Junio 2024 / edición 148

MÁS SEGURIDAD

Magazine

www.revistamasseguridad.com.mx

Control de ACCESOS Y PERIMETRAL en prisiones

Junio / año 16 / No. 148

México y Latam / precio $60.00MX

17° CONGRESO INTERNACIONAL DE CENTROS DE ATENCIÓN DE EMERGENCIAS

23 AL 25 DE OCTUBRE DE 2024

HOTEL PARADISUS. CANCÚN, MÉX.

REGISTRATE AQUI

nena_911mx | Nena 9-1-1 Mx | www.911latinoamerica.org | Nena 9-1-1 México

MÁS SEGURIDAD
Magazine

HUMBERTO MEJÍA HERNANDEZ
DIRECCIÓN GENERAL
humberto@revistamasseguridad.com.mx

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

BEATRIZ CANALES HERNÁNDEZ
COORDINACIÓN EDITORIAL
edicion@revistamasseguridad.com.mx

SERGIO GIOVANI REYES POZO
COORDINACIÓN DISEÑO
diseno@revistamasseguridad.com.mx

TERESA RAMÍREZ OJEDA
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@globaldefense.com.mx

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

JORGE MERCADO ABONCE
SERVICIOS JURÍDICOS INTEGRALES
ANAZALDO-MARTÍNEZ-MERCADO
DIRECCIÓN JURÍDICA
juridico@revistamasseguridad.com.mx

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

CONTACTO
Tel: +52 55 1894 7067
WhatsApp: (+52) 55 1894 7067
asistencia@revistamasseguridad.com.mx
atencion@msglobal.com.mx

SIGUENOS EN:

Revista más seguridad
@revmasseguridad
revistamasseguridad
Revista más seguridad
@revmasseguridad
Revista más seguridad

Revista Más Seguridad Año 16, No 148, Junio 2024, Publicación mensual de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5555272279 / +52 5528732719. **Editor responsable: Humberto Mejía Hernández.** Certificado de Reserva 04-2022-050614181900-102 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: +52 5518947067.

Seguridad penitenciaria

Las prisiones enfrentan desafíos únicos en materia de protección. La prevención de fugas, son aspectos esenciales que deben ser abordados de manera efectiva.

La implementación de sistemas tecnológicos para el control de accesos y perimetral está revolucionando la seguridad en México y América Latina. En el contexto actual, donde la protección es una prioridad debido a las diversas amenazas tanto naturales como sociales, estas tecnologías ofrecen soluciones efectivas para proteger infraestructuras críticas y bienes valiosos.

Los sistemas modernos de control de accesos utilizan una variedad de tecnologías avanzadas como el reconocimiento facial, las huellas dactilares y las tarjetas de identificación, ajustándose a las necesidades específicas de cada organización y brindando un alto nivel de protección y comodidad para los usuarios.

El control perimetral, por su parte, se beneficia de la integración de tecnologías avanzadas como las cámaras de seguridad con capacidades de analítica de video, sensores de movimiento y sistemas de monitoreo remoto. Estas herramientas permiten una vigilancia continua y precisa, capaz de detectar y responder rápidamente a cualquier intento de intrusión.

En entornos de alto riesgo, como instalaciones industriales o áreas remotas, las cámaras termográficas y las analíticas de video son particularmente efectivas para garantizar la seguridad perimetral. En México y otros países de la región, la adopción de estas tecnologías está ayudando a mitigar los riesgos asociados con la violencia y la criminalidad, proporcionando un entorno más seguro tanto para personas como para activos.

La seguridad en centros penitenciarios es un tema crucial que requiere de tecnología avanzada y soluciones innovadoras para garantizar la protección de instalaciones y prevención de incidentes. En este tema especial, exploramos las tecnologías y servicios que diferentes empresas ofrecen para mejorar la protección en prisiones, con un enfoque especial en México, América Latina y Estados Unidos.

La innovación tecnológica juega un papel fundamental en la modernización de los sistemas de seguridad penitenciaria, asegurando no solo la protección del personal y los internos, sino también la eficiencia operativa de las instalaciones.

Las prisiones enfrentan desafíos únicos en materia de protección. La prevención de fugas, detección de contrabando y gestión de comportamientos peligrosos, son aspectos esenciales que deben ser abordados de manera efectiva.

Los profesionales de LATAM

Graduado como Oficial de Fuerza Aérea, por la Universidad del Ejército y Fuerza Aérea Mexicana-UDEFA. Cuenta con una trayectoria en Seguridad, Defensa y Emergencias de más de 20 años, desempeñando cargos en el sector público y privado.

Ha realizado estudios y cursos de mando, protección a funcionarios y seguridad física en instalaciones de Bases Aéreas, inteligencia militar, seguridad y defensa nacional entre otros. Ha participado en distintos seminarios de seguridad hemisférica, nacional y estratégica, en instituciones como el CESNAV (Centro de Estudios Superiores Navales) y el Instituto Mexicano de Estudios Estratégicos de Seguridad y Defensa Nacional, (INSUDE) de Costa Rica, Colombia, Guatemala, y Argentina.

Presidente actual de AIMCSE-FIBSEM Capítulo México (Asociación Internacional de Miembros de Cuerpos de Seguridad y Emergencias, miembro activo de AIMCSE Internacional y FIBSEM Internacional. Secretario de IFPO Comunidad México (Fundación Internacional para Oficiales de Protección). Actualmente es Country Security and Protection Manager para Conservation International en México.

Juan Carlos García Islas

Presidente AIMCSE-FIBSEM
Capítulo México

México

SUMARIO

Tour Internacional 2024

MÁS SEGURIDAD Magazine

EXPO NAVAL®

ESS+ FERIA INTERNACIONAL DE SEGURIDAD

intersec

NENA THE 9-1-1 ASSOCIATION MEXICO

ASIS INTERNATIONAL™ WOMEN IN SECURITY

SEGURIDADEXPO by Fisa | CHILE

Sígue la cobertura informativa en redes sociales, sitio web y revista

Humberto Mejía Hernández, DSE.

Seguridad y defensa con Claudia Sheinbaum

Luego del reciente y cuestionado proceso electoral en México, por primera vez en la historia de nuestro país gobernará una mujer. Medios de comunicación, periodistas connotados e independientes, así como una gran parte del electorado, publicaron en redes sociales que se trató de una elección de Estado, donde principalmente se busca proteger al Presidente saliente y su familia, señalados por corrupción y hasta vínculos con el narcotráfico. Hoy, Claudia Sheinbaum Pardo, no la tiene fácil y ha empezado a designar quienes serán los funcionarios que la acompañarían en las carteras de seguridad y mientras que hasta hoy no sabe quien quedará en defensa, organismos que también han sido muy cuestionados durante el presente sexenio.

La virtual Presidente electa anunció que daría a conocer su equipo de trabajo y anticipó que algunas dependencias (Ministerios) se compactarán.

Omar García Harfuch, electo como senador de la República, fue Secretario de Seguridad y Protección Ciudadana en el gobierno de Sheinbaum en la Ciudad de México, ocupará el mismo cargo a nivel federal. En distintos medios de comunicación y en el libro de la polémica periodista mexicana Anabel Hernández, "La historia secreta", este funcionario ha sido mencionado por supuestos vínculos con el Cartel de Sinaloa y estrecha cercanía con los hoy presos ex funcionarios del ex Presidente Felipe Calderón; Genaro García Luna y Luis Cárdenas Palomino. La misma Sheinbaum Pardo es mencionada en dicho libro por supuestos lazos con el crimen organizado.

Para la Fiscalía General de la República (FGR), suena el nombre de Alejandro Gertz Manero, quien podría repetir en el cargo, luego que se acercó a Sheinbaum Pardo (en tiempos de campaña), y tras mostrarle expedientes de casos en curso, le dijo que estaba interesado en trabajar con ella en el siguiente gobierno.

De aprobarse las reformas constitucionales que desea el Jefe de Estado saliente, la Guardia Nacional, el brazo operativo de la Secretaría (Ministerio) de Seguridad, pasaría formalmente a la Secretaría de la Defensa Nacional. Aunque en la actualidad opera de esa forma, el traslado legal dejaría "sin brazos" a esa dependencia y reducida a coordinar las mesas de seguridad en el país y al control del gasto público.

Como próxima Comandanta Suprema de las Fuerzas Armadas, Claudia Sheinbaum, tiene una baraja de 16 Generales y 16 Almirantes para elegir a sus próximos Secretarios (Ministros) de la Defensa Nacional y de Marina.

Todos estos perfiles, salvo uno de la Marina, llegaron al rango más alto (General de División en el Ejército y Almirante en la Marina) durante la actual administración, lo cual es uno de los requisitos que se establecen en diversos ordenamientos, para ser secretario de la Defensa o de Marina, además de ser menor a 65 años de edad al momento de asumir el cargo.

Para la SEDENA suenan los nombres Gabriel García Rincón, actual Subsecretario y quien ha sido agregado militar en EE.UU., así como Comandante de zonas y regiones militares en el Estado de México, Guerrero, Michoacán y Chihuahua. Estudió en el Colegio de Inteligencia de EE.UU. y realizó una maestría en Estudios Estratégicos en el Colegio de Guerra del Ejército estadunidense. En breve se sabrá quienes son los seleccionados.

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

Inicia el concurso global

▪ ***La manera de demostrar tu experiencia y talento como embajador de productos Hikvision.***

Con la finalidad de fomentar el intercambio de conocimientos y prácticas entre instaladores de productos, mejorar la calidad de las instalaciones, promoviendo el uso de productos de seguridad y reconocer a los instaladores más destacados, Hikvision lanza el concurso global HickTech Star, donde 100 instaladores de todo el mundo ganarán un viaje a China para:

- Visitar las oficinas centrales de Hikvision
- Conocer al equipo de investigación y Desarrollo de Hikvision
- Participar en la ceremonia de premiación
- Conocer la fábrica de Hikvision
- Tour Cultural en Hangzhou

"Este tipo de concursos son muy importantes para Hikvision, pues nos interesa que los mejores instaladores compartan sus conocimientos y experiencia con productos de seguridad, lo cual es una excelente manera de fomentar la educación y la excelencia en el campo", comenta Fran Sánchez, marcom director en Hikvision México.

"Buscamos que los ganadores experimenten en nuestra fábrica inteligente, interactúen con nuestro equipo de investigación y desarrollo, y reciban certificaciones acreditadas. Además de la tecnología, el programa HikTech Star es una puerta de entrada a una vibrante red de entusiastas y profesionales con ideas afines que les permitirá interactuar, compartir experiencias y ampliar su red profesional a través de reuniones y eventos".

"Cuando te conviertes en una estrella de HikTech, eres más que un embajador, eres una parte fundamental de nuestra comunidad, ayudándonos a conectarnos y crecer dentro de la industria", expresa la ejecutiva, quien menciona que en este concurso global, cinco personas de México representarán a la marca y está abierto a cualquier residente legal de México, mayor de 18 años.

A continuación, las pasos para participar: seguir las cuentas oficiales de Hikvision México en Facebook, Instagram y TikTok (@hikvisionmx).

1. Grabar un video creativo que demuestre habilidades tecnológicas o conocimientos sobre los productos de Hikvision. Los videos pueden ser de las siguientes categorías: unboxing, instalación, prueba, demostración, tutorial, etcétera.
2. Subir el video a TikTok, etiquetar a @hikvisionmx y usar el hashtag #HikTechStar.

Forma de participar y bases:

- El premio incluye vuelo redondo, alojamiento y gastos de alimentación durante todo el viaje para una persona.

- Los videos se recibirán del 3 de junio al 15 de agosto de 2024. Los videos y vistas fuera de este periodo no serán considerados. Las vistas serán contabilizadas dentro este espacio de tiempo. El viaje se realizará durante el mes de octubre en las fechas establecidas por la empresa.

- **Cómo participar:** El concurso está abierto a cualquier residente legal de México, mayor de 18 años. El viaje es personal y los ganadores deberán contar con los documentos necesarios para viajar fuera del país. El premio no es transferible y el viaje deberá realizarse en las fechas indicadas por Hikvision.

- **Criterios de selección:** Los videos serán evaluados basándose en creatividad, originalidad, calidad de la presentación, profundidad del conocimiento demostrado y cumplimiento de las instrucciones del concurso. Un panel de jueces de Hikvision seleccionará a los ganadores. Los 5 ganadores de México se elegirán de la siguiente manera.

