Revista

MÁS SEGURIDAD

Abril 2020 / Año 12 / No. 106

www.revistamasseguridad.com.mx

México y Latam / Precio $50.00 MX

Editorial m/s

Feria Internacional

SEGURITEC PERU

Seguridad Física, Personal, Vial, Incendio, Rescate & Policía

Octubre 21 - 23 - 2020
Lima - Perú

Sede:
Centro de Exposiciones Jockey

¡Reserve su Stand Hoy!

www.thaiscorp.com

3 Días - 2 Noches

EXCURSION A:

Machu Picchu

Octubre 24 - 26
2020

Organiza: THAIS CORPORATION - Tel.: (511) 201-7820 - Email: thais@thaiscorp.com

Oficialización:
Perú · Perú · Perú · Perú

Prensa Asociada:
Negocios de Seguridad Argentina · El Guía de Materiales Perú · CONSTRUART Perú · Revista MAS SEGURIDAD México · Revista Industria al día Perú · Actualidad Marítima y Portuaria España

Informes:

INDIA:
Amet Expositions
Tel: +91-9810595236
Mr. Sk Paul - Founder
skpaul@ametexpositions.com

ITALIA:
Guidi Consulting snc
Tel: +39 051 6415376
Mr. Giorgio Guidi
g.guidi@guidimarketing.it

TURQUIA:
Amiral Fair
Tel: 90-533-5435789
Erhan Ersever
info@amiralfair.com

Revista
MÁS SEGURIDAD

HUMBERTO MEJÍA HERNÁNDEZ, / DSE, CPSI
DIRECCIÓN GENERAL
humberto@revistamasseguridad.com.mx

MARÍA ANTONIETA JUÁREZ CARREÑO
DIRECCIÓN COMERCIAL Y RELACIONES PÚBLICAS
marieclaire@revistamasseguridad.com.mx

BLANCA L. ARGUETA PALACIOS
COORDINACIÓN GENERAL
diseno@revistamasseguridad.com.mx

ROSA MARÍA SALAS ASCENCIÓN
COORDINACIÓN EDITORIAL
edicion@revistamasseguridad.com.mx

DANIEL ACOSTA MORALES
fotoyvideo@revistamasseguridad.com.mx

GENARO JUÁREZ
informacion@revistamasseguridad.com.mx
INFORMACIÓN

ARTURO GARCÍA "EL PROFE"
COLUMNISTA

NANCY LARA
VIOLETA ARELLANO
CARMEN CHAMORRO
ANTONIO CELSO RIBEIRO
GUSTAVO GUZMÁN
LUIS GONZÁLEZ NOGALES
LARRY WILSON
ARTICULISTAS INVITADOS

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@revistamasseguridad.com.mx

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

CONTACTO:
Tel/Fax: (52) 55 5527-2279 / 2873-2719
WhatsApp: (+52) 551894-7067
asistencia@revistamasseguridad.com.mx
atencion@mhcorporativo.com.mx

SÍGUENOS EN:
Revista Más Seguridad
@revmasseguridad
revistamasseguridad
revmasseguridad
Revista Más Seguridad

Revista Más Seguridad Año 12, No. 106, Abril 2020 Publicación mensual de MH Corporativo e Imagen Integral, S. de R.L. de C.V., con domicilio en Poniente 62, número 3710, oficina 5, colonia Obrero Popular, Alcadía Azcapotzalco, C.P. 02840, Ciudad de México, Tel/Fax: 5527-2279 / 2873-2719. **Editor responsable: Humberto Mejía Hernández.** Certificado de Reserva 04-2019-080710531500-02 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No.11483 y Certificado de Licitud de Título No.13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: **Grupo Mejía Impresores**, calle La Poza No.72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel. (55) 2166-3555.

Publicación de:

Fortalecido sector transporte vs COVID-19

Los efectos del coronavirus COVID-19 en México se han dejado sentir en todas las industrias. El transporte de mercancías, uno de los sectores clave dentro de la economía nacional, se ha visto impactado por diversos frentes y los expertos prevén afectaciones importantes con esta contingencia mundial.

Por un lado, ante las medidas de seguridad y prevención de contagio emitidas por el gobierno federal, las empresas transportistas, proveedores de tecnología y usuarios, se han visto en la necesidad de disminuir sus operaciones, algunas incluso hasta en más del 50%, o trabajar en horarios especiales.

Pero por otro lado, ante la psicosis generada entre la población por la errónea idea de un posible desabasto de productos, se prevé un incremento de los índices delictivos y atracos específicamente a camiones de carga.

De acuerdo con datos de la Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV), pese a que el robo a transporte de carga mostró de agosto de 2019 a marzo de este año una tendencia positiva a la baja, los proveedores de seguridad para esta industria pronosticaron un incremento en el ilícito.

Esta asociación vaticinó que como resultado de la pandemia, la delincuencia organizada robaría cargas de alimentos y productos de primera necesidad, principalmente en los meses de abril y mayo.

Sobre esto, el presidente de ANERPV, Víctor Manuel Presichi Amador, consideró que los atracos a los automotores de carga provocarían incrementos en los precios de productos, y además un aumento en el robo de mercancías de hasta un 50%.

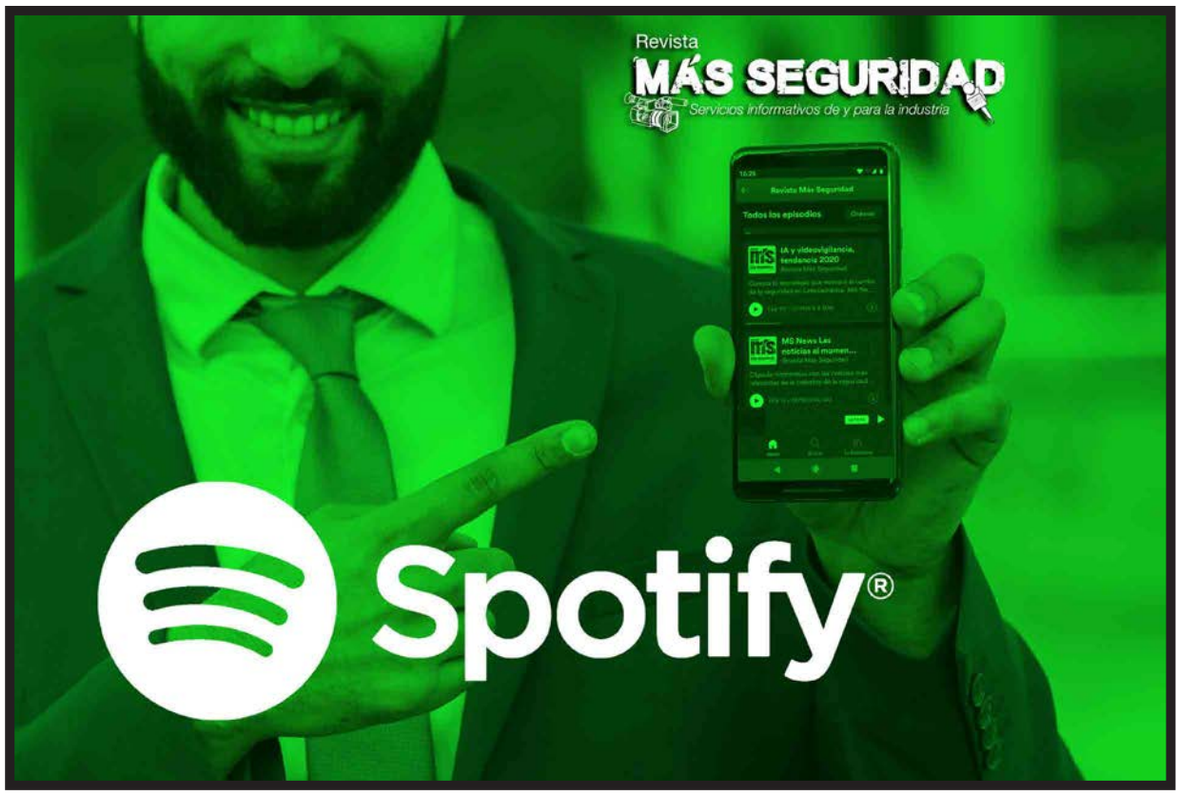
Frente a este panorama, las sinergias entre las asociaciones de transporte, así como las empresas, organismos de seguridad privada y autoridades en sus tres niveles de gobierno, han sido decisivas para fortalecer al sector.

La aplicación de protocolos de contención, reacción y recuperación de mercancías robadas en tránsito, son algunas de las acciones inmediatas que se han puesto en marcha para reducir los efectos negativos. Aunado a eso, el correcto uso de sistemas de rastreo satelital, la denuncia y la colaboración de las autoridades también han jugado un importante papel para la recuperación de unidades robadas.

Por parte de Agrupaciones de Seguridad Unidas por un México Estable (ASUME), el mensaje ha sido enérgico: mantendrán el resguardo de las empresas y sectores clave, y continuarán más unidos que nunca con los principales organismos de la industria y con las autoridades gubernamentales con el objetivo de preservar la seguridad del país.

Vienen tiempos todavía más difíciles para todos, incluidos los medios de comunicación especializados en la industria de seguridad y del transporte. Sin embargo, el fortalecimiento al interior y exterior de las compañías, con la unión de empleados y las sinergias entre los organismos públicos y privados, serán una buena dosis contra este virus. mís

Escucha la cápsula informativa
Las Noticias al Momento



Los Profesionales de LATAM

América Latina se caracteriza por ser una región donde la protección de los activos de las organizaciones, requiere de profesionales con características muy particulares.

Los procesos están liderados por individuos con una sólida formación académica, un claro concepto de valores integros de la sociedad, actitud positiva y orientada al logro de los objetivos, más su vasta experiencia profesional.

Más Seguridad hace un reconocimiento a los líderes de LATAM que se destacan por sus éxitos y trayectoria en el gremio de la protección.

Humberto Rodrigo Santibañez Claros / Chile

Es licenciado en Seguridad y Defensa; titulado de Investigador Policial (PDI); profesional de Protección Certificado (CPP); especialista en delitos económicos. Cuenta con diplomados en seguridad integral de empresas, alta dirección de seguridad, protección informática y física. Además, es consultor en protección corporativa, manejo de crisis e investigaciones internas, diseño e integración de sistemas de seguridad física.

Es ex oficial de la Policía de Investigaciones de Chile. Desde hace 15 años, completó en este país y en el extranjero, diversos cursos y diplomados que le permiten brindar servicios especializados a través de su empresa.

Se ha desempeñado como capacitador y ha dictado charlas en la nación chilena y en el extranjero, principalmente como líder voluntario de ASIS Internacional. Desde el 2005 a la fecha, se ha desempeñado como gerente general de BESAFE Consultores, compañía dedicada a la prestación de servicios de seguridad integral, recursos humanos, sistemas de videovigilancia, salas de operación vía remota, investigaciones y asesorías, consultorías e investigaciones a nivel nacional e internacional. mS

@MatadorMejia Humberto Mejía / DSE, CPSI

El virus que cambió al mundo

Calles semi vacías, comercios cerrados, oficinas sin empleados, escuelas sin alumnos ni profesores, parques sin niños, supermercados abarrotados por "compras de pánico", actividades financieras paralizadas, noticias falsas y reales saturan las redes sociales, mientras los medios de comunicación tradicionales han sido rebasados; por su parte, el gobierno federal sigue ausente y acatando las indicaciones de su Presidente que vive en otra realidad.

¡La llegada del COVID-19 cambió el rumbo del mundo!

México tuvo la oportunidad de anticiparse a los lamentables hechos que ahora conocemos y afectan a todas las actividades de este de por sí ya maltrecho país, pero simplemente las autoridades que para nosotros trabajan, decidieron esperar. Miles de millones de pesos se han perdido, mientras que miles de empleos lamentablemente se perfilan hacia el abismo. En tanto, el enemigo microscópico siguió su nefasto curso. Nuestro escenario se asemeja a una trágica película de ciencia ficción.

Las primeras acciones preventivas fueron propuestas por la iniciativa privada. En el sector de la seguridad privada de inmediato circularon recomendaciones de precaución, se empezó a aplicar el home office y las asociaciones del gremio (ANERPV, ASUME, AMESP, UNESPA, Seguridad por México, entre otras), se coordinaron con autoridades y aplicaron sus propios protocolos ante la emergencia en beneficio de sus clientes, empleados y población en general. Demostraron la importancia de la continuidad de negocio.

En contraparte, el Jefe del Ejecutivo minimizó riesgos, contravino a las indicaciones de la Secretaría de Salud, incluso descartó algún estímulo para las empresa sumidas y afectadas por la pandemia ¿Necedad, arrogancia o ignorancia? Mientras muchos ciudadanos se fueron de vacaciones.

La crisis provocada por el COVID-19 dejó al descubierto el desconocimiento y descoordinación de las autoridades federales con las estatales ante una emergencia mundial de la que no somos ajenos. Lamentablemente al gobierno de la República se le hizo realidad la parábola de "Pedro y el lobo". Cuando la pandemia tocó suelo mexicano no supo ni por dónde, ni qué hacer ¡La 4T no sabe gobernar!

Como sociedad estamos pagando caro que haya llegado al poder una persona que lejos de ser un estadista ante su pueblo y el mundo en medio de una pandemia, que proponga acciones que cuiden, alienten, muevan o unifiquen a la sociedad en acciones beneficiosas, exhiba sus estampitas religiosas como alternativa de protección. Afuera empezaron los saqueos.

Sin duda México está "quebrado" en muchos aspectos: altos índices delictivos, violencia extrema, corrupción, cero crecimiento económico, sector salud colapsado, recesión económica mundial, baja en el precio del petróleo y alza en el dólar; luego llega la pandemia, detiene casi todo y lo único que ocurre es que somos el centro de burlas y críticas del planeta, gracias a nuestro gobierno.

El número de contagiados y sospechosos es incierto si se toma en cuenta que no hay suficientes pruebas médicas aplicadas. En México, la "cifra negra" siempre está presente, aunado a la desinformación y/o manipulación del gobierno. Muchos ciudadanos tenemos "otros datos". El problema de seguridad nacional está ahí.

Sólo por sentido común y responsabilidad apliquemos el #MeQuedoenCasa y #CuidoalosMíos … más

Gracias y nos leemos pronto, pero ¡Fuera de Grabación!

Valor agregado de las herramientas tecnológicas en las cadenas de suministros

En México a partir del año 2008 con las reformas al sistema penal, se han implementado cambios importantes en lo relacionado a la persecución, investigación y procesamiento de probables responsables como participantes en hechos delictivos.

Dentro de las cadenas de suministros existen diversos tópicos que se encuentran expuestos y vulnerables, y para que su objetivo se cumpla sin la desviación de recursos o pérdidas en cuantías económicas derivadas de robo hormiga o por exceso de confianza, incluso negligencia por parte del personal operario, se hace necesario implementar el uso de herramientas tecnológicas.

Es por ello, que el uso adecuado de éstas es un excelente auxiliar en materia de prevención, sanción y suspensión de relaciones laborales, sobre todo para aquellos empresarios que son afectados debido a las pérdidas o menoscabo en sus ganancias.

Uno de los rubros más vulnerables dentro de la cadena de suministros se refiere a la logística. He tenido oportunidad de analizar el motivo de las pérdidas o disminución de las ganancias, sobre todo en medianas y pequeñas empresas; y en su mayoría se relacionan por el exceso de confianza al llevar a cabo la contratación de sus empleados.

Los constantes fraudes por permisionarios encargados de los traslados de mercancías se han incrementado. La solución para atacar este punto es la creación y alimentación constante de una base de datos, en la cual las pequeñas empresas puedan someter a escrutinio los datos que refiere el operador, en donde se alimenten los antecedentes laborales y cartas de recomendación; se dejaría de llevar a cabo una validación telefónica que no es confiable. Por otro lado, se disminuiría de manera importante la falsificación de documentos.

Otras de las herramientas aplicadas son las videocámaras que permiten identificar y observar la manera en la cual el operario lleva a cabo sus funciones. Sin embargo, el mayor problema que se encuentra es que no se les da mantenimiento constante o permiten que alguna de éstas se encuentre sin funcionar, lo que afecta a la visión de los supervisores. Por eso, deben de tener un mantenimiento constante.

Otro mecanismo que se utiliza con mayor frecuencia es el geolocalizador, pero se debe tomar en cuenta que actualmente las señales ya pueden ser bloqueadas y es por ello que no hay que confiar totalmente en el uso de una sola herramienta.

Implementar dispositivos tecnológicos debe verse como una inversión que permitirá incrementar las ganancias a las empresas, además de darles un blindaje jurídico cuando exista el riesgo de la comisión de delitos.

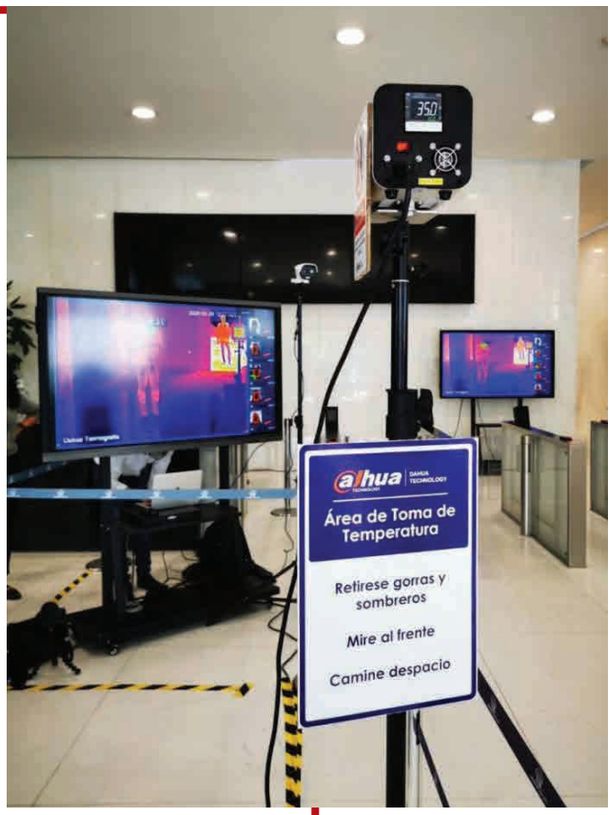
No son un lujo, sino una necesidad y como tal también se debe de saber que no es recomendable apostar por uno solo, sino que hay que crear planes y programas complementarios en el uso de instrumentos tecnológicos de tal forma que impacten de manera positiva en el desempeño de las compañías.

Recordemos que un servicio confiable siempre será recomendado y utilizado de manera constante. Usemos las herramientas como aliadas. Actualicemos, cambiemos, supervisemos constantemente para que cumplan sus funciones; han sido creadas para la obtención de beneficios, así que debemos emplearlas con todo su potencial. mís

*** Nancy Lara**
México

Jefa del Departamento de Investigación en Procuraduría y Administración de Justicia FES Acatlán.
Maestra en Política Criminal. Directora de asesoría y capacitación en CIIS México. Docente en el Diplomado de policías acreditables en la CDMX Coordinadora de Plataforma México en la Coordinación de investigación de campo de la división de investigación de la Policía Federal México.
Asistente del Director General de Secuestros y Extorsiones de Policía Federal México. Productora y conductora programa CIIS através de www.gooradio.com.mx

Contra el COVID-19
cámaras térmicas



En México, Plaza Carso instaló la primera solución de medición térmica de temperatura de Dahua Technology en la entrada a las oficinas corporativas de la Torre II. Ésta es una cámara más un dispositivo denominado Blackbody, que en conjunto conforman un sistema de medición de temperatura de imágenes térmicas humanas de ultra alta precisión, pieza clave para la prevención y control de pandemias como la que se vive a nivel global.

"En este momento México y muchos países de América Latina están viviendo una fase de control epidémico donde es indispensable detectar de manera temprana y con precisión cualquier persona sospechosa de fiebre. Esta es la mejor manera de hacer frente y evitar una propagación masiva que ponga en riesgo la estabilidad del país como ha sucedido en otras partes del mundo", comentó Sánchez Xia, CEO de Dahua Technology México.

Con esto, la empresa fortalece su estrategia de prevención midiendo la temperatura de los visitantes en tiempo real para detectar aquellos con temperatura corporal superior a 37.3 y activar una alarma que permita actuar de manera inmediata. Este parámetro puede ser ajustado de acuerdo a las necesidades particulares de cada cliente o institución sanitaria, de hecho, la cámara térmica, más el Blackbody, garantiza una precisión de ±0.3°C.

Con lentes de 7,5 mm y 13 mm, puede alcanzar una distancia precisa de medición de temperatura de hasta 3 metros, además tiene capacidad para calibrar la temperatura de hasta 80 personas por minuto. Lo que satisface en gran medida las necesidades de despliegue rápido, larga distancia y evaluación precisa de temperatura de multitudes de alta densidad en lugares públicos.

Y en Colombia

La detección de posibles casos del COVID-19 que ingresen a Colombia pueden ser detectados con la tecnología Dahua Thermal Solution, cámaras térmicas de Dahua Techonology, las cuales miden la temperatura corporal de las personas aún si el flujo o el tráfico de individuos es alto.

