro que Juan quiere sacarme el puesto".
- Aparecen otros sesgos como el "pensamiento catastrófico": "Sería terrible darle más participación a José".
- Suelen sobregeneralizar las situaciones desde una mirada negativa a partir de un solo evento. Por ejemplo, cuando fracasan en un objetivo suelen pensar que han fracasado en todo y aparece el miedo a ser desplazados.

- Se mueven con categorías dicotómicas y etiquetadas: los colaboradores son amigos o enemigos, buenos y malos. Sienten que si ceden el control, lo pierden todo. Le cuesta pensar con matices.

- Se autoimponen imperativos morales muy rígidos. Los "debería" generalmente se construyen en la infancia. Son los mandatos familiares que en contextos de maltrato suelen ser limitantes de la creatividad.

- Suelen razonar emocionalmente confundiendo la realidad con las sensaciones emocionales. Por ejemplo: "Me siento ansioso y deprimido, eso quiere decir que mi gerencia no está funcionando".

- Suele culpar a otros de sus emociones y sentimientos negativos y se niegan a asumir la responsabilidad de cambiar por sí mismos.

LA ENTREVISTA

El Dr. Gavin de Becker nos aporta un modelo de preguntas que podemos incluir en la entrevista laboral. A su vez estas técnicas podemos complementarlas con la observación y lectura de las microexpresiones faciales que son microgestos que duran menos de un segundo y que expresan las siete emociones básicas que van surgiendo cuando la persona habla. Cuando una persona intenta esconder lo que verdaderamente siente respondiendo lo "políticamente correcto" podremos observar una incongruencia entre lo que dice y que expresa con los microgestos.

Aprendemos una estrategia en la infancia, por ejemplo generar desconfianza hacia el otro, esa práctica la generalizamos y aplicamos a otras situaciones en la vida adulta

Foto: Creativeart - Freepik

¿CÓMO Y QUÉ PODEMOS PREGUNTAR?

Si bien esto es un modelo, si en mi contexto una pregunta se considera muy personal o invasiva de la intimidad, quizás debamos reemplazarla por otra menos personal.

¿Háblame de un fracaso en su trabajo y cuénteme por qué sucedió?
Aquí podemos observar si asume la responsabilidad o culpa a otros. Si hay generalizaciones, imperativos morales rígidos, etc.

¿Cómo actúa cuando quiere resolver problemas en el trabajo?
Aquí pueden aparecer los "debería", la desconfianza y la necesidad de controlarlo todo. Podemos observar si posterga al enfrentar las situaciones. El pensamiento catastrófico hace que muchas veces surja el miedo al cambio y se postergue la decisión.

Describa al mejor jefe que haya tenido y describa al peor.
Aquí podemos observar si se emplean etiquetas o pensamiento dicotómico, atribución de culpabilidad. Si ridiculiza a sus jefes, si habla desde el razonamiento emocional, por ejemplo desde el rencor. Si asume parte de la responsabilidad en esa relación, etc.

¿Cómo se describiría a usted mismo?
Aquí podemos evaluar si la persona se describe a sí mismo en términos implacables, lo cual denota estándares perfeccionistas o "deberías".

Describa un problema que haya tenido en el trabajo en la que la ayuda de otra persona fuera muy importante para usted.
Si la persona es capaz de recordar alguna situación de este estilo podríamos observar si por ejemplo si es capaz de pedir ayuda y reconoce y expresa su agradecimiento. Recordemos que un sesgo en los gerentes "Cronos" es la desconfianza y la imposibilidad de expresar emociones y necesidades como el pedido de ayuda. ■

REFERENCIAS

[1] *Recomiendo leer mis dos anteriores artículos que introducen a este tema en los números 126 y 127.*
- *Leahy, R (2018) Técnicas de Terapia Cognitiva, Una guía para profesionales, Akadia, Buenos Aires*
- *De Becker, G (1998) El Valor del Miedo, Urano, Buenos Aires.*

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

Más sobre el autor:

Foto: Creativeart - Freepik

La aplicación de la inteligencia y la contrainteligencia al servicio de la seguridad de las empresas es esencial para apoyar los objetivos de la empresa y proteger a sus miembros y activos, sus operaciones, su reputación e imagen

LA INTELIGENCIA DESDE UNA PERSPECTIVA EMPRESARIAL

BRASIL | Sergio Ricardo Dominguito de Oliveira

Al participar en algunas presentaciones he observado algunas ideas erróneas o confusas sobre lo que viene a ser la inteligencia y sus propósitos. Confirmé mis expectativas visitando algunos sitios web y blogs que asocian la inteligencia (Intel) con temas de seguridad corporativa. Sin distanciarnos de los conceptos definidos por la Agencia Brasileña de Inteligencia (ABIN), organismo estatal brasileño responsable del desarrollo de la doctrina de la inteligencia en el Brasil, entendemos que la actividad de Intel al servicio del entorno corporativo debe limitarse al ejercicio de acciones encaminadas a la obtención de datos, producción y difusión de conocimientos que contribuyan a la toma de decisiones informadas a nivel de la junta.

Antes de generar cualquier duda, no me quedaré con el tema de la inteligencia de negocios. Nos centramos en temas de seguridad corporativa. Para una correcta operatividad de esta actividad, entiendo que la empresa debe, en la medida de lo posible, estructurarse para cumplir con las dos ramas de Intel: la propia inteligencia y la contrainteligencia.

ENTENDAMOS MEJOR SUS DIFERENCIAS

La rama de inteligencia se ocupa de producir y difundir los conocimientos necesarios para la planificación, ejecución, seguimiento y evaluación de decisiones dirigidas, por ejemplo, a la inversión de una empresa, a la ejecución de acciones destinadas a prevenir pérdidas o a contribuir a la actualización de los planes de gestión de riesgos y crisis.

La contrainteligencia, a su vez, tiene el propósito de prevenir, detectar, obstruir y neutralizar las acciones de la inteligencia adversa que amenazan la salvaguardia de los datos, los conocimientos, las personas, las áreas y las instalaciones de la empresa. Así, estaríamos atendiendo las medidas necesarias para hacer frente a las vulnerabilidades y amenazas a nuestro negocio.

De forma preventiva, las acciones actúan en la concienciación, orientación y cualificación de los diversos sectores para la protección de los bienes de interés de la empresa. Las medidas de detección, obstrucción y neutralización incluyen el uso de recursos humanos y tecnológicos para frustrar posibles amenazas a la empresa.

Es fácil entender la confusión y sus consecuencias. Los directores de Seguridad de las empresas, que por falta de recursos y/o un perfecto entendimiento, no están estructurados adecuadamente, combinan las tareas de planificación y ejecución simultáneamente y, por lo tanto, sus "entregables" no cumplen con los efectos deseados de la empresa. Hablemos ahora de cómo instrumentalizar, de manera práctica, la inteligencia y la contrainteligencia.

INTELIGENCIA Y CONTRAINTELIGENCIA CORPORATIVA: CÓMO INSTRUMENTALIZARLAS

Ya hemos aclarado la importancia y las diferencias conceptuales sobre las ramas de la actividad de la inteligencia a favor de las empresas. Considerando que la rama de inteligencia se centra en la producción de conocimientos que orientarán las medidas de contrainteligencia, la obtención y el análisis de datos debería emplearse para, por ejemplo:

- Identificación de vulnerabilidades y amenazas a la organización.
- Vigilando las posibles huelgas, los movimientos sindicales y sociales.
- Evaluación permanente de los delitos o acciones terroristas que afectan a la seguridad física de las personas y los negocios de las empresas.
- La vigilancia de las decisiones políticas, económicas o gubernamentales que afectan a la seguridad o a los negocios de la empresa (por ejemplo, la construcción de una prisión cerca de la planta).
- Vigilancia de las empresas asociadas o de los proveedores de servicios subcontratados.
- Evaluación de los asuntos relacionados con los viajes de los empleados y sus familias.
- La vigilancia de las banderas rojas en apoyo de otros sectores de la empresa.
- Monitoreando el análisis estadístico recomendando cambios de procedimiento o nuevos programas de entrenamiento.

En este sentido, los informes de inteligencia regulares, *ad hoc* o proactivos son una de las fuentes de análisis de inteligencia, al igual que las redes sociales y los medios de comunicación, los contactos con otros gestores de seguridad, las autoridades de seguridad pública y defensa, y la contratación de servicios de empresas especializadas en informes a corto plazo. De hecho, somos muy cuidadosos con los informes que contienen análisis previos que no añaden nada a las decisiones futuras.

Desde el punto de vista de la contrainteligencia, las acciones van desde las más simples como la ronda de un vigilante hasta la elaboración de planes y programas que contemplan medidas que previenen, detectan, obstruyen y neutralizan las acciones de la inteligencia adversa.

Ejemplificando:

- La elaboración de planes de gestión de riesgos, seguridad física y gestión de crisis.
- La protección ejecutiva de los expatriados y sus familias.
- Fortalecer la cultura de protección de los conocimientos sensibles; el desarrollo de un programa de mentalidad de seguridad en todos los niveles, incluyendo miembros, proveedores, compañías asociadas y contratistas.
- El establecimiento de estrictos controles de acceso que tengan en cuenta el plan de seguridad física; entrenando a los equipos de seguridad en procedimientos de seguridad, etc.

Estos son sólo algunos ejemplos de las medidas de contrainteligencia resultantes de los conocimientos producidos por el equipo de inteligencia. No hay una plantilla o lista de verificación; cada gerente debe buscar las soluciones que mejor satisfagan sus demandas.

Como hemos visto, la aplicación de la inteligencia y la contrainteligencia al servicio de la seguridad de las empresas es esencial para apoyar los objetivos de la empresa y proteger a sus miembros y activos, sus operaciones, su reputación e imagen.

Concluyo estas breves ideas destacando la importancia de una unidad de inteligencia empresarial bien estructurada para gestionar bien los riesgos corporativos, aumentar la calidad de las decisiones ejecutivas y asegurar un rendimiento financiero de las inversiones realizadas. ■

Sergio Ricardo Dominguito de Oliveira, *Security Manager* en Itaguaí Naval Construction.

Más sobre el autor:

Las medidas de detección, obstrucción y neutralización incluyen el uso de recursos humanos y tecnológicos para frustrar posibles amenazas a la empresa

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

Foto: Creativeart - Freepik

MÉTRICAS DE SEGURIDAD FÍSICA: TIEMPO DE DEMORA DEL ADVERSARIO

El indicador de vulnerabilidad que está en función de la detección, demora y respuesta

PERÚ | Herbert Calderón

Como es sabido por todos los profesionales que integran una organización, la seguridad como tal, cada vez está más relacionada con los procesos productivos de la organización, de acuerdo a las estadísticas del Allianz Risk Barometer, Top 10 Global Business Risks for 2021, Security Industrial Association, Security Mega Trends 2021 y Business Continuity Institute, Horizon scan Report 2021: la interrupción del negocio (BI) ha venido siendo el riesgo general más relevante en su 6° año seguido (42%), debido al tremendo efecto económico, como consecuencia de los crecientes escenarios, de las exposiciones tradicionales y el nuevo de pandemia, así como del daño ocasionado por el impacto de catástrofes e incendios en las instalaciones modernas, interrupción de la cadena de suministros, eventos relacionados con el '*cyber*', de no aparente daño físico, pero sí altos costos económicos, de igual forma los aspectos comerciales como los cambios de modelos antes situaciones externas y regulaciones o licencias de aprobación.

Esto significa en buen castellano que algo está descontinuando la operación, el escenario nuevo de la pandemia y los clásicos temas de '*cyber*', así como la ausencia en la protección de los sistemas y lógicamente la falta de preparación y respuesta de la organización ante crisis. Concluimos que:

a. **La continuidad del negocio es el primer riesgo empresarial:** la pandemia es la principal amenaza frente a la continuidad del negocio.

b. **La seguridad física:** involucramiento, convergencia tareas red información de la empresa. Dependencia mayor con la protección de información de la empresa.

c. **Nuevos requerimientos en los controles de acceso:** mayor intervención en la continuidad del negocio.

SEGURIDAD FÍSICA

Entonces en el proceso de continuidad del negocio, la seguridad física tiene una creciente intervención sobre todo por su alianza con la seguridad IT, sobre todos los aspectos de control de accesos, inteligencia artificial, sistemas de análisis de video y su rol protagónico con los roles en accesos en la actual pandemia. Sin embargo no tomamos el real dimensionamiento de un análisis de vulnerabilidades dinámico y en formato de métricas.

El concepto es muy sencillo de entender y a partir del cual procederemos a explicar los indicadores de vulnerabilidades mencionado anteriormente, esto es llamado tiempo de demora del adversario, los cuales se relacionan con las amenazas principales como intrusión, deshonestidad, sabotaje.

El concepto del tiempo de demora del adversario es el indicador de vulnerabilidad que está en función de la detección, demora y respuesta.

La detección comprende todo el sistema de detección de alarmas internas y externas teniendo en cuenta los posibles errores, fallas, falsas alarmas, malas prácticas de mantenimiento que podrían ocasionar una mala detección que es una vulnerabilidad importante.

La demora, está directamente relacionado con las barreras, paredes, cajas fuertes, bóvedas, muros, puertas, ventanas, techos, pisos, etc. Aspecto importante para el diseño del sistema de detección son las características y eficiencia de la barrera.

Finalmente tenemos el tercer indicador que es la respuesta o detención de la amenaza, constituida por la respuesta propia o de la misma instalación, remota compuesta por personal de empresa de seguridad externo, su efectividad está en función de las comunicaciones, monitoreo efectivo del centro de control, arribo de la fuerza de respuesta al lugar del incidente.

Los indicadores mostrados anteriormente constituyen las alertas de las vulnerabilidades, de no tomar las acciones necesarias pueden ocasionar una pérdida o interrupción del proceso productivo por un daño al patrimonio o ciclo de la operación del negocio. ■

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

Más sobre el autor:

La planificación de una estrategia a favor de la organización

LA IMPORTANCIA DE CONOCER LAS DIFERENCIAS DE INVENTARIO EN UNA EMPRESA

PANAMÁ | Albert Leikin

Foto: Creativeart - Freepik

Pareciera obvio hablar de este tema, sin embargo en todos estos años que vengo trabajando como consultor de seguridad, me encuentro con muy pocas empresas que manejan de forma real y evidenciada sus diferencias de inventarios, y esto muchas veces ocurre debido a un falso concepto generado por el alto volumen de ventas, o alto tráfico de la mercancía que hace que muchos dueños de empresas sientan como no necesario o que interrumpen la operación.

Muchas empresas familiares que han crecido y son hoy grandes compañías siguen teniendo comportamientos empresariales de estilo familiar y no logran incorporar metodologías de carácter corporativo como lo son el seguimiento de estándares y políticas enfocadas al cumplimiento y la calidad, el conocimiento de las diferencias de inventario y los índices de merma, tanto conocida como desconocida son uno de los pilares principales de un sistema de la gestión de la seguridad (SGS), ya que ningún departamento de Seguridad, por mejor que sea, podrá dar una respuesta efectiva en la protección de los activos si éste no conoce el origen de las pérdidas en su empresa.

Un departamento de Seguridad que no planifique su estrategia basado en el conocimiento y trazabilidad de las pérdidas históricas y reales de la empresa sólo podrá trabajar de manera subjetiva y su desempeño será siempre mediocre, si bien es cierto que el profesional de la seguridad debe evaluar y prepararse para todos los escenarios posibles y realizar análisis de riesgo y vulnerabilidad como primer paso para el desarrollo de una estrategia de protección de activos, el aporte de la incidencia histórica de diferencias de inventario brindan un marco esencial para lograr resultados reales en la disminución de las pérdidas.

CONTAR CON MÉTODOS ADECUADOS

Por lo tanto, las empresas deben contar con métodos precisos para la toma de inventario y poseer los mecanismos adecuados que aseguren su correcta divulgación basados en criterios que permitan el uso de esa información y creen indicadores que faciliten la evaluación de su incidencia, estos indicadores no sólo dan el soporte necesario para la planificación estratégica de un SGS, sino que también brindan una herramienta a la empresa para evaluar el desempeño del departamento de Seguridad y de forma objetiva.

Otro problema fundamental que me he encontrado en muchas empresas es la evaluación subjetiva del departamento de Seguridad y sobre todo del gerente o director de Seguridad a cargo. "Es que no atrapan casos", me decían. "Hemos tenido una gran cantidad de incidentes de robo en este último periodo", se preocupaba un CEO de una empresa muy importante de la región, pero cuando uno revisaba cuáles son los parámetros, o las métricas con las cuales evaluaban o cómo se determinaba la casuística de los eventos ocurridos, pues no existía ninguna medición objetiva y esto es muy peligroso en varios sentidos.