- **1 Ganador: Cursos HPP+VIDEO:** El participante deberá subir el video de acuerdo a las instrucciones con la diferencia de que el tema del video será como configurar una solución para Pymes con HPP además de participar en los 6 cursos virtuales sobre Hik-Partner Porque se darán durante junio (12, 19 y 26) y julio (3,10 y 17). Las fechas, horarios, temas y registro a los cursos los encuentras dentro de la sección de eventos de HPP.

- En cada curso daremos 5 regalos sorpresa entre los asistentes a estos 6 cursos, durante la dinámica de preguntas y respuestas. El video ganador será seleccionado por el panel de jueces de Hikvision de acuerdo a los criterios mencionados.

- **3 Ganadores por mejores videos:** El participante tendrá que seguir las instrucciones antes mencionadas y nuestro comité valuador seleccionará al ganador de estos tres pases de acuerdo a los criterios mencionados.

- **1 Ganador por más visitas:** El participante deberá seguir las instrucciones de la convocatoria y el ganador será el creador del video con más vistas.

- **Premios especiales:** Hikvision México 15 monederos electrónicos con valor de $2,000 MXN a los 15 mejores videos que no ganen el viaje con agradecimiento a su participación y esfuerzo.

- **Notificación a los ganadores:** Los ganadores serán mencionados mediante un post en nuestras redes entre el 20 y 31 de agosto. Cada ganador será notificado también mediante un mensaje directo en TikTok y deberán responder dentro de los 5 días hábiles para reclamar su premio. Si un ganador no responde en el tiempo estipulado, se elegirá un nuevo ganador.

- **Derecho de uso de material:** Al participar, los concursantes otorgan a Hikvision el derecho no exclusivo de usar los videos presentados en sus campañas de marketing y promocionales sin compensación adicional. Consulta aquí las reglas aplicables al contenido que se inscribirá al concurso.

- **Aceptación de bases:** La participación del concurso constituye la aceptación de estas bases. Hikvision se reserva el derecho de modificar o cancelar el concurso si lo considera necesario.

Mayor detalle de las bases escaneando el siguiente QR:

Fran Sánchez
marcom director en Hikvision México

Actualiza dahua TECHNOLOGY Cloud Network Solution

▪ Esta actualización proporciona una topología de red generada automáticamente, funciones de administración enriquecidas, y seguridad de red 24/7.

El proveedor de servicios y soluciones AIoT centrado en video a nivel global, Dahua Technology, tiene una actualización en su solución de red integrada, rápida, eficiente y segura: red en la nube. Esta renovación integra CCTV y ciberespacio de TI en una sola plataforma, ofrece una configuración fácil y rápida, y proporciona una topología de red generada automáticamente con funciones de administración enriquecidas, así como seguridad de red las 24/7. Esto permite una fácil configuración y mantenimiento, abordando las necesidades de seguridad basadas en los distintos escenarios que presentan los usuarios.

Una sola red: CCTV integrada y redes de TI

Esta solución inteligente integra todo el producto de red, incluido conmutador de red, punto de acceso inalámbrico, enrutador empresarial y puente inalámbrico en DoLynk Care, plataforma basada en la nube que también puede administrar IPC, PTZ, NVR, XVR, alarma, videoportero y otros dispositivos. Se trata de una solución integral que combina tanto CCTV como redes informáticas, ahorrando costes de despliegue y mantenimiento. Además, esta solución también es compatible con dispositivos de terceros que se muestran en la topología de red con iconos, dirección MAC y demás información relevante.

Dahua Cloud Network Solution Topology

- **Implementación rápida:** configuración de red fácil y rápida. Con esta solución, los dispositivos se pueden agregar fácilmente escaneando un código QR a través de la aplicación móvil o realizar la importación de dispositivos individuales o por lotes en la plataforma web. Los usuarios también pueden escanear el código QR del controlador para conectar todos los dispositivos de red a la red en la nube.

  Además, su integración con DoLynk Care permite la generación automática de la topología correspondiente en función de los dispositivos identificados en la red. Admite la configuración remota de las funciones del dispositivo, incluido el reinicio, actualización, copia de seguridad, restauración, STP, VLAN, adición de enlaces, protección de bucles, etc. También permite saltar sin contraseña de la nube a la WEB del dispositivo, para operar funciones más avanzadas.

- **Mantenimiento eficiente:** mantenimiento de la red mediante topología generada automáticamente y funciones enriquecidas. El panel de datos de la plataforma en la nube muestra los datos gráficos del estado en tiempo real de los dispositivos conectados en la red. Admite el diagnóstico de estado con un solo clic que puede verificar todos los dispositivos y proporcionar guías profesionales de solución de problemas, con sólo hacer clic en un botón. También ofrece alarmas en tiempo real que notifican inmediatamente al operador cuando se produce un error. Los usuarios también tienen la opción de permitir que los instaladores entreguen el dispositivo o confiar su sistema a un operador profesional para su mantenimiento.

Garantía de seguridad: seguridad de red 24/7. Cada dispositivo agregado tiene una clave de cifrado única para garantizar la seguridad al acceder a la red en la nube. Esta solución también implementa un protocolo de transmisión segura, como el protocolo de seguridad de comunicación de red TLS para el cifrado de datos y SHA256 para un algoritmo hash criptográfico de alta seguridad, lo que garantiza una protección confiable contra ataques de fuerza bruta. También se implementa una autenticación efectiva del portal para identificar y verificar a los usuarios en la red, lo que mejora en gran medida la seguridad y confiabilidad de la misma.

Implementa videoseguridad MOTOROLA SOLUTIONS en aeropuerto

▪ Cámaras, análisis y control de acceso para ayudar a mejorar la seguridad y el bienestar de pasajeros, personal y operaciones aéreas.

▪ La videoseguridad es impulsada por IA con Motorola Solutions.

Guayaquil, Ecuador.- La Terminal Aeroportuaria de Guayaquil S.A., TAGSA, que administra el Aeropuerto Internacional José Joaquín de Olmedo en la ciudad de Guayaquil, eligió la solución de video seguridad y control de acceso Avigilon Unity de Motorola Solutions para apoyar operaciones más seguras y eficientes. La plataforma de seguridad on-premise basada en IA simplifica la administración del video y control de acceso en varias instalaciones y permite al personal de seguridad compartir clips de video con mayor facilidad para mejorar el reconocimiento de la situación y la colaboración.

Con sus 180 hectáreas de superficie y un promedio de 4 millones de pasajeros al año, el aeropuerto de Guayaquil desempeña un papel crucial como terminal de tráfico aéreo internacional que conecta Ecuador con más de 15 destinos internacionales. La solución fue elegida para ayudar a mitigar amenazas a la seguridad, comunes a los aeropuertos internacionales de todo el mundo, desde pequeños hurtos y robos hasta el crimen organizado y terrorismo.

"La tecnología es de vital importancia para mantener los altos estándares de servicio que siempre han caracterizado al aeropuerto de Guayaquil y para mantener seguros nuestros pasajeros, personal y operaciones aéreas", afirmó Ángel Córdova, gerente general de TAGSA. "Con nuestra nueva solución de gestión de video y control de acceso, hemos podido extender la seguridad a áreas que antes no estaban cubiertas, a la vez que agregamos capacidades que permiten a nuestro personal de seguridad tomar decisiones más informadas y eficientes".

Las cámaras de seguridad Avigilon de Motorola Solutions se han instalado estratégicamente a lo largo de todo el aeropuerto para proporcionar al personal de seguridad visibilidad en lugares críticos. El análisis de video puede detectar y notificar al personal anomalías que podrían indicar una actividad inusual entre la multitud, acceso no autorizado a áreas restringidas y otras amenazas para la seguridad, como equipajes desatendidos.

También se han instalado cámaras térmicas en zonas extensas del aeropuerto para mejorar la visibilidad nocturna. Estas cámaras de alto rendimiento pueden cubrir zonas amplias, detectar movimientos inusuales y localizar posibles intrusos en áreas restringidas basándose en sus características térmicas. Ello ha reforzado significativamente las capacidades de seguridad y detección en zonas críticas con poca iluminación.

"Con Avigilon Unity, el personal de seguridad del aeropuerto de Guayaquil puede buscar y analizar más rápida y eficientemente el video en vivo y grabado", dijo Ulises Gómez, MSSSI vicepresidente y director de ventas, Videoseguridad & Control de acceso Motorola Solutions Latinoamérica. "Esto les permite detectar, responder e investigar mejor los incidentes a medida que se desarrollan, aumentando la seguridad y la protección en toda la terminal y las operaciones del aeropuerto".

Protección exterior para un sitio de construcción con AJAX

▪ Cómo el sistema inalámbrico de la empresa protege un sitio a gran escala con muchos obstáculos a la comunicación por radio.

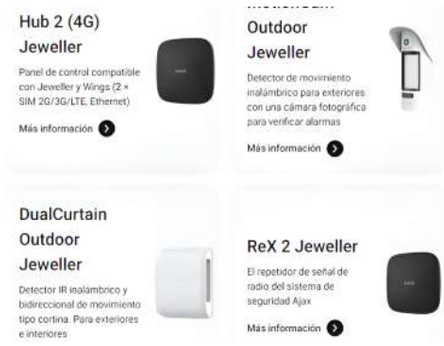
Gamma Immobilien Dresden es una empresa con 25 años de experiencia en el desarrollo de proyectos inmobiliarios de valor estable.

Reto

Proporcionar una solución autónoma con instalación fácil y flexible, que cubre las necesidades de protección del sitio de construcción.

Los sitios de construcción se enfrentan a numerosos retos a la hora de proteger sus instalaciones contra intrusiones y robos. Este sitio de construcción se encuentra en pleno centro de Dresde. Corría riesgo de intrusión y actividad delictiva debido a su fácil accesibilidad.

El sitio de construcción de Gamma Immobilien Dresden almacena equipamiento, maquinaria y materiales de valor, todos ellos objetivos atractivos para los ladrones.



Proteger estos bienes es fundamental para evitar pérdidas financieras significativas y retrasos en la construcción. Sin embargo, un perímetro grande suele tener muchos puntos ciegos. Es por eso que proteger un objeto de este tipo es siempre un reto.

Solución

Sistema de protección del sitio de construcción con un ángulo de visión de 360 grados contra intrusiones y robos.

La solución Ajax fue elegida por su amplia cobertura (de hasta 1.700m) que ofrecen los productos Baseline. Los dispositivos inalámbricos pueden instalarse en sitios a gran escala, garantizando una protección fiable en todo el perímetro.

El panel de control Hub 2 (4G) Jeweller admite la verificación fotográfica y sirve como un componente central del sistema de seguridad. Gracias al protocolo de comunicación Wings, los operadores de la CRA y los usuarios ven la primera instantánea del lugar de la incidencia en tan solo 9 segundos tras la alarma. El hub utiliza dos tarjetas SIM independientes (2G, 3G o LTE) de diferentes proveedores para una comunicación fiable en cualquier situación.

Los edificios construidos con hormigón y hierro pueden obstaculizar las ondas de radio, lo que puede afectar al funcionamiento de un sistema de seguridad inalámbrico. Para evitarlo, MS Alarmanlagen Dresden utilizó los repetidores de señal de radio ReX 2 Jeweller, que también admiten la foto verificación. Todos los eventos se transmiten instantáneamente, incluso a pesar de los obstáculos. Los usuarios y la central receptora de alarmas reciben las alarmas en tan solo 10 segundos.

Todo el perímetro del sitio de construcción está monitorizado por los detectores DualCurtain Outdoor Jeweller. Dos sistemas ópticos independientes con ángulos de visión estrechos y configuración flexible permiten ajustar con precisión la zona de detección, excluyendo posibles fuentes de falsas alarmas.

El software exclusivo ELSA (Extended Live Signal Analysis) reacciona a los intrusos, filtrando las interferencias naturales. Esto es especialmente importante en un sitio de construcción para evitar falsas alarmas provocadas, por ejemplo, por un arbusto que se balancea con el viento. Además, el DualCurtain Outdoor Jeweller reconoce los intentos de bloquear la visión del detector pintando sobre él, cubriéndolo, colocando un obstáculo delante de la lente o de cualquier otra forma.

Los detectores MotionCam Outdoor Jeweller proporcionan un nivel adicional de protección. Estos dispositivos monitorizan continuamente la zona interior del sitio, reconocen la intrusión desde los primeros pasos en el territorio y la confirman con una serie animada de fotos en tan solo 9 segundos. La verificación visual permite evaluar instantáneamente la situación y evitar las preocupaciones de los usuarios y a las compañías de seguridad, los envíos innecesarios de patrullas.