De acuerdo con Chao Wu, gerente general de Dahua para Colombia, con esta solución se calcula la temperatura de 5 mil personas, en aproximadamente 4.2 horas usando un termómetro de frente, uno de los métodos utilizados por la Organización Mundial de la Salud (OMS). Esta tecnología térmica solo toma 30 minutos, está en la capacidad de registrar la temperatura de tres personas por segundo con una precisión de ± 0.3 ^{0}C

Adicionalmente, este sistema puede detectar si alguien lleva puesta una mascarilla, con una precisión del 99%. También dispone de reconocimiento facial, el cual provee los datos de la persona para su seguimiento y genera alarmas cuando ésta presenta temperaturas anormales.

Dahua Thermal Solution es de rápida implementación y se encuentra funcionando en centros comerciales, bancos, parques empresariales, aeropuertos, ministerios y lugares públicos de alta concentración de personas, en China y en varios países de Asia.

Medición de Temperatura Corporal

- **Alta precisión:** ±0.3°C (con blackbody)
- **Alta eficiencia:** Detección de temperatura sin contacto, detección rápida. Larga distancia, amplia cobertura y detección de múltiples personas
- **Precio bajo:** Mecanismo automático de alerta rápida, ahorrando mano de obra y reducir el riesgo de infección cruzada
- **Adaptabilidad rápida:** Se puede aplicar a escenarios pequeños como entradas y salidas. Y también en escenarios grandes como aeropuertos y estaciones de ferrocarril con personal denso.
- **Información en Tiempo Real:** Realice el seguimiento y análisis histórico de datos, combinando la plataforma

Modelos Recomendados

DH-TPC-BF3221-T

DH-TPC-BF5421-T

ISO 9001:2000

DAHUA TECHNOLOGY MÉXICO
Tel: +52 55 6723 1936
Email: berenice.barron@dahuatech.com
www.dahuasecurity.com/la
@dahuatechnologylatam

Serie Easystar de Uniview

para iluminación baja

Uniview presentó la serie Easystar, un nuevo miembro de la familia de la serie Easy, línea de productos que ofrece un rendimiento extremadamente rentable e imágenes a todo color en condiciones de poca luz.

De acuerdo con la empresa, Easystar IPC adopta el sensor CMOS con iluminación trasera, que mejora la utilización de la luz. El diseño de iris F1.6 mejora radicalmente la capacidad de recolección de luz. Mientras tanto, una lente de alta transmisión reduce significativamente la tasa de atenuación de la luz que pasa a través de la lente. Lo que es más importante, la tecnología patentada de VNU UISP mejora la definición y el brillo de las imágenes.

U-ISP presenta una nueva generación de tecnología de reducción de ruido para mejorar la relación señal-ruido y minimizar el desenfoque. Con una combinación perfecta de hardware y software, los IPC Easystar ofrecen increíbles imágenes coloridas de alta calidad con poca iluminación de 0.002Lux.

La firma dio a conocer su línea de productos básicos de la familia Easy, los cuales cumplen con los requisitos de vigilancia de los usuarios para imágenes de alta calidad con poca luz

Los IPC de la serie Easystar también son excelentes en otras condiciones ambientales. La serie completa de productos admite el nivel de impermeabilidad y protección contra el polvo IP67, que puede satisfacer las necesidades de los entornos al aire libre. Todos aceptan una distancia infrarroja de hasta 50 m, combinada con tecnología de poca luz para ofrecer imágenes de alta calidad durante todo el día. Las resoluciones actuales de la serie Easystar son 4MP y 2MP. Para productos de 4MP, y también admiten 120dB de WDR verdadero.

Según Uniview, los productos Easystar cumplen con los requisitos de vigilancia de los usuarios para imágenes de alta calidad con poca luz, con un rendimiento de alto costo como productos de nivel de entrada con poca luz.

Los IPC Easystar del programa VNU pueden utilizarse en escuelas, plazas, estacionamientos, centros comerciales, aeropuertos, hoteles, hospitales o cualquier escena con poca iluminación en interiores o exteriores.

Johnson Controls presenta

codificador de video HD

Se trata de Tyco HD Encoder para una integración completa de tecnología analógica e IP. El hardware del codificador adapta el video analógico para enviarlo a través de redes IP, lo que permite una migración hacia una videovigilancia IP moderna.

Johnson Controls presentó el codificador Tyco HD Encoder, una solución que permite operar cámaras analógicas de definición estándar (SD) y de alta definición (HD) en una infraestructura IP en desarrollo. Este producto es compatible con exacqVision y VideoEdge de American Dynamics.

Disponible con uno o cuatro canales, Tyco HD Encoder permite que los usuarios de un entorno de red mantengan sus cámaras SD y HD, y sumen con el tiempo cámaras IP, de modo que puedan aprovechar los beneficios de la tecnología IP sin sacrificar su infraestructura analógica existente. El hardware del codificador adapta el video analógico para poder enviarlo a través de redes IP, lo que ayuda a migrar los sistemas de CCTV a una organización de videovigilancia IP moderna.

Este codificador HD puede implementarse de inmediato y admite una conexión de energía por Ethernet, lo que permite transmitir energía y datos a través del mismo cable CAT5/6. También incluye características como salida de HDMI, compresión H.264 para cámaras de hasta 2 MP, transmisión de múltiples flujos y soporte para los protocolos analógicos TVI, CVI y AHD.

Johnson Controls informó que Tyco cuenta con una amplia oferta de grabadoras de video en red y sistemas de gestión de video de American Dynamics y Exacq, lo que combina una base sólida para implementar un sistema de video completamente integrado. Comprar todos los componentes de una solución a un mismo proveedor reduce posibles problemas con la durabilidad de los productos y optimiza las tareas de configuración y soporte.

Sistemas de CCTV
en la cadena de suministro 4.0.

Ante el espectacular ritmo de crecimiento que vive el comercio electrónico, con incrementos del 20% anual, el sector logístico se enfrenta a un proceso de transformación digital sin precedentes donde la conectividad, la inmediatez y la imagen reputacional son claves para ser competitivos.

El concepto de industria 4.0 implica la integración técnica de los sistemas ciberfísicos y el uso de internet en los procesos industriales, hasta conseguir "fábricas inteligentes" gracias a la automatización y la digitalización de la cadena de suministro.

Con millones de envíos diarios, almacenamientos, vehículos, productos y personas implicados, la industria 4.0 requiere de un cambio en la logística, por lo que no se entiende la transformación de una sin la evolución de la otra.

Sin embargo, el logístico es un sector muy maduro con márgenes bajos, cuya única inversión en tecnología está ligada a la reducción de costos. En este escenario, ¿qué ocurre por ejemplo si si se extravía una mercancía y perdemos la confianza de grandes clientes?

El siguiente artículo tiene como objetivo explicar cómo las nuevas tecnologías y, concretamente, la incorporación de la inteligencia artificial en los sistemas de video, hacen posible que tanto empresas industriales como logísticas superen los retos que plantea la Cuarta Revolución Industrial.

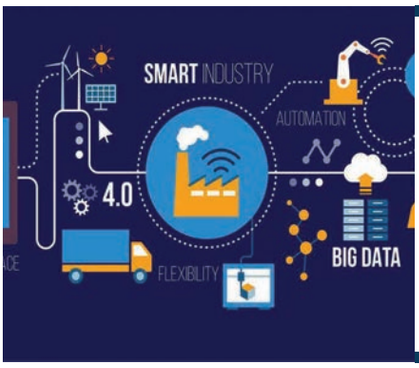
Por ende, invertir en videovigilancia permite que el departamento de seguridad se convierta en un proveedor interno de herramientas de optimización del negocio para mejorar la imagen de marca, enriquecer la experiencia del usuario, la excelencia empresarial y, en definitiva, maximizar los resultados.

Soluciones integrales de seguridad

Como premisa fundamental, la tecnología de videovigilancia debe garantizar la protección integral de la cadena de suministro, incluso en picos de producción fuertes, donde la incorporación de personal temporal se dispara. Por ello, es necesario contar con una solución que garantice la seguridad tanto de instalaciones como de mercancías, y que sea capaz de supervisar los procesos para que la calidad de la producción no se vea afectada.

Gracias a la inteligencia artificial y al big data, la videovigilancia es una pieza clave para superar cualquier desafío de esta nueva era.

Más allá de la seguridad, el CCTV se está convirtiendo en la herramienta esencial para supervisar procesos industriales y/o logísticos, asignar mejor los recursos, garantizar la trazabilidad de los envíos, gestionar y optimizar stocks y, un elemento fundamental en la toma de decisiones de cualquier departamento de la empresa.



La incorporación de la inteligencia artificial en los sistemas de video hace posible que tanto empresas industriales como logísticas superen los retos que plantea la Cuarta Revolución Industrial.

La integración de los sistemas de video con uno de gestión (ERP, SGA, etc.), garantiza la trazabilidad total de los artículos y la resolución total de incidencias con un costo de administración mínimo desde el momento en el que se implementa el procedimiento.

Junto a la captura de imágenes, los sistemas de CCTV recogen y almacenan información asociada a cada mercancía (número de tracking, origen, destino, dimensiones) junto con los instantes de grabación visual del producto.

El acceso rápido y directo al video grabado, asociado a cada mercancía, permite resolver cualquier incidencia en tiempo real, bien a través de la búsqueda de metadatos, o por medio de planos de la propia instalación en cualquiera de los centros distribución, ya que se trata de sistemas multiplataforma.

*Raquel Elías Gutiérrez
*Marketing manager de Scati.

VMS híbrida de Arcules y Milestone Systems

Redacción / @revmasseguridad

Arcules, compañía especializada en servicios integrados de video y control de acceso en la nube, anunció VMS Arcules-XProtect Hybrid™, una solución que combina la videovigilancia como servicio (VSaaS, por sus siglas en inglés) de Arcules con el software de gestión de video (VMS, por sus siglas en inglés) XProtect Corporate de Milestone Systems, que se instala en los servidores del cliente.

El resultado de ambas tecnologías es un sistema híbrido flexible, con múltiples funciones, ideal para organizaciones que buscan centralizar sus operaciones de videovigilancia dispersas.

De acuerdo con las firmas, las organizaciones que requieren tanto la flexibilidad de la VSaaS como la funcionalidad del VMS instalado en sus propios servidores, se beneficiarán con la solución híbrida de VMS Arcules-XProtect, cuyo desempeño está cimentado en una infraestructura y seguridad pensada para el entorno empresarial.

Esta solución combina la videovigilancia como servicio (VSaaS) con el software de gestión de video, y es ideal para organizaciones que buscan centralizar sus operaciones dispersas.

"La solución de VMS Arcules-XProtect Hybrid™ permite a los clientes de Milestone XProtect realizar implementaciones en ubicaciones remotas, de forma rápida y con un mínimo de recursos informáticos y tiempo de interrupción, al tiempo que aprovechan las potentes prestaciones del VMS XProtect, instalado en sus propios servidores. Además, la intuitiva plataforma de Arcules proporciona a las cámaras y a los sitios conectados a la VSaaS de Arcules una infraestructura de base en la nube con ventajas como compatibilidad entre sitios, baja latencia de video, cifrado de datos, redundancia, mantenimiento optimizado con actualizaciones automáticas y fácil incorporación en el sistema", señalaron las compañías.

Bjørn Skou Eilertsen, director de tecnología de Milestone Systems, señaló que los distribuidores y los usuarios finales de Milestone preparan su implementación para aprovechar las numerosas ventajas de la computación en la nube. Esta integración brinda a los clientes de XProtect Corporate de Milestone una nueva opción híbrida de implementación de computación en la nube.

Los usuarios de XProtect Corporate Milestone, indicó el ejecutivo, tienen numerosas sucursales de diferentes tamaños y en distintas ubicaciones. Por lo que aconsejó aprovechar esta opción híbrida para simplificar las implementaciones a gran escala. Una vez que el sistema Arcules está interconectado, el usuario puede utilizar las cámaras conectadas con las prestaciones de XProtect Corporate.

El VMS Arcules-XProtect Hybrid™ utiliza la tecnología Interconnect™ de Milestone que combina la hiperescalabilidad y flexibilidad de licencias del servicio en la nube de Arcules con la funcionalidad que ofrece la gestión de video de XProtect Corporate.

La fusión de estas tecnologías permite disfrutar de acceso unificado a video en vivo, grabaciones y alarmas a través de cámaras conectadas físicamente en las instalaciones de los clientes y virtualmente en la nube de Arcules, a través de XProtect Smart Client, XProtect Smart Wall y los clientes web y móviles.

Las organizaciones que tienen ubicaciones distribuidas como los centros de atención hospitalaria, establecimientos de comercio minorista, centros corporativos, campus educativos y de servicios públicos, aprovechan los servicios en la nube para obtener información en tiempo real en caso de que ocurra un incidente en áreas remotas.

VMS Arcules-XProtect también agrega valor a las estaciones de monitoreo y a los organismos de seguridad que usan XProtect Corporate como su plataforma VMS. Gracias a esta solución, dichas organizaciones pueden acceder directamente desde su sistema Xprotect, instalado en su infraestructura, a cámaras y clientes suscritos al servicio en la nube de Arcules.

Innova EZVIZ con sensor de movimiento

La firma especializada en el diseño y comercialización de gadgets domóticos, EZVIZ, dio a conocer una solución de seguridad para un hogar inteligente y para uso en pequeños negocios. De acuerdo con la compañía, versatilidad y máxima eficiencia son elementos fundamentales de la compacta C1C PIR, con sensor de movimiento pasivo y base magnética.

La C1C PIR es una solución Wi-Fi óptima para interiores. Gracias a un avanzado sensor de movimiento o PIR de última generación, alerta a los usuarios solo en aquellos casos en que desplazamiento proceda de un cuerpo que emite calor, lo cual minimiza al máximo las falsas alarmas (un libro que cae, por ejemplo). La cámara utiliza una función día/noche, con un filtro IR, que proporciona una claridad siempre óptima en condiciones de iluminación variables.

La base magnética de C1C permite adherirla sin necesidad de instalación a cualquier superficie metálica, lo que optimiza su facilidad y comodidad de uso y su flexibilidad para las reubicaciones que puedan ser necesarias.

Las características técnicas de C1C PIR incluyen:

- Video Full HD de 720p/1080p.
- Un ángulo de visión de 110°/130° wide-viewing-angle.
- Visión nocturna HD.
- Máscara de privacidad.
- Audiobidireccional.

Según la empresa, la App gratuita de EZVIZ, disponible tanto para sistemas Android como iOS, garantiza un uso intuitivo y extremadamente sencillo desde el Smartphone o el ordenador. Con esta aplicación, los usuarios pueden visualizar en directo, revisar clips, activar un zoom de hasta x8 para captar detalles y comenzar una conversación en remoto con quien se encuentre en el ángulo de visión de la cámara.

Esta nueva solución, junto al resto de productos EZVIZ, es compatible con Amazon Alexa y el Asistente de Google. La seguridad está a solo unas palabras en caso de que el cliente tenga las manos ocupadas o no posea su teléfono móvil. Los clientes que cuenten con Amazon Echo o dispositivos con Google Home podrán acceder a videos (retransmisiones en vivo/a tiempo real, por ejemplo, Alexa, Enséñame la puerta de entrada), o armar el sistema cuando se vayan de casa (como Alexa, conecta los sensores de movimiento). Los controles de voz extra/adicionales seguirán integrados en todos los productos EZVIZ para una mejor vida conectada.

Al respecto, Aaron Olvera, key account manager de EZVIZ México, explicó que para la compañía es fundamental continuar expandiendo el rango de productos para el hogar, con soluciones accesibles e inteligentes.

"Nuestras tecnologías de vigilancia se han ido desarrollando durante muchos años de experiencia en el sector, de manera que la empresa puede hoy responder a las necesidades cambiantes de los usuarios en materia de seguridad inteligente. El lanzamiento de la C1C PIR coloca a nuestro portafolio en la vanguardia del mercado mexicano", señaló Aaron Olvera.

La cámara C1C PIR tiene un costo de $1499 pesos IVA incluido, y está disponible a través los mayoristas de la firma: Syscom, Tonivisa e Intcomex.

Suma Hikvision más países en Call Center

La empresa mundial de soluciones y productos de videovigilancia y seguridad, Hikvision, incluyó nuevos países para atender las demandas de los usuarios finales mediante su Centro de llamadas para Latinoamérica, el cual está en funcionamiento desde el 2018.

Costa Rica, Ecuador, Guatemala, Paraguay, Uruguay, República Dominicana y Panamá son las nuevas regiones a las que también se les ofrecerá soporte técnico, de lunes a sábado, desde el cual quienes llamen tendrán respuestas rápidas a preguntas frecuentes sobre configuraciones sobre CCTV.

"El crecimiento de nuestra marca en la región hace que recibamos alrededor de 5 mil correos electrónicos de diferentes países cada mes, sobre todo de territorios donde no teníamos una línea telefónica. Hoy, las nuevas nos ayudarán a dar un servicio más eficaz a nuestros usuarios finales", explicó Dilan Cárdenas, call specialist de Hikvision para América Latina.

El ejecutivo agregó que estar certificados en HCSA o Hikvision Certified Security Associate y en HCSP o Hikvision Certified Security Professional, les permite también ayudar a sus clientes a configurar dispositivos de videovigilancia, control de acceso, intercom, EZVIZ, entre otros.

"El servicio de call center ofrece apoyo a solicitudes con un nivel intermedio de conocimiento técnico, y para los casos del ámbito profesional se consulta con otros miembros del equipo en Latam para encontrar la solución correcta a la inquietud del consumidor", indicó Dilan Cárdenas.

Cabe mencionar que, para el resto de las naciones, los usuarios podrán mandar sus consultas a latam.support@hikvision.com, las cuales serán atendidas por el área de soporte de cada región.

Estrategias en México

Como parte de sus acciones de responsabilidad social, Hikvision realizó una donación a la Facultad de Estudios Superiores (FES) Aragón, entidad académica multidisciplinaria de la Universidad Nacional Autónoma de México (UNAM).

El donativo constó de 111 productos, entre los que se encuentran cámaras de diversos tipos —como dispositivos térmicos tipo bala e IP PanoVu, ideal para diseñar un sistema de seguridad en grandes superficies—, sensores de alarmas, infrarrojos, controles de acceso, video porteros, cierres magnéticos, lectores de tarjeta, accesos alfa numéricos, palancas de emergencia, switches, entre otros accesorios complementarios de alta gama.

Axis refuerza

presencia en Latinoamérica

Como parte de las estrategias de crecimiento, Axis Communications tomó la decisión de unificar su división de negocios en Latinoamérica, que anteriormente estaba separada en dos regiones: por un lado, México, Centroamérica y Caribe, y por otro, América del Sur, cada una gestionada bajo su propia estructura y metas de crecimiento.

La resolución fue tomada con la finalidad de alinear los objetivos hacia una sola directriz, darle mayor presencia a la región y hacer más eficiente la administración. La nueva organización, tanto comercial como operativa, permitirá centralizar el mensaje de Axis, unir objetivos comerciales, atender a los clientes y hacer más eficientes las operaciones.

La firma unifica su división de negocios de esta región con el objetivo de centralizar su mensaje, conjuntar objetivos comerciales, atender a los clientes y hacer más eficientes las operaciones

Estas dos zonas estarán bajo la gestión de Leopoldo Ruiz, director Regional de Latinoamérica, quien indicó que en todo momento enfrentaron nuevos desafíos para crecer y evolucionar, y hoy el reto es dar una imagen unificada para América Latina, alineando las estrategias para beneficio de ellos, por lo que los canales y usuarios finales pueden tener la certidumbre de que esta nueva estructura contará con las personas adecuadas para resolver eficaz y oportunamente sus necesidades.

A decir de la empresa, una de las principales ventajas de esta nueva configuración es que los canales que se encuentran en áreas locales podrán tener la oportunidad de ampliarse a nivel regional, lo que abre múltiples alternativas de negocios para todo el ecosistema de socios, distribuidores y usuarios finales, reforzando una de las más importantes alianzas de la organización.

Se anunció que esta unificación se verá reflejada también en áreas estratégicas, como la de Desarrollo de Negocios encabezada por Mauricio Swain, quien asumirá el cargo de Business Development Manager para Latinoamérica. Él gestionará las diversas soluciones que Axis ofrece con el fin de hacerlas llegar a nuevos mercados verticales para esta región.

De igual forma, el área de Marketing será liderada por Mariana Ramírez, quien asumirá el cargo de Marketing Manager para Latinoamérica y buscará expandir los mensajes claves de la compañía a toda la zona, con el objetivo de consolidar un equipo de trabajo que, en conjunto, direccionarán a la empresa a cumplir importantes metas de negocio.

En el equipo de ventas, Denith García asumirá el puesto de Hispanic Inside Sales Team Lead y estará a cargo de los objetivos comerciales de la región. Por otro lado, Francisco Rodríguez estará en el Area Technical Manager y brindará servicio a las zonas de México, Caribe, América Central, Cono Norte, CBP y APU.