Primero, desconocer sobre los resultados reales y cómo este departamento de Seguridad logró o no proteger los activos de la empresa, puede llevar a perder buenos profesionales y, segundo, mantener en sus puestos a mediocres empleados y hasta bandas criminales que podrían desangrar durante años a una empresa hasta llevarla a la quiebra.

Una estrategia que hemos logrado implementar con mucho éxito y que siempre recomiendo es que los departamentos de Inventario y Auditoría estén dentro de la estructura del departamento de Seguridad y no bajo otras direcciones, esto permite una dinámica de trabajo, donde los responsables de la toma de inventario presentan los hallazgos. Auditoría determina el origen de la diferencia y aporta la evidencia necesaria, y Seguridad realiza los ajustes necesarios al SGS para proteger el activo impactado.

Existen muchas estrategias distintas, pero todas requerirán para la protección de los activos y el buen desempeño de los departamentos de Seguridad, así como de toda la operación, es contar con información real, actualizada y disponible de las diferencias de inventario. ■

Albert Leikin,
CEO de Sayeret Group y presidente de la Alianza de Seguridad Empresarial de Panamá (ASE).

Más sobre el autor:

COMUNICACIÓN ASERTIVA DEL LÍDER DE SEGURIDAD

Foto: Freepik - Freepik

El recurso humano tiene un talento infinito que si cuenta con un liderazgo efectivo y asertivo será productivo

VENEZUELA | Abraham Desantiago

Las organizaciones independientemente de cuál sea su orientación, requieren de líderes que sepan practicar una comunicación asertiva. Ante estos tiempos difíciles que aún atravesamos con la pandemia a nivel global, las organizaciones dependen de sus líderes para obtener el máximo potencial de su personal disponible, que en esta "nueva realidad" está en déficit. Citando al conferencista internacional, Adrián Cottin: "El liderazgo debe modelar las prácticas y conductas que alentarán el compartir la información, y más importante aún el compartir los pensamientos".

En tal sentido, la información debe ser continua, clara y concisa. El líder debe transmitir confianza, con el evento global del COVID-19 no se puede ocultar información ni detalles en cuanto al cuidado de nuestra salud y sus afines. Ser líder es sinónimo de poder, y siempre tendrá seguidores a su alrededor, por lo tanto, está en la capacidad y en el deber de dirigir el personal de organización y guiarlos a un norte donde todos estemos obteniendo beneficios.

Foto: katemangostar - Freepik

LA LEY DEL LÁTIGO

Ya hay resultados de estudios en donde hay evidencias que no podemos contar con "jefes". La ley del "látigo" no es productiva en la actualidad. Y cuando hablo de la ley del "látigo" me refiero a que no podemos seguir dando instrucciones y/o órdenes al personal que está a nuestro cargo en "blanco y negro", considero que debe existir un tiempo en donde el líder se aproxime al personal y le explique de manera concreta el "por qué" de las cosas.

Ante tanta incertidumbre que estamos viviendo todos los líderes, independientemente del nivel de comando, deben practicar y aplicar estrategias funcionales para la toma de decisiones desde la más rutinarias hasta las más complejas. Con máxima responsabilidad y moral los líderes deben ser ejemplos a seguir, ya sea que estén siendo observados o no, son quienes llevan y dirigen el personal que protege los activos de la organización.

En Latinoamérica, en líneas generales contamos con líderes en las distintas organizaciones capaces de dirigir y obtener su máximo potencial en todos los aspectos. El recurso humano tiene un talento infinito que si cuenta con un liderazgo efectivo y asertivo será productivo. En esta "nueva realidad" quien tuvo la visión de futuro para prepararse académicamente es con mucha probabilidad quien será el ganador (en sus propias circunstancias) después que pase todo el evento de la pandemia.

Como el líder está visualizando y evaluando constantemente, debe saber premiar y recompensar a quien merezca tal acción, motivado a que no todo se reduce a las necesidades socio-económicas. El personal también influye en el reconocimiento que obtenga. ■

Abraham Desantiago, supervisor de Central de Alarmas (CAMS Supervisor) de la Embajada Americana en Caracas, Venezuela.

Más sobre el autor:

SEGURIDAD® EN AMÉRICA

Suscripción Anual (6 ejemplares)

México: **$650 pesos**

Extranjero: **$270 dls.**

(incluye gastos de envío)

SEA

¡SUSCRÍBETE YA!

(55) 55726005

telemarketing@seguridadenamerica.com.mx

www.seguridadenamerica.com.mx

LOS TIEMPOS ACTUALES DEMANDAN PROFESIONALES DE SEGURIDAD CON ALTOS ESTÁNDARES

Foto: Creativeart - Freepik

VENEZUELA | Carlos Alfonzo Veigt Silva

El profesional en protección de activos de hoy en día debe poseer una preparación académica de alto nivel, capacidad de comunicarse en un idioma universal, dominando además las áreas de gerencia de proyectos y administración de empresas

El siglo XXI ha traído grandes cambios para los profesionales de la seguridad, los eventos del 9/11 obligaron a redefinir las políticas de prevención de riesgos y continuidad de negocios en las grandes corporaciones y con ello una forma distinta de ver a aquellos quienes tienen bajo su responsabilidad la protección de los activos en las organizaciones.

Cada día son más las universidades que incluyen en sus programas académicos a las carreras relacionadas con gerencia de riesgos y seguridad aplicada a diferentes áreas de negocios, entre otras; las certificaciones internacionales han adquirido mayor valor en la evaluación de perfiles profesionales de seguridad y en la misma medida los líderes de las áreas de prevención de pérdidas y gestión de riesgos han ido escalando posiciones estratégicas en los organigramas corporativos.

La opinión de la Gerencia de Seguridad hoy en día es de gran valor para la toma de decisiones en toda organización, desde procesos de rutina como selección de personal hasta grandes inversiones que guiarán el crecimiento de la compañía en los años próximos, involucran un análisis de factores que serán determinantes al momento de dar el visto bueno y para lo cual frecuentemente se solicita la participación de los especialistas en ésta área de desempeño.

Sin duda alguna, hablamos de una profesión que con el paso de los años se ha fortalecido y sin importar el nivel de riesgo con el cual se califique a un país, la prevención de riesgos siempre está presente y es por ello que el mercado laboral cada vez se hace más extenso y con importantes oportunidades en cargos con responsabilidades regionales y globales para los especialistas en prevención de pérdidas y protección de activos.

Tal vez una de las características más fascinantes de esta profesión es que nos da una oportunidad inigualable de hacer grandes aportes a la sociedad, llevando nuestros conocimientos más allá de los espacios de trabajo y llegando a influir incluso en lo más preciado para nuestro futuro, los niños. Cuando un profesional de seguridad dicta una conferencia o imparte un entrenamiento destinado a la prevención de cualquier evento inesperado, está contribuyendo

a fomentar conciencia de seguridad en todos aquellos quienes participan, sin embargo, su mensaje generalmente es replicado al círculo de influencia de cada una de esas personas que conformaron su audiencia.

ANÁLISIS DE RIESGOS

Los riesgos están presentes en todos los aspectos de nuestra vida diaria, en nuestro hogar, en las aulas de clases a las cuales asisten nuestros hijos, en nuestras oficinas, en cada lugar que visitamos y en cada actividad que realizamos. Del mismo modo, todas las decisiones de nuestra vida tienen implícito un riesgo asociado, el cual puede generar enormes beneficios si es acertada o grandes pérdidas si no se han evaluado a fondo todos los factores involucrados.

Amenazas, vulnerabilidades, impacto, entre otras definiciones, son elementos comunes de análisis en nuestra profesión, los cuales a través de la aplicación correcta de los conocimientos adquiridos y el aporte de nuestra experiencia a través de los años, nos permitirán dar una correcta valoración a un riesgo determinado y a su vez decidir la forma correcta de gestionarlo; dando como resultado medidas que deberán ser tomadas para evitar pérdidas y proteger activos de forma eficaz y eficiente, logrando así un aporte positivo en términos financieros para nuestra organización.

Sin embargo, estos principios también pueden ser aplicados a nuestra vida cotidiana para cada decisión que debamos tomar, en la cual será sumamente importante evaluar las amenazas presentes, los factores adversos o negativos al igual que las fortalezas, el impacto económico que será generado si la decisión es acertada o equivocada; siendo éste uno de los motivos por los cuales hoy en día el profesional de seguridad se ha convertido en un elemento valioso dentro y fuera del entorno laboral, ya que al ser un experto en gerencia de riesgos sus capacidades profesionales generan resultados más allá de los límites de su corporación.

Los avances tecnológicos y el desarrollo de herramientas cada vez más completas y versátiles también son parte de las actualizaciones que comprenden hoy en día la gestión de seguridad en toda organización, lo cual demanda personal preparado y capacitado para gerenciar y administrar estas aplicaciones, pero además ha logrado que el mercado de proveedores de servicios sea cada vez más competitivo, con propuestas sumamente innovadoras basadas en iniciativas y criterios de costo eficiencia, con personal certificado y con estándares de calidad que dan garantía de satisfacción en todos los trabajos realizados.

El profesional en protección de activos de hoy en día debe poseer una preparación académica de alto nivel, capacidad de comunicarse en su idioma nativo y por lo menos en un idioma universal, dominando además las áreas de gerencia de proyectos y administración de empresas de manera que pueda ser un asesor cuyas recomendaciones estén focalizadas en su área de especialidad, pero sin perder de vista los aspectos fundamentales del negocio.

De igual modo, es sumamente importante que tenga la capacidad de hacer llegar sus conocimientos a todo tipo de audiencia, desde la junta directiva de su corporación hasta el personal que conforma su comunidad de residencia, convirtiéndose así en un ciudadano valioso que genera grandes aportes a la sociedad. ■

> La prevención de riesgos siempre está presente y es por ello que el mercado laboral cada vez se hace más extenso y con importantes oportunidades en cargos con responsabilidades regionales y globales para los especialistas en prevención de pérdidas y protección de activos

Foto: Creativeart - Freepik

Carlos Alfonzo Veigt Silva, director de Operaciones Internacionales de WSO (Worldwide Security Options).

Más sobre el autor:

SECURITY MONDAY NIGHT DE GRUPO PAPRISA

UN AÑO DE SUMAR EN EL GREMIO DE LA SEGURIDAD PRIVADA EN MÉXICO

GRUPO PAPRISA SIGUE SUMANDO A LA CULTURA DE LA SEGURIDAD EN MÉXICO

La iniciativa ideada por Gabriel Bernal, CEO de GRUPO PAPRISA, y su equipo, parte del compromiso que nuestro colega adquirió hace años como patrocinador en diferentes eventos y causas y que ha refrendado con su liderazgo en diversos puestos de voluntariado en las principales asociaciones de seguridad como ASIS, ASUME (Agrupaciones de Seguridad Unidas por México), AMESP (Asociación Mexicana de Empresas de Seguridad Privada) y ANERPV (Asociación Nacional de Empresas de Rastreo y Protección Vehicular) por mantenernos informados y actualizados con un enfoque crítico y profundo que nos permita desempeñar un mejor papel como ciudadanos.

El segundo lunes de cada mes, desde septiembre de 2020, en este foro virtual convergen los principales actores del gremio para escuchar, cuestionar, debatir e interactuar de la mano del Dr. Sergio Aguayo, para entender los "resortes" de la violencia y la paz en México.

Dr. Sergio Aguayo

La primera temporada del SMN, abordó temas que establecen las múltiples interacciones entre crimen, gobierno, ciudadanía y entorno exterior; ejes temáticos que rigen las investigaciones del especialista y titular de este foro:

- **Cómo se derrotó a los ZETAS en las lagunas.**
- **La seguridad según AMLO. Informe vs. realidad.**
- **Puertos Aduanas y Militares.**
- **Elecciones Presidenciales en Estados Unidos y el impacto en México.**
- **La detención y liberación del General Cienfuegos.**
- **Resultados del Gabinete de Seguridad 2020.**
- **Redes sociales y seguridad.**
- **Emma Coronel y la prensa.**
- **Las migraciones y la seguridad de México y Estados Unidos.**
- **Las elecciones del 6 de junio y el narcotráfico en México.**
- **Los resultados electorales y la seguridad.**
- **La maldición del tercer año, análisis comparativo de la seguridad en tres sexenios.**

¿QUIÉN ES SERGIO AGUAYO?

Profesor - Investigador de El Colegio de México, desde 1977. Analista, periodista, escritor... en sus propias palabras, él comenta de sus proyectos actuales:

1. Desde hace varios años estoy reconstruyendo la historia del crimen organizado en Estados Unidos y México entre 1920 y 2020. Son parte de una historia compartida (y en buena medida desconocida) que permite hacer propuestas concretas para enfrentarlos.

2. En El Colegio de México coordino desde 2013 el Seminario sobre Violencia y Paz. En el Seminario participan unos 70 especialistas mexicanos sobre el tema (académicos, funcionarios, periodistas y activistas). Con un pequeño equipo de tiempo completo organizamos discusiones públicas y privadas, ofrecemos cursos y producimos documentos de trabajo a partir de investigaciones pioneras.

3. En coordinación con la Secretaría de Educación de la Ciudad de México iniciaremos el proyecto "Construyendo redes de paz en los Pilares de la Ciudad de México". El Seminario que coordino instalará un programa para lograr que la ciudadanía organizada establezca relaciones de confianza con las policías para que, entre ambas, atiendan a dos grupos particularmente relevantes: jóvenes y mujeres.

4. Desde 1984 escribo una columna semanal que actualmente publican el diario Reforma y otros trece diarios del país. También participo semanalmente en una mesa de análisis de Aristegui Noticias y en el programa Primer Plano de Canal 11 (principal canal público de televisión). ■

¿QUIÉN ES GABRIEL BERNAL?

Director y fundador de GRUPO PAPRISA, grupo de seguridad privada líder con más de 22 años de experiencia y presencia en toda la república mexicana.

Con una extraordinaria visión de negocio y liderazgo, GRUPO PAPRISA reúne más de 10 unidades de negocio enfocadas y dirigidas a las Seguridad Privada, desde elementos intramuros, seguridad electrónica, geolocalización y rastreo vehicular, equipamiento táctico, seguridad logística y custodia vehicular, evaluaciones en tiempo real, consultoría y capacitación.

Es licenciado en Administración de Empresas por la Universidad Autónoma de Guadalajara, Diplomado en Dirección de Seguridad en Empresas por el ICADE Business School y la Universidad Pontificia de Madrid.

Graduado del IPADE (Instituto Panamericano de Alta Dirección de Empresa), en programas de Alta Dirección de Empresas y Consejeros en Acción, programa de innovación para la alta dirección INNOVAD.

Actualmente se desempeña como vicepresidente de la ANERPV, vicepresidente de la AMESP, tesorero de ASUME y miembro del Consejo Consultivo de ASIS Capítulo México.

Se distingue por su compromiso con el gremio, su interés por la innovación y la digitalización del sector, mismos temas que difunde en diversas participaciones como '*speaker*' en foros de las asociaciones a las que pertenece.

"Cada mes buscamos de la mano de Sergio, el tema idóneo, que permita hacer un análisis profundo para sumar y contribuir con un granito de arena en el proceso de información y actualización continua de los líderes de la seguridad privada. Necesitamos más foros que impulsen el análisis, diálogo y reflexión sobre los temas de seguridad y política que aquejan a nuestro país e impactan nuestras labores".

Gabriel Bernal, CEO GRUPO PAPRISA.

NUMERALIA DEL SECURITY MONDAY NIGHT

Con 12 sesiones virtuales de ZOOM, 36 horas de transmisión y más de 700 colegas conectados en sus diferentes ediciones.

Este foro se posiciona como un 'must' de los profesionales de la seguridad que gustan estar bien informados.

CALENDARIO DE SESIONES DE LA 2° TEMPORADA DEL SMN

SEPTIEMBRE	13	MARZO	14
OCTUBRE	11	ABRIL	11
NOVIEMBRE	08	MAYO	09
DICIEMBRE	13	JUNIO	13
ENERO	10	JULIO	11
FEBRERO	14	AGOSTO	08

Fuente y fotos: Grupo PAPRISA

NO TE PIERDAS EL PRÓXIMO SECURITY MONDAY NIGHT, EL 13 DE SEPTIEMBRE.