¿Por qué Ajax?

- **Bajos costes de mantenimiento:** los detectores Ajax cuentan con una prolongada vida útil de las baterías, lo que garantiza largos periodos de funcionamiento fiable sin necesidad de sustituirlas con frecuencia. Esta característica resulta en un ahorro de costes tanto para los clientes como para las empresas de instalación, ya que permite reducir los costes de mantenimiento y servicio.
- **Comunicación inalámbrica fiable en una gran instalación:** el sistema de seguridad inalámbrico Ajax es una solución ideal para los clientes que no pueden instalar sistemas cableados en sus instalaciones. Su característica distintiva es un largo alcance de comunicación, que puede aumentarse con la ayuda de repetidores. Puede instalar fácilmente el sistema y evitar cualquier obstáculo que pueda surgir en el proceso, mitigando los retos logísticos que suelen asociarse a las grandes instalaciones.
- **Sin falsas alarmas:** al combinar algoritmos de software con una función de verificación fotográfica, el sistema de seguridad no solo ahorra dinero reduciendo las falsas alarmas, sino que también garantiza que ningún intruso potencial pase desapercibido.

CURSOS ALAS

En la segunda mitad del año,

¡Certifícate con ALAS!

JUL
16 al 19

NUEVO

Ciberseguridad y Protección de Activos Digitales

JUL
23 al 26

Alarmas y Detección de Intrusión

AGO
27 al 30

CERTIFICADO DC3

Ventas para la Industria de la Seguridad

SEP
24 al 27

Gerencia de Proyectos

OCT
22 al 25

CERTIFICADO DC3

Video Vigilancia

NOV
12 al 15

Evaluación de Riesgos de Seguridad

DIC
3 al 6

CERTIFICADO DC3

Operadores de Cuartos de Control

Además tenemos cursos a la medida de tu compañía. Pregunta por ellos.

Alarmas y Detección de Incendios • Alarmas y Detección de Intrusión • Ciberseguridad para Alta Gerencia • Ciberseguridad y Proteccion de Activos Digitales • Control de Acceso • Drones en Seguridad • Evaluación de Riesgos de Seguridad • Evaluación del Retorno de la Inversión • Fundamentos de Seguridad Electrónica • Gerencia de Proyectos • Integración de Sistemas de Seguridad • Inteligencia Artificial en Seguridad • Management 3.0 • Operadores de Cuartos de Control • Redes IP e Inhalámbricas • Seguridad Perimetral • Ventas para la Industria de la Seguridad • Video Vigilancia •

ALAS
ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

CRISTIAN MOLINA
Coordinador de Cursos
Whatsapp:
+57 321 6153367

OPTEX
Sensing Innovation

Soluciones para la detección temprana de **amenazas** en **Centros Penitenciarios**

Centros penitenciarios deben garantizar la custodia de las personas encomendadas a la institución. Si no se puede garantizar la seguridad de ello entonces se verá afectado y amenazado el sistema, la procura de derecho, justicia y la paz social.

El riesgo: Internos tratan de escapar a toda costa, sea por el perímetro, por aire o por túneles, incluyendo apoyo del exterior e interior. En la mayoría de los casos lo harán con el fin de salir para cometer nuevos delitos, -probablemente con más sofisticación criminal-.

Los costos y las pérdidas no son cuantificables en dinero. Por ejemplo ¿el costo social y económico de los nuevos crímenes cometidos por un fugitivo?, ¿las pérdidas de vidas humanas por nuevos homicidios?, y, ¿el costo por los esfuerzos de la reaprehensión?, los costos legales, las pérdidas sociales, - pérdida de control, - de confianza, la pérdida de reputación política etc.

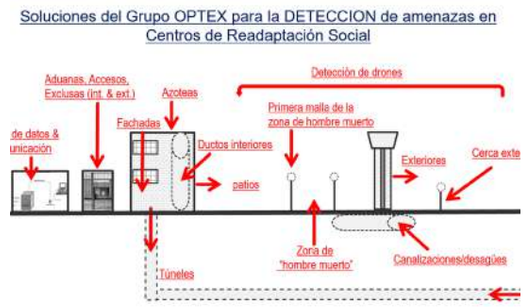
Por todo ello, un centro penitenciario debe contar con instalaciones y tecnologías confiables para poder garantizar una operación segura y su "razón de ser".

¿Cómo puede OPTEX apoyar para mitigar los riesgos y mantener mejor control en centros penitenciarios con los escenarios de riesgos complejos?: Es fundamental comprender que la DETECCIÓN confiable 7/24 es la parte medular de un concepto integral de seguridad en un penal. Si la detección de una amenaza falla, -todo lo demás está destinado a fallar también. Con la detección a tiempo comienza todo-, porque solo a partir de detectar una anomalía se pueden desencadenar una serie de actividades claves para mitigar los riesgos y para una respuesta correcta y efectiva.

Mediante dispositivos que detectan, visualizan y documentan irregularidades e intentos de fugas, se logra la prevención necesaria, además contribuyen en múltiples aspectos para mejorar los indicadores claves de desempeño en instituciones penitenciarias:

- Detección 7/24 confiable anticipada de un intento de fuga u otra amenaza.
- Optimización de procesos de operación, mejor aprovechamiento de RRHH y mejora de los resultados. (cero fugas es la norma)
- Identificación oportuna de movimientos no autorizados o sospechosos dentro las instalaciones o exterior.
- Mejor tiempo, y mejores condiciones de respuesta ante contingencias; más seguridad para los policías.
- Detectar, monitorear, documentar y archivar información relevante de los puntos importantes del centro penitenciario en sitio y remotamente.
- Los sistemas de detección, visualización y documentación nos brindan información verídica para hacer "contable" las actividades por el bien de la institución y la sociedad.

Algunos lugares relevantes en cárceles donde se nos ofrecen oportunidades para prever eficientemente irregularidades o intentos de escapes con DETECCIÓN confiable, optimizando la seguridad y el control del centro:



Las empresas del Grupo OPTEX (Optex/ Japón, Fiber SenSys/EE. UU., Raytec/Inglaterra) ofrecen soluciones flexibles para todas estas y más situaciones en Centros de Readaptación Social. Contamos con décadas de experiencia en investigación, desarrollo y manufactura de soluciones tecnológicas para detectar intrusión y amenazas, aplicadas y reconocidas en todo el mundo.

Optex ofrece el porfolio más amplio y completo en el mercado mundial de soluciones y tecnologías que detectan amenazas, escapes o intrusión. Desde sistemas de cable sensor de fibra óptica para detectar intrusiones en cercos, muros o pisos, sistemas de cable enterrado con campo de detección volumétrico de "radar-guiado", detectores LiDAR con cámara (Onvif) integrada para detectar en azoteas, fachadas, patios o perímetros; torres antivandálicos con IR-activos inteligentes, microondas, sensores duales para detectar en ductos y registros, sensores para exclusas permitiendo que solo una persona pueda pasar a la vez ("tail-gate"); complementamos con soluciones inteligentes de iluminación idóneas para centros penitenciarios, con luz infrarroja, luz blanca o hibrida con tecnología LED de más alto rendimiento, versiones IP & PoE, antivandálico, integrables a cualquier plataforma de gerenciamiento de seguridad. (VMS, NVMS, PSIM etc.)

OPTEX
Sensing Innovation

www.optexamerica.com

EL LÍDER MUNDIAL EN SOLUCIONES DE DETECCIÓN

Con soluciones de detección en interiores y exteriores para cada nivel de amenaza, los sensores OPTEX proporcionan flexibilidad, rendimiento y fiabilidad garantizada. Con 45 años de experiencia y más de 25 empresas en nuestra cartera global, OPTEX ha establecido una reputación mundial por su calidad, innovación y excelencia técnica.

HIGHLIGHTS DEL PRODUCTO:

REDSCAN Pro Advanced LiDAR Series

Extremadamente fiables y versátiles, los sensores de seguridad REDSCAN PRO utilizan tecnología LiDAR para crear una pared o plano láser virtual de alta resolución de hasta 100 m (330 pies) de largo, ideal para proteger perímetros, edificios, techos y activos.

Modelos disponibles:
RLS-50100V: 50 x 100 m (165 x 330 ft.), Modelo de interior y exterior
RLS-3060V: 30 x 60 m (100 x 200 ft.), Modelo de interior y exterior

REDSCAN mini-Pro LiDAR Series

Proporciona una precisión y flexibilidad sin precedentes para aplicaciones de alta seguridad, utilizando tecnología de tiempo de vuelo de vanguardia para rastrear con precisión el movimiento objetos. Con una cámara FHD incorporada (modelo RLS-2020V) y cumplimiento de ONVIF, mejora la seguridad con verificación visual y una integración perfecta.

Modelos disponibles:
RLS-2020V: 20 x 20 m (65 x 65 ft.), modelo de 95° para interiores y exteriores, con cámara FHD
RLS-2020A: 20 x 20 m (65 x 65 ft.), 95° modelo de interior y exterior

CHeKT Video Bridge Series

Potentes dispositivos de puerta de enlace de última generación que permiten la seguridad profesionales para conectar cámaras compatibles con ONVIF, sensores de alarma, sistemas de audio e iluminación a la verificación visual basada en la nube portal impulsado por CHeKT para eliminar el 100% de los despachos falsos.

Modelos disponibles:
CKB-308: 8 channel PoE-powered CHeKT Video Bridge
CKB-312V2: 12 channel PoE-powered CHeKT Video Bridge

Contact Us: 800.966.7839

sales@optexamerica.com

Informe sobre el estado del **control de acceso físico**

▪ Las cinco principales tendencias tecnológicas en el control de acceso físico: una visión hacia el futuro.

La empresa HID, experta en soluciones confiables de control de acceso físico e identidad, anuncia su informe sobre el estado del control de acceso físico para 2024, donde se destacan cinco tendencias fundamentales que están definiendo el futuro del sector.

Para el reporte (elaborado por IFSEC Global en asociación con HID), se encuestaron a más de 1200 profesionales de la seguridad en todo el mundo. Esta muestra permitió ofrecer una representación clara de una industria que ha venido experimentando una transformación sustancial. Administrada entre noviembre de 2023 y enero de 2024, la encuesta revela las siguientes cinco tendencias:

1. Se prevé el uso generalizado del acceso móvil y las identificaciones digitales

Aunque las acreditaciones físicas siguen siendo comunes en la industria del control de acceso, no cabe duda de que las credenciales de acceso móviles y las identidades digitales están ganando terreno rápidamente.

Según este informe, casi dos de cada cinco organizaciones (39%) ya utilizan activamente identidades móviles. Los encuestados señalan a las soluciones sin contacto (48%) y al acceso móvil (44%) como las dos tendencias más importantes que están configurando la industria del control de acceso en general.

2. Los estándares abiertos promueven el fenómeno de los edificios inteligentes

Los estándares abiertos se han convertido en factores determinantes para la adopción de soluciones de seguridad más convergentes, en los que los datos recolectados por los sistemas de control de acceso físico ayudan no solo a decidir quién se debe admitir en el edificio, sino también la forma de optimizar el uso de los espacios físicos.

Como muestra el informe, casi la mitad de las organizaciones (48%) ya cuentan con sistemas de control de acceso o escaneo de credenciales para monitorear el uso de las instalaciones a lo largo del día, al menos parcialmente. Asimismo, el 43% de los encuestados indicó que los edificios inteligentes y los espacios de trabajo flexibles están entre las tres principales tendencias que están incidiendo en la industria del control de acceso en su conjunto. La integración con otras áreas operativas de las organizaciones también fue considerada como una tendencia importante por uno de cada tres encuestados (32%).

3. La sostenibilidad gana protagonismo en las decisiones de las compañías

La sostenibilidad está teniendo una influencia significativa en el control de acceso: Casi dos tercios (63 %) de los encuestados señalaron que los responsables de gestionar la sostenibilidad en las organizaciones tienen alguna incidencia o se les consulta de forma exhaustiva en las decisiones sobre la actualización de los sistemas de control de acceso físico

4. El crecimiento significativo en el uso de la inteligencia artificial en análisis de datos

El uso de las funcionalidades que proporciona la inteligencia artificial en el control de acceso físico se está volviendo más frecuente, gracias al desarrollo continuo de las tecnologías de IA y al aumento de la competencia técnica en este campo. Cuando se les preguntó si estaban considerando incorporar IA/aprendizaje automático en sus soluciones de control de acceso, el 38% respondió afirmativamente (aunque el mismo porcentaje expresó incertidumbre sobre los beneficios). Sólo el 23% aseguró no tener planes de incorporar tecnologías de IA.