En conjunto formarán un equipo sólido de trabajo que estará liderado por el actual director Regional de Latinoamérica, Leopoldo Ruiz, con el propósito de cumplir un sólo objetivo comercial que posicionará a la demarcación como una de las principales de negocio tanto para la empresa como para el sector.

"Queremos que el mercado sepa que nuestro objetivo es dar continuidad a nuestra área de negocios, a la par de mejorar nuestro modelo de distribución. Esto es lo que hemos cuidado y que seguiremos impulsando como un compromiso hacia la industria. Otro de los sustentos de la compañía que queremos reforzar es la constante innovación tecnológica a través de la cual se busca potenciar nuestras soluciones con el fin de seguir constituyendo un mundo más inteligente y seguro", puntualizó Leopoldo Ruiz, director Regional de Latinoamérica. mís

Flir Systems presenta cámara Flir Quasar 4k IR PTZ

Redacción/ @revmasseguridad

FLIR Systems anunció la cámara FLIR Quasar™ 4K IR PTZ, dispositivo que brinda videovigilancia e iluminación de IR de largo alcance, lo que proporciona una resolución 4K de nivel probatorio y un rendimiento superior en escenarios de baja luminosidad para aplicaciones de seguridad urbana, infraestructuras críticas y zonas exteriores.

De acuerdo con la empresa, la baja y predecible velocidad de bits del equipo, el amplio rango dinámico mejorado y las características de estabilización de imagen optimizadas, proporcionan una calidad de video para conseguir una detección óptima.

Este equipo ofrece también compatibilidad con ONVIF, más funciones de control PTZ, protocolos de ciberseguridad más estrictos, una interfaz web simplificada e integración con FLIR United VMS, lo que la convierte en una solución integral.

La cámara Quasar 4K IR PTZ, diseñada para la ciberseguridad, incluye una interfaz web actualizada para garantizar un acceso seguro. Este dispositivo, que unifica lo más reciente en tecnología PTZ, óptica y mecánica, permite una integración con sistemas de gestión de video, por lo que, a decir de la empresa, es la solución integral ideal para instalaciones de videovigilancia urbana, infraestructuras críticas, aeropuertos y otras aplicaciones exteriores de alta seguridad.

FLIR Systems destacó que la resolución 4K de nivel probatorio ofrece un video nítido con capacidad de baja luminosidad y zoom óptico de 22 aumentos, así como velocidad de bits baja y predecible sin degradación en la calidad de video, incluso en movimiento y rango dinámico amplio mejorado e iluminación de IR integrada.

Soluciones unificadas de seguridad de Genetec

La estrategia de Genetec es ir más allá de la oferta únicamente de soluciones para la industria de seguridad. A través de su producto insignia Security Center, equipo unificado que incluye videovigilancia, control de acceso y lectura de placas¬, está presente en el mercado en diferentes verticales.

Lo anterior lo afirmó José Arellano, account manager de Genetec México, en entrevista con **Más Seguridad**. El directivo explicó que la compañía ha evolucionado al integrar la inteligencia en sus sistemas tecnológicos, lo cual otorga mejoras operacionales, en donde no sólo convergen los dispositivos, sino que también permite generar un ambiente más colaborativo y fomentar la protección cibernética de las organizaciones y sus empleados.

José Arellano, account manager de Genetec México

"Hemos sido bien aceptados como una solución que unifica sistemas de seguridad, somos exitosos en la parte de gobierno e iniciativa privada, actualmente tenemos presencia a nivel global con más de mil empleados. Haciendo un enfoque del perfil del personal que colabora en la empresa, podemos decir que es más del 75% de ingenieros", afirmó Arellano.

Como Genetec, afirmó el ejecutivo, "somos una plataforma abierta de software que desarrolla seguridad, prácticamente nos enfocamos a todas las verticales… tenemos más de 250 mil cámaras en las tiendas target en Estados Unidos, y así como este caso de éxito, contamos con otros también en educación, universidades, minería, industria, edificios, etc.

Actualmente, esta organización ha incrementado su participación de mercado tanto en gobierno como en iniciativa privada. No obstante, desde hace tiempo ha buscado impulsar las verticales de industria, educación y retail.

Solución Biométrica Sin Contacto para el control del COVID-19

Durante las últimas semanas una ola de temor e incertidumbre se ha vivido tras la aparición del virus COVID-19, por lo que la Organización Mundial de la Salud (OMS) recomendó evitar el contacto directo entre personas para prevenir el contagio como saludos de mano y el uso de terminales de acceso sin contacto.

El COVID-19 es un virus que puede causar distintas afecciones tales como fiebre, tos y dificultades respiratorias. Una persona puede contagiarse al estar en contacto con alguien que está infectado, o bien, puede propagarse entre seres humanos a través de las gotículas procedentes de la nariz o boca que salen despedidas cuando una persona tose o exhala, mismas que caen sobre los objetos y superficies que rodean a la persona, de modo que quien tenga contacto con estos puede contraer la enfermedad.

ZKTeco, proveedor y líder mundial de tecnología de verificación biométrica, ha lanzado al mercado terminales de control de acceso denominadas: “Solución Biométrica Sin Contacto”, aptas para cualquier entorno corporativo o empresarial, mismas que a través del reconocimiento facial o de palma, puede permitir el acceso a trabajadores, usuarios o visitantes a cualquier lugar sin necesidad de tener contacto físico.

Estas terminales de control de acceso son aptas para cualquier entorno corporativo y mediante el reconocimiento facial o de palma, permiten la entrada a trabajadores, usuarios o visitantes a cualquier lugar sin necesidad de contacto físico.

Dicha solución también cuenta con un dispositivo que detecta la temperatura de las personas para identificar posibles riesgos de contagio a tiempo sin necesidad de poner en peligro a los que lo rodeen.

“Sin duda es un gran método de control de acceso y, sobre todo, seguro pues al no necesitar que se coloque alguna parte física de tu cuerpo en una superficie, totalmente queda excluida la posibilidad de tener un contagio, de la mano de nuestra línea de productos “Luz Visible”, estas terminales de control de acceso poseen detección de fiebre, de palma y de cubre bocas”, afirmaron ejecutivos de ZKTeco Latinoamérica.

La firma cuenta actualmente con sedes en más de 60 ciudades alrededor del mundo y ofrece varias líneas de productos de control de acceso, entrada peatonal y vehicular, cerraduras inteligentes, productos IoT, softwares de gestión de personal y diversas soluciones que pueden ayudar a mejorar y automatizar.

ZKTeco

Control de Acceso e Inspección sin Contacto con Medición de Temperatura Corporal

ZK-D3180S TD

Detector de metales con detector de fiebre

SBTL8033

Solución de control de entrada sin contacto con detector de fiebre

+/- 30

ProFace X TD

Terminal de reconocimiento facial con detector de fiebre

+/- 30

ZN-T1

Cámara de red de detección de temperatura corporal

HID® presenta línea de lectores HID Signo

La empresa mundial en soluciones confiables de identificación, HID Global, lanzó HID® SignoTM, su icónica línea de lectores que marca un nuevo punto de referencia en la industria como la solución más adaptable, interoperable y segura para el control de acceso.

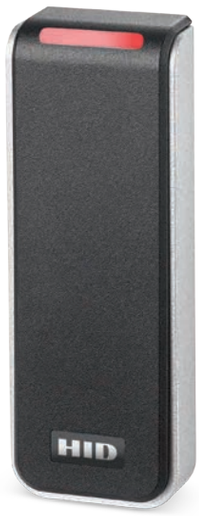
Al respecto, Harm Radstaak, vicepresidente y director ejecutivo de Soluciones de Control de Acceso Físico de HID Global, expresó: “En un momento en que la industria busca utilizar los sistemas de control de acceso como eje principal para crear entornos inteligentes, es cada vez más frecuente que los consultores, integradores y usuarios finales exijan soluciones más versátiles y de más alto desempeño”.

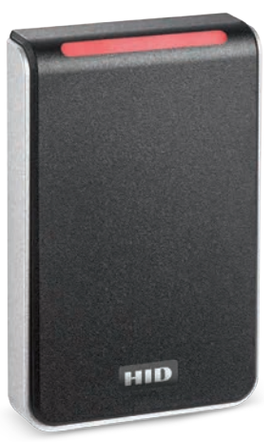
Indicó que HID Signo se basa en una plataforma abierta y es fiel a su compromiso con la innovación, gracias a su flexibilidad sin precedentes y a un conjunto robusto de funciones vanguardistas que optimizan las experiencias en los entornos laborales.

“Nuestro objetivo es brindar más opciones a nuestros clientes y darles tranquilidad, pues saben que pueden adaptar continuamente sus sistemas a medida que vayan cambiando sus requerimientos”, precisó Harm Radstaak.

Para maximizar la versatilidad, los lectores son interoperables con más de una docena de sistemas de credenciales físicas y móviles, lo que permite a las organizaciones usar la tecnología que elijan y migrar fácilmente, y a su propio ritmo, a las más avanzadas soluciones. Además, con el soporte del protocolo ECP (Sondeo sin contacto mejorado) de Apple, que admite las identificaciones estudiantiles en Apple Wallet, los lectores HID Signo están impulsando una nueva era de flexibilidad y practicidad en el acceso móvil.

De acuerdo con HID Global, los nuevos lectores cuentan con múltiples funciones inteligentes, como la detección automática de superficie que recalibra y optimiza el rendimiento de lectura, según el lugar del montaje. Para un rendimiento resistente en montajes al aire libre, los dispositivos también tienen una estructura robusta, con grado de protección IP65, que no requieren la instalación de juntas adicionales, y poseen un teclado táctil capacitivo que proporciona resistencia en condiciones climáticas difíciles.



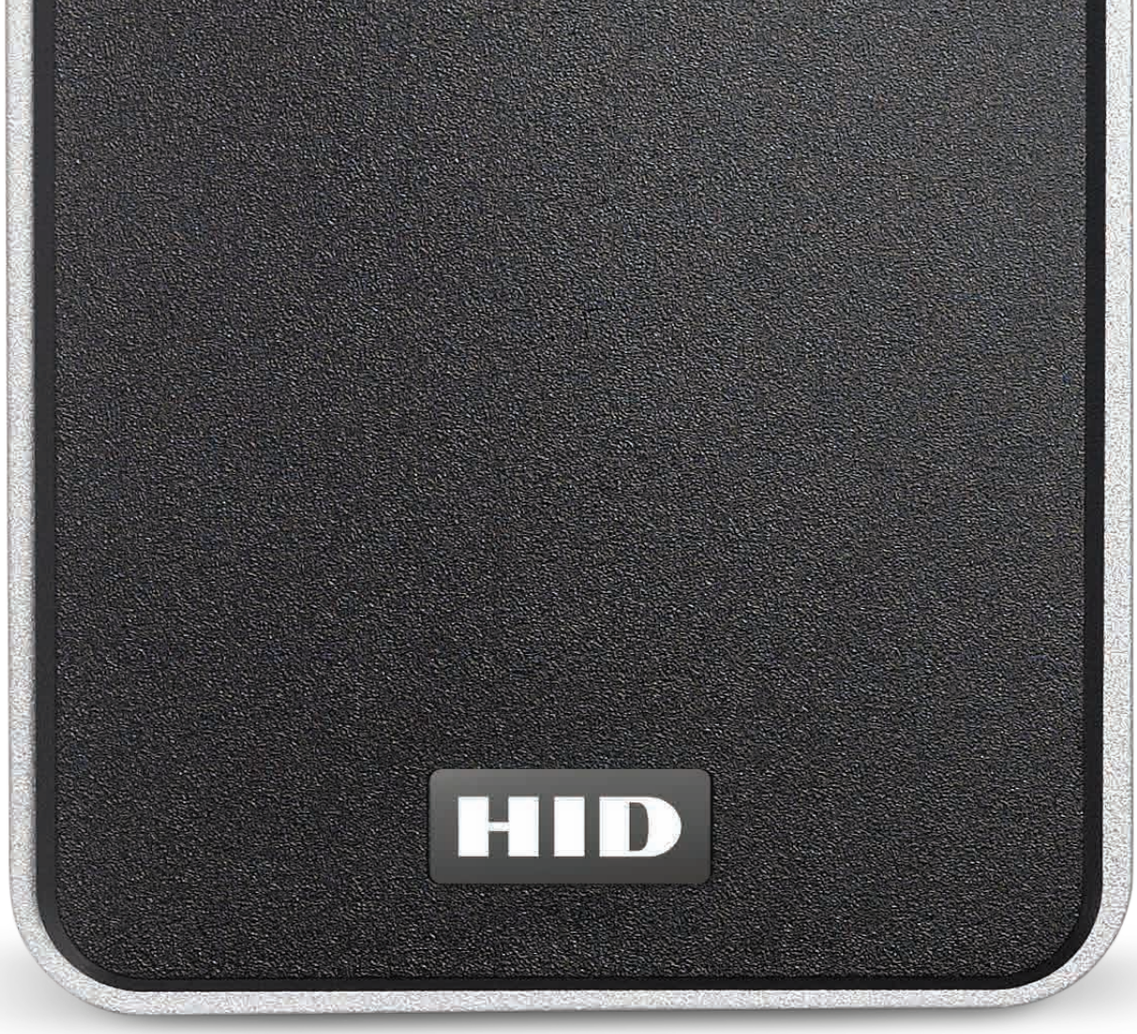


Los nuevos lectores simplifican la implementación y gestión del sistema, cumplen con los requerimientos de seguridad de los dinámicos entornos actuales y preparan a las organizaciones para un control de acceso más inteligente y conectado

La conectividad inherente de los lectores HID Signo permite a los administradores configurarlos y diagnosticarlos de forma remota, así como supervisar su estado a través de un ecosistema de lectores conectados y administrados desde una ubicación central. Además, la configuración se puede optimizar aún más mediante el controlador, a través del OSDP (Protocolo de dispositivo supervisado abierto).

“El innovador enfoque de HID para el control de acceso también sienta las bases para un futuro de sistemas conectados a la nube que permitirán nuevas aplicaciones y prestaciones innovadoras, como la posibilidad de anticipar y hacer frente de forma proactiva a los problemas antes de que ocurran”, concluyó Radstaak.

Los lectores ofrecen un modelo de seguridad de varios niveles con compatibilidad integrada con el protocolo OSDP de canal seguro y la reconocida tecnología SIO (Objeto de Identidad Segura) de HID. De igual manera almacenan claves criptográficas en hardware con elemento seguro certificado (EAL6 +) y se pueden usar combinaciones de autenticación personalizadas para mayor seguridad. HID Signo está disponible a través del programa de socios Advantage Partners en los principales mercados del mundo. El lanzamiento se realizará de forma gradual en determinadas regiones y en países de América Latina.



HOLA SIGNO

La línea icónica de lectores de control de acceso de HID Global

Conozca más sobre SIGNO en hidglobal.com/es/**signo**

HID

Powering **Trusted Identities**

Biometría eficaz contra fraude en centros de contacto

La incidencia del engaño en el contact center crece con rapidez. La consultora Gartner calcula que durante 2020, el 75% de las organizaciones que se relacionan con sus clientes por varios canales sufrirán un ataque fraudulento en el que el centro de contacto será el punto de entrada principal.

La mayoría de los servicios basados en voz de los contact centers están a menudo aislados, en su organización y arquitectura, de otros canales, como el autoservicio web o las aplicaciones móviles, lo que significa que no están protegidos por las medidas de prevención del fraude y de pérdidas orientadas a los canales digitales.

El alcance de estos ataques también es importante. Según un estudio de 2018 de Javelin Strategy & Research:

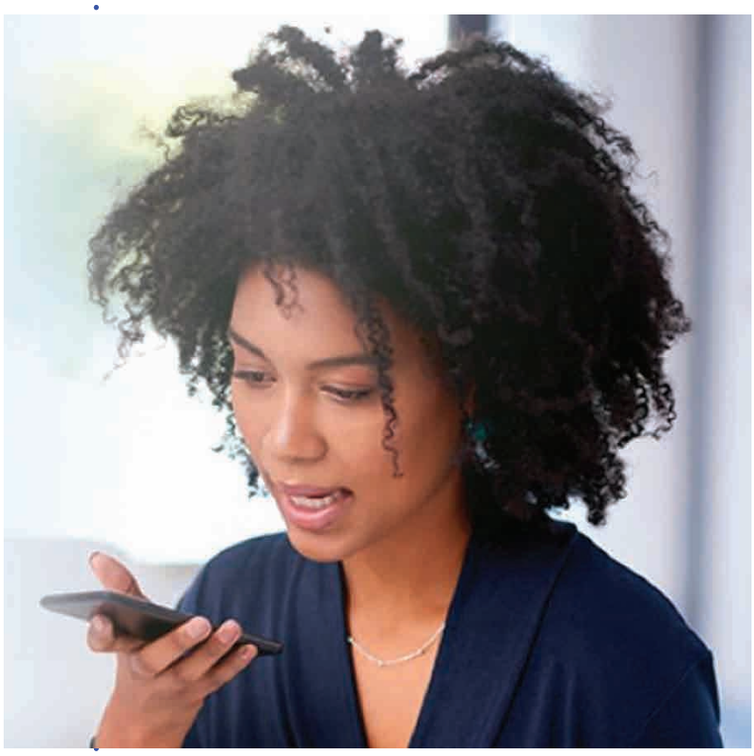
- El número de personas afectadas por fraudes de identidad aumentó 8%, hasta llegar a los 16.7 millones de consumidores en Estados Unidos.
- Los estafadores obtuvieron 1.3 millones más de víctimas en 2017, robando 16 mil 800 millones de dólares a los consumidores.
- La apropiación de cuentas se triplicó el año pasado, lo que supuso 5 mil 100 millones de dólares en pérdidas.
- Los perjudicados pagaron una media de 290 dólares y dedicaron 15 horas de su tiempo para solucionar estos incidentes.

Carlos Vázquez, gerente regional de ventas de Nuance Communications para América Latina, indicó que los estafadores -como los clientes- aprovechan varios canales usando una variedad de teléfonos y dispositivos digitales. Tienden a realizar los ciclos a través de ellos con mucha más frecuencia que los usuarios legítimos, a medida que tratan de evadir las técnicas de prevención de fraude heredadas.

Explicó que al igual que con la autenticación, un enfoque biométrico para la prevención del fraude permite identificar a los estafadores para siempre, no importa qué dispositivo usen, dónde estén ubicados o a través de qué canal. La prevención de la estafa basada en la biometría reduce las pérdidas por timo más que cualquier otro planteamiento, pero también proporciona la capacidad de enfrentar el problema impulsando el arresto, el procesamiento y el encarcelamiento de los defraudadores, argumentó.

Nuance Communications revela que se están usando cada vez más estos sistemas de voz como estrategia para verificar la identidad en numerosas aplicaciones de seguridad

Indicó que para lograr el equilibrio entre la experiencia del cliente y la necesidad de seguridad, los expertos de la industria están usando cada vez más la biometría de voz como estrategia importante para verificar la identidad en numerosas aplicaciones de seguridad.



"La biometría puede desempeñar una función clave en el contact center y en múltiples canales de interacción a través de la autenticación y la prevención del fraude. Comienza por la voz. Cuando el supuesto titular de la cuenta llama al contact center, un sistema biométrico compara su frase con la "huella de voz" guardada con el fin de confirmar que la persona que se comunica es quien dice ser. No hace falta proporcionar más información ni responder a preguntas de verificación, así que el proceso es rápido y seguro. Esto permite al agente de ventas continuar con confianza y ofrecer una experiencia totalmente personalizada al cliente", precisó Carlos Vázquez.

La firma cuenta con la herramienta Nuance Security Suite, la cual es utilizada por organismos de seguridad a nivel mundial para resolver el problema del fraude. Esta solución ofrece una autenticación y prevención de estafas amplia en canales digitales y de voz; brinda dos factores biométricos para este conducto; entrega tres credenciales y es la única que utiliza redes neuronales profundas de tercera generación para respaldar sus algoritmos.

Expo Seguridad México cambia de fecha

Debido a la incertidumbre en la región y a nivel global generada por el COVID-19, Reed Exhibitions México informó que Expo Seguridad México y Expo Seguridad Industrial, previamente programados del 21 al 23 de abril, se realizarán del 18 al 20 de agosto de 2020.

De acuerdo con el comité organizador, el anuncio se hizo después de una amplia consulta con actores relevantes de la industria, y está alineada a las recomendaciones emitidas por las autoridades mexicanas de salud pública con respecto a los viajes desde y hacia los países afectados, así como a las restricciones para eventos que reúnen a más de 5 mil personas.

Expo Seguridad es un encuentro de tres días en torno a la protección electrónica e industrial, con tecnología, soluciones y capacitación para fabricantes, distribuidores, integradores y usuarios finales, nacionales y extranjeros.