SI TE PERDISTE ALGUNA DE SUS SESIONES, LAS PUEDES VER EN: WWW.SECURITYMONDAYNIGHT.COM

ESCANEANDO ESTE CÓDIGO QR PODRÁS REGISTRARTE:

CRIMINOLOGÍA Y POSITIVISMO, ENLAZAMIENTO PARA LA ORGANIZACIÓN SOCIAL

El positivismo criminológico, también conocido como escuela positivista, es una corriente criminológica cuyas principales ideas consisten en la aplicación de los métodos de las ciencias naturales para explicar la delincuencia y que la delincuencia está determinada biológicamente

MÉXICO | Wael Sarwat Hikal Carreón

INTRODUCCIÓN

La corriente del positivismo nace de Augusto Comte, postulando momentos en los que el entendimiento humano va abordando los fenómenos que le rodean para interpretarlos. Esos momentos están acompañados de etapas de construcción del conocimiento, donde pasa por la percepción y autodescripción basado en sí mismo o los conocimientos previos, para luego ir avanzando en la comprensión hasta llegar al punto donde se tiene contacto directo con lo que se quiere conocer.

César Lombroso empleó el método positivo en auge de la época mezclado con sus estudios de formación de medicina, así, en los inicios de sus estudios, observaba ciertas minorías en las cuales resaltó la atención en aquel periodo también por la conocida evolución de las especies que postuló Carlos Darwin.

Enrico Ferri, al no notar claridad en las clasificaciones de Lombroso, se propusieron enfocarse en los criminales, así la aplicación del método positivo experimental sería una aproximación considerada comprobable a los ojos de los requisitos positivistas, tradición que se legó al tiempo en el que se busca estar en contacto con lo estudiado o técnicas de interpretación precisa para la comprobación de los resultados.

Por otra parte, los alcances del positivismo están en la organización, con lo que aplicado al campo filosófico y político, a través de éstas en sus ramas positivas, buscan el poner orden a las cosas, lo mismo en la criminología positiva, busca la reorganización del caos social a través de la propuesta a los elaboradores de las políticas públicas.

Foto: Creativeart - Freepik

EL POSITIVISMO EN LOS INICIOS DE LA CRIMINOLOGÍA SISTEMÁTICA

A la par de los estudios publicados de Darwin, Lombroso (médico), quien hoy es considerado como "Padre de la Criminología", en su época realiza estudios sobre la tendencia biológica hacía la criminalidad, ganando gran popularidad en el tiempo donde el biologismo logró empoderarse, principalmente en la figura de Darwin (Narváes, 2005), llevando a que la atención se volteara a la evolución o involución de las especies, renunciando de cierto modo a las visiones teológicas de la concepción del todo en la vida, parte importante también del positivismo de Comte (Marías, 2017).

Con la clasificación de las ciencias o la enciclopedia de las ciencias de Comte (Marías, 2017), parte de la supremacía biológica se deriva de la importancia que éste atribuye a tal, siendo de las seis ciencias básicas más importantes, la penúltima, antes de la sociología, la biología, por lo que la explicación de la criminalidad, se realizaba a través de técnicas de las ciencias naturales y el método científico (Narváes, 2005).

Se usaba como modelo médico el referirse a la sociedad como un cuerpo, que podía enfermar, así, la criminalidad, es una patología social, una enfermedad. De entonces que surgieran términos compuestos como profilaxis criminal, patología social (Mimbela, 1960, p. 151), psicopatología del delincuente (Ingenieros, 1906).

Con la búsqueda de explicaciones al problema de la criminalidad, se adoptó el término de escuelas, propio del positivismo, refiriéndose a la sectorización de los conocimientos teóricos y discursos (Narváes, 2005), por lo que

A pesar que hace poco más de 100 años a través de Porfirio Díaz se introdujo el positivismo en México, estamos en un momento de involución, con descontrol en muchos aspectos de la vida, donde la educación popular o vulgar es predominante

Foto: Creativeart - Freepik

surgieron las llamadas escuelas del derecho penal y/o escuelas de la criminología, como un conjunto de saberes que explicaban desde diversas ópticas el fenómeno de la criminalidad, siendo una de éstas la titulada Escuela Criminal Positiva, fundada por Ferri, opuesta a la escuela Clásica.

Así, la criminología como ciencia sistematizada nace en aquel ambiente comtiano, mediante el cual, urgía una necesidad de utilizar el método científico para todo, con lo que se llegó a sinomizar que todo lo que era positivo, es científico, a la criminología le antecede la antropología criminal (también encontrada en su momento como criminología biológica), que luego se convirtió en criminología positiva.

De inicio, así como Darwin a las especies animales, Lombroso a la especie humana, distinguiendo la competencia entre hombres, mujeres, niños de adultos, blancos de negros, donde la jerarquía, auguraba la supremacía sobre otros, por ello se refería a una antropología (Narváes, 2005).

Aquellas especulaciones (teológicas) sobre el criminal, fueron trascendiendo (metafísica) (Marías, 2017) a la observación directa por parte de Lombroso a restos óseos de sujetos que en vida, fueron delincuentes, por lo que se afirmaba la observación directa, más allá de la especulación que proponía el derecho con afirmaciones sobre la supuesta voluntad y conciencia en los actos criminales por parte de sus ejecutores, mientras, las posturas jurídicas atribuían carácter de voluntad en el delito, Lombroso señalaba causas internas que predeterminaban su comportamiento.

Posteriormente, Ferri (autor de *Socialismo y Ciencia Positiva*) y Raffaele Garófalo se unen a los estudios de Lombroso, teniendo otra visión de este último, el primero, al ser este jurista, sociólogo y antrópologo, mientras que el segundo, criminólogo de formación jurista, permitieron autocorrecciones en la teoría explicativa de la criminalidad, pasando por el plano biológico al sociológico, juntando ambos. Aquellos estudios italianos, traducidos luego al español de España, permitió la llegada a México del positivismo criminológico (Narváes, 2005).

FILOSOFÍA CRIMINAL Y EL MÉTODO POSITIVO CRIMINAL

Salgado García (2010) postula al sujeto antisocial como punto de partida para las reflexiones en torno a la filosofía criminológica, se refiere al "ser antisocial", y engloba en su estudio a la pena, su ejecución, resocialización, reclusión, y el origen, naturaleza, generación del crimen. En este sentido, la filosofía criminológica organizará los conocimientos referentes a lo criminal como cuerpo de conocimientos para el entendimiento y transformación sobre la génesis trabajada y las necesidades individuales y colectivas.

"En el aspecto más sistemático, la nueva filosofía asigna directamente, como destino necesario, a nuestra existencia entera, a la vez personal y social, el mejoramiento continuo" (Marías, 2017, p. 40).

Por otra parte, la adaptación del método positivo al estudio criminal, deriva en la observación y experiencia, así los primeros positivistas criminólogos, miran al delincuente y el entorno que le circundaba para comprender sus motivos, le llamaron "método experimental", por tener objetos de estudio observables, estadísticos, frontales, no aislados, sino casos, sobre lo cual sostenían la construcción del conocimiento (Galfione, 2012).

POSTULANDO AL POSITIVISMO PARA LA PREVENCIÓN DEL DELITO Y ORGANIZACIÓN SOCIAL

El positivismo, en sus diversas acepciones y atributos, busca ordenar el caos existente; es decir, lo opuesto a lo negativo, sino a organizar, a construir (Marías, 2017, p. 20). En particular razón al ámbito de la política criminal, se busca ordenar la destinación negativa que la política en general tiende ahora, a reconstruir la moral, a la misma política, erradicar la corrupción y la incompetencia de los líderes políticos (Núñez Carpizo, 2010, p. 370), donde en este ejercicio, pocos en la población son los interesados en la política, sino los que se benefician de ésta y forman parte de la misma (Marías, 2017).

La criminología positiva "buscó establecer lo más claramente posible el *status* del criminal a fin de poder controlar el aumento/disminución de la criminalidad, una aspiración que llega cargada de necesidad hasta nuestros días" (Narváes, 2005, p. 163). En el actual, se distanció el sentido de progreso, siendo una premisa que "el destino necesario de todas nuestras sanas especulaciones para el mejoramiento continuo de nuestra verdadera condición, individual y colectiva, en lugar de la vana satisfacción de una estéril curiosidad" (Marías, 2017, p. 29), pero en la política actual, se va por camino opuesto.

El contexto mexicano requiere urgentemente una reorganización, que vista desde el positivismo, constituye el camino al verdadero mejoramiento de

La criminología como ciencia sistematizada nace en aquel ambiente comtiano, mediante el cual, urgía una necesidad de utilizar el método científico para todo, con lo que se llegó a sinomizar que todo lo que era positivo, es científico, a la criminología le antecede la antropología criminal

la humanidad. A pesar que hace poco más de 100 años a través de Porfirio Díaz se introdujo el positivismo en México (Núñez Carpizo, 2010, p. 370), estamos en un momento de involución, con descontrol en muchos aspectos de la vida, donde la educación popular o vulgar es predominante, alejándonos del conocimiento científico, sistemático, comprensible, que nos permita salir del individualismo, y unirnos al interés colectivo de progresar de manera ordenada, ocurre lo opuesto.

De tal modo, una filosofía positiva busca "estimular y consolidar el sentimiento del deber, desarrollando siempre el espíritu de colectividad" (Marías, 2017, p. 48). Tal es la importancia, como se indicó a la similitud médica de la sociedad, de aislar o eliminar a los elementos nocivos que provocan la criminalidad.

"Los factores que intervienen como causas de la actividad delictuosa son variadas: el clima, la pobreza, la miseria, el analfabetismo, etc." (Orellana Wiarco, 2007, p. 162). La filosofía positiva aporta un conocimiento organizado de la realidad, cuyo producto debe ser tomado por los líderes políticos para orientar a cambios sociales que lleven al progreso de la sociedad, actualmente, como hace 100 años, México es tierra fértil para instaurar un pensamiento positivo comtiano (Núñez Carpizo, 2010, p. 374). Anteriormente, el conocimiento filosófico era atribuido a los sabios, políticos, doctores, abogados, como agentes culturales de cambio, siendo hoy necesario retomar el saber y destinarlo de manera reconstructiva.

Considerando una política social reconstructiva, "nada verdaderamente grande puede emprenderse, ni para el orden, ni para el progreso, por falta de un (sic) filosofía realmente adaptada al conjunto de nuestras necesidades" (Marías, 2017, p. 36).

Partiendo del análisis de estas necesidades, sectorizándolas para atender aquello que se ha descuidado y vulnerado, interviniendo en las relaciones familiares, grupos sociales, la educación y valores cívicos, religiosos, el empleo, vivienda, urbanidad, salud, grupos sensibles al riesgo, entre otros factores que promuevan la violencia (Oficina de las Naciones Unidas contra la Droga y el Delito, 2007, pp. 292 y 293).

CONCLUSIONES

Someramente se mostró la articulación del positivismo con la criminología, siendo que con los conocimientos que en ésta convergen y el ordenamiento que ella puede dar, busca la organización social, mediante el conocimiento del fenómeno criminal, visto desde diversas ópticas de las ciencias que han tomado en su objeto de estudio, los temas de criminalidad, violencia o antisocialidad. El fin último de esto, es proponer soluciones a los operadores de las políticas sociales, para con el saber de la dinámica social y sus problemáticas, buscar vías de regeneración del tejido social y humano. ■

Foto: Creativeart - Freepik

REFERENCIAS

- *Comte, A. (2017). Discurso Sobre el Espíritu Positivo. Alianza Editorial.*
- *Galfione, M.C. (2012). La sociología criminal de Enrico Ferri: entre el socialismo y la intervención disciplinaria. VII Jornadas de Sociología de la Universidad Nacional de La Plata. http://jornadassociologia.fahce.unlp.edu.ar/vii-jornadas-2012/actas/Galfione.pdf*
- *Mimbela, E. (1960). La Criminología en la Universidad de Roma. Derecho PUCP, (19), 149-153. https://dialnet.unirioja.es/descarga/articulo/5236523.pdf*
- *Narváez, J.R. (2005). Bajo el signo de Caín: La criminología positiva en México. Anuario Mexicano de Historia del Derecho, (17), 157-175. http://www.cienciaspenales.net/files/2016/11/7_jose-ramon-narvaez.pdf*
- *Núñez Carpizo, E. (2010). El positivismo en México: impacto en la educación. Universidad Nacional Autónoma de México. https://www.derecho.unam.mx/investigacion/publicaciones/librosfac/pdf/pub03/11DraNunez.pdf*
- *Oficina de las Naciones Unidas contra la Droga y el Delito (2007). Recopilación de Reglas y Normas de las Naciones Unidas en la Esfera de la Prevención del Delito y la Justicia Penal. https://www.unodc.org/pdf/criminal_justice/Compendium_UN_Standards_and_Norms_CP_and_CJ_Spanish.pdf*
- *Orellana Wiarco, O.A. (2007). Manual de Criminología. México: Editorial Porrúa.*
- *Salgado García, A. (2010). Filosofía criminológica: Una primera aproximación al "ser-antisocial". Quadernos de Criminología: Revista de Criminología y Ciencias Forenses, (10), 38-43. https://dialnet.unirioja.es/servlet/articulo?codigo=3308140.*

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

Más sobre el autor:

E-Mail Blast

SEGURIDAD EN AMÉRICA

Permítanos transmitir su mensaje a través de nuestra base de datos que se compone de más de 45 mil contactos de toda Latinoamérica.

Nuestro servicio de correo masivo le ofrece apoyo de diseño para sus anuncios, HTML's y formulario de contactos.

(55) 55726005

krauda@seguridadenamerica.com.mx

www.seguridadenamerica.com.mx

LOGÍSTICA PARA LA SEGURIDAD EN EVENTOS

MÉXICO | David Chong Chong

La gestión de seguridad para un evento se aborda como una problemática de manejo de multitudes, por lo cual la logística debe considerar el potencial de riesgos derivado no sólo de los aspectos de espacios y dinámica del evento en sí mismo, sino también lo que se refiere a los motivos de convocatoria y, sobre todo, las posibilidades de satisfacción de las expectativas de los asistentes

Un evento consiste en la permanencia temporal de una multitud en un mismo espacio, convocados por un interés común, que no necesariamente puede ser de entretenimiento, como los espectáculos, sino también por alguna forma de gestión, como los procesos de inscripciones escolares o de vacunación, e incluso de protesta por alguna causa de reivindicaciones sociales. Asimismo, el desarrollo de un evento contempla tres etapas: el ingreso, la permanencia y el desalojo, cada una con su propio perfil de dinámica, y por ende de potencial de riesgos, que se puede describir como de movilidad ordenada, inmovilidad relativa y movilidad posiblemente desordenada, respectivamente.

Adicionalmente, un evento puede ser de tipo puntual, con cada una de estas etapas ocurriendo en un momento diferente, por lo general mutuamente excluyentes, como sería el caso de espectáculos y algunos procesos de gestión, o bien de tipo continuo, con las tres etapas ocurriendo simultáneamente en todo momento, como es el caso de los visitantes a museos o parques de diversiones. Finalmente, un evento puede ocurrir de manera organizada, improvisada o espontánea, y puede ser de única vez, recurrente o bien de alguna manera establecido o permanente.

Foto: Creativeart - Freepik

POTENCIAL DE RIESGOS

Los factores que configuran el potencial de riesgos para un evento comprenden, de manera enunciativa, mas no limitativa:

- El propósito o motivo de convocatoria (entretenimiento, gestión, distracción, confrontación), el sentido de urgencia (apremiante o aplazable) y las posibilidades de satisfacción (positiva o negativa, es decir, conseguir algo o rechazarlo).
- La perspectiva de expectativas y realidades de satisfacción, con la probabilidad de que las expectativas sobrepasen las realidades.
- Las condiciones del espacio en que se realiza el evento, y las facilidades y recursos de apoyo disponibles.
- El perfil de actitud de los asistentes (amigable, cooperativo, neutro, hostil, agresivo).
- El perfil de dinámica del evento, en particular en lo que se refiere a la actividad esperada de los asistentes (activa como actor principal, pasiva como espectador, semiactiva con alguna interacción con el protagonista del evento).
- El perfil de Carencias, Deficiencias e Insuficiencias en los espacios, facilidades y servicios para la permanencia, así como en los accesos para el ingreso y desalojo de los asistentes.
- El perfil de incomodidades y dificultades para el desarrollo, derivadas del tipo de facilidades disponibles, que pueden ser dedicadas, adaptables o de plano inexistentes.

Que de manera individual o concurrente pueden atemperar o exacerbar la actitud de los asistentes, y por ende aumentar o disminuir el potencial de riesgos.