5. Mayor relevancia de la biometría, especialmente las soluciones sin contacto

El mercado de la biometría está expandiéndose a un ritmo acelerado. Para 2031, se espera que el mercado mundial alcance un valor de 136,18 mil millones de dólares. En particular, se proyecta que el mercado global de reconocimiento facial crecerá a 16,74 mil millones de dólares para 2030, comparado con los 3,83 mil millones de dólares en 2020. Esto representa una tasa anual compuesta del 16% de 2021 a 2030.

Introduce SIASA Space de MOCA SYSTEM BY SUPREMA

▪ La solución innovadora para control de acceso en México y Latinoamérica.

▪ Su arquitectura basada en la nube lo hace ideal para sitios grandes, múltiples sucursales, cualquier lugar donde se requiera un control de acceso eficiente y seguro.

El distribuidor mayorista en soluciones tecnológicas, SIASA, anunció la distribución en México de Airfob Space, revolucionario sistema de control de acceso basado en la nube desarrollado por MOCA System.

Respecto a esta nueva distribución, el director comercial de SIASA, Fernando Loret de Mola, comentó: "estamos emocionados por nuestra nueva alianza estratégica con MOCA System. La combinación de nuestra experiencia en control de accesos y la innovación de Airfob Space, sistema de control de acceso basado en la nube, nos permitirá ofrecer soluciones aún más seguras, convenientes y escalables a los clientes. Juntos, estamos abriendo puertas hacia un futuro más conectado y eficiente".

¿Qué es Airfob Space?

Es el sistema de control de acceso más escalable del mundo, 100% en la nube y móvil. No requiere servidores locales, cableado extenso ni controladores de puerta adicionales. Ofrece una actualización instantánea del control de acceso para oficinas, espacios de coworking, basados en membresías, como gimnasios o clubes, y apartamentos, que buscan una solución segura, escalable y conveniente. Con este esquema de tarjetas de plástico y sistemas convencionales quedan atrás. En cambio, los usuarios pueden acceder a áreas con un simple toque en su teléfono inteligente.

Beneficios clave de Airfob Space:

- **Seguridad:** garantiza la identidad digital verificada y elimina los riesgos asociados con la pérdida o préstamo de tarjetas de acceso.
- **Conveniencia:** los usuarios pueden almacenar y usar sus credenciales seguras en la aplicación (app) Airfob Space, sin costo adicional.
- **Escalabilidad:** desde pequeñas empresas hasta grandes corporaciones, se adapta a cualquier tamaño, actualizando fácilmente la infraestructura existente con soluciones como Airfob Tag y Airfob Patch. Agregar nuevas puertas también es muy sencillo con las soluciones Airfob Edge Reader conectadas a la nube.
- **Ahorro de tiempo y dinero:** elimina gastos innecesarios y largas filas para entrar o checar.
- **Control total:** los administradores pueden gestionar todo el sistema desde cualquier lugar utilizando aplicaciones móviles y web.

Cómo Funciona:

- **Aplicación (app) Airfob Space:** inspirada en una billetera, proporciona todo lo que los empleados y miembros necesitarán para almacenar sus credenciales de acceso seguro. Las organizaciones ahora pueden personalizar sus tarjetas de acceso móvil para ajustarlas a su identidad de marca.
- **Portal web y App Airfob Pro:** los administradores ahora pueden gestionar puertas y usuarios sin esfuerzo desde cualquier lugar, con el portal web intuitivo y la aplicación móvil Airfob Pro.
- **Hardware Airfob:** los lectores Airfob Edge, Airfob Edge Ultimate, y X-Station 2 son fáciles de instalar y requieren solo energía y conexión de red. Airfob Tag y Airfob Patch, solo necesitan cinta adhesiva.

¿Dónde puede usarse Airfob Space?
La arquitectura basada en la nube lo hace ideal para sitios grandes, múltiples sucursales y cualquier lugar donde se requiera un control de acceso eficiente y seguro.

Erik Cornelius Head of Business Overseas de MOCA System dijo al respecto de la alianza con SIASA: "la colaboración con SIASA es un paso crucial para la expansión de Airfob Space. Nuestra tecnología de identificación digital y la infraestructura de control de accesos de SIASA son complementarias. Al unir fuerzas, estamos llevando la seguridad y la gestión de accesos a un nivel superior. Esperamos que esta alianza beneficie a empresas, clubes y organizaciones en todo el mundo, brindándoles una experiencia de acceso más fluida y segura".

Erik Cornelius
Head of Business Overseas de MOCA System

Amplía Genetec™ presencia mundial con centros de I+D y Experience Centers

▪ Nuevas oficinas que sirven como centros de innovación, fomentando la colaboración entre desarrolladores, a medida que se construye tecnología con visión de futuro para apoyar su rápido crecimiento.

El proveedor mundial de tecnología de seguridad unificada, seguridad pública, operaciones y soluciones de inteligencia empresarial, Genetec Inc. anunció la apertura de nuevos centros de I+D, Experience Centers y la ampliación de varias oficinas en todo el mundo.

Nuevos centros de I+D

Para reafirmar su compromiso con la innovación, la empresa está ampliando su presencia mundial con el establecimiento y expansión de nuevos centros de investigación y desarrollo en lugares estratégicos de todo el mundo. Situados en Viena (Austria), Cracovia (Polonia) y Orleans (Francia), estos centros de I+D complementarán el campus existente de la empresa en Montreal y sus otros centros de I+D en Québec y Sherbrooke (Canadá), París (Francia) y Brujas (Bélgica).

"Estas nuevas oficinas sirven como centros de innovación, fomentando la colaboración entre nuestros desarrolladores a medida que construyen la tecnología con visión de futuro por la que Genetec es conocida. Nuestros nuevos centros de I+D reforzarán las iniciativas existentes y las capacidades, como la automatización inteligente", afirmó Christian Morin, vicepresidente de Ingeniería de Productos. "No es sorprendente que, para satisfacer la creciente demanda de innovación de la firma, hayamos aumentado nuestro equipo de I+D en un 50% en los últimos cinco años".

Experience Centers y ampliación de oficinas

La empresa abrió recientemente tres nuevos Experience Centers de última generación en Washington D.C. (EE.UU.), Sydney (Australia) y Dubai (EAU), además de sus Experience Centers insignia existentes en Montreal (Canadá), París (Francia), la ciudad de Londres (Reino Unido), Singapur y Ciudad de México (México). La organización también sigue ampliando el campus de su sede en Montreal, al que recientemente añadió más de 100 mil metros cuadrados, incluidos dos bistrós subvencionados para sus empleados de Montreal; también ha extendido considerablemente sus oficinas en Londres, París, Viena y São Paulo (Brasil).

"Al lanzar nuevos Experience Centers y oficinas en estas ubicaciones estratégicas, no solo estamos expandiendo nuestra presencia global; también escalando para satisfacer la creciente demanda de soluciones en todo el mundo. El objetivo es proporcionar a los clientes, socios de canal y clientes potenciales un encuentro práctico con nuestra tecnología innovadora y una experiencia de marca inolvidable", dijo Michel Chalouhi, vicepresidente de Ventas Globales.

Desde 2020, la empresa aumentó su plantilla total en un 52% y actualmente cuenta con más de 2 mil 100 empleados repartidos en 20 oficinas de cuatro continentes. Como parte de sus esfuerzos continuos para adaptarse a su crecimiento orgánico, la empresa está contratando personal para cubrir más de 80 nuevos puestos, entre ellos más de 30 vacantes en I+D en las regiones de América, Europa, Oriente Medio y Asia-Pacífico.

MATHIESON ELCO S.A. DE C.V. y sus principales casos de éxito

ASIPONA dos Bocas

La contribución de Mathieson ELCO en diversos proyectos clave en México ha sido fundamental para fortalecer la seguridad y eficiencia en infraestructuras críticas del país. A través de soluciones innovadoras y tecnológicamente avanzadas, Mathieson ELCO ha dejado una marca indeleble en casos emblemáticos, destacando su participación en la Refinería Dos Bocas en Tabasco, la Central Nucleoeléctrica Laguna Verde, y ASIPONA en Coatzacoalcos. Estos casos de éxito ilustran cómo la empresa ha sido un socio confiable en la implementación de sistemas de seguridad integrales, garantizando un entorno seguro y propicio para el desarrollo económico y social en México.

Refinería Dos Bocas Tabasco

Con el objetivo de incrementar la elaboración de productos de mayor valor agregado en el país, cuidar la balanza comercial e impulsar el desarrollo económico y social del sureste mexicano, el gobierno de México impulsó la construcción de la Refinería Olmeca en Dos Bocas, municipio de Paraíso, Tabasco.

Mathieson Elco fue uno de los principales proveedores de la solución de seguridad en la refinería junto con su partner Samsung Engineering, integrando más de 150 cámaras de la marca Synectics a prueba de explosión Clase I División I, en fabricación de acero inoxidable 316L, así también más de 400 estaciones de voceo de la marca Gai-Tronics con alarmas seleccionables por el usuario con el sistema central InSyL Server desarrollado por Mathieson. Todas estas soluciones preparadas para un crecimiento a futuro de la refinería.

Central Nucleoeléctrica Laguna Verde

La Central Nucleoeléctrica Laguna Verde (CNLV) es una instalación de producción de energía eléctrica, basada en la energía nuclear y en la fisión nuclear para generar electricidad, la cual además es la única en México.

Con máxima prioridad en la seguridad y una sólida cultura organizacional, la CNLV genera 5 % de la energía total del país, siendo una empresa que no contribuye al cambio climático porque no genera gases de efecto invernadero.

Mathieson ELCO ha incrementado la seguridad en la Central implementando más de 40 estaciones de voceo Gai-Tronics en donde se integran alarmas de riesgo por medio del sistema central InSyL que permite que el usuario configure dichas alarmas según se vayan presentando las necesidades de protección.

Esto ha permitido que el sistema sea amigable para los usuarios que hacen la vigilancia día a día de la central.

ASIPONA Coatzacoalcos

El puerto de Coatzacoalcos ubicado en el Istmo de Tehuantepec, se crea por decreto federal el 8 de octubre de 1825. la historia de su desarrollo se entrelaza con los principales acontecimientos que han influido con la configuración de la región. Actualmente el puerto se encuentra en 3er. lugar nacional en carga total, movilizando 28.7 millones de toneladas, esto incluyendo petróleo y derivados, respecto al manejo de la carga comercial actualmente se movilizan 5 millones de toneladas, en el puerto.

Mathieson ha contribuido en la seguridad del puerto entrelazando más de 100 cámaras de seguridad, entre ellas de ambiente marino de la marca Synectics, siendo el primero en desarrollar una solución completa integrando e implementando estaciones de voceo de la marca Gai-tronics, sistema de protección perimetral de más de 6 km de la marca Detection Technologies, radares de vigilancia perimetral, alarmas visuales y audibles, así como más de 20 controles de acceso, que mediante analíticos inteligentes se pueden realizar reconocimiento facial y de placas en los accesos del recinto.

La colaboración de Mathieson ELCO en estos proyectos no solo ha fortalecido la seguridad de infraestructuras críticas en México, sino que también ha sentado un precedente para futuros desarrollos en el campo de la seguridad y la tecnología. Con su enfoque innovador y su compromiso con la excelencia, Mathieson ELCO continúa siendo un socio confiable y un líder en su industria.

Desafíos de la seguridad penitenciaria

***Beatriz Canales Hérnandez**

▪ *La capacidad de innovar y adaptarse a las necesidades cambiantes es fundamental en el sector de la protección penitenciaria.*

La seguridad en centros penitenciarios es un tema crucial que requiere de tecnología avanzada y soluciones innovadoras para garantizar la protección de instalaciones y prevención de incidentes. En este tema especial, exploramos las tecnologías y servicios que diferentes empresas ofrecen para mejorar la seguridad en prisiones, con un enfoque especial en México, América Latina y Estados Unidos.

Las prisiones enfrentan desafíos únicos en materia de seguridad. La prevención de fugas, detección de contrabando y gestión de comportamientos peligrosos, son aspectos esenciales que deben ser abordados de manera efectiva.