Al respecto, Jorge Hagg, director de la exposición, expresó: “Nuestro sentir está con los afectados por el COVID-19. La decisión de posponer el evento fue difícil; nuestros clientes, socios y personal han trabajado diligentemente para hacer realidad esta edición de Expo Seguridad. Sin embargo, nuestra prioridad es salvaguardar la salud de todos. Estamos seguros de que nuestros eventos continuarán cumpliendo los más altos estándares que los participantes esperan y brindaremos un servicio relevante para la industria: ofreceremos oportunidades de negocios, colaboración, educación y crearemos formas para que la comunidad de seguridad se conecte, manteniendo a la industria avanzando durante este difícil momento”.

A nombre de Reed Exhibitions, Jorge Hagg expresó su agradecimiento a todos los expositores, socios, asistentes, proveedores, medios de comunicación y personal, por su apoyo y mensajes durante este difícil momento; confió en dar la bienvenida a la comunidad global de la seguridad electrónica, física e industrial en la Ciudad de México en agosto.

Novedades y mayor interacción

En la edición 2020 de Expo Seguridad México, se presentará por primera vez la “Zona Demo”, en donde se mostrarán, de manera presencial e interactivamente, equipos de rescate, trabajos en alturas, una extinción de incendios virtual y otras soluciones.

Se darán a conocer productos y tecnologías de punta, dirigidas a la protección, salud ocupacional y a la seguridad física y digital con desarrollos especiales tanto para el sector privado como para el público.

A diferencia de 2019, en ésta se ofrecerán casos de éxito y conferencias técnicas de mayor especialización y mejores prácticas y experiencias vivenciales. El objetivo de los organizadores es que los visitantes conozcan los productos, soluciones y sus aplicaciones, para así contribuir a que el país esté mejor preparado en temas de seguridad.

Esta exposición atiende a un mercado especializado que desde el 2012 muestra un aumento de demanda de soluciones; se compone de compañías que brindan empleo a entre 240 mil y 600 mil personas, y contribuye aproximadamente con el 1.5% del PIB, lo cual equivale a una cifra de 240 mil millones de pesos, según datos de Reed Exhibitions México, organizadora de Expo Seguridad.

La meta de los organizadores es superar las cifras que alcanzó en la edición 2019. Por ejemplo, su piso de exhibición será de 13 mil 136 metros cuadrados, cantidad mayor a los anteriores 12 mil 653 metros cuadrados; se espera contar con 648 expositores y recibir a más de 21 mil visitantes. Son números que consolidarán al evento como el más grande e importante en su especialidad.

En opinión de “El Profe”

DE HACKERS Y OTROS DEMONIOS INFORMÁTICOS

Divide y vencerás

El viejo refrán prueba ser aplicable una vez más, y ahora en circunstancias como la que hoy vivimos con el COVID-19: separar a las personas para mitigar la transmisión de unas con otras y tratar de no asistir a lugares concurridos. Una persona enferma (aunque sea asintomática) puede infectar a muchas más y así el efecto multiplicador. Todos los estudios han revelado que para aplanar la curva de contagio es necesario “dividir para vencer”.

Esto mismo es lo que ocurre con una infección informática: un hacker se apropia de alguna forma de una computadora, normalmente a través de un mensaje por correo engañando al inocente, una liga a internet a un sitio malicioso que visitará el cibernauta, o un USB que deja tirado para que lo inserten en el equipo de la oficina. Y ¡zas! El atacante obtiene su primera víctima. Esto es lo que comúnmente se conoce como “compromiso inicial”.

Sí, es solo un ordenador, y generalmente es una máquina un tanto descuidada y sin importancia sistémica. No es para nada la computadora súper fortalecida ni la que todo el mundo está viendo. Posiblemente es una triste computadora y olvidada por los rincones como la muñeca fea… pero ¡conectada a la red de la organización!

Un verdadero hackeo ahí comienza: un delincuente informático conocedor no pretenderá atacar inicialmente y en forma directa al sistema crítico ni las computadoras sensibles de la organización. Tendrá paciencia y se moverá lentamente hasta alcanzar su meta final, como encontrar documentos confidenciales o realizar traspasos de dinero. Por ejemplo, dicen que una empresa regularmente tarda más de 100 días en saber que fue atacada exitosamente. Así que lo que el hacker quiere es simplemente entrar, por donde sea, como sea. Tener conectividad para su siguiente movimiento: dispersión de la infección y finalmente ¡caos!

¿Cómo se puede evitar? Posiblemente eludir una infección inicial sería posible, pero altamente complicado (si no imposible) cuando hablamos de decenas o centenas de computadoras. Lo que sí se puede hacer es segmentar la red para que la contaminación solamente afecte a algunos equipos, pero no a todos ni los más importantes. Hay que contener el daño.

En fin, lo mejor sería no contagiarse ni ser víctima de los hackers. Pero si asumimos que hagamos lo que hagamos seremos atacados exitosamente, posiblemente la segmentación es la mejor recomendación. Recuerden: divide y vencerás.

Bueno, esta es mi opinión, ¿cuál es la suya?

El demonio del mes: El demonio del mes: Los hackers que en estas fechas están atacando los sistemas de los hospitales o infectando a cuantas máquinas visitan sitios “quesque” de alertas y con videos sobre la calamidad del COVID19. Por cierto, ¿usted ha entrado a esas páginas?, ¿ha descargado videos? Puede estar contagiado. Ahí se lo dejo de tarea… mís

Cualquier comentario o sugerencia no dude en consultar al Profe de seguridad.

¡Hasta el próximo número!

ElProfeSeguro@gmail.com Sígueme en Twitter: @ElProfeSeguro

Solo 24% de mujeres ocupa puestos en ciberseguridad

Julia Urbina-Pineda, conferencista y consultora en la gestión de riesgos cibernéticos, aseguró que existen mujeres preparadas para hacerse cargo de departamentos y proyectos de ciberseguridad en organizaciones de cualquier tipo y tamaño, “pero la condición actual a nivel global nos muestra que los varones siguen a cargo de los puestos de liderazgo y nos desplazan. De acuerdo con un estudio de ISC, organismo certificador en esta especialidad, somos solo 24% que trabajamos en la ciberprotección, por lo que la brecha es bastante amplia”.

El estudio arrojó que paulatinamente el sexo femenino está ocupando más puestos de liderazgo, ya que está más capacitado y cuenta con más certificaciones que sus pares masculinos. Como muestra, en cinco años la cifra de mujeres ha aumentado: de ser el 11% en 2014, para el año pasado ya se había alcanzado casi un cuarto del total de la fuerza laboral, enfocada en la ciberseguridad, ubicada en distintos cargos organizacionales.

De acuerdo con Julia Urbina-Pineda, se detectó que en el terreno académico, cuando a las mujeres se les pregunta si les gustaría estudiar alguna carrera relacionada con este campo, al final desisten porque se les dice que es una labor más identificada con el género masculino.

“Podemos dedicarnos sin problema a estudiar carreras de TI, y más allá de eso, tenemos más facilidad para hacer una lectura de puertos, interpretar gráficos y elaborar complejos análisis de riesgos, entre otras acciones. Como complemento, tenemos la capacidad de liderazgo y dirección suficiente para ejecutar planes de prevención y corrección, indicando qué acciones se deben aplicar, aunque sea a un grupo de líderes varones”, explicó Urbina-Pineda. mís

Designed by fullvector / Freepik

Designed by Freepik

principal objetivo de ciberataques en México

La empresa global en soluciones de ciberseguridad amplias, integradas y automatizadas, Fortinet, anunció los hallazgos para el 2019 de su plataforma Fortinet Threat Intelligence Insider Latin America, herramienta que recopila y analiza miles de incidentes de seguridad en el ciberespacio a nivel global, la cual arrojó que los bancos son el principal objetivo de ataques cibernéticos en México.

Los datos de la plataforma revelaron la alarmante realidad del cibercrimen en América Latina y el Caribe, registrando 58 billones de intentos de ciberataques en el 2019. En México, se realizaron más de 12.8 billones de intentos de estos delitos el año pasado. Eso se traduce a alrededor de 35 millones de intentos por día, la mayoría de los cuales siguen la tendencia de Latinoamérica y están especialmente diseñados para entrar en redes bancarias, obtener información financiera y robar dinero.

De acuerdo con la compañía, entre las amenazas más detectadas el año pasado, se encuentran dos ataques dirigidos específicamente al sector bancario: DoublePulsar y Emotet. DoublePulsar es una agresión tipo “backdoor” que ha sido utilizada por el ransomware WannaCry y en intrusiones a bancos de la región en 2018. Teniendo en cuenta que aprovecha vulnerabilidades ya resueltas, su uso continuo evidencia la gran huella de software sin actualizaciones en México que afecta tanto a empresas como a individuos.

Por otro parte, Emotet es un botnet dirigido a bancos que permite que un atacante remoto pueda emitir comandos para realizar diferentes operaciones como descargas de malware y ransomware. mís

Big data

inteligencia artificial y ciberseguridad

Introducción

El aumento de las amenazas vinculadas al ciberespacio se ha convertido en una fuente de preocupación no sólo para la mayoría de los Estados Nación, sino también para los sectores industriales de manufactura, seguridad, comercio, transporte, financieros, y las empresas en general. Un factor detonante sin duda alguna ha sido la adopción de la industria 4.0 y las tecnologías asociadas a la misma como: el big data (BD), la inteligencia artificial (AI), machine learning, el internet de las cosas, entre otras. Y al mismo tiempo, el creciente número de dispositivos conectados a internet.

Ante tales circunstancias, las empresas y los diversos sectores han incrementado el porcentaje de inversiones sobre sistemas de defensa ante las numerosas amenazas y los constantes ataques en el ciberespacio, dejando como reto ampliar y mejorar constantemente el nivel de seguridad en sus programas.

Desarrollo

El incremento de los ataques en contra de las infraestructuras críticas, activos y redes de información de naciones y empresas, demuestra la existencia de grupos criminales y organizaciones dispuestas a explotar el ciberespacio con propósitos hostiles. Grupos que han encontrado en las nuevas tecnologías asociadas a la industria 4.0 un aliado para incrementar en sofisticación, grado de impacto y efectividad los ciberataques.

El big data y la inteligencia artificial son dos desarrollos tecnológicos que se han vuelto tendencias que forman parte indispensable de este creciente sistema digital, ya que cada sensor y dispositivo genera grandes volúmenes de datos (demográficos, estadísticos, geográficos, entre otros), que deben ser protegidos y gestionados de formas segura. Los gobiernos y empresas necesitan adoptar las nuevas tecnologías garantizando que toda esta información sea utilizada responsablemente para realizar una gestión inteligente y dar cumplimiento a las leyes y normas correspondientes.

Las amenazas cibernéticas en la actualidad son globales, por lo que se requiere desarrollar soluciones mundiales que minimicen el impacto de estas advertencias que día con día crecen en sofisticación e impacto. De tal forma, la inteligencia artificial y el big data son tecnologías que bien enfocadas pueden estrechar la brechas de ciberseguridad, por lo cual se considera indispensable el uso de las mismas para desarrollar soluciones más efectivas que permitan incrementar y resguardar los activos e infraestructuras críticas de las organizaciones.

El uso del BD y la AI, en coordinación con otras tecnologías, proporcionan capacidad a las compañías para desarrollar algoritmos y modelos de seguridad sofisticados que identifiquen posibles vulnerabilidades de forma preventiva y no reactiva, lo cual otorga una ventaja competitiva ante las soluciones de ciberseguridad tradicionales. En este sentido, es preciso resaltar que la AI y los otros sistemas serán aliados estratégicos ante los crecientes ciberataques, pero no asumirán todas las funciones de seguridad dentro de las organizaciones, sino que proporcionarán los elementos necesarios para prevenir y reaccionar oportunamente ante un incidente o un ataque.

Conclusiones

La incorporación de la inteligencia artificial, el big data, el machine learning y otras tecnologías nuevas no sólo brindarán capacidad para operar grandes volúmenes de datos, monitorear actividades y predecir hasta cierto punto incidentes dentro de la red de la organización, sino que están siendo incorporadas en las instituciones públicas y privadas que atienden temas críticos cómo energía, salud, seguridad, finanzas, transporte, entre otros.

A esta incorporación de las nuevas tecnologías asociadas a la industria 4.0 con los programas y soluciones de ciberseguridad se les ha comenzado a llamar “sistemas de ciberseguridad híbrida”, y alrededor del mundo han despertado el interés de grandes empresas tecnológicas, pues las soluciones de la seguridad en la red ante las amenazas cibernéticas son cada día más rentables.

Es importante entender que, además de los elementos técnicos (direccionamiento IP, infraestructura, desarrollo tecnológico) es indispensable la participación activa de todos los actores clave para generar el marco regulatorio adecuado para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y no repudio de la información y la seguridad de los usuarios. Sin olvidar que la concientización sobre una cultura de seguridad de la información de los recursos humanos dentro de las organizaciones, será complemento perfecto para incrementar el nivel de resiliencia y las capacidades cibernéticas de la empresa, minimizando el impacto de los crecientes ataques en la red, incluidos los que están usando la AI como base del desarrollo de armas de los ciberatacantes. mís

* **Gustavo Guzmán Hernández**
México

Académico y especialista en el área de gobierno de TI y ciberseguridad. Es Ingeniero en Comunicaciones y Electrónica con especialidad en Telecomunicaciones por la Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME) del Instituto Politécnico Nacional (IPN).
gguzmanh01@gmail.com
Tw @GustavoG_Kc

REFERENCIAS

[1] Goosen, R., Rontojannis, A., Deutscher, S., Rogg, J., Bohmayr, D. (2018). Artificial Intelligence is a threat to cybersecurity. It´s also a solution. BCG Research. Recuperado de: https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx

[2] Warner, Michael, “Cybersecurity: A Pre-history”, Intelligence and National Security, pp. 781-799; y Rudner, Martin, “Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge”, International Journal of Intelligence and CounterIntelligence, 26, 3, pp. 453-481, 2013.

Designed by pikisuperstar / Freepik

Descubre Check Point vulnerabilidades en iluminación inteligente

Investigadores de Check Point Software Technologies, proveedor especializado en ciberseguridad a nivel mundial, descubrieron vulnerabilidades críticas que permitirían a un cibercriminal infectar con ransomware o cualquier otro tipo de malware las redes corporativas o domésticas tras acceder al sistema de control de los focos inteligentes.

Los expertos de la compañía indicaron que un cibercriminal tan sólo necesitaría tener a su disposición una antena y un ordenador portátil, así como encontrarse a una distancia menor de 100 metros del objetivo.

Además mostraron cómo un ciberatacante podía explotar una red IoT (focos inteligentes y su controlador) para lanzar ataques a sistemas informáticos convencionales en hogares, negocios o incluso ciudades inteligentes. Asimismo, los especialistas se centraron en los focos y el puente de control de Philips Hue, y encontraron debilidades que les permitieron infiltrarse en la organización utilizando un exploit remoto en el protocolo inalámbrico de baja potencia ZigBee, que se utiliza para controlar una amplia gama de dispositivos de IoT.

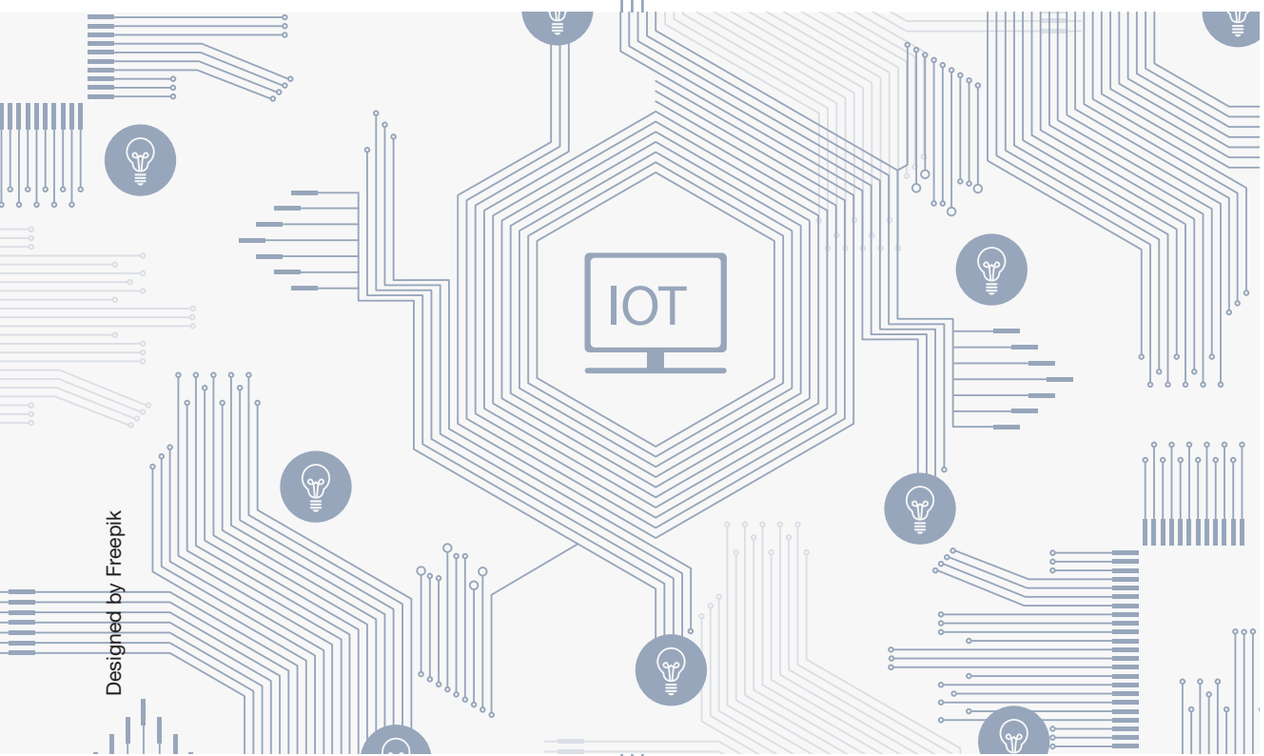
En un análisis de seguridad centrado en las lámparas inteligentes controladas por ZigBee que se publicó en 2017, los científicos demostraron que se podía tomar el control de una bombilla Hue conectada a una red, instalar firmware malicioso y propagarlo. Aprovechando esta debilidad, Check Point decidió llevar este trabajo previo un paso más allá y utilizó el foco Hue como plataforma para adentrarse en el puente de control de los demás aparatos y, en última instancia, atacar la red informática del objetivo. Es importante destacar que las lámparas con una versión de hardware más reciente no han experimentado estos fallos.

La firma explicó la forma en cómo se da el proceso del ataque:

1. El hacker controla el color o el brillo del foco para hacer creer a los usuarios que no funciona correctamente. Esta, además, aparece como “inalcanzable” en la aplicación de control del usuario, por lo que tratan de “reiniciarla”.
2. La única forma de reiniciar la bombilla es borrarla de la aplicación, y luego configurar el puente de control para que vuelva a reconocerla como disponible.
3. Una vez el puente ha reconocido el aparato, el usuario puede volver a añadirlo a la red.
4. El foco controlado por el hacker con el firmware actualizado se sirve de las fragilidades del protocolo ZigBee para producir fallos en el puente de control debido a la gran cantidad de datos que recibe. Esta información permite al hacker instalar malware en el puente, que a su vez está conectado a la red empresarial o doméstica.
5. El malware se vuelve a conectar con el hacker y, utilizando un exploit conocido como EternalBlue, puede infiltrarse en la red IP de destino desde el puente para difundir ransomware o software de espionaje.

Mario García, director general de Check Point para España y Portugal, indicó que los dispositivos IoT pueden suponer un riesgo para la seguridad. Sin embargo, esta investigación muestra cómo incluso los elementos más simples y aparentemente inofensivos como las bombillas, pueden ser explotados por los cibercriminales, que los emplean para apoderarse de las redes, o infectarlas con malware.

Por lo que aconsejó a las organizaciones y a los usuarios protegerse contra los posibles ataques actualizando sus dispositivos con los últimos parches, pero también separándolos de otros aparatos conectados a la misma red, para limitar así la propagación de malware.



Designed by Freepik

Radiocomunicación al servicio de los cuerpos de emergencias Hytera™

La propagación del COVID-19 a nivel global nos demuestra lo interconectados que estamos en el planeta, nos ha enseñado que las acciones de un lugar o persona se reflejan en el sitio opuesto y, sobre todo, ha puesto a prueba nuestra capacidad de reacción. La velocidad con la que se han presentado los distintos brotes y su propagación ha generado que grupos de expertos en los gobiernos y las empresas tengan que tomar decisiones estratégicas en beneficio de todos. Preservar la salud al menor costo es el objetivo de los líderes en el mundo.

Los cuerpos de emergencia juegan un papel preponderante en este contexto; las instituciones gubernamentales y privadas encargadas de preservar el bienestar y la vida de los ciudadanos, requieren de dos importantes elementos: personal capacitado y herramientas que les ayuden a cumplir con su trabajo. La capacitación es esencial para afrontar de manera oportuna esta o cualquier crisis que se presente, los equipos de trabajo deben estar a la vanguardia de las estrategias que se implementan en todo el mundo y generar protocolos de reacción ante distintos escenarios.