Por ello se pueden proyectar como los objetivos de seguridad para un evento:

1. Proteger a las personas.
2. Facilitar el desarrollo del evento.
3. Proteger las instalaciones del espacio.

Para lo cual las premisas de seguridad proyectadas para un evento contemplan: alguna forma de control de acceso en el ingreso, la preservación del orden y tranquilidad durante la permanencia, y la protección de personas, y en algunas ocasiones cierto control de salida, en el desalojo; que requieren facilidades con funcionalidades que permitan:

- En el ingreso, una movilidad confinada y la validación de los instrumentos de franqueo (tarjetas, pases, boletos, o simple conteo para control de aforo), en condiciones de restricción y agilidad de ingreso al espacio del evento.
- En la permanencia, la restricción de la ubicación asignada y la contención de la conducta de los asistentes a los parámetros proyectados para el tipo de evento.
- En el desalojo, una movilidad razonablemente ordenada, y si es necesario la aplicación de algún control de salida del espacio.

Para estos propósitos se requiere de recursos humanos, como elementos de eficacia, indispensables, para las funciones de vigilancia y restricción, como tareas normales, y de intervención, cuando sea necesario, así como de recursos de tecnología, como elementos de eficiencia, necesarios y deseables, de apoyo a las funciones de vigilancia, por medio de sistemas de videovigilancia, fijos en recintos dedicados o reubicables (cámaras inalámbricas, drones) en espacios no dedicados, con analíticos de video y reconocimiento facial o de patrones de conducta, e incluso de restricción, para el conteo de personas y la validación de los instrumentos de franqueo, como torniquetes o lectores digitales de códigos QR o de tarjetas de proximidad.

Foto: Creativeart - Freepik

Las premisas de seguridad proyectadas para un evento contemplan: alguna forma de control de acceso en el ingreso, la preservación del orden y tranquilidad durante la permanencia, y la protección de personas

Otros aspectos que se deben considerar son las previsiones para el manejo de multitudes, acordes al perfil de conducta esperado (casual y amigable, expresiva, hostil y agresiva) y su posible evolución por el curso de desarrollo del evento, además de la instrumentación de las normativas vigentes aplicables en materia de Protección Civil, con una atención particular al manejo de Personas con Limitaciones de Movilidad, y en especial a las Personas con Discapacidad en caso de emergencias, con previsiones como las establecidas en la NOM-008-SEGOB-2015.

En consecuencia se puede establecer que la perspectiva de efectividad, y por ende de éxito de la logística de seguridad para un evento estará determinada por el nivel de cobertura de todos los aspectos antes descritos en la planeación, el perfil de suficiencia e idoneidad de las facilidades y recursos disponibles, y la oportunidad de su suministro en la preparación, y el nivel de cumplimiento de las previsiones y la pertinencia en la toma de decisiones durante la operación, en particular ante condiciones o situaciones imprevistas. Para ello, lo más recomendable no es buscar lo más costoso o sofisticado, sino lo que mejor se adapte a las necesidades de cada caso, con los recursos disponibles que por lo regular serán escasos. Asimismo, se debe tener presente que la realidad, como resultante de la conducta humana, rara vez ocurre según lo planeado, en particular en el ámbito de la seguridad, en donde nunca se tendrá certeza absoluta, sólo se puede aspirar a reducir la incertidumbre, de tal suerte que siempre puede ocurrir lo imprevisible, lo inesperado, que obligará a "hacer lo mejor que se puede, con lo que se tiene (Adm. Ernest King U.S. Navy)". ■

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

Más sobre el autor:

EL ABC DE LA SEGURIDAD EN **EVENTOS MULTITUDINARIOS**

Foto: Creativeart - Freepik

¿Qué aspectos se deben considerar previamente, durante y después de un evento masivo?

MÉXICO | José Luis Sánchez Gutiérrez

En muchas ocasiones se desconoce cómo actuar para no lamentar una desgracia durante los eventos masivos. Es de suma importancia garantizar la seguridad cuando se celebran grandes eventos, esto debido al gran número de personas que se congregan.

Recordemos que organizar un evento requiere de medidas de prevención y protección, y más aún si este implica gran aglomeración de personas. Esto ayuda a evitar que los asistentes tengan que enfrentar situaciones de riesgo o que salgan lesionados.

En general, la música, el ruido y las bebidas alcohólicas, aunque estén prohibidas, se juntan en estos eventos multitudinarios. Es por ello que una buena gestión y ubicación son factores que se deben trabajar en conjunto para brindar un adecuado control y organización para eventos.

Es necesario contar con vías de evacuación; asegurar la estabilidad del inmueble; limitar la presencia de materiales peligrosos; disponer de equipos técnicos en buen funcionamiento y medios de auxilio de intervención inmediata, además de formar y dar las instrucciones adecuadas al personal. Tanto para acontecimientos deportivos, culturales, religiosos, artisticos, políticos, conciertos u otras reuniones masivas, todos los grandes eventos necesitan un cuidado especial con las situaciones que generan condiciones de riesgo en materia de seguridad y manejo de emergencias.

En cada evento masivo se deben garantizar vías de evacuación seguras, indicadas claramente, que permanezcan abiertas y libres de todo obstáculo. Garantizar la estabilidad del inmueble donde sea realizado el evento durante el tiempo necesario para permitir a los ocupantes salir sanos y salvos. Limitar la presencia en el inmueble de componentes o materiales peligrosos, como los materiales inflamables.

Mantener en buen estado y funcionamiento los equipos y aparatos técnicos a utilizar, sistemas de evacuación, así como los sistemas. Las consignas de seguridad de cada elemento asignado y los planos de evacuación expuestos en cada ubiación ocupada; así como restringir el tráfico de vehículos pesados (si pesan más de tres toneladas) y retirar obstáculos de la vía pública, además de habilitar carriles de emergencia de manera preventiva.

En el día a día vemos cómo los campos de futbol se llenan todas las semanas de aficionados, los festivales de música se han ido generalizando por toda la geografía mundial concentrando enormes multitudes; los parques de atracciones y de ocio también generan

una gran concentración de personas. El control de accesos es fundamental para evitar consecuencias muy graves en estos eventos.

Se ha identificado que los incendios son uno de los riesgos más comunes en espacios de grandes eventos, cuando se reúnen miles de personas en un edificio, campo de futbol o, sala de conciertos. Si bien en la mayoría de los casos no pasa de un conato —que se apaga con los sistemas disponibles y cuyo costo se asume sin problemas por la compañía de seguros—, en otros las graves consecuencias, incluidas muertes, hacen mantener activa la preocupación y ejecución correcta del diseño, la instalación y los mantenimientos de protección de los equipamientos contra incendios.

Debemos prever que el acceso esté abierto con suficiente antelación al evento para conseguir una entrada más escalonada, aunque siempre en los momentos previos aumentará la afluencia, disponiendo de varias filas de accesos

LAS FASES ESENCIALES

A la hora de garantizar la seguridad y la prevención en el manejo de eventos masivos existen tres fases esenciales:

1. **Planificación:** hay que estudiar a detalle cuáles son los elementos de riesgo susceptibles de producirse durante el evento y al mismo tiempo diseñar todas las acciones de seguridad que los prevenga.

2. **Intervención:** en esta fase se llevará a cabo el plan de seguridad elaborado previamente. Esta segunda fase es dinámica, por lo que los profesionales que estén interviniendo tienen que seguir analizando el evento para adecuar en cada momento las medidas en caso de que fuera necesario.

3. **Evaluación:** en esta fase es muy importante reflexionar y analizar la gestión del riesgo realizada para poder mejorar la efectividad de cara a futuras intervenciones en este tipo de eventos masivos.

Foto: Creativeart - Freepik

Siempre debemos tomar en cuenta que el control de accesos es una función que en los últimos tiempos asume un alto grado de responsabilidad, dados los acontecimientos que se han sucedido en eventos deportivos o festivales musicales, sumando el actual nivel de alerta terrorista por las amenazas terroristas en algunos casos.

Es conveniente en todo evento masivo saber si se trata de lugares cerrados o al aire libre, aunque delimitados mediante barreras físicas fijas o móviles; como son el caso de los macro festivales donde se habilitan grandes extensiones de terreno para ello.

Por el tipo de actividad que se va a desarrollar y el horario podremos tener un perfil del tipo de público que va a asistir, adolescentes, jóvenes, familias, etc. Y dentro de éstos se podrán ir haciendo otro tipo de clasificaciones importantes en lo que a seguridad se refiere.

Con toda la información podemos ir trazando el plan de seguridad para el evento concreto y dentro de éste estableceremos el subsistema de control de accesos en donde debemos considerar:

a) Legislación o normativa aplicable (ley del deporte, espectáculos públicos, etc).

b) Riesgos a evitar y controlar.

c) Funciones a realizar (cacheos, registros, identificación, acreditación, etc.).

d) Recursos y medios necesarios (personal de seguridad, torniquetes de acceso, detectores de metales, videovigilancia, lectores, etc.).

A partir de aquí, debemos considerar:

a) Para realizar un control de accesos eficaz no podemos quedarnos escasos de personal en la entrada al evento, tanto por efectivos en general o por personal insuficiente de un determinado sexo (masculino o femenino), ya que daría lugar a largas colas o que al final no se pueda controlar todo lo que se haya determinado.

b) Debemos prever que el acceso esté abierto con suficiente antelación al evento para conseguir una entrada más escalonada, aunque siempre en los momentos previos aumentará la afluencia, disponiendo de varias filas de accesos.

c) Igualmente, la utilización de medios tecnológicos facilitará el trabajo de seguridad, tales como torniquetes de acceso, detectores de metales, utilización de cámaras, lectores de identificaciones y entradas etc.

d) Por último, la utilización de barreras físicas para la conducción del público, facilitando llevarlo hacia las zonas de acceso y evitar la entrada por lugares no habilitados son un gran apoyo para la seguridad.

Independientemente de que se trate de un recinto dotado o no con determinadas medidas de seguridad; hoy en día cualquier tipo de dispositivo puede ser instalado con el contenido necesario y volverlo a quitar sin que esto suponga un desembolso extraordinario.

También si como individuo deseas asistir solo o con tu familia te hago una serie de sugerencias en el plan que pueden ayudarte a mantenerte con un mínimo riesgo y una criticidad controlada para ti y tu familia; el plan de tres fases es el siguiente:

ANTES DE IR AL EVENTO MASIVO:

1. Define varios puntos de reunión.
2. Utiliza ropa adecuada al evento, busca información meteorológica con la intención de prevenir lluvia, granizada, nevada o temperaturas extremas.
3. Se recomienda que niños menores a siete años no deben de acudir a eventos masivos, por su seguridad, pero en caso de hacerlo, se debe asignar un adulto por cada niño.
4. No lleves contigo botellas u objetos puntiagudos que puedan causarte a ti o a alguien daño.

EN EL MOMENTO DE ESTAR EN EL EVENTO MASIVO:

1. No te separes del resto de la familia o define a un adulto responsable asignado a cada menor.
2. Si están perdidos, no actúes de forma sospechosa, elige un lugar despejado y contacta por teléfono, espera de 5 a 10 minutos, si no llegan es posible que estén en el punto de reunión elegido más cercano.
3. Identifica las rutas de evacuación y salidas más próximas a tu lugar de llegada.
4. Existen puestos de primeros auxilios y de combate contra incendios, solicita su ubicación con el fin de que en caso de presentarse algún siniestro puedas acceder de forma rápida.
5. No obstruyas pasillos, escaleras o salidas.
6. Si el ambiente se torna violento o peligroso, elige retirarte, tu seguridad y la de tu familia siempre es primero.
7. En caso de emergencia guarda la calma y evita correr.
8. Si detectas comportamientos peligrosos de otras personas, notifica a las autoridades correspondientes.
9. Evita utilizar ropa holgada o con cordones sueltos, ya que al momento de recorrer pasillos podrías atorarte.
10. No caigas en provocaciones si la multitud se vuelve agresiva.
11. Si existe pirotecnia contemplada en el evento, evita colocarte en zonas cercanas.
12. Si la multitud avanza, evita colocarte en puertas para evitar empujones, es mejor buscar un punto alto, esquinas o espacios libres a los lados. Si caes al piso, procura incorporarte rápidamente, para ello es preferible avanzar en parejas.

Foto: Creativeart - Freepik

DESPUÉS DEL EVENTO MASIVO:

1. Si te vas a retirar procura hacerlo unos minutos antes de terminar el evento, con el fin de evitar las aglomeraciones, en caso contrario espera a que se desaloje del 40% al 50% el lugar.
2. Si se perdieron durante el evento o poco antes de terminar, es mejor esperar a que termine para reunirse en un punto fijado previamente, pero procura contactar vía telefónica o por mensaje de texto.
3. Al final de los eventos es común que se presenten pleitos entre asistentes, evita acercarte, si estás cercano a la salida espera que la autoridad los retire o busque una segunda opción para salir. ■

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

Más sobre el autor:

SEGURIDAD®
EN AMÉRICA

SÍGUENOS EN NUESTRAS REDES SOCIALES Y MANTENTE INFORMADO DE LAS ÚLTIMAS TENDENCIAS DE SEGURIDAD

www.seguridadenamerica.com.mx

Foto: Creativeart - Freepik

La integración de sistemas de seguridad para resguardar los fraccionamientos

LA SEGURIDAD **FÍSICA Y TECNOLÓGICA EN BARRIOS CERRADOS,** UN SERVICIO ESENCIAL

ARGENTINA | Alejandra Dressel

Sin dudas la "sensación de vivir seguros" fue entre otras razones el gran motivo por lo que los barrios privados tuvieron su auge hace casi cuatro décadas en la Argentina, tener un hogar seguro era para muchos el sueño a cumplir, "dormir tranquilos", "que nuestros hijos crezcan en un lugar seguro", "mi casa es mi lugar en el mundo y vivo sin miedo" era el pensamiento de la mayoría, pero ¿hoy los habitantes de estas urbanizaciones siguen con esa sensación de "vivir seguros"?

Los profesionales de la seguridad debemos analizar este fenómeno, cada año que pasa las amenazas se acrecientan, la delincuencia va tomando diferentes *modus operandi* para flaquear esa sensación de tranquilidad que los habitantes de los barrios cerrados tenían.

Sabiendo que la seguridad pasó de ser un servicio opcional, a un servicio esencial para estos emprendimientos, debemos estar a la altura de la demanda de los habitantes del lugar.

La empresa prestadora de la seguridad, además de brindar seguridad física, debe tener un Departamento Tecnológico, que trabaje en conjunto con el Área Operativa, para poder brindar las soluciones más acertadas a las amenazas.

El mercado es ágil, cambiante y nos ofrece diversidad de soluciones para cada caso, no todas las urbanizaciones presentan la misma problemática.

¿ES POSIBLE SEPARAR LA SEGURIDAD FÍSICA DE LA SEGURIDAD ELECTRÓNICA?

La respuesta más acertada y acorde a esta época es no. La tecnología es una gran aliada, nos permite tener alertas tempranas de posibles intrusiones, que hacen que los planes de contingencias puedan ser ejecutados a distancia por personal idóneo, que trabaje en conjunto con el personal *in situ*.

¿LA SEGURIDAD ELECTRÓNICA ES UNA INVERSIÓN MUY COSTOSA?

Si pensamos en realizar un plan de seguridad que se mantenga en el tiempo, que nos genere herramientas que enriquezcan la infraestructura del lugar a nivel seguridad sin tanta dependencia de cantidad de vigiladores, nos daremos cuenta que el costo de las instalaciones electrónicas son una inversión y no un gasto.

¿QUÉ TIPO DE SEGURIDAD ELECTRÓNICA ES LA MÁS ACERTADA PARA LOS BARRIOS PRIVADOS?

Partimos de la base que cada emprendimiento es diferente, debemos comenzar por analizar la estructura del lugar, ya que cada urbanización tiene sus propias necesidades, riesgos y requerimientos.

Lo ideal sería que al momento que se proyecte cómo será el emprendimiento, la empresa desarrolladora sumara a un grupo de profesionales en seguridad que diseñen un sistema de seguridad electrónica para dicho lugar, ya que en la mayoría de los casos cuando nos llaman ya está terminado y se debe comenzar con una inversión millonaria por no prever que la seguridad en la actualidad es como ya hemos mencionado en la nota un servicio esencial.

> La empresa prestadora de la seguridad, además de brindar seguridad física, debe tener un Departamento Tecnológico, que trabajen en conjunto con el Área Operativa, para poder brindar las soluciones más acertadas a las amenazas

¿CUÁLES SON LAS ÚLTIMAS TENDENCIAS EN SEGURIDAD ELECTRÓNICA PARA ESTAS URBANIZACIONES?

En la actualidad contamos con infinidad de *software*, que nos permiten a distancia saber qué está pasando en el lugar, haciendo así el trabajo de supervisión más efectivo.