Innovación y tecnologías inteligentes

La innovación tecnológica juega un papel fundamental en la modernización de los sistemas de seguridad penitenciaria, asegurando no solo la protección del personal y los internos, sino también la eficiencia operativa de las instalaciones. A continuación, una muestra de empresas de vanguardia que desarrollan soluciones destacadas en el mercado mundial:

Genetec: seguridad integrada y eficiencia operativa

Esta firma se ha destacado por sus soluciones integradas que permiten una gestión eficiente y segura en entornos penitenciarios. Michel Nieto Hernández, vertical sales manager en Genetec para la vertical de gobierno e infraestructura crítica, explica las soluciones que ofrece para la gestión de prisiones con control de acceso y seguridad perimetral.

"La plataforma Security Center es una solución unificada que integra sistemas de control de acceso y seguridad perimetral. Incorpora tecnologías de videovigilancia, permitiendo a los usuarios monitorizar eventos desde una única interfaz. Security Center facilita la integración de diversos sistemas de seguridad, proporcionando una visión holística de las instalaciones.

Con Innovación en barreras inteligentes, la misión es unificar toda la información de los sensores perimetrales, transformando las barreras físicas en barreras inteligentes con videovigilancia, radares, cables, sensores y microondas. Toda esta información se normaliza y correlaciona para proporcionar a los usuarios el contexto completo de los eventos, ayudando a identificar intrusiones, evasiones y la presencia de personas o vehículos, filtrando y evitando falsas alarmas.

El Control de acceso personalizado en prisiones, permite configurar reglas y roles para definir los accesos necesarios en cada punto. Los factores de autenticación varían según la criticidad, desde huellas dactilares hasta autenticación doble o triple, utilizando biometría, tokens y contraseñas. Toda esta orquestación se realiza a través del Security Center, una solución de arquitectura abierta compatible con diferentes fabricantes de sensores", explica Michel Nieto.

Michel Nieto Hernández
Vertical Sales Manager de Genetec

Magal Solutions: control de accesos y perimetral

Juan José García Ruiz, director comercial para América Latina de Magal Solutions, detalla las avanzadas soluciones de seguridad que la empresa ofrece para el sector penitenciario.

Portafolio:

- **Integración y PSIM** (Gestión de Información de Seguridad Física): plataforma que unifica diversas tecnologías de seguridad.
- **Vigilancia con radares y cámaras:** supervisión continua y detallada.
- **Cercas inteligentes y sistemas anti-túneles:** barrera física y tecnológica contra intrusiones y fugas.
- **Herramientas de gestión de actividades operativas y salas de control principal:** facilitan la administración y monitoreo de las instalaciones.
- **Sistema de control de disturbios:** gestiona y mitiga situaciones conflictivas dentro de las prisiones.

Para fortalecimiento de la seguridad, García Ruiz explica que en los Centros Federales de Readaptación Social (CEFERESOS) en México, las tecnologías de seguridad se alinean con los requerimientos del Órgano Administrativo Desconcentrado de Prevención y Readaptación Social (OADPRS) y la Plataforma México. A pesar de limitaciones en la actualización de tecnología debido a especificaciones contractuales, los sistemas existentes son sometidos a mantenimientos preventivos y correctivos para asegurar su eficacia.

Respecto a la ventaja competitiva, Magal Solutions destaca por su baja tasa de falsos positivos gracias a su sistema de detección basado en fibra óptica que utiliza inteligencia de datos para aprender y adaptarse al entorno, minimizando errores y garantizando una alta precisión en la detección de intrusiones.

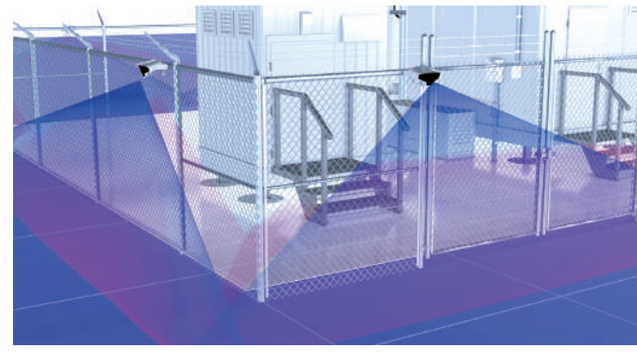
Para prisiones de máxima seguridad, incluidas las militares, la empresa tecnológica ofrece también cámaras de vigilancia térmica y de largo alcance, globos de observación y drones para un monitoreo exhaustivo. Asimismo, monitoreo celular, anti-drones, radares y jammers para protección contra comunicaciones y drones no autorizados; sensores subterráneos, barrera masiva, cercas inteligentes y video analíticos para detección y prevención de intentos de fuga.

Además, la firma ha desarrollado un sistema innovador contra drones que monitorea el espacio aéreo de manera continua y puede identificar, rastrear y neutralizar drones no autorizados. Con estas soluciones, se posiciona como un jugador líder en la implementación de tecnologías avanzadas para la seguridad perimetral y el control de accesos en prisiones, no solo en México, sino en todo el mundo.

Juan José García Ruiz
director comercial para América Latina de Magal Solutions

Senstar Inc.: seguridad perimetral de precisión

Empresa canadiense con más de 42 años en el mercado, especializada en seguridad perimetral. Jorge García, sales manager en México, destaca que la marca se dedica a la manufactura de equipos para la detección de intrusos en el perímetro y cuenta con laboratorios de desarrollo de software para la gestión inteligente de video, el cual es su *core business*.



En cuanto a sus tecnologías y soluciones, Senstar trabaja en verticales como correccionales y prisiones, energía y logística. Su portafolio incluye sistemas de detección microfónicos, sensores de fibra óptica, equipos de microondas y sensores por campo

electromagnético. Todas sus tecnologías están implementadas en varias prisiones de México y se administran mediante su software propietario que funciona como una plataforma común de operación y gestión para diversas tecnologías.

La empresa se caracteriza por su capacidad de innovar y adaptarse a las necesidades de los clientes mediante algoritmos que se mejoran continuamente. Esto permite ser precisos en diferentes entornos y adaptarse a diversas condiciones meteorológicas, aumentando la precisión en la detección. En el conocido foro Expo Seguridad presentó su Multisensor, que combina seis sensores en uno se incorpora Sensor Fusion con IA, reduciendo los falsos positivos con un índice de detección del 90%.

Con implementaciones, experiencia y una sólida presencia en México, Estados Unidos y Latinoamérica, Senstar ha desplegado su tecnología en América y Europa, protegiendo estructuras críticas con un análisis de riesgos de cada sitio. Sus soluciones incluyen cables, sensores montados en mallas, integración de otras señales y equipos volumétricos con el objetivo de disminuir las falsas alarmas mediante la fusión de sensores y el análisis con Inteligencia Artificial (AI).

Jorge García
sales manager en México, Senstar Inc

Hikvision: más que tecnología de vanguardia para prisiones

La empresa global en soluciones de videovigilancia, ha implementado una serie de tecnologías avanzadas para mejorar la seguridad en prisiones mexicanas a nivel federal y estatal. Dai Romero, business development manager de Hikvision México, destaca que la fortaleza de sus soluciones reside en la capacidad de ofrecer una gestión integral para los diversos escenarios dentro de las prisiones, fortaleciendo la integración entre los sistemas y protegiendo la información generada.

Con soluciones integrales, Hikvision maneja una variedad de equipos que incluyen videovigilancia, control de acceso, lectura de matrículas, reconocimiento facial, voceo IP, escáneres de vehículos y una plataforma centralizada de gestión. La empresa ha centrado sus esfuerzos en el sistema penitenciario mexicano y también ha implementado sus tecnologías en China. Una de las principales ventajas competitivas es la integración de sistemas y protección de datos.

Entre los casos de éxito e innovaciones recientes, se encuentran los Centros Federales de Readaptación Social No. 4 “Noroeste”, Número 8 “Nor-Poniente” y Número 5 “Oriente”, donde se han implementado tecnologías como CCTV, almacenamiento, videowall y la plataforma de gestión HikCentral. Hikvision sigue innovando con productos como la cámara gran angular DS-2CD6W32FWD-IVSD, diseñada para evitar vandalismo y montarse en esquinas, y el sistema de voceo DS-PA0103-B para enviar mensajes dentro del penal.

Dai Rome
business development manager de Hikvision México

Optex Incorporated: detección de amenazas con alto desempeño

René Cuenca, gerente de ventas para México y Norteamérica de Optex Incorporated, destaca las soluciones de la firma en control de accesos y seguridad perimetral. La empresa es fabricante de tecnología avanzada en detección de amenazas, especialmente diseñada para el sector penitenciario. Ofrece detectores de movimiento, sensores de fibra óptica, sensores soterrados y su innovadora tecnología de sensor láser con inteligencia artificial, que permite detectar objetos y personas que representen amenazas de intrusión o fuga.

La empresa ofrece tecnologías específicas para penales:

- Sensores de azoteas (lira-láser)
- Sensores con fibra óptica para mallas perimetrales
- Sensor de campo electromagnético
- Proyección y mantenimiento

La experiencia de Optex en diversos países les ha permitido proteger prisiones de baja, media y alta seguridad, lo que les otorga una sólida reputación respaldada por casos de éxito. En el ámbito de prisiones, es necesario actualizar las tecnologías cada cinco años, ya que los delincuentes suelen adelantarse a las medidas de seguridad tecnológica. Además,

el mantenimiento es crucial debido a la complejidad de estas instalaciones, y uno de los estándares es usar tecnologías que requieran el menor número de intervenciones técnicas.

René Cuenca
gerente de ventas para México y Norteamérica de Optex Incorporated

Eficiencia en seguridad penitenciaria

Integración y flexibilidad

La integración de sistemas es un aspecto clave en la modernización de la seguridad penitenciaria. Genetec, Senstar, Hikvision y Optex ofrecen soluciones que permiten la integración de diferentes tecnologías, proporcionando una gestión centralizada y eficiente. Genetec, con su plataforma Security Center, permite la unificación de sistemas de videovigilancia, control de acceso y sensores perimetrales.

Senstar, por su parte, destaca en la detección perimetral con su plataforma de gestión inteligente de video. Hikvision ofrece una solución integral que abarca desde la videovigilancia hasta el reconocimiento facial y la gestión centralizada, mientras que Optex se enfoca en la detección de amenazas mediante tecnologías avanzadas como sensores láser y de fibra óptica.

Precisión y reducción de falsos positivos

La precisión en detección y reducción de falsos positivos son esenciales para garantizar una respuesta eficiente a las amenazas. Las soluciones de Magal Solutions, Genetec y Senstar se destacan por su capacidad para analizar y correlacionar datos de múltiples sensores, proporcionando un contexto completo y reduciendo las alarmas falsas. El Multisensor de Senstar, por ejemplo, que combina seis sensores en uno con IA, es un ejemplo de cómo la tecnología puede mejorar la precisión en la detección.

Ciberseguridad y protección de datos

La ciberseguridad es otro aspecto estratégico en la gestión de sistemas de seguridad penitenciaria. Genetec incorpora ciberseguridad integrada por diseño en sus soluciones, asegurando que las mejores prácticas y mecanismos robustos estén en su lugar para proteger los datos sensibles. Hikvision también pone un fuerte énfasis en la protección de datos, asegurando la integridad y confidencialidad de la información generada por sus sistemas. La capacidad de innovar y adaptarse a las necesidades cambiantes es fundamental en el sector de la seguridad penitenciaria.

Las empresas destacadas en este tema central, demuestran un compromiso continuo con la innovación. Genetec y Senstar mejoran continuamente sus algoritmos y tecnologías para adaptarse a diferentes condiciones y entornos. Hikvision introduce nuevas tecnologías y productos como cámaras gran angular y sistemas de voceo para mejorar seguridad y comunicación dentro de las prisiones.

Optex, por su lado, ofrece su sensor láser y tecnologías de fibra óptica, soluciones avanzadas para la detección de amenazas, al igual que Magal Solutions, que desarrolla tecnologías avanzadas para la seguridad perimetral y el control de accesos en prisiones, no solo en México, sino en todo el mundo.

El panorama de la seguridad penitenciaria está en constante evolución, impulsado por la necesidad de innovar y adaptarse a desafíos cada vez más complejos. Genetec, Magal Solutions, Senstar, Hikvision y Optex lideran este cambio, ofreciendo tecnologías que no solo mejoran la precisión en la detección y prevención de incidentes, sino que también integran sistemas diversos para una gestión centralizada y eficiente.

La implementación de plataformas unificadas que permiten el monitoreo integral hasta sistemas de detección perimetral basados en inteligencia artificial, a través de soluciones tecnológicas están redefiniendo los estándares de seguridad en prisiones. La capacidad para reducir falsos positivos y la fortaleza en ciberseguridad aseguran que los datos sensibles estén protegidos, garantizando la integridad de las operaciones.