Esta tecnología es una herramienta apta para instituciones de gobierno, así como servicios médicos: hospitales, ambulancias, paramédicos, etc.

Una de las herramientas de mayor necesidad son los sistemas de comunicación. Éste es un sector crítico que requiere de soluciones de información y transmisión de datos estable, eficaz y seguro, pues de ellos depende la vida de muchas personas. Es importante que los organismos de prevención y atención se comuniquen rápidamente para indicar en dónde existe un brote, qué insumos se requieren, qué personal está disponible, entre otras necesidades. La radiocomunicación profesional de misión crítica es la solución óptima para estos grupos, ya que ofrece inmediatez, estabilidad, seguridad y rentabilidad.

A diferencia de la comunicación vía celular, la radiocomunicación profesional cuenta con un espectro de banda único que no se satura, por lo cual siempre estará disponible; además basta con pulsar un botón llamado PPT para comunicarse con una persona o un grupo de manera inmediata. Las instrucciones se emiten a un conjunto de individuos que en milisegundo recibe la información. Las redes se diseñan conforme las demandas de las organizaciones y dependerá de cada una, la infraestructura que se implemente, así como de los equipos y aplicaciones; de tal manera, que cubra las necesidades de las distintas agrupaciones de emergencia.

Es importante resaltar que las comunicaciones críticas como la seguridad, el transporte público, los sistemas de hidrocarburos, así como los cuerpos de emergencia y rescate no deben tratarse de la misma manera que otros sectores, puesto que en ellos recae la responsabilidad de salvaguardar la integridad y vida de las personas.

La radiocomunicación ha evolucionado para cubrir las necesidades actuales de los grupos de emergencia. Se han creado aplicaciones especializadas tanto de voz como de datos que incrementan la capacidad de respuesta, por ejemplo, el uso del GPS con lo cual el operador central puede saber en tiempo real en dónde está cada uno de los elementos y contactar al más cercano. También se han desarrollado funcionalidades como trabajador solitario, que emite una alarma en intervalos de tiempo que debe responder el portador del radio, en caso de no hacerlo, se manda una señal de alarma a la central que indica que algo no está bien.

En Hytera tenemos la misión de proveer de herramientas y soluciones integrales para hacer un mundo mejor, más seguro. La innovación es una de nuestras fortalezas y la consultoría de nuestros socios comerciales ayuda a las organizaciones a obtener la mejor solución para sus necesidades actuales y futuras.

*Claris González Monreal
Gerente de Marketing de Hytera México.
Conoce más en www.hytera.mx /
mercadeo@hytera.mx

MISIÓN CRÍTICA

PROTECCIÓN PARA USUARIOS PMR

-Seguridad de información

-Operación ininterrumpida de un sistema de comunicación de radio móvil y un centro de control

CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD

Para más información:
www.hytera.mx

Facebook:
Hytera México

Prevención de violencia laboral

y sexual en los centros de trabajo

El centro de trabajo se convierte en un segundo hogar, ya que es uno de los lugares donde más tiempo pasamos. En ocasiones frecuentamos más a nuestros compañeros que a la propia familia. Desafortunadamente, no siempre es todo miel sobre hojuelas.

Los centros de trabajo pueden convertirse en un espacio donde podemos ser violentados. A continuación, algunas cifras:

- Datos del INEGI indican que en el país, el 79.1% de los casos de violencia laboral contra la mujer sucede en los centros de trabajo, y ésta suele ser emocional (48.45%) o sexual (47.9%).
- Según el "Diagnóstico de hostigamiento sexual y acoso sexual en la administración pública federal 2015-2018", elaborado por la Comisión Nacional de Derechos Humanos, de 402 víctimas que reportaron hostigamiento y abuso en instituciones, 94.53% fueron mujeres. De acuerdo con este mismo informe, en 2017:

o En 91% de los casos registrados las presuntas víctimas son mujeres, el 8% son hombres y en 1% de los casos no se especifica el sexo de la persona que denuncia.

o El 90% de las personas denunciadas son hombres y el 5.5% son mujeres.

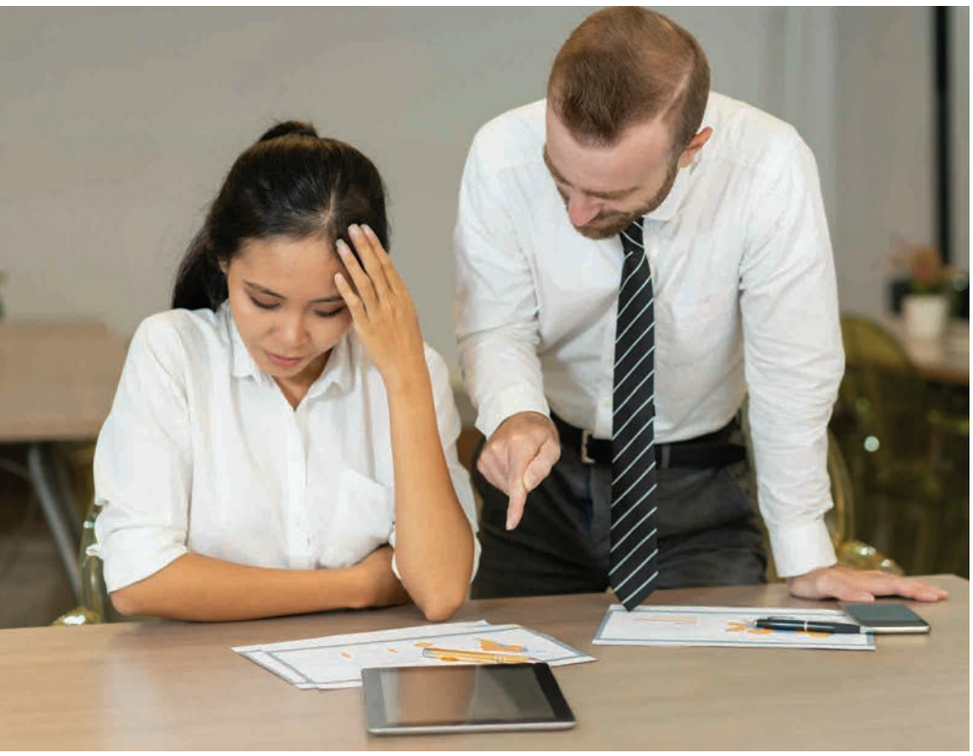
- Encuesta Nacional de Ocupación y Empleo que muestra que el porcentaje de personas, cuyo motivo principal para separarse del trabajo fue el acoso o falta de respeto, se ha incrementado en un 70% de 2005 a 2019.

Las cifras indican que la violencia sexual va en incremento, es mayor en contra de las mujeres (pero no exclusiva) y que es una de las principales causas para que una persona decida abandonar su empleo.

Muchas empresas tienen algunas medidas de prevención y atención a las víctimas, pero para estandarizar estos procesos, la STPS publicó el 6 de marzo de este año, el modelo de Protocolo Para Prevenir, Atender y Erradicar la Violencia Laboral, que tiene por objetivo definir el procedimiento, vías y/o mecanismos para brindar atención a las presuntas víctimas de algún caso de violencia laboral; señalar las vías e instancias competentes al interior y exterior del centro de trabajo que puedan apoyar en estos temas en materia laboral; así como promover una cultura organizacional de igualdad de género y un clima laboral propicio para la erradicación de la violencia laboral en el centro de trabajo.

Los puntos de implementación que abarca el Protocolo son:

1. Contar con una Persona Consejera que dará atención de primer contacto y asesoría a la presunta víctima sobre vías, instancias y mecanismos para la atención de casos de violencia laboral.
2. Constituir un Comité de Atención y Seguimiento cuyas funciones son:
   a. Determinar el plan de trabajo para la sensibilización y capacitación.
   b. Analizar los casos de violencia laboral y determinar medidas de protección en caso de que lo considere necesario.



Violencia laboral

Se ejerce por las personas que tienen un vínculo laboral, (…) independientemente de la relación jerárquica, consistente en un acto o una omisión en abuso de poder que daña la autoestima, salud, integridad, libertad y seguridad de la víctima, e impide su desarrollo y atenta contra la igualdad.

Puede consistir en un solo evento dañino o en una serie de eventos

Acoso sexual y hostigamiento sexual

Se expresa en conductas verbales, físicas o ambas, relacionadas con la sexualidad o con fines lascivos.

Acoso sexual

Es en la que, si bien no existe la subordinación, hay un ejercicio abusivo del poder que conlleva a un estado de indefensión y de riesgo para la víctima, independientemente de que se realice en uno o varios eventos.

Hostigamiento sexual

Es el ejercicio del poder, en una relación de subordinación real de la víctima frente al agresor en el ámbito laboral.

Acoso laboral

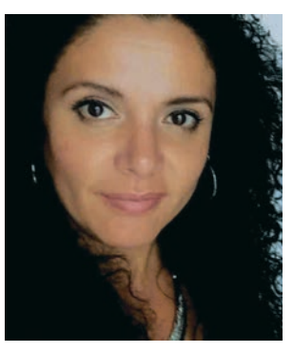
Se presenta en una serie de eventos que tienen como objetivo intimidar, excluir, opacar, aplanar, amedrentar o consumir emocional o intelectualmente a la víctima, causando un daño físico, psicológico, económico y laboral-profesional.

3. Establecer mecanismos de atención que podrá elegir la presunta víctima, entre ellos:
   a. Centro de trabajo, a través de la misma Persona Consejera y/o Comité de Atención y Seguimiento.
   b. PROFEDET.
   c. Centros de Conciliación.
   d. Juzgados Laborales.

4. Establecer los procedimientos que se llevarán a cabo en el centro de trabajo al presentarse una queja de violencia laboral.
5. Propuestas de medidas de protección durante las indagaciones.
   a. Reubicación física o cambio de área de la presunta víctima o de la presunta persona agresora.
   b. En caso de considerarse necesario, licencia con goce de sueldo mientras la denuncia esté en investigación.
   c. Otras medidas que a consideración del Comité coadyuven para la protección de la presunta víctima y del ambiente laboral.
6. Medidas para la Modificación de Conducta.
   a. Cursos y talleres de sensibilización y concientización sobre la igualdad de género y violencia laboral para la persona agresora.
   b. Acciones de sensibilización al área afectada por las conductas de violencia laboral.
   c. Terminación de la relación laboral de la persona agresora.
   d. Otras medidas, que se consideren para la modificación de la conducta, incluyendo el apercibimiento privado a la persona agresora.
7. Resolución del procedimiento.
   a. El Comité de Atención y Seguimiento revisará las evidencias y la narrativa de los hechos para tomar una decisión.
   b. Dicha decisión deberá ser plasmada en un acta de cierre con las medidas de protección y de modificación de conducta establecidas para las partes, además del carácter definitivo y obligatorio de la misma.

El Protocolo incluye también ejemplos de cartas compromiso, formatos, plan de trabajo, seguimiento e incluso un cuestionario de hostigamiento sexual laboral muy completo y una guía para calificarlo.

Así que no hay pretexto para implementar una política de prevención a la violencia laboral, ya que el modelo está muy completo, de fácil acceso y gratuito. mas



* **Violeta E. Arellano Ocaña**
México

Gerente Seguridad Integral
Corporación Interamericana de Entretenimiento (CIE)
15 años de experiencia el campo de Seguridad Integral
varellano@cie.com.mx

SoftGuard desarrolla App Coronavirus Alert

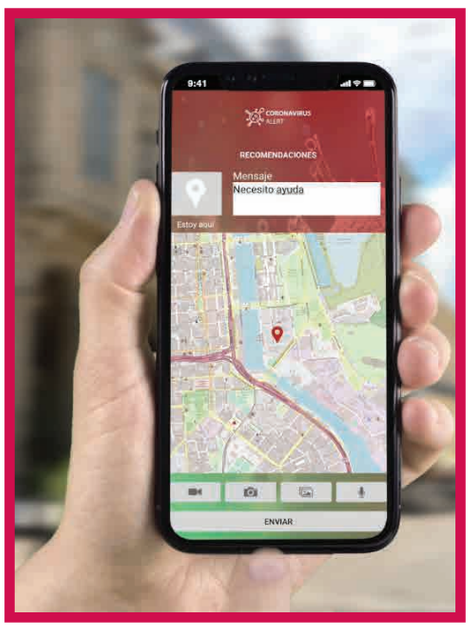
En un contexto de alerta mundial por la emergencia sanitaria de la pandemia, SoftGuard lanzó la App Coronavirus Alert para trackeo o seguimiento de ciudadanos infectados con COVID-19.

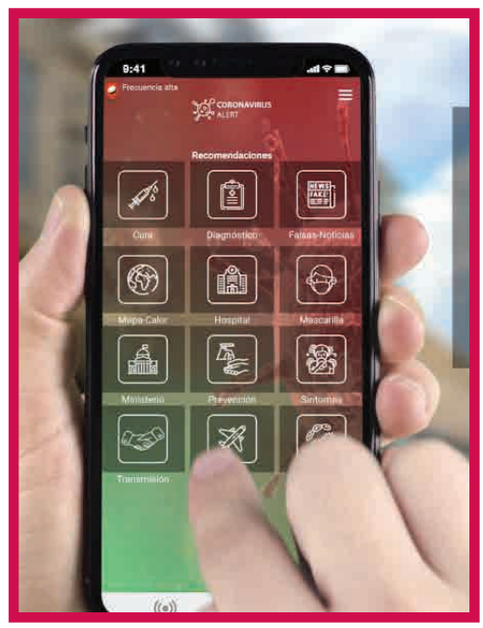
De acuerdo con la compañía, Coronavirus Alert es una aplicación diseñada para reportar y monitorear casos de esta enfermedad para uso municipal y gubernamental. La App permite al ciudadano enviar alarmas por confirmación y portabilidad del virus. La persona puede ser trackeada, reportar síntomas y dar aviso a las autoridades del país en caso de confirmarse la enfermedad en su cuerpo.

Desde esta herramienta, que opera a través de un centro de control, se pueden reportar y monitorear casos de esta enfermedad.

Esta herramienta da cobertura a nivel nacional para reportar síntomas y solicitar asistencia de las autoridades de salubridad. Cada emergencia reportada es acompañada de su posición satelital para que el individuo pueda encontrarse rápidamente.

El sistema cuenta con un centro de control, desde donde se reciben reportes de síntomas y en el caso de recibir alguno positivo, se puede hacer un recall del individuo, localizarlo y prestarle asistencia. El paciente que reporta síntomas por medio de Coronavirus Alert, en lugar de ser trasladado a un centro de salud con el riesgo de transmitir el virus, recibe instrucciones sobre lo que debe hacer y la unidad médica designada indica los protocolos a seguir.





La APP cuenta con 12 botones para informar y dar consejos a la población:

- ¿Qué es el coronavirus?
- ¿Cómo se transmite?
- ¿Cómo se hace el diagnóstico?
- ¿Cuáles son los síntomas?
- ¿Hay una vacuna, medicamento o tratamiento?
- ¿Cómo se previene?
- ¿Cuándo llevar una mascarilla?
- Información para viajeros.
- Noticias falsas.
- Ubicación de hospitales y centros de salud más cercanos.
- Contacto con el ministerio de salud.

#8 La continuidad de la complacencia y el "cuándo" vs el "qué"

Larry Wilson

Hola y bienvenidos nuevamente a la serie "Cambio de Paradigmas"

Descubrir "cuándo", se convierte en el eje de la discusión. A menos que sepamos la hora en que estos momentos sucederán, saber por qué nos lastimamos gravemente no nos ayudará a prevenir el siguiente evento. Por lo tanto, descubrir la parte del "cuándo" es la clave.

Desafortunadamente, por muchos años, el enfoque se ha centrado en "qué" era lo que las personas estaban haciendo y en la cantidad de energía peligrosa que manejaban, lo que es importante, pero no tanto como el cuándo, que es el principal cambio de paradigma aquí.

¿Cuándo será más probable que cometamos ambos errores críticos? Bueno… posiblemente cuando realiza una actividad que ha estado haciendo durante algún tiempo, porque al principio de cualquier tarea donde hay un poco de energía peligrosa y el potencial de lesiones (ver la Figura 1), el nivel de "conciencia" u "ojos y mente en la tarea" es muy alto.

Durante este primer periodo de tiempo, es bastante natural concentrarse en la cantidad de energía peligrosa. Y por lo tanto, es fácil mantenerse enfocado. Incluso puede parecer que será imposible volverse complaciente. Sin embargo, el miedo inicial no dura para siempre. Y durante un periodo de tiempo, llegamos a la primera etapa de la complacencia. Esta sucede sin tomar la decisión de pensar en otra cosa (Figura 1).

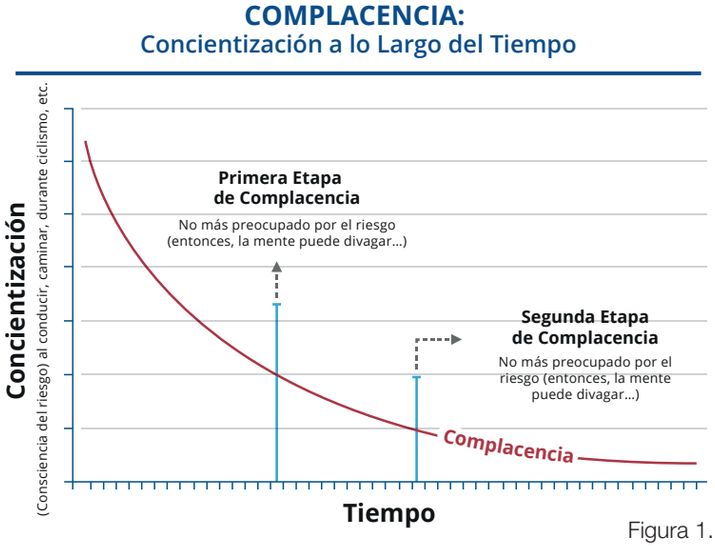


Figura 1.

Por consiguiente, aunque no tenga nada más en que pensar, su mente todavía puede alejarse. Pero si tiene prisa, es posible que sea por una razón. Lo más probable, es que no quiera llegar tarde. Luego, el estímulo se torna más fuerte para empezar a pensar sobre el tema nuevamente. Por esta razón, concentrase en el estado de la prisa es fácil, pues las señales son sencillas de identificar (Técnica de Reducción de Errores Críticos #1). Es bastante simple darse cuenta de que usted se está moviendo más rápido o haciendo demasiadas cosas a la vez. Lo que no es tan factible, es que la razón por la cual tiene prisa o las consecuencias de llegar tarde, suelen ser más persuasivas, para hacer que su mente no esté en la tarea en ese momento.

Lo mismo es válido para la frustración. Cuando está realmente enfurecido, es factible reconocerlo, así que puede concentrarse en el estado de la desilusión, respirar profundo, volver al momento y hacer un esfuerzo para mantener sus ojos y su mente en la tarea al conducir (TREC#1).

Sin embargo, si la etapa es intensa, usted puede reconocerla fácilmente. Cuando está realmente fatigado, es fácil detectarla. Pero el problema es que, cuando está solo un poco cansado, no es tan simple reconocerlo, y todos nosotros nos cansamos a lo largo del día, así que no es inusual. Pero si se le agrega un poco de prisa y frustración a la fatiga, la combinación de todos podría ser suficiente para causar errores, lo que probablemente causaría aún más desengaño y más prisa.

En consecuencia, el concepto de concentrarse en los estados, puede parecer fácil de entender: como cuando usted está realmente cansado y confiado, puede ser muy sencillo tener períodos en los que su mirada se cierre por uno o dos segundos o tres… Y obviamente, si usted está conduciendo con sus ojos cerrados, o peor, cuando estuvo dormido por algunos segundos, es fácil entender el concepto de estar momentáneamente indefenso.

Con el paso del tiempo, llegamos a la segunda etapa de la complacencia. En este momento, ya no hay más miedo interno. Sin embargo, si casi nos choca un camión de carga, entonces empezaremos a pensar en el riesgo nuevamente. Pero eso exigió un "estímulo externo". Otra cosa que es interesante sobre la segunda etapa es la forma como impacta en nuestra toma de decisiones. Y también es bastante accesible reconocerla, porque probablemente algunas personas le dirán algo como: "Yo he estado haciendo esta actividad desde hace 20 años y todavía no me he lesionado". Y debido a que todavía no se ha lastimado, es posible que no esté motivado a cambiar.

En la segunda etapa, preocupará por el por qué tienen prisa o qué les sucederá si llegan tarde, en quién o qué los frustra o cuándo pueden hacer una pausa. Y es este alto nivel de complacencia lo que puede afectar sus decisiones con los ojos puestos en la tarea. Pueden decidir alejar la mirada de la carretera para recoger su teléfono o para sacar algo de la guantera, y ahora tiene otro "momento de vulnerabilidad". Y aunque estos instantes, pueden suceder con mayor frecuencia a medida en que alguien pasa a la segunda fase de la complacencia, cuando su mente está mayormente lejos de la actividad, es probable que no lo noten… a menos que algo malo acontezca.