En Giomon, empresa de seguridad argentina con 35 años de experiencia, entendemos que el valor agregado es el monitoreo *online* de todos los productos de seguridad electrónica instalados, basados en este concepto hemos desarrollado una herramienta de verificación a distancia, donde combinamos el rastreo satelital y los protocolos con el monitoreo, brindando a nuestros clientes una verificación constante del trabajo de lo vigiladores.

El mercado es amplio y rico en productos para proteger lugares, pero el secreto es la integración de sistemas de seguridad, la misma nos permite combinar diferentes marcas, tecnologías y protocolos para que funcionen en forma unificada. ■

Foto: Creativeart - Freepik

Alejandra Dressel,
directora técnica de la empresa Giomon.

Más sobre el autor:

LA EXPERTICIA FORENSE Y LOS PERFILES CRIMINALES

Foto: Creativeart - Freepik

¿Cómo se puede identificar plenamente a los autores de un crimen?

PERÚ | César Benavides Cavero

En el año 1892, Hans Gross, abogado y juez del crimen en Viena, Austria, publicó su texto intitulado: El juez y las ciencias criminalísticas, donde se incluían todas aquellas que se iban incorporando para la investigación científica del delito; y que los policías, fiscales y jueces necesitaban para poder condenar a los autores. El avance tecnológico sobrepasaba largamente a la investigación científica del delito y la policía tenía que estar por encima de éste.

En el año 2008, cuando nos encontrábamos en Nueva York, Estados Unidos, tuvimos la oportunidad de encontrar el libro *You can't lie to me* (*Tú no puedes mentirme*) de la profesora del FBI (Buró Federal de Investigaciones), CIA (Agencia Central de Inteligencia) y ATF (Agencia de Alcohol, Tabaco, Armas de Fuego y Explosivos), Janine Driver, obra que deben leer todos los jefes y personal de la Policía Nacional del Perú y de todo el mundo. Lamentablemente dicho texto está escrito en el idioma inglés.

EL PERFIL CRIMINAL

Es la técnica forense proveniente de las pesquisas criminalísticas y criminológicas derivadas del análisis que se realizan de los diferentes patrones conductuales para con ello definir y crear tipologías y así cooperar con la resolución de crímenes en los casos que se desconoce al responsable o a los autores. A partir de los indicios físicos y psicológicos encontrados en la escena del crimen.

Esta actividad científica forense se inicia en Estados Unidos el año 1978 con la creación de la unidad de Ciencias del Comportamiento en la Academia del FBI en Quántico. El proceso utilizado por los investigadores tienen que preparar un "perfil" de la personalidad del presunto sospechoso, sobre la base de la información recibida de los testigos y personas que pueden haber conocido de las personas. Así como de los testimoniales recepcionados. De esta manera se puede llegar a la identificación absoluta del o de los autores.

Foto: Creativeart - Freepik

Con la información y rastros recibidos se reconstruye la escena del delito, se construyen hipótesis, se deben formular hipótesis sobre imágenes de probables culpables, se realizan perfiles sobre probables autores. Con el auxilio de dibujantes y reconstructores de rostros. Se puede llegar a identificar plenamente a los autores.

La formulación del documento o informe (atestado) policial se deben presentar con todas las evidencias posibles para poder obtener una sentencia firme contra el autor y/o autores, sin embargo hoy en día las diferentes policías del mundo cuentan con máquina para identificación rostros, de huellas digitales, de identificación de ADN (ácido desoxirribonucleico), olores, etcétera. Ojalá algún día existieran máquinas que se adelanten al delito. La ciencia trata de encontrarse a "un paso delante de los delincuentes". ■

César Benavides Cavero,
Summa Cum Laude, director del Instituto Peruano de Criminalística.

Más sobre el autor:

CURSOS ALAS

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

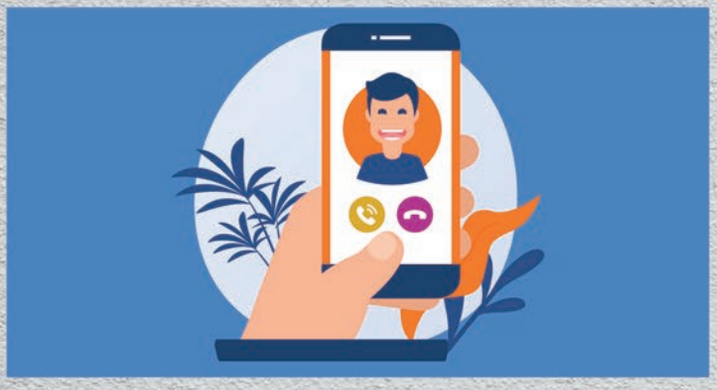
CREA TU GRUPO, NOSOTROS LO CERTIFICAMOS.

Cursos In Company es la mejor opción para tu empresa.

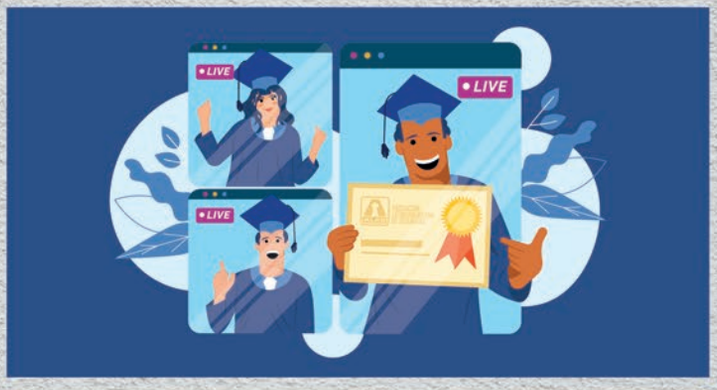
ALAS te ofrece la oportunidad para que lleves la profesionalización de tus empleados al **siguiente nivel.** ¡Es muy simple! Te contamos cómo:

1. Crea tu grupo empresarial con los empleados que quieras certificar.

2. Escoge la tecnología en la que tienes una mayor necesidad de capacitación.



3. Háblanos hoy mismo para acompañarte en el proceso.



4. Certifica en línea a tu equipo con la calidad y respaldo internacional de nuestros Cursos ALAS.

¡Empieza hoy mismo!

ISABEL COLIN Ejecutiva de Ventas
Whatsapp: +52 1 55 7907 2481 - Email: isabel.colin@alas-la.org

Para conocer toda nuestra oferta de Cursos ALAS:

www.alas-la.org/cursos-en-linea

Foto: Creativeart - Freepik

SEGURIDAD EN LA NUEVA NORMALIDAD

ECUADOR | Raúl Morán

Debido a la crisis económica y el desempleo por la pandemia del coronavirus, diversos delitos han ido en aumento

Luego de haber revisado las estadísticas de seguridad de los últimos meses, se puede deducir que la delincuencia está mutando de acuerdo a las circunstancias. Si bien los números nos indican que el índice delictivo se redujo durante los meses que duró el confinamiento por la presencia del SARS-CoV-2, también podemos ver que en el mismo tiempo se intensificó la incidencia de otro tipo de delitos en los que la tecnología fue la principal herramienta, ahora que el teletrabajo y las clases de escuelas, colegios y universidades se realizan desde casa a través del Internet.

Adicional a lo mencionado, también se debe considerar el deterioro de las condiciones económicas en los países, el aumento de los índices de desempleo debido al cierre de muchas empresas y el consecuente descontento social, sumado a un intento de reactivación desordenada de la economía básica, lo que ha sido aprovechado por la delincuencia para actuar en contra de las personas y sus bienes, en los sitios y condiciones en los que esta nueva normalidad lo permite.

Foto: Creativeart - Freepik

DELITOS MÁS COMUNES

Las estafas, el robo a domicilios, los asaltos callejeros, son ejemplos de incidentes que bajo estas circunstancias se están intensificando y en los que debemos poner mucha atención.

Como he mencionado, el uso de la tecnología es una de las principales herramientas que los delincuentes están usando para estafar a través de aplicaciones de chat, redes sociales o llamadas telefónicas. De hecho, existen muchos casos reportados públicamente en los que personas inescrupulosas, usurpando perfiles sociales, han intentado estafar a la gente ofertando participación en negocios muy lucrativos o solicitando ayuda de emergencia por supuestas necesidades apremiantes durante viajes.

Otro tipo de delitos reportados durante este tiempo, tienen que ver con la suplantación de autoridades de control o vendedores, quienes llegan hasta los domicilios fingiendo verificaciones u ofertando servicios o productos, tomando ventaja de la presencia de la gente que se queda en casa.

Los asaltos y robo de vehículos se están focalizando en los exteriores de los sitios a los que obligatoriamente debemos ir, como supermercados, bancos, farmacias, clínicas o también aprovechando el exceso de confianza de la gente cuando deja su vehículo sin las respectivas seguridades.

Otro punto que ha llamado la atención en las últimas semanas, posiblemente a propósito de los altos niveles de ansiedad en la gente por el confinamiento y la presencia del virus, es el aumento de accidentes de tránsito en las ciudades, lo que requiere que conduzcamos siempre a la defensiva.

Para finalizar, dar a conocer que inclusive las medidas de bioseguridad usadas para prevenir el contagio del virus están siendo empleadas por los delincuentes cuando comparten escopolamina en lugar de gel desinfectante o usan la mascarilla estando seguros de que las cámaras de seguridad y sus grabaciones no podrán identificarlos cuando cometan algún delito.

Con todo lo mencionado, la recomendación principal es mantener nuestro nivel de alerta elevado todo el tiempo. Si bien, el foco por el momento es prevenir el contagio del virus, considerar que también estamos expuestos a otro tipo de riesgos a los que debemos poner atención, por nuestra seguridad y la de nuestras familias. ■

Raúl Morán, CPP,
Security Advisor en la empresa Schlumberger Ecuador.

Más sobre el autor:

SÉ PROTAGONISTA DE LA TRANSFORMACIÓN DE TU ENTORNO

Participando en el **RETO DE 21 DÍAS DE LA LEGALIDAD** de Seguridad por México con acciones diarias concretas que traerán resultados impresionantes en tu persona y tus grupos.

Para más detalles contáctanos por alguno de nuestros medios.

EN TEMAS POLÍTICOS Y DE SEGURIDAD NO HAY CASUALIDADES

PERÚ | César Ortiz Anderson

La cifra de víctimas mortales por la pandemia nos coloca en la peor situación a nivel mundial

Foto: Ministerio de Defensa del Perú_WikimediaCommons

Si usted ve a un desconocido varias veces por su cuadra, lo más probable es que lo estén reglando (observando) para cometer algún delito; si se le empiezan a perder cosas en su hogar, atentos a un empleado que trabajen en su domicilio o un pariente con problemas de adicciones, así de simple y claro; lo mismo ocurre en mi opinión, cuando se da a conocer por este gobierno, el número probable de muertos a causa del virus del COVID-19, digo probable, ya que soy un convencido que es mucho mayor.

Tengo que reconocer que el periodista Phillips Butters, a mediados del año pasado advertía mostrando algunos videos que la cifra era mucho mayor, pero la cifra de más de 195 mil decesos (cifra hasta el 28 de julio) nos coloca en el primer lugar del mundo de muertes por millón de habitantes, entonces como no hay casualidades en política, hay un mensaje oculto para el pueblo y en mi opinión no es otro que el que no debemos esperar nada de las élites que nos gobiernan o que manejan las principales instituciones del Estado como Economía, Seguridad o Salud, como el caso de "Vacunagate", protagonizado por el impresentable de Vizcarra, el que inició según mi opinión toda la desgracia que hoy vivimos.

Los peruanos recién en febrero de este año con indignación nos enteramos que el ex presidente Vizcarra y su familia se habían vacunado de manera totalmente irregular, junto a una larga lista de funcionarios de alto nivel, empresarios, periodistas y hasta el Nuncio Apostólico en el Perú, nada menos. Lo cierto es que hasta el día de hoy desconocemos a ciencia cierta quiénes fueron todos los que se vacunaron.

CIFRA EN ASCENSO

Este recuento estadístico de las víctimas mortales por COVID-19 en el Perú que asciende a más de 195 mil personas, el triple de lo que se asumía oficialmente por el gobierno, es un mensaje "harakiri" planificado, según mi análisis por el mismo Vizcarra y su entorno de poder actualmente, incluyendo al gobierno de Sagasti, donde se juega su última carta, ya que sabe perfectamente que de ganar Fuerza Popular acabará juzgado y en prisión, repito esa es mi opinión o elucubración.

Por eso Sagasti sincera la cifra de víctimas mortales por la pandemia, que nos coloca en la peor situación a nivel mundial, con la finalidad de responsabilizar al modelo económico que defiende de Keiko Fujimori y a la Constitución Política de 1993, esperando producir una catarsis reflexiva en las mentes de millones de peruanos que verían en Pedro Castillo el fin a esta desgracia. Aunque al mismo tiempo esto signifique al "harakiri político" de Vizcarra y de Sagasti, los dos presidentes que han gobernado el país desde que se declaró la pandemia. Sacrificio que valdría la pena con tal que Keiko Fujimori pierda la 2ª vuelta.

En ese lapso desde el 7 de junio al 28 de julio la sociedad en su conjunto vivió con incertidumbre y temor, por varios factores siendo el principal el de la pandemia y con muchas urgencias.

Finalmente elegimos un candidato que no está preparado para ser un estadista y vinculado a la extrema izquierda y una candidata envuelta en un proceso judicial, que incertidumbre hay que tanto el Ejecutivo como el Legislativo tendrán serios problemas de legitimidad, ojalá por mi país yo esté equivocado en esta última apreciación. ■

César Ortiz Anderson,
presidente de Aprosec (Asociación Pro Seguridad Ciudadana del Perú).

Más sobre el autor:

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

M360

Para quienes aspiran a un deportivo alemán

Powered by

SEPSISA

RANGER SWAT MÉXICO

Foto: Creativeart - Freepik

TIEMPO DE REINVENTARSE

Muchas inercias de toda índole se rompieron durante 2020 para dar espacio a la formación de nuevos hábitos en 2021

MÉXICO | Jorge Uribe Maza

En el mundo entero, 2021 será recordado como un año parteaguas en muchos sentidos. Tras un encierro voluntario o impuesto que habrá durado más de un año e implicado una toma de conciencia colectiva en cuanto a la dinámica social, económica y laboral que se buscará establecer para las siguientes generaciones, esta pausa habrá permitido una introspección profunda y partir de cero en la concepción de cómo se produce valor en muchos sectores y actividades económicas.

En inglés se usa la expresión *silver lining* para referirse al borde plateado que rodea las nubes grises, cuya belleza acaba opacando lo desolador del cielo lluvioso, analogía de la esperanza o aspecto positivo y enriquecedor que es posible encontrar en cualquier situación negativa. La tragedia sanitaria del COVID-19, con su costo en vidas humanas y desplome económico, tendrá de igual modo aspectos rescatables en cuanto a la huella que perdurará en cambios de lógicas y conductas, tanto a nivel personal, como empresarial e incluso cultural.

NUEVOS HÁBITOS

Para el último trimestre de este año, muchos sectores se habrán reactivado casi por completo, pero pocos recuperarán las mismas condiciones que tuvieron en 2019. En muchos casos, el trabajo en casa perdurará, lo cual será considerado como benéfico tanto para las empresas que se ahorran el costo de contar con oficinas activas sin forzosamente sacrificar productividad, como para los colaboradores que se mantienen más cercanos a sus familias e invertirán menos tiempo y recursos en trayectos, vestimenta o alimentos en la calle.

Las reuniones presenciales de trabajo difícilmente volverán a ser tan frecuentes como antes, con ventajas tanto en administración de la jornada laboral como ambientales. Los eventos masivos se llevarán a cabo bajo nuevas reglas, con menos aglomeraciones y mayor respeto al espacio personal. Al interior de las familias, la dinámica también se habrá transformado, con ajustes en horarios, actividades y, en particular, en el involucramiento de cada miembro en tareas que antes no atendían o incluso ignoraban.

El consumo también habrá evolucionado, menos impulsivo, más razonado y moderado, orientado a las compras en línea con entrega a domicilio. Finalmente, el cuidado de la salud propia y ajena se convirtió en un tema central en las conversaciones y decisiones de vida, incluso en aquellos que solían tratar su cuerpo con mucha negligencia.

Muchas inercias de toda índole se rompieron durante 2020 para dar espacio a la formación de nuevos hábitos en 2021. Se suele decir que el primer paso no te lleva a donde quieres ir, pero te saca de donde estás. Tanto individuos como organizaciones están frente una oportunidad única de reinventarse, puesto que el primer paso se dio solo.