A pesar de los desafíos presupuestarios y contractuales, especialmente en México, la continua actualización y mantenimiento de estas tecnologías evidencian un compromiso por mantener un entorno seguro y controlado. La integración flexible y la adaptabilidad a las necesidades específicas de cada instalación demuestran la efectividad de estas innovaciones en distintos entornos y condiciones.

En última instancia, la modernización de la seguridad penitenciaria no solo protege a los internos y al personal, sino que también optimiza la gestión operativa de las instalaciones.

Con una visión centrada en la eficiencia y la precisión, estas empresas continúan avanzando en la protección de los centros penitenciarios, reafirmando su liderazgo en el sector y su contribución a la seguridad pública a nivel global.

El poder la seguridad cuántica con QuantPaths

Bogotá, Colombia.- QuantPaths® es una compañía británica dedicada al desarrollo de productos y servicios basados en tecnologías avanzadas como la inteligencia artificial, la ciberseguridad y la computación cuántica.

Sus productos superponen dichas tecnologías para alcanzar los más altos niveles de seguridad requeridos en soluciones de comunicaciones seguras, protección de redes y hardware, utilizados especialmente en gobiernos, agencias de inteligencia, seguridad y defensa nacional. Para alcanzar este hito tecnológico, el equipo científico de QuantPaths® ha desarrollado una técnica que hace posible el aseguramiento de los datos, tanto en tránsito como en reposo, desde computadoras clásicas (programación binaria), y luego transferirlos bidireccionalmente hacia computadoras cuánticas.

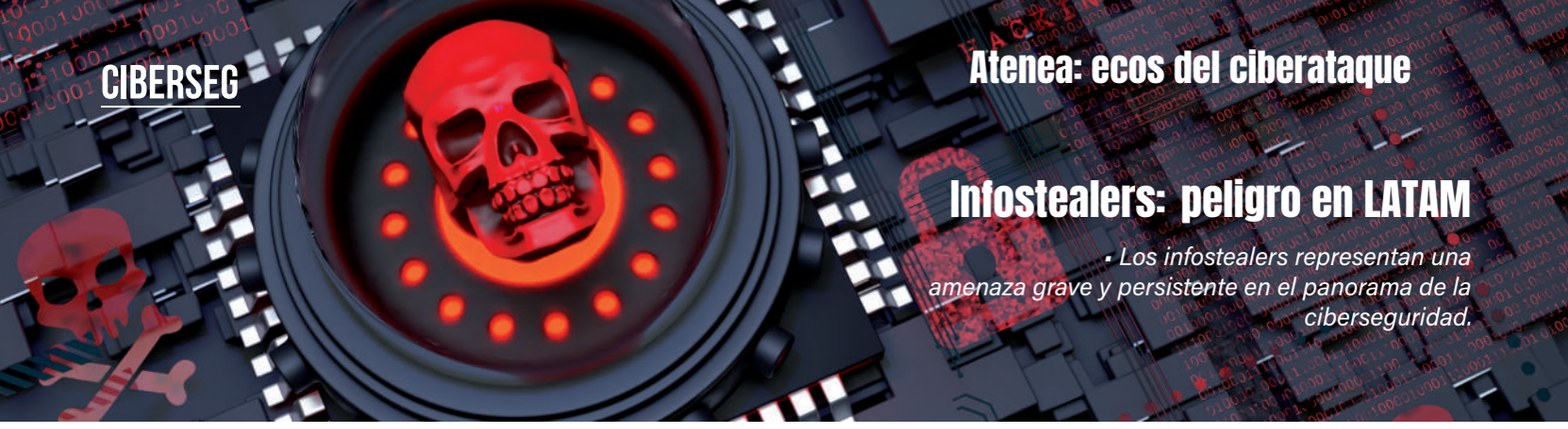
"A través de alianzas estratégicas con partners globales, la empresa tiene acceso a sofisticadas máquinas informáticas con tecnología cuántica para generar cúbits (bits cuánticos) mediante el uso de partículas atómicas llamadas iones. Sus algoritmos posibilitan migrar cálculos en binario a un sistema cuántico, obteniendo como mayor beneficio, una exorbitada capacidad de procesamiento y también, los más altos niveles de aseguramiento y protección de la información. Estas dos características impiden la penetración y robo de datos perpetrados por los métodos tradicionales que usan los ciberdelincuentes más avezados y experimentados. Además, permiten la resolución de problemas que actualmente no se pueden abordar con las supercomputadoras más potentes del mercado, refiere Eddie Velásquez", director Operativo de Quant Paths Ltd.

Por su lado, la compañía ha lanzado al mercado el primer smartphone convencional llamado QuantPhone® que usa además de la seguridad estándar a QuantWall®, que es una barrera construida con cúbits, que lo hace inaccesible e infranqueable ante ataques de ransomware, programas malignos, phishing o software espía, toda vez que se encuentra en el intermedio de la comunicación punto a punto.

Dicha barrera es proveída por una computadora cuántica que transforma los bits a un estado de partículas cuánticas en cada dispositivo. Este dispositivo usa una App para comunicaciones seguras con capas de encriptación post-cuántica certificada y también, un servicio propio de datos en itinerancia con cobertura global, evitando así la tediosa gestión ante operadoras locales.

El equipo de desarrollo de QuantPaths® -asevera Eddie Velásquez- promete en un futuro, implementar sus algoritmos en computadoras portátiles, tabletas y servidores, ampliando el espectro de la seguridad en la industria Oil & Gas, infraestructura crítica, aeroespacial, manufactura y sector financiero, que requieren de la máxima seguridad de sus activos digitales y físicos.

info@quantpaths.com



Atenea: ecos del ciberataque

Infostealers: peligro en LATAM

• Los infostealers representan una amenaza grave y persistente en el panorama de la ciberseguridad.

Son múltiples los riesgos y amenazas que rodean la seguridad y muchos los datos e información con los que interactuamos día con día, como personas y como organizaciones. Por ello, seguridad de la información y gobernanza de los datos se han convertido en aspectos clave e indispensable en nuestras actividades diarias. Entre las diversas amenazas cibernéticas, los infostealers se destacan por su capacidad para robar información confidencial y sensible con cierto grado de "facilidad" y resulta preocupante su creciente actividad y efectos en América Latina y el Caribe. En las siguientes líneas exploraremos más sobre los infostealers, cómo operan y los grupos criminales más notorios que los utilizan.

Los infostealers son un tipo de malware diseñado específicamente para infiltrarse en sistemas informáticos y extraer información valiosa. Esta información puede incluir credenciales de usuario, datos financieros, información personal y otros tipos de datos sensibles. Los infostealers se distribuyen a menudo a través de correos electrónicos de phishing, sitios web comprometidos y descargas de software malicioso. Su capacidad para operar en segundo plano y sin ser detectados los convierte en una amenaza particularmente engañosa.

El peligro creciente sobre los infostealers radica en su capacidad para robar datos sensibles sin el conocimiento del usuario, se dice que los infostealer son un mal peligroso y sigiloso, que puede llevar a pérdidas financieras significativas, como el robo de identidad y compromisos de seguridad a gran escala. La información robada puede ser vendida en mercados clandestinos, donde puede ser usada múltiples veces para cometer fraudes y delitos. La rapidez con la que los infostealers pueden extraer y transmitir datos a servidores controlados por atacantes los hace extremadamente peligrosos. La información objetivo de ellos puede ser (sin ser limitativa):

1. **Credenciales de usuario:** pueden capturar nombres de usuario y contraseñas almacenadas en navegadores web, aplicaciones de correo electrónico y otros programas. Esto permite a los atacantes acceder a cuentas personales y corporativas.
2. **Información financiera:** datos de tarjetas de crédito, información bancaria y otros detalles financieros son objetivos comunes. Esta información puede ser utilizada para realizar transacciones fraudulentas o venderse en mercados clandestinos.
3. **Datos personales:** pueden capturar información personal, como números de seguro social, direcciones y números de teléfono. Esto puede llevar a robos de identidad y otros problemas relacionados con la privacidad.

Los infostealers se valen de diferentes formas de operar para lograr su objetivo, algunas de las formas más comunes son:

- Registro de pulsaciones: registran cada tecla que es presionada, pueden capturar contraseñas y datos confidenciales.
- Escaneo de archivos: buscan y roban archivos específicos del dispositivo.
- Acceso a contraseñas: roban las contraseñas y credenciales almacenadas en los navegadores web.
- Captura de pantallas: realizan capturas de pantallas periódicamente para registrar la actividad e información sensible y confidencial.
- Espionaje de comunicaciones: vigilan los correos electrónicos y conversaciones en tiempo real en búsqueda de información sensible.

Infostealers y grupos criminales en LATAM

Los infostealers han presentado un incremento en su actividad en Latinoamérica y el Caribe, los países con mayor actividad* de este tipo en el primer semestre del 2024 son: Brasil (462,938), Argentina (146,427), México (118,784), Colombia (118,700) y Perú (118,566).

Los infostealers más relevantes en la región en el mismo periodo fueron: Lumma, Redline y Risepro. Estos se caracterizan por que es posible encontrarlos como Malware como servicio (MaaS), por sus múltiples capacidades y múltiples canales de C2.

Varios grupos criminales organizados utilizan infostealers como parte de sus operaciones. Estos grupos son conocidos por su sofisticación y la escala de sus ataques. A continuación, se describen algunos de los grupos más notorios:

- **TA505:** este grupo es conocido por sus campañas de phishing a gran escala y el uso de infostealers como FlawedAmmyy y ServHelper. TA505 ha atacado a instituciones financieras, minoristas y organizaciones de salud en todo el mundo.
- **FIN6:** este grupo se enfoca principalmente en el robo de datos de tarjetas de pago. Utilizan infostealers para capturar información de puntos de venta (POS) y han sido responsables de algunas de las brechas de datos más grandes de la última década.
- **Evil Corp:** conocido por desarrollar el infostealer Dridex, Evil Corp ha llevado a cabo numerosos ataques contra empresas en todo el mundo. Dridex es particularmente efectivo para robar credenciales bancarias y ha causado daños financieros significativos.

Para finalizar, es imprescindible mencionar que los infostealers pueden distribuirse de varias maneras, entre las que se incluyen:

- **Correos electrónicos de phishing:** mensajes diseñados para engañar a los usuarios para que descarguen y ejecuten el malware.
- **Sitios web comprometidos:** páginas web que explotan vulnerabilidades en los navegadores para descargar infostealers sin el conocimiento del usuario.
- **Software malicioso:** programas que parecen legítimos pero que en realidad contienen infostealers.

Los infostealers representan una amenaza grave y persistente en el panorama de la ciberseguridad. Su capacidad para robar información crítica de manera silenciosa y eficaz los convierte en una herramienta poderosa para los ciberdelincuentes. Para combatir esta amenaza, es esencial que las organizaciones implementen medidas de seguridad robustas, como la autenticación multifactor, la educación continua en ciberseguridad y el uso de software de seguridad avanzado.

Además, la colaboración internacional y el intercambio de información sobre amenazas emergentes son fundamentales para mitigar el impacto de los infostealers en nuestra sociedad conectada. Sin mencionar que, con un conocimiento adecuado y la implementación de mejores prácticas de seguridad, es posible reducir significativamente los riesgos asociados con estos ataques cibernéticos.

Dr. Gustavo Guzmán Hernández
gguzmanh01@gmail.com
Tw @GustavoG_Kc
México
Articulista Invitado

Maps integra a su portafolio de servicios a Vicarius

▪ Hoy las vulnerabilidades en las empresas tienen solución a través de la detección, y así proponer una solución ad-hoc a su problema.

A siete años de haber iniciado operaciones, Vicarius, empresa de origen israelí con presencia en varios de los países de Latinoamérica, ofrece la solución que ayuda a las organizaciones a proteger sus activos críticos, a través de una herramienta que permite hacer remediación automática de vulnerabilidades. En México actualmente, cuenta con una referencia de más de 80 clientes aproximadamente.

Hoy todo lo que es ciberseguridad está basado en las vulnerabilidades, cualquier equipo (de ciberseguridad) se encarga de mitigar o solucionar una vulnerabilidad, las cuales al mes llegan hasta 2 mil. Es aquí donde entra Vicarius con la remediación a debilidades a través de parches tecnológicos, ahora ya digitales para desinstalación de softwares y volver a instalar para protección de los programas establecidos para servicios de las empresas; solucionar la cobertura de ciberseguridad con mejora en la continuidad operativa.