Recuerdo la primera vez que ingresé al negocio de la protección. Estaba vendiendo videos de seguridad y no podía entender por qué seguía escuchando que "los jóvenes se lastiman más que las personas mayores… pero son las personas de ma-

yor edad las que mueren". Y no podía entender el por qué, ya que también era de conocimiento común que los inviduos se lastimaban porque no tenían un entrenamiento de resguardo. Así que, no podía comprender por qué los trabajadores bien entrenados, sufrían tantas lesiones graves. Y se percibía que alguien que hubiera conocido en la gerencia o en la profesión de seguridad, tampoco tuviera una buena explicación.

Pero en retrospectiva, todo es muy simple: más tiempo o repetición significa más complacencia, y más de ésta supone más momentos vulnerables cuando los ojos y la mente no están en la tarea. Entonces, cuando el estado es intenso, descubrir la parte del "cuándo" no es difícil debido a la facilidad de reconocer la etapa. Pero si ésta no es intensa o si hay más de uno involucrado, entonces esto podría no ser muy fácil de reconocer. Y si los cuatro estados están inmiscuidos puede ser muy difícil reconocerlo y concentrarse para evitar el error.

Anticipando el error

Lo importante aquí es que reconozca que está lidiando con un poco de frustración y de fatiga, lo que podría aumentar el riesgo de que pueda decir algo negativo a un compañero de trabajo o cliente. Entonces, tenemos una herramienta sencilla que nos ayudará a reconocer las combinaciones de estados, incluso si las etapas individuales por sí mismas no son intensas. Todo lo que tenemos que hacer ahora es tratar de determinar cuándo probablemente estaremos en estos estados, o cuándo permaneceremos en más de uno al mismo tiempo.

La mejor persona para responder a esta pregunta es usted (o yo) porque sabemos cuándo nos fatigamos. Identificamos quién o qué normalmente nos frustra, lo que nos apresura, y cuáles serían los peores escenarios desde el punto de vista del error más costoso que podría cometer, o el que podría hacerlo perder más tiempo, etc.

Aunque la equivocación o el error crítico siempre son inesperados, las etapas que los causan no lo son. Podemos anticipar cuándo y dónde estaremos en uno o más de los cuatro estados. Y si programa una alarma y luego evalúa su fase en ese momento, aunque sea solo un poco de prisa, o un poco de frustración combinada con la complacencia, usted estará mucho más consciente y mucho menos propenso a que sea "atacado con su guardia baja".

Sí, esto requiere un poco de esfuerzo, pero no toma mucho tiempo y seguramente no cuesta dinero. Sin embargo, si hace el esfuerzo de hacerse estas preguntas y luego establece una alarma para evaluar su estado en esos momentos, o lo instaura en la rutina previa al turno de trabajo, podrá minimizar o evitar muchos de estos momentos de vulnerabilidad.

¿Cuándo tendremos estos momentos de vulnerabilidad, donde nuestros ojos y mente no están en la tarea? Y si piensa en ello, o en todas las lesiones que usted ha experimentado, probablemente habrá un patrón mucho más fuerte en términos de "cuándo", contrario al modelo que había para el "qué". m/s

Próxima edición:
Decisiones críticas Parte 1 – Riesgo normal Vs. Excepcional

Cargo Week Americas | expo carga

SE UNE AL GRAN EVENTO

SITL™ AMERICAS

Transport & Logistics Innovation Week

PRESENTADO POR ups

16.17.18 JUNIO 2020

CENTRO CITIBANAMEX, CDMX

¡VIVE CON NOSOTROS LA 1ª EDICIÓN DE SITL AMERICAS!

Un lugar de encuentro para usuarios logísticos y profesionales de la industria, con lo último en tendencias y los gurús que están marcando el futuro logístico.

Lionel van der Walt
President & CEO, The Americas at Pay Cargo LLC

PANEL: ¿Cómo la inteligencia artificial y el machine learning están evolucionando la logística?
Jueves 18 de junio
13:15 - 14:15 h

Karl McDermott
Global Head of Business Development, Morpheous.Nertwork
Presentado por ISCEA

Aplicación de tecnologías emergentes: los secretos del blockchain

Jueves 18 de junio
16:30 - 17:30 h

Fernando de Mateo
Coordinador del Diplomado sobre Negociaciones Comerciales Internacionales en el Colegio de México y Ex Embajador ante la OMC

Política Comercial Exterior de México al 2024

Martes 16 de junio
12:00 - 13:00 h

Obtén tu pase de acceso TOTAL SIN COSTO
www.sitlamericas.com

Presentado por ups

Patrocinador Zona demo EnerSys Power Full Solutions

Más información: 55.8852.6000
www.sitlamericas.com

Síguenos en:

Sprinter 5.5t

Seguridad e innovación en un solo vehículo

La firma Mercedes-Benz Vanes presenta la Sprinter en su versión 5.5t de peso bruto vehicular que destaca por su mayor capacidad de carga, seguridad, innovación y tecnología, disponible en Cargo Van, Chasis Cabina y Chasis doble Cabina.

Manteniendo el liderazgo en el segmento de Vanes, Sprinter ahora llega con la versión de 5.5t de peso bruto vehicular que destaca por su seguridad, innovación y tecnología, lista para conquistar nuevos segmentos de mercado.

Tiene una capacidad de carga de 3,068kg hasta 3,422kg y se encuentra disponible tanto en Cargo Van, Chasis Cabina y Chasis doble Cabina.

Esta nueva gama de Mercedes-Benz Vanes, cuenta con los más innovadores sistemas de seguridad como lo son el Adaptive ESP (ABS, EBV, BAS, ASR.), Asistente de Viento Lateral, Asistente de Atención y el Asistente de Frenado Activo que ayudan a reducir la posibilidad de accidentes con los vehículos que se encuentran enfrente y con peatones cruzando la vía. Opcionalmente, se tiene disponible como equipo de seguridad activa; el control de ángulo muerto y asistente activo de conservación de carril.

Sprinter Cargo Van marca la pauta en cuanto a la capacidad de transporte: gracias a la ampliación de la gama a un peso bruto vehicular de 5.5t. Ésta tiene dos longitudes disponibles: mediana y extra larga.

De acuerdo con la firma, el modelo Cargo Van Mediana de 5.5t posee una capacidad volumétrica de 9m³ y 10.5m³ y un tonelaje de carga de 3.103kg y de 3,068kg, respectivamente, siendo en México la única van integral en su tipo con este volumen de carga.

La Sprinter Cargo Van Extra Larga de 5.5t alcanza una capacidad volumétrica de 15.5m³ en la versión de techo alto, y de 17m3 con el equipo opcional de techo súper alto, y una capacidad de carga de 2,862kg y 2,827kg, respectivamente, combinando una mezcla perfecta entre un gran volumen y una extraordinaria capacidad de mercancía.

Cabe destacar que la Sprinter Cargo Van es un vehículo desarrollado para aquellas operaciones que buscan una unidad integral con una gran capacidad de carga y que gracias a sus variantes en longitudes se adaptan a cualquier negocio. Algunas de las aplicaciones donde se puede usar son: construcción, food truck, refrigerado, refresquero, entre muchas otras

Sprinter Cargo Van marca la pauta en cuanto a la capacidad de carga: gracias a la ampliación de la gama a un peso bruto vehicular de 5.5t con dos longitudes disponibles: mediana y extra larga.

aplicaciones que requieren un vehículo con alta capacidad de carga.

Las posibilidades de los chasis Sprinter son asombrosas: gracias a sus nuevas variantes de 5.5t de Peso Bruto Vehicular que brinda soluciones que pocos pueden alcanzar.

Sprinter Chasis Cabina tiene dos longitudes disponibles, mediana y larga que permiten la instalación de cajas de hasta 24m³ con una capacidad de carga de 3,422kg y de 3,379kg, respectivamente. Ambas versiones destacan por sus soportes extendidos de espejos laterales que permiten tener una gran visibilidad con cajas de hasta 2,300mm de ancho.

Además, es un vehículo desarrollado para aquellas operaciones que buscan la combinación de una gran capacidad de carga, tecnología y seguridad con una unidad que se adapte a cualquier terreno en México. Esta nueva gama es ideal para ese segmento de carga como lo es el refresquero, grúa-plataforma, caja seca o refrigerada, redilas, gasero, food truck, entre muchas otras.

Por otra parte, la Sprinter Chasis Doble Cabina de 5.5t cuenta con dos longitudes, mediana y larga, con una capacidad de carga de 3,234kg y de 3,187kg, respectivamente. Al igual que la cabina sencilla, esta gama fue creada con soportes extendidos de espejos laterales, lo que permite tener una caja de hasta 2,300mm de ancho. Esta variante de Sprinter es ideal para quienes buscan llevar hasta siete pasajeros en el área de cabina combinado con una gran capacidad de carga, enfocado a soluciones como: bomberos, vehículos de emergencia, vehículos de seguridad, caja seca o refrigerada, redilas, construcción, entre muchas otras.

Como equipo opcional para esta gama de producto, se dispone de tomas de fuerza en transmisión y parte frontal del motor.

Sprinter Chasis Cabina es un vehículo desarrollado para aquellas operaciones que buscan la combinación de una gran capacidad de carga, tecnología y seguridad con una unidad que se adapte a cualquier terreno en México.

Sprinter Chasis Doble Cabina es ideal para soluciones como: bomberos, emergencia, vehículos de seguridad, entre muchas otras.

La toma de fuerza en la parte frontal del motor permite usar un compresor de agente frigorígeno adicional para la instalación de un sistema de refrigeración o congelación en la parte trasera del área de carga en las versiones de chasis cabina o cargo. La potencia máxima que puede aprovecharse es de 8 kw.

La toma de fuerza en la transmisión se ofrece con 2 variantes:

- Toma de fuerza con brida que gira en sentido horario, visto en el sentido de la marcha que permite el accionamiento de un equipo adicional, por ejemplo; una bomba hidráulica en la aplicación de vehículos de reparto de gas. La toma de fuerza tiene una potencia continua máxima de 28 kw a 2526 rpm y un par motor máximo de 140 Nm a 1200 rpm.
- Toma de fuerza sin brida que gira en sentido horario visto en el sentido de la marcha que permite el accionamiento de una bomba hidráulica; por ejemplo, bomba hidráulica Meiller 265/1 para aplicaciones de grúas de plataforma, telescópicas o con canastilla de elevación.

La toma de fuerza tiene una potencia continua máxima de 28 kw a 2,526 rpm y un par motor máximo de 140 Nm a 1200 rpm.

Toda esta gama de Sprinter de 5.5t tiene un motor a diésel Mercedes-Benz de 2.2l de 4 cilindros, con 163 HP y un torque de 280 lb ft, así como con una trasmisión manual de seis velocidades como equipo de serie y una transmisión automática de siete velocidades como equipo opcional. mS

Síguenos:
Mercedes-Benz Vanes Mx @mbvanesmx /mercedes-benzvanesmx
www.mercedes-benz.com.mx/vans

Mercedes-Benz

Escanea el código QR y regístrate para obtener más información.

Precios sugeridos de venta desde:
Cargo Van: $813,900
Chasis cabina: $715,900
Crew-Cab: $729,900
PSV para las nuevas versiones de Sprinter 5.5t, año modelo 2021 (no incluyen equipo opcionales, ni carrocerías)

Estrategias y equipamiento

Seguridad logística en tiempos de pandemia

Rosa María Salas / @revmasseguridad

Ante un escenario nacional o internacional de grandes magnitudes como un desastre natural, conflicto bélico o pandemia, ¿qué sucede con la proveeduría de medicamentos, alimentos o artículos de primera necesidad si un eslabón de la cadena de suministros falla?

Esta es una de las grandes interrogantes que se ha formulado la población con motivo de la pandemia que se vive actualmente del COVID-19. Aquí, la logística y el transporte juegan un papel determinante para mantener el abasto de insumos y servicios, desde los centros de distribución, vía carretera, hasta el anaquel de las tiendas departamentales o puntos de abastecimiento, a fin de poder llevar los productos hasta la mesa del consumidor final.

Cabe mencionar que más del 80% de las mercancías que se entregan en México se mueven por transporte carretero. De acuerdo con datos de la Secretaría de Comunicaciones y Transportes (SCT), en territorio mexicano, el traslado de carga representa el 3.2% del Producto Interno Bruto (PIB), además contribuye con el 50% del PIB logístico, lo que equivale al 6.5% del total.

Respecto de cuánto impacta el costo logístico en una empresa que trabaja con un modelo de este tipo y de distribución primaria de grandes volúmenes, éste puede ser menor al 3%; mientras que en una organización que mueve distribución secundaria, puede llegar hasta el 4% de sus ingresos. El costo total logístico incluye transporte primario, distribución de última milla y almacenamiento, reveló José Ruiz, socio de Asesoría en Cadena de Suministro y Compras de KPMG en México.

Para Salvador Saavedra, especialista en logística de la consultora Tecnología en Transporte y socio fundador de la Alianza Nacional por la Seguridad Vial (ANASEVI), en tiempos de crisis la logística desempeña no sólo una función importante, sino que ésta se mejora debido a que las empresas que se dedican a prestar estos servicios, deben reaccionar de manera rápida para atender los cambios en los patrones de consumo de los ciudadanos. Los riesgos son enseñanzas para poder mejorar los procesos logísticos en un futuro, apuntó.

En entrevista con **Más Seguridad**, Samuel Cacho Cámara, director de Operaciones de CR Nova Security; Leonardo Rosillo Cataño, director de Operaciones de Grupo Corporativo Solcat; y Víctor Manuel Presichi Amador, presidente de la Asociación Nacional de Empresas de Rastreo y Protección Vehicular (ANERPV), describen las estrategias que ejecutan en acontecimientos difíciles y los desarrollos tecnológicos que existen en el mercado para contar con un transporte seguro, el cual es uno de los eslabones clave en la supply chain del país.

En una crisis como el COVID-19, sólo aquellas empresas que estén mejor preparadas y que su cadena de suministro sea más flexible para moverse rápidamente, atiendan nuevos comportamientos de demanda en los diferentes canales y generen estrategias de seguridad, saldrán favorecidas

Cadenas de suministro disruptivas

Actualmente, la logística en la República Mexicana y en el mundo se ha visto severamente afectada con la emergencia sanitaria, sobre todo por la incertidumbre en el surtimiento de insumos, materias primas e incluso de componentes y partes de tipo industrial, “ya que al estar prácticamente todas globalizadas, la primera disrupción es cuando el proveedor tiene restricciones de actividades y la búsqueda de alternativas es más compleja, pues las mercancías no pueden ser embarcadas hacia una región del mundo, o bien se quedan paradas en algún punto y la cadena que se tenía trazada se rompe”, indicó Salvador Saavedra.

José Ruiz refirió que crisis como la del COVID-19 genera un replanteamiento en la forma en cómo las organizaciones hacen negocio para mantener su continuidad, incluso, su supervivencia. El impacto va desde la cadena de valor, el abasteci-

Foto: Designed by kjpargeter / Freepik

miento, compras, hasta la comercialización y entrega de los productos, afirmó.

Cuando ocurre una catástrofe una de las primeras cosas que se deben cuidar es la seguridad de la población. En opinión del especialista de Tecnología del Transporte, con el coronavirus se pensó en cómo mantener seguras a las personas que trabajan en toda la cadena logística, con higiene y sanas distancias, además de las empresas de traslado y logística y quienes conducen vehículos de carga con el objetivo de implementar las medidas sanitarias correspondientes.

El experto de KPMG en México complementó que hoy la seguridad logística es un reto para el país. Y aunque dijo que ya lo era antes del coronavirus, consideró que este tema se puede volver más crítico para el transporte, por lo que dependerá de cómo se visualicen los factores macroeconómicos del país y qué acciones se tomen a nivel de gobierno federal.

Las empresas de rastreo satelital, de seguridad privada, proveedores tecnológicos y de servicios de logística, así como asociaciones, se mantienen unidos contra el coronavirus

En ese sentido, José Ruiz aconsejó a las compañías logísticas a buscar una proveeduría local para, por un lado, mitigar los impactos del tipo de cambio; y por otro, para tener a la mano proveedores estratégicos, confiables, cercanos al punto de consumo y que ayuden a ganar agilidad en la cadena.

Traslados en México

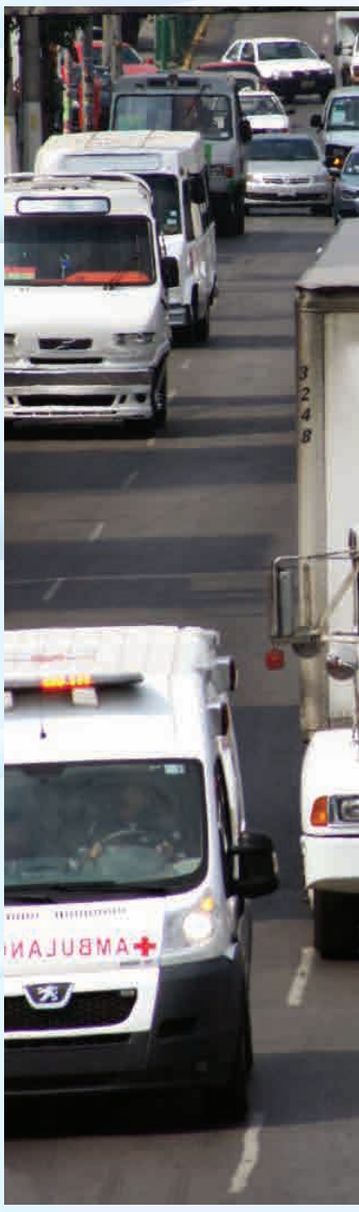
El transporte, explicó Salvador Saavedra, es una de las pocas actividades que se mantiene activa pese a la coyuntura por la que atraviesa el país y no para mientras haya demanda de abastecimiento. Precisó que ésta tampoco trabaja al 100%, ya que las mercancías que más se exportan, que son vehículos y electrodomésticos, están totalmente detenidas y, por ende, esa demanda de entregas que se hacen vía carretera para posteriormente ser llevadas a puertos marítimos para su envío, está parada.

Antes de la pandemia y el confinamiento de los habitantes, señaló Saavedra, la delincuencia tenía muchos puntos donde atacar a la industria del transporte. Sin embargo, este sector ha trabajado en conjunto con las autoridades de los tres órdenes de gobierno para tener tramos carreteros videovigilados y dar respuesta rápida ante cualquier ilícito. El reto, dijo, es cómo combatir la delincuencia con o sin pandemia.

De acuerdo con la Cámara Nacional del Autotransporte de Carga (CANACAR), cada año el robo tiene un impacto económico de 92 mil millones de pesos, lo que representa aproximadamente el 0.5% del PIB nacional.

Con la alerta sanitaria, que ha provocado que gran parte de la fuerza laboral se mantenga en confinamiento y se contraiga la economía, no se descarta un incremento en los robos de mercancías, las cuales, señaló Leonardo Rosillo, se van para un "mercado negro" en donde se ofertan a un menor precio.

Desde el punto de vista de Víctor Presichi, la pandemia obliga a todos los actores de la cadena de suministro, y en específico a la industria del transporte, a prepararse y tomar otras medidas ante la inminente escalada de disturbios y robo por gente oportunista, así como por delincuentes que tampoco descansan.



Designed by macrovector / Freepik

El representante de la ANERPV indicó que como consecuencia de la idea equívoca en la gente de un posible desabasto de productos de primera necesidad, las tiendas de autoservicios se vieron abarrotados por compras masivas, lo cual generó un pico de demanda excedida en los productores, en el transporte y, por ende, una gran actividad de logística y de distribución.

Por su parte, Samuel Cacho destacó que las custodias se verían afectadas; sin embargo, dijo que con el apoyo y sinergias de las autoridades, además de diversas asociaciones de seguridad, la CANACAR, y a través del monitoreo del GPS, se organizaron por grupos de negocios, abarroteros, tiendas de autoservicio y transportistas para reforzar la logística.

Leonardo Rosillo añadió que ante la ola de saqueos a tiendas departamentales y los robos en carretera, la industria de transporte incrementó el trabajo y la colaboración con compañías relacionadas con logística, almacenes, centros de distribución y propietarias de mercancía de alto riesgo.

Innovación en camino

En nuestro país, la industria del transporte se compone de sistemas tecnológicos como rastreo satelital, custodias físicas y virtuales, controles de acceso y videovigilancia. Todos tienen el objetivo de supervisar procesos industriales y/o logísticos, garantizar la trazabilidad de los envíos, gestionar y optimizar stocks, e inhibir los robos tanto de productos como de vehículos.

Para la protección en carretera y el seguimiento o tracking de las unidades, mercancías, valores y el personal que participa en el proceso de distribución, es importante contar con los sistemas que permiten un monitoreo en tiempo real. Sin embargo, desde el enfoque del presidente de la ANERPV no es suficiente que los usuarios cuenten con las herramientas, sino que también las exploten para obtener la información y hacer una mejor toma de decisiones.