Del algún modo, los principales obstáculos para conseguir cambios sustantivos se redujeron en este nuevo contexto: hubo una ruptura súbita e involuntaria con el modelo anterior, el entorno que prevalecía se esfumó para dar lugar a la creatividad, sin mucho margen de titubeos y resistencia al cambio, todos fuimos requeridos a adaptarnos de forma ágil, aunado a la posibilidad de continuar haciendo ajustes en el mediano plazo.

Las reuniones presenciales de trabajo difícilmente volverán a ser tan frecuentes como antes, con ventajas tanto en administración de la jornada laboral como ambientales

Foto: Creativeart - Freepik

En aras de mantener la moral colectiva en alto, al interior de cada empresa se echó a andar un proceso permanente de monitoreo de la calidad de vida de las personas, su equilibrio emocional, el balance entre la vida familiar y la laboral, la organización de su tiempo entre actividades productivas, recreativas y de desarrollo. De forma paralela a los indicadores de desempeño, se dio una toma de conciencia sobre la importancia de la salud mental, tan relevante como la salud física. El estado anímico de cada persona comenzó a ser observado con detenimiento y responsabilidad.

Si bien del lado de la organización se requiere continuar con el análisis de la pertinencia de las tareas encomendadas a cada colaborador y en qué medida éstas representan un estímulo o una frustración con respecto a sus propias expectativas de desarrollo profesional; del lado del colaborador hay un reto individual relacionado con su motivación y el sentido que le encuentre a las funciones que le son asignadas. El auto cuestionamiento y la auto gobernanza cobran la máxima importancia en el diálogo interior de cada persona, tanto para fijarse metas ambiciosas como para trazar un plan viable para irlas alcanzando.

Este último constituye el reto crucial tanto de la persona como de la empresa: ¿En qué medida cada individuo tendrá la capacidad de aprovechar este efecto hoja en blanco para darle un mayor significado a sus funciones, de manera que se empaten con sus aspiraciones y anhelos? ¿Y hasta qué punto la empresa sabrá fomentar este impulso de cambio en quienes forman parte de ella?

Foto: Creativeart - Freepik

PROPÓSITO DE VIDA

En Grupo IPS estamos conscientes que dedicarse a la seguridad implica lidiar con condiciones adversas. Más aún en un país donde este sector ha sido históricamente vinculado a la corrupción, los abusos y la escasa preparación. Revertir este sentir requiere un esfuerzo amplificado en el sentido opuesto: se espera que todo colaborador actúe, bajo cualquier circunstancia, con integridad plena, respeto y profesionalismo. Cuando estas virtudes se ejercen de forma ardua, quien lo observa se siente inspirado y busca adoptar este modelo como parte de su actitud dentro y fuera del trabajo. Se convierte en un propósito de vida, tan importante como un sueldo justo o un horario laboral conveniente.

Cuando en cada interacción se percibe una combinación de firmeza, confiabilidad y congruencia, en automático se busca incrementar el nivel de responsabilidad de quien a leguas se percibe sabrá asumirlas con rectitud. Esto es básico en el sector de la seguridad privada donde por mucho tiempo se ha observado un círculo vicioso de desmotivación, inestabilidad y deterioro de la función. Es imperativo romper con el modelo donde los elementos hacen un mero acto de presencia y registro básico de accesos u operaciones.

Quien resguarda la vida, libertad e integridad de la comunidad debe estar en posición de tomar decisiones de mayor alcance, de aplicar criterios complejos e incluso de coordinar la respuesta ante eventos críticos. El camino para empoderar a nuestros Técnicos en Seguridad Patrimonial empieza cuestionando todos los factores que hasta ahora han limitado el alcance de su labor y culmina con el compromiso de la organización en quitar trabas a su cargo como garante de una dinámica armoniosa entre la espontaneidad de las personas y la aplicación rigurosa de los procesos establecidos. ■

Jorge Uribe Maza,
director comercial de Grupo IPS México.

Más sobre el autor:

TEST
PARA AUTOEVALUACIÓN EN SEGURIDAD INTEGRAL

Preguntas para las personas que han recibido capacitación

GUATEMALA

Enrique Jiménez Soza

Es importante supervisar las actividades del personal a su cargo, así como el funcionamiento de las instalaciones de seguridad del establecimiento, de acuerdo a los procedimientos establecidos, políticas del establecimiento normas de seguridad y salud ocupacional. Es por ello que la capacitación juega un papel fundamental en la seguridad integral, a continuación le presentamos unas interrogantes para poder evaluar su conocimiento en el tema:

¿Cómo le ha ayudado a usted la capacitación en seguridad integral para su trabajo en seguridad preventiva? _____.

¿Ha aplicado alguno de los conceptos aprendidos en las actividades de su trabajo o departamento dentro de la empresa? _____.

¿Cuál tema en especial aplicó y qué resultados obtuvo? _____
_____.

¿Cuáles son, en su opinión, los ilícitos más frecuentes, que pueden afectar a su departamento en especial? _____.

¿Cómo identificaría el riesgo, dentro de la empresa? _____
_____.

¿Cuáles son los niveles de seguridad preventiva adecuados (código de colores)? ___
_____.

¿Riesgos y eventualidades amenazantes más frecuentes en el área empresarial? ___
_____.

¿Qué opina sobre las técnicas de seguridad y vigilancia? _____
_____.

¿Y de las acciones preventivas preincidente? _____
_____.

En seguridad industrial, ¿cuáles son las lesiones más frecuentes en el trabajo? _____
_____.

PREGUNTAS Y COMENTARIOS

¿Ha tenido la oportunidad de compartir conocimientos adquiridos de seguridad preventiva en grupo o con otros compañeros de trabajo?: Sí:_____ No: _____

¿Le parece adecuado el material aprendido y las capacitaciones realizadas para su capacitación de seguridad?
Sí: _____No: _____

¿Cuál tema de seguridad considera que debería de ser estudiado o ampliado por parte de la empresa capacitadora? _____
_____. ■

Foto: Creativeart - Freepik

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

Más sobre el autor:

EXPO SEGURIDAD MÉXICO

VIDEOVIGILANCIA

DRONES

FUERZAS DEL ORDEN

CIENCIAS FORENSES

02-04 Noviembre 2021

Ciudad de México
Centro Citibanamex

Powered by ISC INTERNATIONAL SECURITY CONFERENCE & EXPO

La mayor exhibición de productos y soluciones de seguridad en América Latina

GPS

CONTROL DE ACCESO

CIBERSEGURIDAD

ALARMAS

¡Te esperamos!

Regístrate en línea antes del 29 DE OCTUBRE para asistir sin costo

www.exposeguridadmexico.com

Patrocinadores Fundadores

WE MONITOR CENTRAL PARA CENTRALES

EQUIPOS DE SEGURIDAD MAGOCAD. Un Servicio de Experiencia ¡Seguro!

SYSCOM

f in SAFETY SHOWS

Built by RX In the business of building businesses

En conjunto con EXPO SEGURIDAD INDUSTRIAL MÉXICO

ACONTECIMIENTOS DE LA INDUSTRIA DE **LA SEGURIDAD PRIVADA**

Fecha:
del 24 al 29 de mayo de 2021.

Lugar:
Lima, Perú.

Asistentes:
más de mil 400 invitados.

"Securitec Perú" se lleva a cabo con éxito por segunda ocasión de manera virtual

La 2ª edición virtual de la Feria "Seguritec Perú", incluyó a asociaciones como: Asociación Pro-Seguridad Ciudadana (APROSEC), Asociación de Serenos del Perú (ADESEP), Red de Seguridad Latinoamérica (REDSEG) y Sociedad Nacional de Protección contra Incendios (SNPCI).

En el evento se presentaron más de 50 empresas expositoras de seguridad física, personal, ciberseguridad, contra incendios, electrónica, EPPS (Equipos de Protección Personal), vigilancia, anti-COVID, protección, serenazgo y comunicaciones. El evento se desarrolló en la plataforma MEGAFIP, en donde los expositores a través de un *stand* virtual presentaron sus productos y servicios.

Thais Corporation S.A.C., organizador de Seguritec Perú, tiene como uno de sus pilares la educación del sector, incrementar el conocimiento técnico, profesional y concientizar a toda la audiencia acerca de la importancia que tiene la seguridad en todas las industrias. ■

Fecha:
26 de mayo de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 60 participantes.

AMESP lleva a cabo el evento "La importancia de AMESP en el mercado de la seguridad: tendencias y oportunidades para empresas alemanas en México"

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) llevó a cabo el evento "La importancia de AMESP en el mercado de la seguridad: tendencias y oportunidades para empresas alemanas en México", en colaboración con Global Business Partners, México S.C. (GBP).

En el evento participaron distintos expertos en seguridad y parte de la junta directiva de AMESP, como el Cap. Salvador López Contreras, presidente; Verónica Torres Landa Castelazo, directora ejecutiva; Gabriel Bernal, vicepresidente; Daniel Espinosa, secretario; Adrián Domínguez, tesorero; y Roberto Rivera, delegado de Relaciones Interinstitucionales. Karina Rubín De la Fuente, *Trade Specialist* en Global Business Partners México, fue el vínculo con la AMESP. Mientras que Franziska Wegerich, gerente *senior* y consultora de AHP International, fue la moderadora de las empresas alemanas del evento. ■

Fecha:
27 de mayo de 2021.

Lugar:
Ciudad de México.

Celebran el **"Tyco Security Show"**

La empresa Tyco realizó el "Tyco Security Show", un evento digital donde presentaron la gran variedad de opciones tecnológicas de seguridad que ofrece dicha firma. Beatriz Helena Álvarez, comunicadora social y periodista colombiana, fue la encargada de presentar el evento; acompañada de Luis Enrique Bonilla, gerente de Desarrollo de Negocios Latinoamérica y el Caribe de Tyco Security Solutions; y Wilson Aguilar, supervisor de Productos, Control de Acceso y Video de la firma, para solucionar dudas de los espectadores.

Beatriz Álvarez presentó el portafolio de Inteligencia Artificial (IA) de Tyco para enfrentar retos actuales y futuros, a través de automatizar procesos, toma decisiones y presentación de reportes, para una gestión de negocios completa. La IA que Tyco ofrece en el control de acceso no sólo garantiza video inteligente, también evita suplantación de personas y detecta posibles amenazas. ■

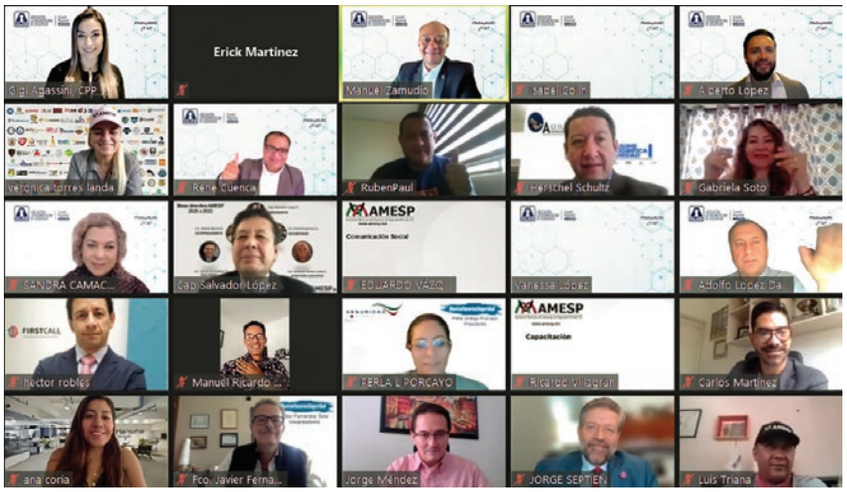
Beatriz Helena Álvarez,
comunicadora social y periodista colombiana

Fecha:
16 de junio de 2021.

Lugar:
Ciudad de México.

Asistentes:
90 invitados.

ALAS y AMESP firman convenio de colaboración



La Asociación Latinoamericana de Seguridad (ALAS) llevó a cabo de manera virtual la firma de convenio de colaboración con la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), ambas asociaciones con el gran compromiso hacia la profesionalización del sector y en apoyo a los socios de ambas asociaciones, adaptándose a las nuevas necesidades del mercado apostando hacia la tecnología como base, así como las regulaciones actuales.

En la mesa de la firma del convenio estuvieron presentes: como testigo de honor, Jorge Septién, presidente de la mesa de Comisión de Enlace con asociaciones de AMESP; el Cap. Salvador López Contreras, presidente de AMESP; José Luis Calderón, presidente de la Comisión de Comunicación de AMESP; Ricardo Pulido, presidente de ALAS Internacional; Gigi Agassini, vicepresidenta consultiva de ALAS Comité Nacional México; y Manuel Zamudio, presidente de ALAS Comité Nacional México. ■

Fecha:
9 de junio de 2021.

Lugar:
Ciudad de México.

Seguridad en América realiza *Roadshow* **"Seguridad en la industria farmacéutica"**

Eduardo Téllez,
Chief Security Officer en Laboratorios LIOMONT

Seguridad en América llevó a cabo el *Roadshow* dedicado a la seguridad en la industria farmacéutica, donde múltiples expertos compartieron información precisa sobre las necesidades de esta industria, estrategias implementadas y las soluciones más innovadoras del mercado. El evento fue presentado y dirigido por Alex Parker, *Sales Manager* de esta casa editorial.

Miguel Ángel Champo, presidente de ASIS Capítulo México, invitó a los asistentes a ser parte de la asociación de seguridad más grande del mundo: ASIS Internacional. Comprometida en la profesionalización a través de distintas comunidades de participación, entre ellas la comunidad de energías limpias que recién se inauguró.

CHARLAS MAGISTRALES

Adrián Álvarez Delgado, *Dir. Supply Chain Security* de MSD Pharmaceuticals, dictó su conferencia titulada "La importancia de la profesionalización del ejecutivo de seguridad después de tiempos de COVID-19", en la que habló acerca de cómo la situación de la pandemia ha afectado en diferentes ámbitos al ser humano y la sociedad mundial. "A pesar del cercano regreso a las actividades presenciales, ya nada será igual", enfatizó.

También participó Eduardo Téllez, *Chief Security Officer* en Laboratorios LIOMONT, con la ponencia titulada "Seguridad paralela a productos estratégicos y no estratégicos", enfocada en identificar los activos estratégicos para la operación de la industria. Los recursos con los que se cuenta para la operación: a) agua potable, b) drenaje, c) electricidad y d) sistema de gas.

PATROCINADORES

Alejandro Espinosa, *PACS Director of Sales* en LAM *North* de HID Global, participó con la ponencia "Sistemas de control de acceso: ¿Seguridad de por vida?", en la que explicó la evolución de la credencial en el mercado, a través de la seguridad y funcionalidad.

Espinosa recomendó como prácticas de actualización: hacer un inventario completo de las tecnologías existentes, brindar soporte a menor cantidad posible de tecnologías preexistentes, elegir nuevas soluciones compatibles con acceso móvil, empezar a pequeña escala, involucrar a otras aéreas para dividir presupuestos y evaluar soluciones que se ofrecen como servicio y no como producto.

Posteriormente participó Martín Yánez, *Sales Manager* para Latinoamérica de la empresa Nedap, con su ponencia "Cómo impacta el control de vehículos en la industria farmacéutica", en la que habló acerca del portafolio de soluciones que ofrecen al mercado, como fabricantes de lectoras y periféricos, que a su vez están divididos en cuatro familias, cada una con *tags* valiosos enfocados a las diferentes necesidades.

Martín agregó que Nedap ha ido evolucionando en el concepto de control de vehículos, entendiendo que no se queda sólo en el acceso de vehículos a una planta, sino que es necesario saber el paso de vehículos y cómo se mueve dentro de la industria: el pesaje, los montacargas, despacho, los accesos y el tiempo de carga. ■

Adrián Álvarez Delgado,
Dir. Supply Chain Security de MSD Pharmaceuticals

ASIS INTERNATIONAL™
CAPÍTULO MÉXICO 217

MEMBRESÍA

ÚNETE A LA RED DE PROFESIONALES DE SEGURIDAD MÁS GRANDE DEL MUNDO

ASIS Capítulo México
$5,650 pesos netos

ASIS Internacional
$100 UDS

Tu membresía anual te brinda:

- Oportunidades de networking inigualables en eventos locales, regionales y globales, como GSX de ASIS Internacional.
- Acceso a "ASIS Connects", nuestra exclusiva comunidad en línea para establecer contactos, colaborar y encontrar soluciones comerciales.
- Recibe noticias galardonadas, tendencias y artículos destacados de Security Management, la revista mensual de ASIS.
- Obtén grandes ahorros en educación dirigida por expertos, incluidos seminarios web, conferencias globales, desarrollo ejecutivo y más.
- Conoce nuestras certificaciones profesionales reconocidas a nivel mundial que validan tu competencia en la industria de la gestión de la seguridad.
- Acceso digital gratuito a todos los estándares y pautas de ASIS.