La tecnología utilizada por la empresa de protección electrónica, es compatible en varios equipos utilizados por el personal para la protección contra vulnerabilidades en las organizaciones, esto es, no solo con las personas dedicadas a la ciberseguridad, sino con la gente de IT, Compliance, Retail o los dedicados al Desarrollo, al final, todos ellos trabajan con debilidades.

Actualmente existen varias soluciones de ciberseguridad, el problema es la cantidad de licencias que se requieren para el uso de estas herramientas, en donde resulta un problema la integración de todas ellas para hacerlo de manera más funcional, por ello Vicarius es una empresa de seguridad que cuenta con una sola licencia para la realización de operación a todas estas tareas, un only one. Solucionar y mitigar las vulnerabilidades bajo cualquier método mediante la automatización del parche en todos los dispositivos de la empresa.

La herramienta permite realizar puntos básicos: **detecta** los problemas que tiene la compañía, **prioriza** los problemas encontrados, y **propone** una remediación a ejecutar sin problema, para después **automatizar**. La Inteligencia Artificial no es suficiente para la solución de los problemas de ciberseguridad, el apoyo de Vicarius con esta solución detecta, prioriza y propone las soluciones adecuadas para cada una de las áreas de la empresa que necesita ayuda. La evolución de la herramienta de la firma para dar solución a los problemas de vulnerabilidad de las empresas, es constante.

Alianza como estrategia

Para poder llegar a más clientes, siempre será necesario aliarse con otras marcas para que de esta manera se obtengan ventajas de crecimiento, y con ello mejor posicionamiento en el mercado de la ciberseguridad en México y el resto del mundo.

Hoy con el apoyo de Maps, la marca Vicarius con sus herramientas de solución para las verticales de seguridad llegará a más clientes. Con esta alianza se complementa el portafolio de servicios de los partners de protección en los diferentes sectores.

El reto para Maps con la integración de esta marca y este tipo de solución, es cambiar la manera de ver la ciberseguridad, no solo se trata de aplicar una solución de control perimetral o instalar un nuevo antivirus, es explicarle al cliente las ventajas de integrar las mejores soluciones a sus diferentes equipos de las diferentes áreas que componen su infraestructura de IT para hacerla más robusta.

Con respecto a las empresas conscientes del control de vulnerabilidades, la misión de Maps en cuanto a la ciberseguridad (en un año en particular con ataques en México y a nivel mundial), se ha dado a conocer que no solo debe existir una seguridad en cuanto a los partners, sino en soluciones más específicas. En este entorno de ataque en particular, las soluciones de Vicarius podrán solventar y robustecer el esquema de ciberseguridad que tiene la empresa.

Maps empezará la introducción de las soluciones de Vicarius con sus clientes, dirigir la vertical que lo necesita (financiera, pymes, entre otras), no se va a dirigir a una vertical en particular, pero sí enfocada a los canales con los que cuenta actualmente para convertirse en un futuro como canales Vicarius.

Martín Mexia, director general de Maps, **Guillermo Gurvich**, vicepresidente Latam Vicarius y **Joel Guerrero**, territory director México, Centro América y el Caribe, Vicarius.

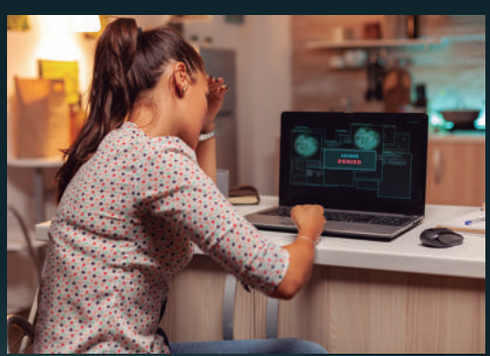
Las empresas deben ser **proactivas** y **no reactivas** a las **amenazas cibernéticas** en 2024

São Paulo, Brasil- Mediante el uso de inteligencia de amenazas completa y contextual, impulsados por capacidades avanzadas de IA, podemos identificar las tendencias que probablemente afectarán a las empresas.

Durante el último año, hemos sido testigos de la evolución de las motivaciones de los ciberdelincuentes a medida que colaboran y ofrecen sus habilidades por encargo, con el objetivo de causar trastornos financieros y caos social. A medida que los ciberdelincuentes emplean agresivamente la Inteligencia Artificial, ganan más eficiencia y precisión en sus ataques, lo que lo convierte en un desafío dinámico que requiere estrategias de ciberseguridad proactivas y adaptativas. En otras palabras, es necesario anticiparse a la adaptación en el contexto cibernético para 2024.

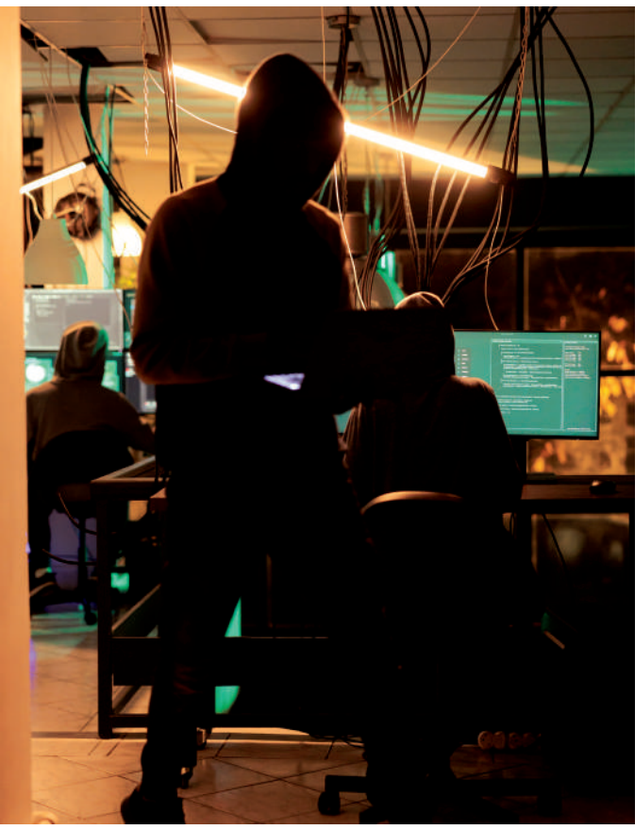
Hoy, la ciberseguridad es una función crítica para el negocio. A medida que la guerra cibernética se extiende por las geografías globales, el aumento de la actividad maliciosa ha llevado a una mayor cooperación internacional entre gobiernos y proveedores de ciberseguridad para combatir tales amenazas. Con la ayuda de la IA y otras tecnologías avanzadas, los defensores cibernéticos están mejorando en su oficio.

Ahora nos enfrentamos a tácticas más sofisticadas, impulsadas por tecnologías perfeccionadas, objetivos más amplios y mayores riesgos. Para adelantarse a los hackers, las empresas deben pasar de medidas de ciberseguridad reactivas a proactivas. Un punto fundamental del cambio de actitud es la necesidad de que las empresas cuenten con inteligencia externa e interna sobre ciber amenazas que sea relevante y dentro del contexto de la especificidad de cada empresa, considerando factores como superficie de ataque y efectividad de los sistemas, y procesos de ciberseguridad.



En el ámbito de la ciberseguridad, es imposible predecir lo que sucederá de la noche a la mañana. Mediante el uso de inteligencia de amenazas completa y contextual, impulsados por capacidades avanzadas de IA, podemos identificar las tendencias que probablemente afectarán a las empresas. Es inevitable que los

ciberdelincuentes encuentren formas de trabajar mejor, más rápido y de forma más inteligente. Sin embargo, los ciber defensores también deben contar con procesos y sistemas que anticipen y den tiempo a la adaptación. Aquí hay cuatro tendencias principales en Inteligencia Artificial, basadas en varios estudios de mercado:



Tendencia 1
La IA evolucionará para ser más accesible a medida que los proveedores de ciberseguridad continúen abordando confiabilidad, diversidad y privacidad de los datos. De ChatGPT en noviembre de 2022, el principal tema de conversación sobre ciberseguridad ha sido la IA. Con un enfoque en las herramientas de Inteligencia Artificial y la introducción de versiones empresariales, el uso de estas soluciones aumentará significativamente en 2024.

Tendencia 2
Los piratas informáticos utilizarán la IA como una herramienta para ataques precisos, efectivos y destacados. Los delincuentes utilizarán la Inteligencia Artificial generativa para automatizar ciberataques a gran escala, crear correos electrónicos maliciosos con contenido mucho más estructurado, específico para sus objetivos.

Tendencia 3
Rendición de cuentas: Existe una tendencia a responsabilizar a los ejecutivos y a las juntas directivas por prevención y proactividad. Las empresas deberán demostrar la priorización de vulnerabilidades y práctica de la gestión de riesgos cibernéticos. La actualización NIST CSF 2.0 demuestra esta predicción, con la inclusión y el énfasis de la gobernanza en los riesgos cibernéticos.

Tendencia 4
Amenazas geopolíticas: Estas cuestiones ampliarán las motivaciones de los atacantes más allá de las ganancias financieras, lo que dará lugar a un conjunto creciente de objetivos, vectores de ataque y nuevas estrategias. De esta forma, la proactividad de la ciberseguridad con el uso de CTI –Cyber Threat Intelligence- cobra importancia.

Estas cuatro tendencias muestran claramente que las empresas deberían invertir en IA, centrándose en su proactividad, identificando nuevas vulnerabilidades, basándose en las estrategias de los hackers.

El CTI es un programa amplio y holístico para anticipar las formas de ataques, incluyendo el Estado Final Deseado del agresor, sus intenciones reales, en función del perfil del hacker. Con este programa estructurado, las empresas podrán ser objetivamente más efectivas y asertivas en la implementación de medidas, procesos y sistemas de ciberseguridad.

Antonio Celso Ribeiro Brasiliano
PhD, Doctor en Filosofía en Ciencias de la Seguridad Internacional, Cambridge International University, Inglaterra. Presidente de Brasiliano INTERISK.
abrasiliano@brasiliano.com.br
Brasil
Articulista Invitado

Estrés por calor en el trabajo

▪ Al trabajar en condiciones de estrés térmico, el cuerpo se altera. Sufre una sobrecarga fisiológica, debido a que, al aumentar su temperatura, los mecanismos fisiológicos de pérdida de calor tratan de que se pierda el exceso del mismo.

En ambientes con temperaturas altas se puede presentar estrés térmico, el cual influye en la capacidad de concentración, entre otros aspectos. La Organización Internacional del Trabajo (OIT) estima que, en condiciones climáticas superiores a 30 grados, una persona puede ver reducida hasta la mitad su capacidad productiva.

Con los fuertes calores del verano, especialmente al mediodía y teniendo en cuenta que se espera que aumenten las olas de calor debido al cambio climático, esta amenaza se extiende a muchos más tipos de trabajos y condiciones. Sobre todo, se hace especialmente peligrosa en los trabajos al aire libre.

¿Qué es el estrés por calor?

Si la temperatura del aire aumenta sobre los 35°C, en vez de extraer calor del cuerpo se lo transfiere, el cual sumado al calor generado en su interior producen un aumento en la cantidad del sudor. Si, además, se suma la radiación solar o la radiación que produce un horno, el sudor no será suficiente para eliminar todo el calor que recibe el cuerpo y comenzará a calentarse aumentando su temperatura por encima de los 37°C, situación que se conoce con el nombre de estrés por calor.

Al trabajar en condiciones de estrés térmico, el cuerpo se altera. Sufre una sobrecarga fisiológica, debido a que, al aumentar su temperatura, los mecanismos fisiológicos de pérdida de calor (sudoración y vasodilatación periférica, fundamentalmente) tratan de que se pierda el exceso de calor. Si pese a todo, la temperatura central del cuerpo supera los 38° C, se podrán producir distintos daños a la salud, cuya gravedad estará relacionada con la cantidad de calor acumulado en el cuerpo.

¿Cuáles son las causas del estrés por calor?

En general, cuando la temperatura del aire en un ambiente de trabajo supera los 34 °C, ya sea por la condición del tiempo o porque el proceso de producción genera calor, se puede dar el estrés por calor, si además se suma alguna de las siguientes condiciones: humedad alta, trabajo pesado, ropa de trabajo que impide la evaporación sudor, radiación solar o radiación de superficies calientes de un horno o un equipo similar.