El director de Operaciones de CR Nova Security, contextualizó que al equipo de GPS en sí no se le han hecho muchas innovaciones, lo que ha avanzado, son las mejoras en su software con la implementación de algoritmos que permiten alertar de manera oportuna, múltiples situaciones que pasan durante el trayecto, a fin de que el operador pueda reaccionar de manera más rápida.

Las grandes compañías, detalló el ejecutivo, cuentan con estos avances en los equipos, mientras que las pequeñas aún utilizan dispositivos básicos, incluso ellas mismas monitorean sus propias unidades.

Al respecto, Leonardo Rosillo indicó que las empresas deben valorar el uso de otros sistemas o aditamentos, además del GPS, para tener los resultados adecuados en materia de seguridad. Ejemplificó que es ideal utilizar botones de pánico, paros de motores automatizados, activación de claxon, sensor en puertas, chapas magnéticas, entre otros.

Además, aconsejó constatar que los sistemas que se contratan, adicionales al GPS, sean de proveedores certificados y confiables. Lo anterior, no significa que no habrá ningún hurto, sin embargo, sí se minimiza el riesgo.

Para CR Nova Security, el elemento más eficiente en la industria transportista a la fecha sigue siendo la custodia física, ya que, en ésta se combinan tanto el guardia como lo virtual, hay mayor visibilidad y permite una reacción más rápida en caso de un ilícito o de un problema con el operador.

El director de Operaciones de Grupo Corporativo Solcat informó que la custodia virtual ha tenido un crecimiento importante en su demanda y la calificó como una excelente herramienta siempre y cuando se haga un monitoreo activo virtual.

Acerca del papel que juegan los centros de monitoreo, el representante de la ANERPV resaltó que éstos son un factor importante para el transporte seguro en todos sus aspectos. Por lo tanto, consideró que una buena capacitación del monitorista es decisivo para que identifique de manera oportuna cualquier situación y actúe en consecuencia; la interacción humana, no se puede dejar a un lado con las autoridades a la hora de atender una situación de crisis.

Víctor Presichi adelantó que la controlada vía remota, tendrán mayor demanda, y eso va a permitir visualizar no sólo la ubicación de los vehículos, sino también lo que sucede dentro de cabina y en la carretera. La inteligencia artificial, abundó, permitirá identificar si el conductor está cansado, si parpadeó o si realizó cualquier otro movimiento que pudiera significar un riesgo.

La telemetría, complementó Presichi Amador, es fundamental y es una excelente herramienta, no solo por el control de la seguridad, sino para la reducción de riesgos de la cadena de suministro. No obstante, existen muchas oportunidades de mejora para el transportista con los nuevos dispositivos y plataformas que permitan asegurar que el operador cumple con sus viajes establecidos y para que pueda calificarlo en entregas, consumo de combustible, etc., y todo en tiempo real.

Acciones en todos los eslabones

Para la ANERPV, a fin de que se procure un proceso logístico en carretera eficiente para todos sus actores, es fundamental preservar la seguridad y es responsabilidad del Estado brindar las condiciones, pero aclaró que la iniciativa privada debe ser coadyuvante de la autoridad y tomar las medidas preventivas, sin importar el giro en el que se encuentren las compañías.

Este organismo cuenta con la plataforma Centinela para la vigilancia y monitoreo satelital en tiempo real. Desde un centro de control se realiza el rastreo de unidades para su posible recuperación.

CR Nova Security brinda servicios de custodia física y virtual, y actualmente a través del monitoreo GPS, ofrece valor agregado tanto en la logística como en seguridad para la gestión del transporte. También cuenta con equipos de rastreo satelital para aquellas organizaciones que desean hacer su propio monitoreo.

Para Grupo Corporativo Solcat, los usuarios de transporte deben hacer una actualización de su seguridad logística con el objetivo de revisar las rutas en donde existen mayores puntos de inseguridad y llevar a cabo un resguardo de los camiones en caso de siniestro. Lo anterior, se logra con un trabajo de campo que consiste en auditorías a las unidades y a las carreteras para que el monitoreo virtual realmente funcione.

Esta empresa posee un desarrollo propio denominado Smart Shild, que es un módulo que va conectado a la unidad de transporte y fue pensado para evitar errores humanos, ayudar al usuario a autoproteger sus camiones y mercancías y, por consiguiente, mitigar los robos.

Los transportistas, compañías de rastreo satelital, empresas de seguridad privada, proveedoras de tecnología y servicios de logística, no claudicarán frente a la inseguridad y la extensión de la pandemia en México. Todos están conscientes de la urgencia de fortalecer protocolos de seguridad internos, evitar horarios más críticos en cuestión de asaltos, no circular por territorios donde la cobertura policiaca es más frágil y, sobre todo, hacer uso de la tecnología.

Tanto la industria del transporte y rastreo satelital, así como los centros de monitoreo siguen operando, quizá no de manera normal, pero darán seguimiento permanente y activo en coordinación con autoridades. La consigna es clara: adaptarse a las condiciones de operación y estar preparados para enfrentar la emergencia, hasta sus últimas instancias. m/s


Víctor Manuel Presichi Amador, presidente de ANERPV


Samuel Cacho Cámara, director de Operaciones de CR Nova Security


Leonardo Rosillo Cataño, director de Operaciones de Grupo Corporativo Solcat


José Ruiz, socio de Asesoría en Cadena de Suministro y Compras de KPMG en México


Salvador Saavedra, especialista en logística de la consultora Tecnología en Transporte

SEA donde SEA

TE PROTEGEREMOS

1. Protección a Ejecutivos
2. Protección de bienes inmuebles
3. Protección traslado de mercancía
4. Capacitación en uso y manejo de armas de fuego y protección a funcionarios
5. Monitoreo de Cámaras, controles de accesos y alarmas a través de nuestro C4
6. Asesoría en manejo de crisis
   Asesoría en estrategias de seguridad patrimonial
7. Seguridad del Personal
   Centro de Evaluación y Confianza
8. Administración de proyectos de infraestructura de sistemas electrónicos de seguridad

VENTAS | 662.18.50 | EXT. 147

Seguridad privada aplica protocolos ante contagios y saqueos

Redaccion / @revmasseguridad

La Asociación Mexicana de Empresas de Seguridad Privada (AMESP), expresó su total apoyo y respaldo a las medidas que tome la autoridad sanitaria del país para proteger y auxiliar a la población durante la emergencia que vive México, a causa del coronavirus COVID-19.

Es por ello que las compañías asociadas a la AMESP empezaron a laborar en sectores estratégicos como los sistemas aeroportuario nacional, bancario, de abastecimiento y otros que no pueden detener su operación.

Esta asociación, integrada por las principales empresas de seguridad privada del país y miembro de Asociaciones de Seguridad Unidas por un México Estable (ASUME), colabora con las autoridades sanitarias en la aplicación de los protocolos aprobados en este tipo de instalaciones. De esa forma, apoya a la población con personal y equipo para auxiliarla.

Asimismo, y en forma paralela, se implementaron estrategias con algunos clientes para reforzar sus instalaciones ante saqueos en tiendas de abastecimiento, robos en comercios, fugas en prisiones y otro tipo de expresiones criminales.

Tiene también a disposición de los interesados, 375 expertos en plataformas digitales para consulta a fin de ofrecer las mejores prácticas y escenarios en materia de seguridad

Junto con ASUME, ha llevado a cabo tres sesiones de webinar colaborativos con sus asociados con el tema de Continuidad de la operación y Ayuda Mutua para atender la contingencia. Los integrantes del Comité Directivo Nacional de ASUME, del cual forma parte AMESP, tiene comunicación con el Secretario de Protección Ciudadana de la Ciudad de México para definir la forma de colaboración con esta parte del sector privado de la seguridad.

Ambos organismos trabajan con autoridades federales y de algunos estados, para fortalecer los esquemas de coordinación e intercambio de información a fin de garantizar un mejor servicio a los usuarios de servicios de seguridad privada.

Directivos de la AMESP consideran que la crisis sanitaria y otros factores externos como el tipo de cambio y la depreciación del petróleo, reducirán drásticamente la actividad económica nacional generando condiciones adversas en algunos grupos de la población que se quedarán sin alternativas de trabajo. Lo anterior pudiera generar un incremento en cierto tipo de delitos y actividades crimínales como el robo, secuestro y extorsión.

Empresas apoyan áreas estratégicas como los sistemas aeroportuario y bancario, en especial el traslado de valores.

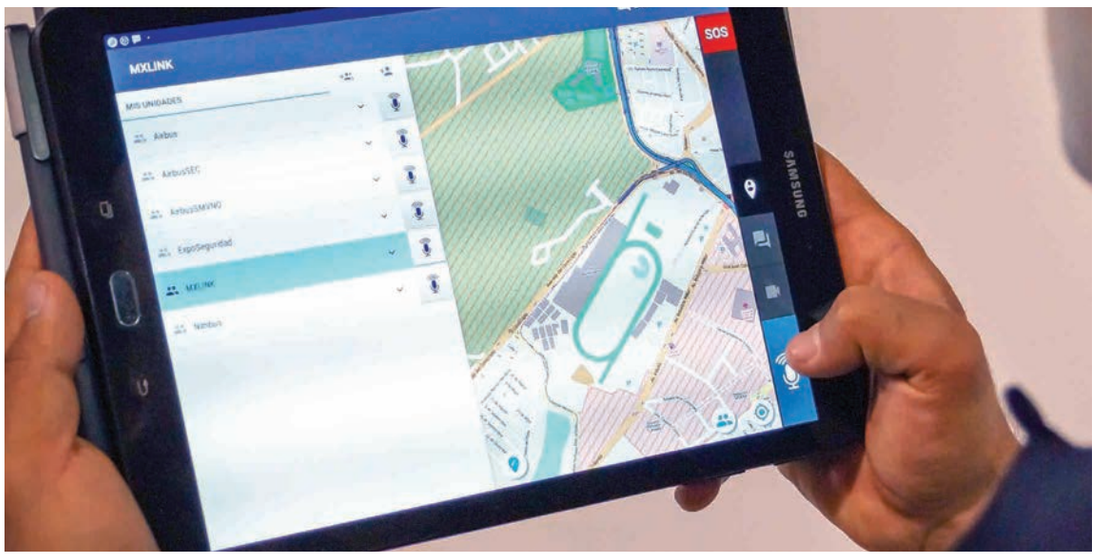
Asociados de la AMESP reportan el aumento de la demanda por parte de sus clientes en tecnologías para fortificar los filtros y controles de accesos con equipo termográfico para medición de temperatura; reforzamiento de guardias de seguridad y escolta de vehículos; blindaje de fachadas y apuntalamiento de perímetros, así como investigaciones y consultorías orientadas a la gestión, protección y resilencia de esta crisis por diversas corporaciones.

La asociación aseguró que se mantiene atenta a las medidas que dispongan sus clientes, autoridades sanitarias y de seguridad pública, para auxiliar, en la medida de sus posibilidades y capacidades, su aplicación en beneficio de la ciudadanía.

Este organismo tiene como asociados a las compañías nacionales e internacionales más grandes y representativas de la seguridad privada, que actúan en el territorio nacional, en todas las modalidades previstas como monitoreo de alarmas, guardias intramuros, traslado de valores, seguridad electrónica, logística y aeroportuaria, protección a ejecutivos, consultoría, entre otros.

En Chihuahua

AIRBUS actualiza radiocomunicación de seguridad pública



La firma incorporó banda ancha para la seguridad pública; con esto, el estado inició su migración a Tetrapol IP, lo que permitirá una comunicación a través de transmisión de voz, datos, mensajería multimedia, video en tiempo, etc. Junto con Chihuahua, ya son 12 las entidades que actualizan sus redes Tetrapol al protocolo IP

Airbus SLC en México inició la modernización de la red estatal de radiocomunicación. A través de esta migración, el gobierno del estado de Chihuahua ratifica su confianza en la tecnología de protocolo abierto Tetrapol, provista por la empresa Airbus que soporta las comunicaciones de la Red Nacional de Radiocomunicación.

La compañía indicó que la red se beneficiará de los servicios de banda ancha de misión crítica con tecnología LTE provistos por MXLINK, el primer operador móvil virtual de seguridad en su clase en México y América Latina. De esta forma, las fuerzas de seguridad podrán comunicarse a través de transmisión de voz, datos, mensajería multimedia, video en tiempo real y geolocalización de forma totalmente segura uno a uno y/o en grupos.

Al respecto, la empresa señaló: “Entre los muchos beneficios adicionales de MXLINK están los diferentes módulos de la suite Secure Software Solutions (3S) de Airbus SLC, como el Sistema de Seguimiento de Actuaciones Policiales (SSAP), que permite monitorear la participación de las policías en su calidad de primer respondiente, clave para un correcto proceso de judicialización del delito. El SSAP da la posibilidad generar mecanismos de control y supervisión y así garantizar el buen actuar del policía, desde su llegada hasta la integración del expediente para el Ministerio Público”.

Por su parte, el Informe Policial Homologado (IPH), brinda el acceso digital a este formato, creado conforme a la normatividad expedida por el Consejo Nacional de Seguridad Pública. De esta forma, se reducen los tiempos y la probabilidad de errores, a partir de una interfaz intuitiva y de fácil comprensión que guía al usuario por medio de un menú de opciones, evitando el uso de papel y sustituyendo al llenado manual del informe.

Además, el gobierno de Chihuahua aprovechará las ventajas de la estación móvil MBSc de Airbus SLC, que reforzará y ampliará la cobertura donde sea necesario. La firma dio a conocer que la infraestructura móvil permite hacer despliegues con el beneficio de ahorros en tiempo, costos de infraestructura y energía, permitiendo a la red ampliarse en el momento y lugar más conveniente.

Al final del proceso, la red alcanzará una cobertura del 93% de la población del estado con una total integración a los Centros de Atención de Llamadas de Emergencias 911, además de garantizar las comunicaciones críticas de la operación y despliegue policial de las instancias de seguridad pública de los tres órdenes de gobierno.

Airbus SLC informó que, junto con el gobierno de Chihuahua, ya son 12 los estados que actualizan totalmente sus redes Tetrapol al protocolo IP. Aguascalientes, Baja California Sur, Colima, Hidalgo, Jalisco, Morelos, Nayarit, Querétaro, Quintana Roo, Tamaulipas y Tlaxcala.

Lo anterior, precisó la empresa, permite dar cabal cumplimiento a lo establecido en la Estrategia Nacional de Seguridad Pública definida por el actual gobierno federal. Adicionalmente, 14 entidades operan actualmente de forma híbrida: Baja California, Campeche, Chiapas, Durango, Estado de México, Guerrero, Nuevo León, Oaxaca, Puebla, Sinaloa, Tabasco, Veracruz, Yucatán y Zacatecas.

SEDENA y SEMAR convocan a médicos contra COVID-19

Las secretarías de la Defensa Nacional (SEDENA) y Marina-Armada de México (SEMAR) convocaron a profesionales de la salud, mano de obra calificada y especialistas en sanidad para apoyar en la atención de la emergencia de salud ocasionada por el COVID-19.

A través de un comunicado, SEDENA lanzó la solicitud bajo el lema: "¡MÉXICO TE NECESITA!", e informó que se lleva a cabo el proceso de contratación de personal y mano de obra calificada (civiles y militares en situación de retiro) en las siguientes áreas:

- Médicos especialistas (medicina crítica, interna, neumología, cardiología y urgencias).
- Médico general.
- Enfermeras (os) especialistas (medicina crítica en adultos, pediátricos y neonatos).
- Enfermera (o) general.
- Administrativos (capturistas y secretario [a]).
- Servicios generales (personal de intendencia).

Quienes deseen ser contratados deberán cumplir con los siguientes requisitos:

1. Médicos especialistas y generales, enfermeras (os) especialistas y (os) generales:

- Título profesional (original y dos copias).
- Cédula profesional (original y dos copias) o en su caso carta pasante y/o certificado de estudios (original y dos copias).
- Credencial del INE (original y dos copias).
- Cédula de Identificación Fiscal (original y dos copias).
- C.U.R.P. (dos copias).
- Comprobante de domicilio (original y dos copias).

Nota: En caso de contar con una especialidad deberá entregar título y cédula profesional de la licenciatura y de la especialidad.

2. Administrativos (capturistas y secretarios [as]):

- Certificado de bachillerato (original y dos copias).
- Credencial del INE (original y dos copias).
- Cédula de Identificación Fiscal (original y dos copias).

Las dependencias hicieron un llamado a especialistas y enfermeras tanto civiles como militares en retiro a atender el llamado de contratación en diversas especialidades; además de labores de carácter administrativo y servicios generales.

- C.U.R.P. (dos copias).
- Comprobante de domicilio (original y dos copias).

3. Servicios generales (personal de intendencia):

- Certificado de secundaria (original y dos copias).
- Credencial del INE (original y dos copias).
- Cédula de Identificación Fiscal (original y dos copias).
- C.U.R.P. (dos copias).
- Comprobante de domicilio (original y dos copias).

En esta primera etapa, los interesados podrán acudir a diversas instalaciones hospitalarias. Consulte la página de la SEDENA las direcciones: www.gob.mx/sedena

Profesionistas en la rama de medicina

Por su parte, SEMAR invitó a mujeres y hombres especialistas en el área de sanidad que deseen trabajar "Para Servir a México" durante un periodo de seis meses desde esta institución: médicos generales, intensivistas, internistas, neumólogos, urgenciólogos, licenciados en enfermería, especialistas en enfermería intensivista y de urgencias.

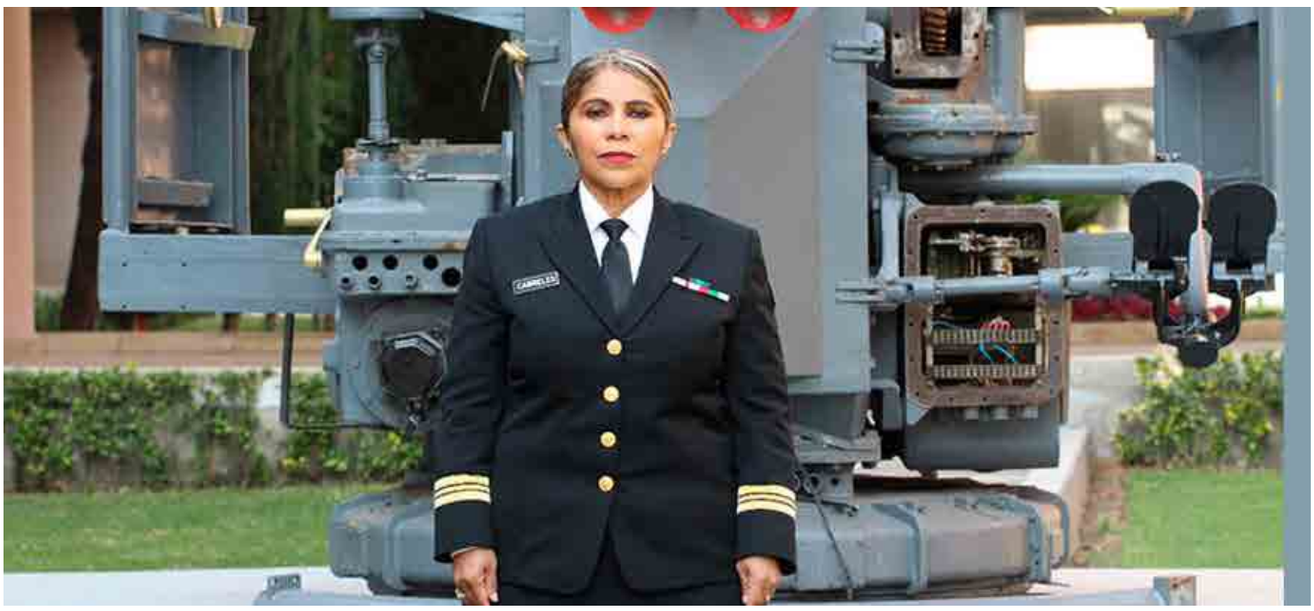
Los interesados en enlistarse a las filas de la Secretaría de Marina-Armada de México podrán obtener mayores informes en el teléfono 56 24 65 00 extensión 7958 o presentándose de lunes a viernes en horario de 08:00 a 16:00 horas en: Avenida Heroica Escuela Naval Militar número 669, edificio Revolución (primer nivel), colonia Presidentes Ejidales segunda sección, Alcaldía Coyoacán, código postal 04470, Ciudad de México.

Las personas que se encuentran fuera del Área Metropolitana podrán acudir al mando naval más cercano. La SEMAR recalcó que los interesados deberán cumplir con los requisitos establecidos por la institución, por ello recomendó tener en regla la documentación que acredite su nivel académico.

Capitán Leticia Rivera

de la vida militar a la enseñanza

Rosa María Salas / @revmasseguridad



Con 26 años de servicio dentro de la Secretaría de Marina-Armada de México (SEMAR), autora de dos ejemplares (más 25 obras en coautoría) y una de las dos historiadoras que existen actualmente en esa institución, la Capitán Leticia Rivera Cabrieles, catedrática de la materia Historia Naval y Militar del Centro de Estudios Superiores Navales (CESNAV), habla en entrevista con **Más Seguridad** sobre sus logros profesionales, así como de la incorporación del género femenino en el ámbito naval, en el marco de la conmemoración del Día Internacional de la Mujer.