No esperes más, escríbenos a socios@asis.org.mx o visítanos en nuestra webpage o redes sociales para encontrar los pasos para afiliarte.

#ASISLoConstruimosTOD@S

Fecha:
16 de junio de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 70 participantes.

STid realiza *webinar* sobre credenciales virtuales

La empresa STid, representada por Susana Gallegos, *Business Development Director* de STid, junto con **Seguridad en América** (**SEA**) llevaron a cabo el *webinar* "Conoce STid Mobile ID: credenciales virtuales, manos libres, seguras y masivas con opciones gratuitas". El evento fue presentado por Alex Parker, *Sales Manager* de **SEA**.

STid es una empresa de origen francés, con trayectoria de más de 25 años en el mercado enfocada a dos ramas de la seguridad, control de acceso intuitivo y trazabilidad segura, RFID e *Internet of Things* (IoT). En este *webinar* se enfocó al primero de ellos.

El posicionamiento como diseñador y fabricante es proveer de soluciones integradas de *software*, *hardware* y servicios para control de acceso, distribuidores y consultores de equipos de seguridad. "Nuestra misión es proteger los activos estratégicos de su organización", mencionó Susana Gallegos. ■

Susana Gallegos,
Business Development Director de STid

Fecha:
23 de junio de 2021.

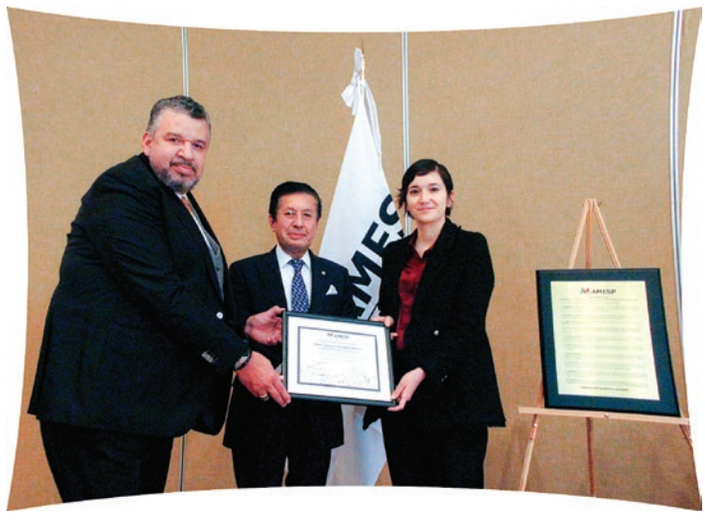
Lugar:
Hacienda de Los Morales, Ciudad de México.

Asistentes:
75 invitados.

AMESP realiza Asamblea General Ordinaria

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP) a través de su Mesa Directiva y Dirección Ejecutiva, llevaron a cabo la Asamblea General Ordinaria de manera virtual y presencial, con todas las medidas de protección sanitaria, uno de los requisitos obligatorios para asistir al evento fue presentar un comprobante de vacunación contra el SARS-CoV-2. La empresa Human Center, socia de la AMESP, ofreció el servicio de prueba rápida (prueba de antígeno) a quienes no contaran aún con vacuna, para tener acceso a la asamblea.

El evento lo inauguró Marcela Figueroa Franco, subsecretaria de Desarrollo Institucional de la Secretaría de la Seguridad Ciudadana (SSC) de la Ciudad de México, quien en nombre del titular de la SSC, Omar García Harfuch, agradeció a los asistentes. Estuvieron presentes el presidente de AMESP, Cap. Salvador López Contreras; Gabriel Bernal, vicepresidente de AMESP; la directora ejecutiva de AMESP, Verónica Torres Landa; y el invitado de honor: Carlos Romero Aranda, Procurador Fiscal de la Federación. ■



Gabriel Bernal, vicepresidente de AMESP; **Cap. Salvador López Contreras,** presidente de AMESP; y **Marcela Figueroa Franco,** subsecretaria de Desarrollo Institucional de la Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México

SEGURITEC PERU

3RA. FERIA VIRTUAL DE SEGURIDAD

Octubre 25 - 30 2021

Venta de Equipos y Suministros para Seguridad


FÍSICA


INCENDIO


PERSONAL


VIAL


RESCATE


POLICÍA

¡Separe su Stand hoy!

www.megafip.pe/seguritec

Informes:

THAIS CORPORATION

gdelatorre@thaiscorp.com

+51 982-508-607

+51 987-421-834

MegaFip
Mega Feria Internacional del Perú

Oficializ ación:

Centro de Exposiciones Jockey

Prensa Asociada:

Fecha:
22, 23 y 24 de junio de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 400 invitados.

Seguridad en América realiza *Roadshow* **"Seguridad en bancos"**

Seguridad en América (SEA) realizó el *Roadshow* "Seguridad en bancos" de forma virtual. El primer ponente fue Miguel Ángel Champo, presidente de ASIS Capítulo México, quien invitó a los asistentes a formar parte de la asociación.

DÍA 1

Fernando Gómez, director de Seguridad en Compartamos Banco; y Hugo Montes, director de Seguridad y Prevención en CIBanco, dictaron la ponencia "Modelo integral de seguridad corporativa ante la transformación digital". Posteriormente Antelmo Cuellar, gerente nacional de Seguridad Patrimonial en Bancoppel, con su conferencia "Localizacion satelital en la banca".

Diego De la Torre, gerente ejecutivo de Seguridad en BANBAJIO, habló sobre los "Fraudes con cheques", en la que comentó cómo evitar este tipo de fraudes y lo que están haciendo los expertos para disminuir los delitos. Después César Santillán García, *Presales Manager* de la empresa SISSA, dictó la ponencia "Las 4 soluciones de seguridad imprescindibles en instituciones bancarias".

Alejandro Espinosa, encargado del área de Control de Acceso Físico en HID Global, participó con el tema "Sistemas de control de acceso, ¿seguridad de por vida?". Por último Marcos Avalos, *Country Manager* de SoftGuard, con su ponencia "La transformación de la seguridad bancaria".

DÍA 2

Javier Hernández, director de Continuidad de Negocio y Seguridad Física para Latinoamérica en Grupo Financiero Banorte, dictó su ponencia "Capability Maturity Model for Security Risk". Así como Luis Meza, director regional de Proyectos de Seguridad en Citibanamex, quien mencionó que la usurpación y robo de identidad, es la apropiación de la identidad de la persona y asumirse frente a otras personas, el objetivo es acceder a recursos o información a nombre del titular. También participó Pedro Villanueva, director de Seguridad en INBURSA, el cual señaló que en México el robo de identidad ocupa el número ocho en materia de legislación.

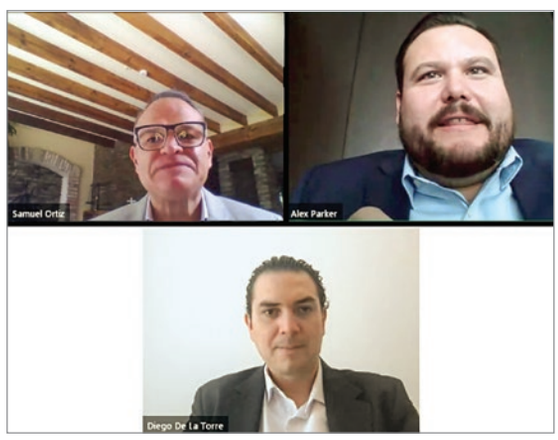
Más adelante participó Jorge Uribe, director comercial de IPS, con su plática "Medidas para reforzar la seguridad en instituciones bancarias"; y Juan Castro, *Manager* México en la empresa VIVOTEK, con su ponencia compartida con Virginia Encinas, gerente de Ventas en Monterrey de ADISES, titulada "*Smart and Secure*: soluciones de videovigilancia de alta tecnología para sector bancario y financiero".

DÍA 3

Manuel Ferrer, gerente de Seguridad de Actinver Banco; y Víctor Durán, director de Seguridad de la misma empresa, participaron con la conferencia "Alarmas en sucursales". Para continuar con Epigmenio Treto, subdirector de Infraestructura Crítica y Tecnología en Banorte, quien comentó que debe existir una coordinación y relación con altos mandos, de los diferentes niveles gobierno y autoridades.

Ciro Ortiz, director de Seguridad en SEPROBAN, habló acerca de la colaboración y coordinación con las autoridades, y en el papel que desarrolla la empresa, esto ha logrado el generar convenios de colaboración con los cuerpos de seguridad y procuración de justicia. Carlos Sanroma, director de Seguridad en BBVA, mencionó que en México existe la necesidad de colaboración para combatir cualquier delito, en esa línea se enfrentan una complejidad muy importante.

Alberto Pérez, director comercial de SCATI, con la ponencia "Videovigilancia inteligente", así como Jonathan Sánchez, ingeniero de Soporte en la empresa Carrier, con la conferencia "Lleve la detección de alarmas contra incendios y la seguridad de sus edificios y ocupantes a un nuevo nivel con el sistema EST4 de Edwards". Por último, Pablo Ramírez, *Tech Division Director* de ILSP, participó con la ponencia "Productividad en centros de contacto mediante inteligencia artificial". ■



NUESTROS SERVICIOS

Manned Security: Nuestro personal altamente capacitado brinda seguridad y ayuda en la mitigación de riesgos. Contamos con servicios de:

- Oficiales de Seguridad
- Custodia de mercancías
- Protección ejecutiva
- Monitoristas

Technology: Las soluciones de tecnología comprenden servicios básicos de monitoreo hasta complejos desarrollos de automatización:

- CCTV
- Control de Accesos
- Detección de incendios
- Alarmas

Risk: Brindamos servicios de:

- Consultoría de gestión de riesgos de seguridad
- Planeación y asesoría en manejo de crisis
- Investigaciones y verificación de información
- Pláticas de seguridad
- Evaluación de C-TPAT
- Inspecciones y análisis de seguridad
- Análisis de riesgo
- Entrenamiento de manejo evasivo/defensivo

SÚPER EMPRESAS EXPANSIÓN 2021 TOP companies

ventas@mx.g4s.com | (+52) 55 5337 0400 | www.g4s.mx

Fecha:
23 de junio de 2021.

Lugar:
Club de Banqueros, Ciudad de México.

Asistentes:
200 concurrentes.

Toma protesta nuevo **Consejo Consultivo de NFPA México**

Armando Zúñiga, presidente de COPARMEX CDMX; y **José Arturo Ortega Porcayo,** presidente de NFPA Capítulo México

La NFPA Capítulo México (National Fire Protection Association) llevó a cabo la toma de protesta del nuevo presidente de la asociación: José Arturo Ortega Porcayo, director general de Mak Extinguisher de México, y su mesa directiva para la gestión 2021-2023. El evento fue conducido y moderado por Salvador Gómez Martínez, presidente del Consejo Consultivo de NFPA Capítulo México. Se contó con la presencia de Armando Zúñiga, presidente de COPARMEX CDMX, y presidente de Asociaciones de Seguridad Unidas por México (ASUME); y Eduardo Eguiluz Navarro, presidente saliente, entre otros.

Eurídice Ibarlucea, vicepresidenta de NFPA Capítulo México, se encargó de moderar el panel "Visión 360° de la industria, hablemos de Seguridad Contra Incendio en México", en la que participaron Amet Novillo Suárez, director general de Equinix México; Carlos Arredondo Sánchez, gerente de Ingeniería Suscripción de Daños de AXXA; y Eduardo Téllez, *Chief Security Officer* para Laboratorios Liomont. ■

Fecha:
30 de junio de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 120 participantes.

UL celebra cierre del mes de la prevención contra incendios

David Wroth,
Director of Data Science de UL

Underwriters Laboratories (UL) en colaboración con el Consejo Nacional de Protección Contra Incendios (CONAPCI) y la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI), unieron esfuerzos en el mes de la prevención de incendios y realizaron una serie de conferencias virtuales con el objetivo de compartir datos e información con actores clave del ámbito público, mediático e industrial que componen al ecosistema de protección contra incendios, para fomentar una cultura social sobre este tema.

Los conferencistas invitados fueron: Phil Piqueira, vicepresidente de Estándares Globales de UL; Víctor Espínola, director general de CONAPCI; Mariano Katase del Colegio Mexicano de Profesionales en Gestión de Riegos y Protección Civil; Denice Durrant, *Standards Program Manager* de UL; David Wroth, *Director of Data Science* de UL. El evento fue clausurado por María Iafano, *International Standards Manager* en Canadá, México y Latinoamérica. ■

Fecha:
14 y 15 de julio de 2021.

Lugar:
América Latina (*online*).

Asistentes:
más de 400 personas.

Seguridad en América realiza con éxito la Cumbre Latinoamericana de Seguridad Privada 2021

Patricio Undurraga, presidente de la Asociación de Empresas de Seguridad y Transporte de Valores de Chile (ASEVA); y **Antonio Montero,** gerente general de ASEVA

Seguridad en América (**SEA**) llevó a cabo la "Cumbre Latinoamericana de Seguridad Privada 2021", en la que participaron múltiples expertos de empresas y asociaciones de diferentes partes de la región, donde ofrecieron charlas del papel de la seguridad privada en cada nación, así como las mejores prácticas, innovaciones tecnológicas, regulaciones, entre mucha más información. El evento fue inaugurado y conducido por Samuel Ortiz Coleman, director general de **SEA**, junto con Alex Parker, *Sales Manager* de la misma empresa.

DÍA 1

Representando a México, Armando Zúñiga Salinas, presidente de Agrupaciones de Seguridad Unidas por México (ASUME) y de COPARMEX (Confederación Patronal de la República Mexicana) Ciudad de México, junto con el Cap. Salvador López Contreras, presidente de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), hablaron de "La nueva ruta para la seguridad privada".

Por su parte Eduardo Aberg Cobo, presidente de la Cámara de Empresas de Seguridad de Buenos Aires (CAESBA); y Cintia Saino, gerente de la misma organización, hablaron de "Los desafíos que enfrenta la industria de seguridad privada en Argentina".

En representación de Costa Rica, Johan Vargas Mejías, presidente de Asociación Costarricense de Empresas de Seguridad y Afines (ACES), junto con Albert Lorenete Marenco, vicepresidente; y César Tapia, director ejecutivo de la misma organización, con su ponencia titulada "Experiencia de VMA seguridad en la implementación de la norma ISO 18788".

Para finalizar la primera jornada de la Cumbre, por parte de Panamá estuvo Franklin Rafael Chaparro Rojas, presidente de Grupo Serseco, quien habló de la sistematización de la seguridad, la cual definió como: "La interpretación critica de una o varias experiencias que a partir de su ordenamiento y reconstrucción explica la lógica del proceso vivido, los factores que han intervenido y cómo se han relacionado entre sí".

Jhon Jairo Vélez,
director nacional de Gestión Humana en FedeSeguridad

DÍA 2

El segundo día de la Cumbre Latinoamericana de Seguridad Privada inició con la participación del colombiano Jhon Jairo Vélez, director nacional de Gestión Humana en FedeSeguridad, quien presentó su ponencia "El profesional de la seguridad a través de una visión integral", en la que habló acerca de su libro *Cómo ser feliz*.

Por su parte, Patricio Undurraga, presidente de la Asociación de Empresas de Seguridad y Transporte de Valores de Chile (ASEVA); Aldo Vidal, General de Carabineros en retiro y miembro del Comité Técnico de la misma organización; y Antonio Montero gerente general de ASEVA, participaron con la ponencia denominada "Capacitación, el camino de la profesionalización".

Por Perú, César Ortiz Anderson, presidente de la Asociación Pro Seguridad Ciudadana (APROSEC), y colaborador de SEA, centró su ponencia acerca de cómo está situado el mundo antes de la pandemia del SARS-CoV-2, y para ello tomó como ejemplo la pandemia de la gripe española de 1918-1920, cuando en el mundo había tan sólo 1,800 millones de personas, la pandemia del coronavirus ha provocado al menos cuatro millones de muertos en el mundo desde que se apareció la enfermedad en 2019.

Finalmente, el Cap. Rodolfo Muñoz, presidente de la Cámara de Seguridad de Guatemala (CSG), participó con su ponencia titulada "Transformación digital para la competitividad y supervivencia". La Cumbre Latinoamericana de Seguridad Privada cerró con gran éxito esta edición *online*. ■

Fecha:
19 de julio de 2021.

Lugar:
Ciudad de México.

Construyendo seguridad con **ISO 22341 & CPTED**

Se llevó a cabo el curso *online* "Construyendo Seguridad con ISO 22341 & CPTED" a cargo de Eduardo Hernández Ruiz, director en Supply Chain Security Council; y la Dra. Mercedes Escudero Carmona, directora regional LAC de la International CPTED y presidente de CPTED México ICA Chapter.

El evento inició con la Dra. Mercedes hablando acerca de Crime Prevention Trough Enviromental Design (CPTED), que en español se traduce como Prevención del Delito a Través del Diseño Ambiental, el cual la segunda generación incluye cinco principios: vigilancia natural, reforzamiento territorial, control natural de accesos, mantención de espacio público y participación comunitaria, mientras que la tercera generación se aplica para la planificación del barrio, y éstos están alineados con los Objetivos de Desarrollo Sostenible (ODS) de la Organización de la Naciones Unidas (ONU). Por su parte, Eduardo Hernández Ruiz habló sobre el "ISO 22341, Sistema de gestión de riesgos sociourbanos CPTED". ■

Eduardo Hernández Ruiz,
director en Supply Chain Security Council

Fecha:
22 de julio de 2021.

Lugar:
Ciudad de México.

Asistentes:
más de 140 participantes.

Reunión virtual en apoyo a la **Fundación ASIS**

Se llevó a cabo una reunión con motivo de apoyo a la Fundación ASIS, por parte de ASIS Capítulo Bajío *Chapter in Formation* y los Capítulos de la Región 7A. María Teresa Septién, vicepresidenta de Fundación ASIS, habló acerca de las acciones implementadas de la fundación, la cual cuenta con más de 250 apoyos a nivel mundial, ofrecen becas para certificaciones con acuerdos para otras instituciones y actualmente cuentan con tres proyectos de investigación sobre tendencias en seguridad e inteligencia artificial (IA).

Se contó con la participación de Eduardo Lima Gómez, socio fundador de Villasana & Abogados S.C.; Gabriel Escobar González, subdirector de Seguridad en Banco Santander México; Uwe Fischer, director de seguridad para Latinoamérica para The Chemours Company; M.C. Carl-Christian Steger, director general de Techno Alarme; Hans-Dieter Mokross, director de Seguridad Corporativa LATAM de Adidas; Gilberto González, presidente de ASIS Capítulo Puebla-Sureste; Mercedes Escudero Carmona, directora regional LATAM de la International CPTED Association; e Issac Garrido, director general de Protect México. ■

incluye gastos de envío

SUSCRÍBASE HOY MISMO A

Revista **SEGURIDAD EN AMÉRICA**

VERSIÓN IMPRESA

DE ACUERDO AL PAÍS EN QUE RADIQUE SELECCIONE LA OPCIÓN DESEADA. (Marque así X)

	Envío a México	Envío a otros países
Suscripción a la revista por un año (6 ejemplares)	☐ $ 650 MN	☐ $ 270 dólares
Suscripción a la revista por dos años (12 ejemplares)	☐ $ 1,250 MN	☐ $ 530 dólares
Ejemplares atrasados	☐ $ 130 MN	☐ $ 50 dólares
Directorio de Seguridad SEA 2021	☐ $ 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 envío de la revista):

Nombre: _____

Compañía: _____ Cargo: _____

Calle: _____ No. _____ Colonia _____

Delegación _____ C.P. _____

Ciudad / Estado / Provincia / Departamento _____ País _____

Tel: _____ E-mail corporativo: _____

E-mail personal: _____

DATOS DE FACTURACIÓN:

Razón social: _____ RFC: _____

Dirección fiscal: _____

E-mail para envío de factura electrónica: _____

MÉTODO DE PAGO

☐ Transferencia
☐ Depósito
☐ T. de crédito

Para mayor comodidad y rapidez, favor de enviar este formato vía: →

e-mail: telemarketing@seguridadenamerica.com.mx

Cupón válido del 1 de enero al 31 de diciembre de 2021

HID Global amplía su oferta de credenciales de control de acceso físico con MIFARE® DESFire®

HID Global anunció la implementación con más variedad de funciones de la última credencial MIFARE DESFire EV3. "Nuestra credencial basada en la MIFARE DESFire EV3 de NXP ofrece todas las avanzadas funciones de seguridad y privacidad de esta tecnología y las robustece con el potente modelo de protección de datos de identidad de HID", explicó Harm Radstaak, vicepresidente *senior* y director de Soluciones de Control de Acceso Físico de HID Global. "Esta reciente incorporación a nuestro portafolio reafirma el compromiso de HID de expandir continuamente nuestra oferta de credenciales con soluciones que son fáciles de personalizar, implementar y mantener. Ayuda a las organizaciones a optimizar aún más la seguridad a través de un entorno de desarrollo sencillo que admite múltiples medios físicos y protocolos de comunicación", señaló. ■

Milestone Systems promueve a Barry Norton como vicepresidente de Investigación

Milestone Systems ascendió al Dr. Barry Norton a vicepresidente de Investigación. En este nuevo papel, además de que continuará liderando el creciente departamento de Investigación de Milestone, será responsable de una mayor colaboración con las universidades. Esto ayudará a avanzar en el aprendizaje automático (*machine learning*), especialmente en relación con la visión por computadora. El Dr. Barry será fundamental para ayudar a crear la próxima generación de tecnología de *software* de video, que no sólo será innovadora, sino que se utilizará para un mayor bien social. "Milestone Systems tiene grandes ambiciones para el futuro. Necesitamos comprender y predecir tecnologías y megatendencias futuras para ayudar a acelerar el ambicioso viaje de crecimiento de Milestone Systems", afirmó Bjørn Skou Eilertsen, director de Tecnología de la firma. ■

Hanwha Techwin presenta sus nuevas cámaras con Inteligencia Artificial 2MP

Hanwha Techwin expuso cinco nuevas cámaras con Inteligencia Artificial (IA) de dos megapixeles Wisenet Serie P, las cuales están diseñadas para complementar los modelos 4K con IA y también están equipadas con análisis de video basado en *Deep Learning*. Estas cámaras hacen que la amplia funcionalidad de la Inteligencia Artificial sea mucho más accesible que la serie 4K existente. Esto, gracias al precio, así como a la incorporación de la última generación de la tecnología de compresión adicional WiseStream III. Esto aplica a una baja tasa de compresión a los objetos y personas detectados y rastreados por IA, mientras que la alta compresión se aplica al resto del campo de visión. Las cinco cámaras cuentan con iluminadores IR Led para una mejor visualización en escenas de poca luminosidad. ■

Illustra Flex de Tyco se refuerza con ocho cámaras nuevas de **Johnson Controls**

Johnson Controls anunció la introducción de ocho nuevos productos a su popular línea de cámaras Illustra Flex de Tyco. Con procesamiento de imágenes optimizado, mejor desempeño con poca iluminación y protección de arranque seguro contra ciberataques, las nuevas cámaras Illustra Flex Gen3, que cumplen con la Ley de Autorización de Defensa Nacional (NDAA) de Estados Unidos, están diseñadas para ofrecer soluciones con una buena relación costo/beneficio y un alto rendimiento para casi cualquier aplicación de videovigilancia. La Illustra Flex Gen3 puede conectarse a la plataforma OpenBlue de Johnson Controls, un completo paquete de soluciones conectadas que ofrece sostenibilidad, nuevas experiencias saludables para los usuarios y herramientas de protección y seguridad. ■

Hikvision crea la primera solución PTZ de radar todo en uno

Se dice que dos tecnologías son mejores que una, y las soluciones de seguridad que integran capacidades de video y radar son un gran ejemplo de ello. Al combinar ambas tecnologías, se aumenta la seguridad del perímetro con una percepción multidimensional, lo que ayuda a ver y responder a los incidentes con mayor rapidez, una necesidad que compañías de cualquier tamaño tienen. "Para superar estos desafíos y maximizar la protección del perímetro, Hikvision ha creado la primera solución PTZ de radar todo en uno de la industria. Esto combina un sensor de radar Hikvision con una cámara PTZ Hikvision de última generación, y con capacidades *Deep Learning* para identificar amenazas a la seguridad y responder más rápidamente ante cualquier incidente", dijo Camilo Muñoz, *Channel Sales director* en Hikvision México. ■

Axis Communications e **Ingram Micro** se unen para potenciar las soluciones de seguridad electrónica en México

Axis Communications agregó a Ingram Micro a su cartera de distribuidores autorizados. Las empresas anunciaron su unión para los países de Centroamérica, Caribe y Sudamérica; con la integración de México ambas compañías pretenden liderar el mercado de soluciones de video y audio en red a nivel Latinoamérica, además de potenciar un núcleo de solución de seguridad que se materializa en el *software* de gestión de video (VMS) AXIS Camera Station. "Los beneficios para nuestros canales existentes, y los que logremos capitalizar en el inicio y transcurso de esta alianza, no sólo serán a nivel financiero, sino que nuestros socios existentes y nuevos, podrán encontrar un abanico de soluciones de seguridad que les permitirá robustecer su oferta para los clientes", señaló Leopoldo Ruiz, director regional para Axis Communications en Latinoamérica. ■

Genetec obtiene el reconocimiento como el proveedor de *software* de control de acceso de más rápido crecimiento en el mundo

Genetec Inc. fue reconocido una vez más como el proveedor de *software* de control de acceso de más rápido crecimiento en el mundo, esto lo indica el último informe de la organización de investigación Omdia. El informe muestra a Genetec desplazando a los proveedores tradicionales de control de acceso y reclamando la posición número dos a nivel mundial (desde el cuarto puesto en 2019). "Mientras que el mercado mundial de *software* de control de acceso se vio duramente afectado por la pandemia y disminuyó en 2020, Genetec creció más de un 30% a nivel mundial, ganando terreno en la región de las Américas y convirtiéndose en uno de los 10 principales proveedores en EMEA", dijo Bryan Montany, analista de seguridad física de Omdia. ■

Bolide Technology Group se expande a nivel mundial en Estados Unidos, Colombia y México

Bolide Technology Group se expandió a nivel mundial con oficinas en Estados Unidos, Colombia y recientemente en México, quiere facilitar el acceso de sus equipos certificados con ISO y NDAA (National Defense Authorization Act), que garantizan su seguridad y excelente funcionamiento *in situ* a más lugares de Latinoamérica, por eso llegan a formar parte del equipo de Bolide dos expertos comerciales que impulsarán aún más la marca en dos nuevos países: José Vidal para Perú y Bolivia —Ingeniero Electrónico con Maestría en Electrónica y Telecomunicaciones—; y Alejandro Romero para América Central, con amplia experiencia en el área de Seguridad Electrónica, gerente de Proyectos de Sistemas de Seguridad. ■

SEGURIDAD EN EL RETORNO LABORAL

Conforme avanza el proceso de vacunación, los semáforos de riesgo epidemiológico en los diferentes lugares van cambiando de forma progresiva de naranja a verde, por lo que las empresas se deben preparar para un retorno laboral seguro y la aplicación de las medidas de bioseguridad que impidan en lo posible contagios por COVID-19. Es por ello que **Seguridad en América** (**SEA**), describe con información de la Organización Internacional del Trabajo (OIT) los 10 pasos para que #NoContagiemosAlEmpleo.

NO PIENSE "A MÍ NUNCA ME VA A PASAR"

1. **Establecer un equipo bipartito para organizar el retorno al trabajo.** Reunir al Comité de Seguridad y Salud o en su defecto crearlo, para capacitar al personal sobre los lineamientos de seguridad sanitaria.

2. **Decidir quién regresa y cuándo.** Se debe garantizar que antes de reactivar las actividades, las medidas de prevención y control sean aplicadas, así como informar previamente al personal sobre éstas.

3. **Adoptar las medidas de ingeniería y organizacionales.** Promover, en la medida de lo posible, el trabajo a distancia y el *home office*. Revisar los espacios de trabajo a fin de reducir el contacto entre las personas.

4. **Adoptar medidas de limpieza y desinfección de locales en forma regular.** Proceder a una limpieza y desinfección minuciosa de las instalaciones antes del retorno a los lugares de trabajo.

5. **Promover medidas de higiene personal.** Proporcionar a los trabajadores el material necesario para el lavado de manos y la desinfección de éstas y su área de trabajo.

6. **Proveer equipos de protección personal y velar por su uso efectivo.** Identificar el equipo de protección personal apropiado relacionado con las tareas y la seguridad que enfrentan los trabajadores.

7. **Vigilar la salud de los empleados.** Monitorear de forma constante su salud, tomar temperatura en la entrada y no tolerar la discriminación en caso de contagio.

8. **Considerar los factores de riesgo psicosocial.** El retorno laboral puede representar un riesgo para la salud emocional de las personas; se debe ofrecer asesoramiento psicológico en caso necesario.

9. **Revisar y actualizar los planes de emergencia y evacuación.** Hay riesgos que seguirán vigentes además de los contagios de COVID-19, como un terremoto, incendio, asalto, etc.

10. **Monitorear y actualizar las medidas de prevención y control.** Revisar las medidas de prevención y control implementadas para determinar si han sido adecuadas. ■

FOMENTE LA CULTURA DE LA SEGURIDAD
Consulte la revista digital en
www.seguridadenamerica.com.mx y envíe los tips a sus amistades y/o empleados.

SEGURIDAD EN AMÉRICA

ÍNDICE DE ANUNCIANTES

EN NUESTRO TRABAJO ESTÁ
SU SEGURIDAD

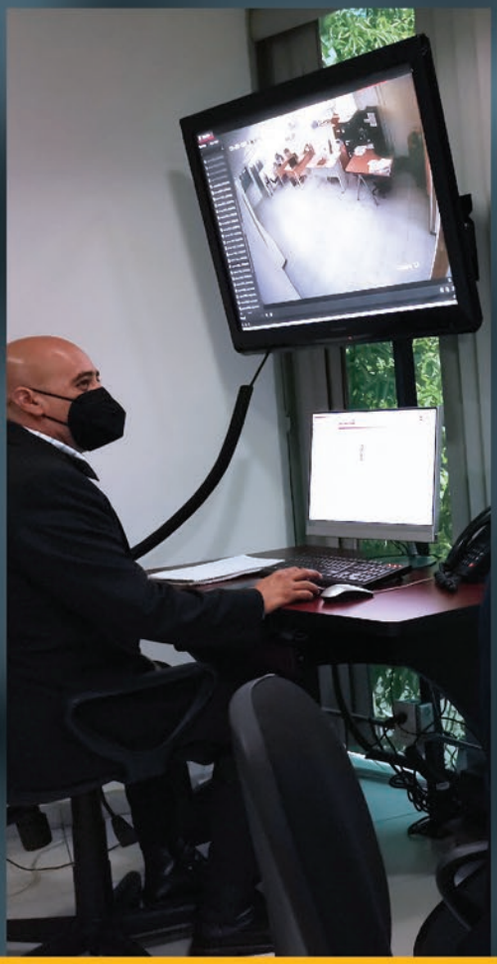
TECNOLOGÍA Y SEGURIDAD, UNIDOS
PARA BRINDARLE EL MEJOR SERVICIO

GSI
GRUPO SEGURIDAD INTEGRAL

impactoTOTAL

NUESTROS SERVICIOS

- Patrullaje y reacción con motocicleta
- Rastreo y localización
- Vigilancia Aeroportuaria
- Custodia de mercancía y bienes
- Oficiales intramuros y patrullas
- Videovigilancia y controles de acceso



ESR EMPRESA SOCIALMENTE RESPONSABLE

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

ASIS INTERNATIONAL

DNV·GL

COPARMEX

Atención a clientes 01 800 461 0457 www.impactototal.mx

"SEPSISA se ha transformado en SER grande"

Facility Services

Grupo

SEPSISA®

SEGURIDAD PRIVADA

El camino a la excelencia comienza por la seguridad.

- Guardias
- Comercializadora
- Limpieza
- Consultoría
- Custodia
- Seguridad Electrónica
- GPS / Monitoreo

17 YEARS ANNIVERSARY

EMPRESA SOCIALMENTE RESPONSABLE

ISO 9001:2015 COMPANY

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

CNSP CONSEJO NACIONAL DE SEGURIDAD PRIVADA A.C.

ASIS

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

BASC

COPARMEX®

CDMX, Estado de México, Monterrey, Guadalajara, San Luis Potosí, Aguascalientes, Hermosillo, Querétaro, Guanajuato, Pachuca, Puebla, Cuernavaca, Acapulco, Veracruz, Villahermosa, Mérida, Cancún, Mexicali, Chihuahua, Tijuana, Ensenada.

www.sepsisa.com.mx ventas@sepsisa.com.mx 5662 6039