¿Qué experiencia le ha dejado pertenecer a este Centro?

Estar en el CESNAV —que el 9 de marzo cumplió 50 años de haberse fundado— me ha permitido crecer profesionalmente, soy Doctora en Historia, cuando ingresé a la SEMAR únicamente tenía la licenciatura; en estos 26 años que llevo de servicio cursé una maestría también en esta disciplina y tengo la Condecoración al Mérito Docente Naval por el periodo que llevo dando clases.

¿Qué materia imparte?

Historia Naval de México a nivel posgrado, y es muy gratificante, ya que los alumnos conocen más de este tema y de la Marina. Escribí dos libros: uno con motivo del 40 aniversario del CESNAV en 2010, y en marzo salió el nuevo ejemplar sobre los 50 años de esta máxima casa de estudios.

Como mujer, ¿cuál ha sido su mayor logro en esta Secretaría?

La institución me ha dado la oportunidad de escribir su historia, estoy muy orgullosa de la jerarquía que he obtenido, se me han otorgado las facilidades para poder estudiar tanto la maestría como el doctorado, pero, sobre todo, la mayor satisfacción es ver cómo la SEMAR se ha transformado, hay mayor apertura para las mujeres.

¿Cómo ha crecido el papel de las mujeres?

En 2008 se le empezó a admitir en la Escuela Naval Militar. Antes estaba reservada para varones. El hecho de que haya féminas es una apertura, por ejemplo en CESNAV las había desde la década de los 90, cuando crearon el curso de Diplomado de Estado Mayor que ahora es la Maestría en Administración Naval. Tenemos compañeras que han llegado al grado de Contraalmirante. Nuestros mandos están conscientes de que ocupamos un lugar muy importante dentro de la institución.

¿Qué porcentaje del sector femenino toma clases en el CESNAV?

Es poca la proporción, no te podría dar cantidades exactas, pero sí es mayor el número. Es diferente a hace 20 años cuando comencé a dar clases, antes solo veías a una o dos, ahora en los salones hay mucho más.

¿Hay muchas historiadoras?

Sólo somos dos. Antes de mí hubo otros historiadores que ya se retiraron. Es importante la labor de quienes hemos abierto paso para que se entienda la importancia que tiene esta materia para cualquier nación e institución. La SEMAR ha venido impulsando el desarrollo de estos libros, hay libertad de cátedra, se busca que sea crítica y constructivista.

¿Quién está detrás de la historiadora?

Soy mamá, tengo un hijo de 30 años que es diseñador. El desarrollo que he logrado en el sector naval se debe a mi familia; he tenido que estar ausente por mis comisiones y quien lo resintió fue mi hijo, pero hoy él entiende la naturaleza de mi trabajo, ya que de aquí salió el sustento para darle una carrera.

¿Qué sigue para usted?

Estoy próxima para irme de retiro, es cuestión de meses. Pienso continuar dando clases en esta institución o en alguna otra. En la Universidad Iberoamericana impartí la materia de Historia de la Marina, que muy poco se conoce en nuestro país. Les diría a las mujeres que sigan adelante, que cumplan todas sus metas, nada es imposible, es cuestión de esfuerzo, de tenacidad y de estudio. mís

Llega a Madrid el posible

líder de la Cuba poscastrista

Madrid, Esp.- El presidente del movimiento cubano Somos+, Eliecer Ávila se reunió por vez primera con la disidencia cubana en Europa y adelantó a esta corresponsal que le gustaría poder mostrar su proyecto político a toda la ciudadanía cubana. El que se erige como un posible líder de la Cuba poscastrista, dentro de un proceso pacífico hacia la transición, declaró: "Cuanto más nos aprietan, más nos estamos uniendo. "Mi intención es levantar el ánimo del cubano que está disperso", dijo.

En una reciente reunión de toda la diáspora cubana asentada en España, el que fuera un aplicado y osado universitario enfrentado, hace 10 años, al presidente de la Asamblea Nacional del Poder Popular de Cuba, Ricardo Alarcón de Quesada, anunció el futuro lanzamiento de dos iniciativas a nivel internacional: de un lado, "Gran operación retorno" (más de 200 cubanos no pudieron viajar a Cuba durante el pasado año por estar "regulados"); y de otro, hacer una emblemática manifestación, "rueda de casinos gigantes", prevista para el 20 de mayo en Berlín.

En este sentido, Eliecer Ávila aprovechó la coyuntura para denunciar el caso de cientos de cubanos, residentes en otras naciones, quienes al visitar la isla, son obstaculizados, regulados y retenidos, "por activismo en países extranjeros"; tal es el caso del ciudadano cubano, residente en Uruguay, Lidier Hernández Sotolongo. "Inhiben nuestro derecho a la libertad de expresión, aun estando afuera", manifestó Ávila.

* **Carmen Chamorro**
España

Carmen Chamorro García
Corresponsal española de América Latina y Oriente Medio (Directiva CIP/ ACPE)
Miembro ADESyD
Member Journalists Digital of NewYork
The Canadian Association of journalists (CAJ)
Diplomada en SEI (Sociedad de Estudios Internacionales)
Experta en temas de Seguridad, Defensa y terrorismo global

Su idea es unificar a todos los jóvenes a través de las artes, que no del discurso político. Incluso, han superado el reto de crear una matriz tecnológica de alto alcance a toda la comunidad cubana porque desde a fuera no solo se "puede hacer algo", sino que las voces disidentes empiezan a aunarse y a desempeñar un papel esencial en la lucha contra los totalitarismos, precisamente por el auge de las redes sociales. "Se está creando un frente mundial que quiere hablar alto y claro y no bonito".

Asimismo, Ávila es conocedor de la efectividad del sistema propagandístico de los que apoyan la dictadura en Cuba, al igual que sabe que el país que mayormente puede influir en la política interna y externa de su país es España.

En una sala en Madrid de más de un centenar de personas, Eliecer Ávila aludió a tener el pleno convencimiento de no hacer nada malo, pero sí de ser víctima de una campaña de difamación en el extranjero. "Tenemos el potencial para lograr cambios. Empieza a perderse el miedo en la universidad cubana".

Por lo visto, la comunidad cubana es cada vez más participativa, gracias al espíritu agitador en las redes sociales y la ayuda de la oposición en el exterior. Se trata de mediatizar cada cuestión, haciendo uso de las nuevas tecnologías, "calentando", como se refiere Ávila, en una lucha por la democracia, con adeptos isleños in crescendo que cada vez padecen menos miedo. "No me voy a conformar con vivir afuera de mi país". "Un ejército que respete a la libertad, velará siempre por todos y cada uno de sus hermanos".

Igualmente exaltó la labor de los youtubers cubanos Carlitos Madrid y J.J Almeida, en su demostración diaria de fuerza porque el factor común es Cuba y "ello nos mantendrá fuertes".

El coordinador de la organización Somos+ tuvo la intención, en este periplo por Europa, de denunciar los nexos existentes entre Cuba y el actual gobierno de coalición español. "Resulta, cuanto menos preocupante, la relación intrínseca entre la dictadura cuabana y Sánchez, gracias a las garras del régimen castrista en el mundo", matizó.

Sobre Rocío Monasterio —diputada de VOX y natural de Cienfuegos, quien no pudo acudir al encuentro de Ávila por motivos de agenda— dijo ser una mujer que lleva en sí el decoro de muchos y la esperanza de los que queremos vivir en la verdad y la libertad.

intersec
BUENOS AIRES

26 – 28 Agosto 2020, La Rural Predio Ferial
Buenos Aires, Argentina

Exposición Internacional de Seguridad, Protección contra Incendios, Seguridad Electrónica, Industrial y Protección Personal

intersecbuenosaires.com.ar

#IntersecBA

casel

Cámara Argentina de Seguridad

messe frankfurt

Horarios: miércoles a viernes de 13 a 20 hs.
Evento exclusivo para empresarios, usuarios y profesionales del sector.
Para acreditarse debe presentar su documento de identidad.
No se permite el ingreso a menores de 16 años incluso acompañados por un adulto.

Messe Frankfurt Argentina: + 54 11 4514 1400 - intersec@argentina.messefrankfurt.com

En tiempos de coronavirus,

¿su empresa está segura haciendo oficina en casa?

Río de Janeiro, Bra.- La carrera hacia la oficina en casa o home office ha traído varios desafíos a la seguridad del acceso remoto. En cierto modo, las organizaciones ya tenían soluciones del trabajo en el hogar configuradas para dar acceso a un pequeño grupo de usuarios.

Las empresas de todo el mundo están siendo afectadas por la pandemia de COVID-19, con el fin de contener la contaminación masiva. Esto está llevando a las organizaciones a adoptar el modelo de oficina en casa, un escenario que requiere la protección de los activos más valiosos de la organización: factor humano y datos. Si a la compañía no le importa proporcionar seguridad para el trabajo remoto, la vulnerabilidad de los ciberataques crece a niveles exponenciales.

Los corporativos generalmente no tienen protocolos de home office con sus empleados. Los planes de continuidad del negocio, aunque afirman que las funciones críticas deben funcionar en la oficina y en el hogar, una gran mayoría no tiene nada formalizado. Imagínese cuando la mayoría de los empleados tendrán que trabajar desde casa debido al aislamiento social. Eso es un escenario que CISO tendrá que estructurar con el evento que sucede, tipo pandémico de COVID 19. Llega la determinación: el estado de Sao Paulo, desde el lunes, está en cuarentena, hasta dentro de 20 días. Los roles administrativos ya no pueden acceder a las instalaciones de la empresa. ¿Cómo lo hace la compañía?

Afirmo, basándome en mi experiencia, de los últimos 30 años y en esta pandemia COVID 19, que ninguna empresa está 100% preparada, ya sea brasileña, americana, china, inglesa. Cualquiera de ellas. ¿Por qué es eso? ¿Por qué sus ejecutivos y junta no creen en un escenario de esta magnitud? Cuando sucede siempre es un cisne negro, imposible de predecir. ¿Cómo? Si las pandemias son cíclicas y el mundo ya tiene suficiente experiencia para hacerlo. Los países asiáticos son un ejemplo, basta con mirar las curvas, Japón, Singapur y Hong Kong han logrado contener la pandemia COVID 19, mientras que las naciones occidentales, todas, se están poniendo al día. ¿Por qué es eso? Los asiáticos aprendieron del SARS (síndrome respiratorio agudo en 2003). Los gobiernos estaban mejor preparados para reaccionar con mayor rapidez y fuerza, la sociedad, las empresas y las poblaciones más dispuestas a cooperar.

Debido a que la ciberseguridad ya no tiene un perímetro, con el trabajo remoto, la situación se vuelve más sensible, abriendo brechas para que los hackers hagan sus ataques. Así que pasemos a algunas premisas estratégicas de ciberseguridad con continuidad del negocio:

1. Sobreviven. La primera premisa es la supervivencia del negocio, sabiendo cuáles son los procesos críticos, los sistemas de TI que soportan estos procesos y funciones cruciales: las personas. ¿Puedes trabajar de forma remota? Si pueden, ya deberían tener una estructura para ellos.
2. Estructura. ¿Necesito saber si mis empleados podrán trabajar? ¿Tienen infraestructura en casa? ¿Y la cadena de suministro? ¿Vas a laborar? ¿Tenemos una banda para todas las funciones críticas? ¿VPN para todos? ¿Poseo alternativas para trabajar sin VPN? ¿Ordenadores portátiles? ¿Los sistemas son asequibles y seguros? ¿Vamos a permitir el uso de máquinas personales? VPN es una alternativa, desde tener múltiples factores de autenticación, y monitorear capas hasta llegar a los datos más valiosos de la empresa. Se debe considerar el acceso a sistemas menos críticos sin VPN, especialmente los de la nube, aliado a un proveedor de identidades y la supervisión de acceso y datos.
3. Seguridad. Nuestro trabajo como ciberseguridad es buscar alternativas para trabajar en la extranet. ¿Qué aplicación de uso compartido de ar-

Designed by senivpetro / Freepik

Designed by senivpetro / Freepik

chivos debe utilizar el usuario? ¿Cómo configuro la navegación para disminuir la exposición? ¿Cómo garantizar la protección contra el phishing en máquinas externas?

4. Formación de personas. No hay que olvidar, que en la mayoría de los casos, las empresas relegadas, es la formación de los usuarios. Muchos trabajarán desde casa por primera vez, y demasiados lo harán más tiempo del que lo han hecho nunca. ¡No sabes cómo tratar con este extraño!
5. Seguridad web. Permite al empleado remoto navegar por internet protegido de contenido malintencionado.
6. Correo electrónico seguro. Respalda la protección de las cuentas de mail administrándolas para eliminar la suplantación de mensajes, el malware en los archivos adjuntos y el phishing, simulando notificaciones y eventos relacionados con temas (COVID-19).
7. Aproveche las soluciones en la nube. Garantice la visibilidad y el control de las actividades y los flujos de datos en las aplicaciones en la nube, con seguridad.
8. Control avanzado de amenazas. La empresa será objetivo con certeza, y el cebo será información que sobre la pandemia y el funcionamiento de la organización en este periodo.
9. Arquitectura flexible de soluciones de ciberseguridad. Le permite tener modelos híbridos o en la nube que le posibilitan contar con el mismo conjunto de políticas y nivel de seguridad en un escenario de configuración regional flexible.

Hoy en día, este es un proceso importante, sobre todo si se tiene en cuenta que, según los datos recogidos por numerosos investigadores, hay más de 4 mil dominios relacionados con el nuevo coronavirus. Todos ellos han sido registrados en todo el mundo y son 50% propensos a ser maliciosos. Por esta razón se sugiere que practiquemos los nueve temas mencionados anteriormente, con el objetivo de la ciberseguridad y un trabajo remoto de forma segura. ¡Buena suerte!

* **El Prof. Dr. Antonio Celso Ribeiro Brasiliano**
Brasil
CIGR, CRMA, CES, DEA, DSE, MBS. Doctor en Science et Ingénierie de L'Information et de L'Intelligence Stratégique, por la Université East Paris - Marne La Vallée – París – Francia, autor de diversos libros y artículos sobre riesgos; consultor hace más de 28 años en mercado brasileño, sudamericano, africano y europeo; profesor de cursos de especialización en Riesgos, Desarrollador del Software INTERISK; hoy es CEO de la Brasiliano INTERISK Gestión de Riesgos. abrasiliano@brasiliano.com.br

El umbral de incompetencia gerencial

Manuagua, Nic.- Con este antiguo refrán inicio esta nueva columna en esta prestigiosa revista, donde trataré de abordar temas de diferente índole relacionados con la seguridad privada a través de sus diferentes actores en el espíritu de generar una sana discusión de los tópicos que iremos desarrollando. Para comenzar deseo compartir algunas reflexiones sobre la falta de implementación que he observado en diferentes países de Latinoamérica del Principio de Peter, aplicado a los gerentes en las empresas de servicios de seguridad electrónica y principalmente física.

El Principio de Peter —desarrollado por Laurence Johnston Peter (1919-1990) y publicado en 1969— es uno de los temas básicos de estudio para las carreras relacionadas con recursos humanos y en las maestrías, master o como se deseen denominar de administración de empresas, y cuyo principal asunto es el umbral de la incompetencia que todas las personas desarrollamos por diferentes causas en algún punto de nuestra vida laboral.

Este fundamento que se aplica ampliamente en los mandos medios para evaluar ascensos y cambios de puestos, es prácticamente inexistente en la cultura empresarial de las organizaciones de seguridad en los niveles de los cargos superiores.

Lo anterior está dado por varios factores siendo algunos de ellos los siguientes:

Una importante parte de las compañías está constituida con menos de 50 años de vida y de éstas, casi la mayoría son de carácter familiar y fueron formadas por los actuales gerentes que son a la vez dueños o socios de las mismas.

Su desarrollo empresarial no se ha institucionalizado a través de procesos y procedimientos establecidos en el tiempo de vida de ellas y, por lo tanto, no están marcadas con una cultura basada en resultados y mejora continua, sino que dependen todavía de una fuerte toma de decisiones de la gerencia y basan parte de sus gestiones de mercado en el origen de relaciones establecidas a través de los años.

Hay excepciones donde los socios y dueños han realizado programas de traspaso generacional a sus descendientes o institucionalización de procesos y contratación de personal para la continuidad del negocio. No hacerlo de esta manera es un signo de reconocimiento de que la máxima autoridad de la empresa o ya está en su umbral de incompetencia, o está a punto de entrar en el mismo y se niega a reconocerlo y a que la evalúen en su desempeño gerencial, ya sea personal interno o profesionales externos de la compañía. Y lo anterior no se encuentra necesariamente unido al tema de la jubilación formal, ya que lo común en estos casos es que ya se haya sobrepasado la edad correspondiente.

Las principales señales a las cuales se debe prestar atención para conocer los indicios de que está entrando en su nivel de incompetencia son: no se entiende el lenguaje de los nuevos empleados de tecnologías de la información cuando explican las diferentes propuestas para solucionar o mejorar algún aspecto; no se comprenden los fenómenos de cambio en los comportamientos de los clientes (que se creían para toda la vida) y que inician procesos de contratación o subastas en línea de los servicios.

Asimismo, causa incomprensión que compañías de reciente formación ofrezcan mezclas de productos y servicios que nosotros siempre hemos tenido, pero que no hemos podido desarrollar con la eficiencia de estos nuevos competidores y esto normalmente está condicionado a que no se entiende bien el uso de estas tecnologías y los nuevos modelos de negocio que día a día van surgiendo. Generalmente, el nivel de resiliencia en esta estructura gerencial es bajo, sobre todo en lo relacionado a las nuevas y cambiantes tecnologías.

Reconocer uno su umbral de incompetencia no es, ni debe ser, motivo de frustración o depresión, sino todo lo contrario. Es reconocer que tiene un amplio bagaje y experiencia que puede y debe ser transmitido en aquellas áreas donde se es fuerte y que todavía se puede aportar a la mejora de la empresa, el sostenimiento y engrandecimiento de la misma en otras áreas de asesoramiento y dejar que las nuevas generaciones gerenciales ocupen los puestos y cargos para los que se han preparado, esperando que los nuevos y recién nacidos nativos digitales en unas décadas les señalen su umbral de incompetencia y se reinicie el ciclo, porque recuerde lo que es bueno para el ganso….

¿Y usted amigo gerente ya midió su umbral de incompetencia? mS

* **Luis González Nogales**
Nicaragua

El autor es CEO Fundador de Instituto Centroamericano de Seguridad Privada; cuenta con 40 años de experiencia en seguridad pública y privada. Tiene cuatro libros publicados y decenas de artículos en revistas especializadas. Actualmente impulsa la digitalización de empresas de seguridad a través del desarrollo de herramientas de software en la nube para seguridad privada. www.incaspri.com
incaspri@incaspri.com


SEGURI
EXPO
ECUADOR
FERIA Y CONFERENCIA INTERNACIONAL
www.seguriexpoecuador.com
15 - 17
JULIO 2020
CENTRO DE CONVENCIONES
DE GUAYAQUIL
VII FERIA INTERNACIONAL DE SEGURIDAD
Salón de Exhibición y Conferencias
Vídeo vigilancia - incendio - inteligencia artificial - blindaje
seguridad ciudadana - telecomunicaciones - redes - seguridad
informática - prevención de desastres - seguridad industrial
automatización - Protección personal - seguridad física
Revista
MÁS SEGURIDAD

ESS+

FERIA INTERNACIONAL DE SEGURIDAD

21-23 octubre 2020

Corferias • Bogotá Colombia

EXHIBICIÓN **TECNOLÓGICA**

RUEDA DE **NEGOCIOS**

ESS ACADEMY **CONFERENCIAS TÉCNICAS**

FOROS **ACADÉMICOS**

CENTRO DE **EXPERIENCIA**

ANALÍTICA | CIBERSEGURIDAD | INTERNET DE LAS COSAS IOT | INTERCONEXIÓN
INTELIGENCIA ARTIFICIAL | PREVENCIÓN Y PROTECCIÓN

SECURITY
SEGURIDAD Y ELECTRÓNICA

EFFICIENCY
CIBERSEGURIDAD Y TICS

SAFETY
PROTECCIÓN Y PREVENCIÓN

FIRE
PROTECCIÓN ACTIVA Y PASIVA

ORGANIZADORES

PAFYC Se mueven los negocios

corferias Generadores de Oportunidades y Progreso

CONTACTO

Adriana Márquez | amarquez@securityfaircolombia.com
Calle 127A N° 71A - 25 | Tel.: (571) 510 34 94 - 510 33 30

ALIADOS

seguridad latam laboral

Sociedad Colombiana de Medicina del Trabajo

ALAS Asociación Latinoamericana de Seguridad

COLADCA

IntegrA

TECNOSeguro

IPUserGroup Latinoamérica

Revista MÁS SEGURIDAD

Visítenos

www.SECURITYFAIRCOLOMBIA.COM