Síntomas

Los primeros síntomas o señales que alertan de un posible estrés térmico son:

- Dolor de cabeza
- Debilidad
- Fatiga
- Calambres musculares
- Náuseas
- Abundante sudoración
- Confusión

De no atenderse, estos síntomas pueden agravarse y causar las siguientes afectaciones en la salud de los trabajadores:

- Reducción de la capacidad de atención y concentración.
- Disminución de la capacidad de percepción y memoria.
- Apatía e irritabilidad.
- Alteraciones del sistema vascular.
- Temblores, pérdida de conocimiento, mareos o vértigos.
- Trastornos circulatorios y cardíacos.

El primer síntoma que aparece es la fatiga, aumentando el riesgo de tener un accidente. Después aparecen agotamiento y calambres.

Un síntoma más grave corresponde al colapso o golpe de calor, el cual se produce porque la sangre fluye principalmente a las extremidades, el cerebro se queda sin oxígeno y la persona se desmaya. Finalmente, si la temperatura corporal llega al orden de 41 °C, en casos extremos, puede producir la muerte.

Prevención

Entre las medidas que los centros de trabajo deben implementar están:

- Informar y capacitar a los trabajadores sobre los riesgos relacionados con el calor, sus efectos y las medidas preventivas a adoptar.
- Si es posible, modificar la temperatura del aire, eliminar la radiación o la alta humedad del lugar de trabajo.
- Organizar turnos rotativos para reducir el tiempo de la exposición al calor siempre que sea posible y realizar descansos frecuentes.
- Permitir al trabajador, en la medida de lo posible, adaptar su propio ritmo de trabajo.
- Si es un trabajo al aire libre, evitar las horas de mayor exposición solar.
- Habilitar zonas de descanso climatizadas, así como ambientes frescos y a la sombra.
- Proporcionar agua potable en las proximidades de los puestos de trabajo.
- Evitar realizar un gran gasto de energía. Proporcionar ayudas mecánicas y equipos de trabajo para la manipulación de cargas.
- Suministrar equipos de protección individual adecuados a los trabajadores (ropas amplias, transpirables, de tejido ligero y colores claros).
- Evitar el trabajo aislado, favoreciendo el trabajo en equipo para facilitar la supervisión mutua de los trabajadores.

En el caso de las empresas de seguridad privada, los guardias, laboran en instalaciones y centros de trabajo ajenos a su empleador, por lo que se sugiere que, antes de montar el servicio, el empleador conozca el sitio y las condiciones en las que el guardia prestará sus servicios y en conjunto con el cliente, se lleguen a acuerdos para adecuar los espacios, horarios, sitios de descanso y protecciones necesarias para reducir la exposición a las altas temperaturas.

Violeta E. Arellano Ocaña
gerente seguridad corporativa
Corporación Interamericana de Entretenimiento
varellano@cie.com.mx
México

Articulista Invitada

Sub estándares por exceso en **trabajos verticales**

▪ Cabe señalar que existen países que regulan el uso del método de trabajo en alturas conocido como acceso por cuerda, limitando su empleo solo donde no sea posible el uso de más maquinaria o estructuras como plataformas elevadoras y andamios.

El trabajo vertical es un sistema que permite al técnico alcanzar zonas remotas por medio de técnicas de acceso por cuerdas (rope access). Se trata de una metodología que entra dentro de los trabajos en alturas, ya que presenta los mismos riesgos derivados de la fuerza de gravedad y a la vez, subyace al común sistema regulatorio de cada país.

Si bien se tiene que reconocer la elevada complejidad del método de trabajo vertical que requiere de la competencia para que el técnico defina y arme el sistema de acceso al lugar de trabajo, acompañado por el sistema de seguridad contra caídas, al mismo tiempo es importante recordar lo que ya bien se sabe: Todos los trabajos conllevan escenarios de riesgo multíplices, que van mucho más allá de los peligros intrínsecos en la actividad, ya que a estos se le deben sumar los demás riesgos presentes en las operaciones y en el entorno de trabajo.

Es por esto que el uso del sistema de acceso por cuerda debe ser anticipado por un atento análisis que considere los resultados de la interrelación de riesgos de distintas naturalezas, para poder adoptar un procedimiento de trabajo acorde a eso. En línea con lo anterior, queda claro que la complejidad del armado del sistema de acceso y protección contra caída realizado por medio de técnicas estandarizadas es mucho menor con respecto a las adaptaciones y modificaciones requeridas a partir de un análisis de riesgo.

No obstante, la tendencia de los técnicos verticales, de las escuelas y varias asociaciones que enseñan esta metodología de acceso, parece ser contraria a lo anteriormente descrito, en cuanto estas se centran en la difusión y adopción rigurosa de modelos estándares rígidos, y basados casi exclusivamente en los riesgos de alturas. Por supuesto que esta omisión y carencia de flexibilidad (requerida para atender el conjunto de riesgos detectados), no facilita para nada la creación de procedimientos de seguridad adecuados a los peligros presentes en los distintos escenarios de trabajo.

Además, hay que resaltar que la tendencia sobre mencionada ha evolucionado con la adopción injustificada de esquemas aún más excesivos y orientados a la sobreprotección para los riesgos de las alturas, esto, dificultando aún más la necesaria adaptación de las técnicas con base a los demás riesgos presentes en una obra. La redundancia extrema (sistemas dobles de acceso y protección contra caída) y el abuso de la metodología de trabajo vertical, son dos ejemplos de cómo el exceso -en ambos sentidos-, han alejado principios fundamentales de seguridad y salud ocupacional, como lo es la buena práctica de analizar riesgos y crear procedimientos adecuados para ellos.

Posiblemente, la redundancia extrema (allá donde no justificada por la inexistencia de incidencias ya sea en los historiales de casos de accidentes, que de los incidentes por rotura de equipos), haya servido para convencer de la infalibilidad de las técnicas de acceso vertical y con esto, ampliar su uso hasta para aquellos casos donde no resulta ni conveniente, ni seguro.

Sin embargo, no se debe olvidar que la adopción de un sistema complejo sobre otro más simple, siempre tiene la potencialidad de exacerbar los riesgos de operación en alturas, y además puede aumentar o generar más riesgos de distinta naturaleza a los cuales está expuesto el trabajador. De aquí la importancia de que estas elecciones sean bien justificadas y sustentadas, antes de adoptarse. A continuación, se intentará dilucidar ambos fenómenos mencionados que, por convertirse en prácticas o escenarios inseguros de trabajo, se han indicado como subestándares del método de trabajo con cuerdas.

Cabe resaltar que estos escenarios tienen que ver ya sea con el trabajo vertical que se aplica comúnmente en instalación, mantenimiento y verificación con las cuerdas, así como en el rescate vertical industrial (servicio de emergencia privado) o en la aplicación inapropiada de criterios de acceso por cuerda a escenarios de trabajos en distintas alturas, y que solo requieren de la adopción de un sistema anti caída.

1. Redundancia extrema:
Consideramos dentro de esta práctica el uso de sistemas dobles, no requeridos, no justificados y que cuenten con la potencialidad de generar más situaciones de peligro o interferir con la gestión correcta de otros riesgos presentes en la obra. Va de la mano que todos los demás casos donde se aplique la duplicación oportuna de los equipos presentes en el sistema de acceso y de protección contra caída, no entran en el rubro de la nombrada redundancia extrema, si es que no se den las condiciones anteriormente descritas.

Unos ejemplos claros de estos excesos son el uso de doble sistema de anti caída, con estructuras de acceso distintos a las cuerdas (escalera, andamios, techos inclinados, etc.) y la instalación de abundantes elementos redundantes en los sistemas de teleféricos para rescates, especialmente para aquellas componentes que no presenten ninguna incidencia sobre casos de rotura (elementos metálicos como conectores, placas multiplicadoras, etc.).

También existen más eventualidades donde la redundancia se pudiera convertir en un riesgo mayor, y estos tendrán que analizarse caso por caso: Un ejemplo es el uso de múltiples puntos de anclaje, allá donde se cuente con dispositivos debidamente certificados y en más maniobras como el cambio de cuerdas, paso de fraccionamiento, etc. Sin embargo, hay que resaltar que, independientemente de que el caso sea más o menos evidente, siempre es importante analizar muy bien cada esquema operativo con la pericia que requiere un trabajo tan complicado.

De la mano con los escenarios presentados, unos ejemplos de los riesgos que la redundancia extrema fomenta pudieran ser eventuales fallos por error humano en el armado de los sistemas de acceso y anti caída, atoramientos críticos de los sistemas con posible insurgencia del síndrome de suspensión inerte por parte de las personas suspendidas, el agravarse de las condiciones de salud de los heridos transportados durante un rescate que no cumpla con los tiempos máximos establecidos, o la creación de sistemas complejos, que obstaculicen la gestión oportuna y minimización de otros riesgos presentes en la obra.

2. Abuso del acceso por cuerda:
Los trabajos verticales además de contar con muy bajos niveles de ergonomía con respecto a otros sistemas de acceso a las alturas, se realizan por medio de sistemas de cuerdas y más equipos de protección personal (EPP) que poco concilian con la presencia de peligros originados por energías mecánicas y fuentes de calor, entre otros.

Con respecto a estas consideraciones, es de suma importancia jerarquizar y limitar el uso del método de acceso por cuerdas, privilegiando otros sistemas que permitan una mayor protección para el trabajador, ya sea para evitar la insurgencia de enfermedades musculo esqueléticas, que para evitar accidentes derivados por ruptura o fundición de los EPP, que pudieran ocurrir, por ejemplo, en actividades de soldadura o con manipulación de materiales pesados, punzocortantes, etc.

Al respecto de este tema, cabe señalar que existen países que regulan el uso del método de trabajo en alturas conocido como acceso por cuerda, limitando su empleo solo donde no sea posible el uso de más maquinaria o estructuras como plataformas elevadoras y andamios (D.lgs. 81/08, Gobierno de la República Italiana).

Franco Grasso
Director de la IWR Academy y Ronin Lift México
Responsable del Área de Rescate Vertical de los Topos Birta
Director de la Escuela Nacional de Alpinismo y Rescate Alpino ItalianTREK
franco.grasso@iwr-mexico.com.
www.IWR-Mexico.com
#IWRAcademy #SelloIWR
Italia

Articulista Invitado

La ambigüedad de los "niveles plus" de blindaje automotriz

▪ Es necesaria y urgente una revisión a toda la reglamentación del blindaje en México, con una sola norma que regule a toda la industria como el caso brasileño.

Desde el pensamiento ortodoxo, que es aquel que parte de lo ya establecido, respeta lo que viene dado de antemano, es algo correcto o verdadero, aceptado por una mayoría. Podemos afirmar que los llamados niveles plus que se comercializan en México no son más que una ilusión netamente comercial, debido a sus ambigüedades y falta de evidencia balística que carece del rigor que exigen los métodos de prueba internacionalmente aceptados.

En teoría, los niveles plus se refieren al hecho de que el blindaje ofrece más protección que el nivel anterior, pero no puede cumplir con el estándar del siguiente nivel, por lo que generalmente está medio paso por encima.

Es más recurrente designar un plus en blindaje transparente, los fabricantes están constantemente en busca de crear productos más ligeros y resistentes, en ese camino van encontrando formulaciones intermedias, pero al no cumplir o ajustase a normas establecidas ni cumplir con los patrones de impacto, se convierten en una protección basada en la simple fe humana de que va a cumplir con su objetivo de proteger la vida.

Después, vienen los plus que son meramente diferencias en la configuración de los blindajes y áreas protegidas, y accesorios que solo vienen a agravar las confusiones en los usuarios.

Y aunque están fuera de todas las normas, son ampliamente aceptados y peor aún, solicitados por los usuarios de vehículos blindados en México ¿por qué sucede esto? ¿Por desconocimiento?, sí, ¿por una desinformación generada por la misma industria del blindaje? también, ¿por la necesidad de adaptar la protección a la realidad de inseguridad actual? sin duda.

Lo anterior solo ha generado una oferta de vehículos blindados que pareciera que se adapta a cada necesidad de los clientes en particular, se hace más grande el problema cuando cada blindadora designa a los niveles con una propia nomenclatura en aras de diferenciar su producto con el resto de los competidores.

La legislación mexicana exige someter los materiales balísticos a la Norma Oficial Mexicana vigente, pero ante la nula vigilancia al cumplimiento de esta, se ha generalizado el uso de normas como la NIJ y CEN principalmente. Si ya se va a dejar de lado la NOM-142-SCFI-2000, lo correcto sería comercializar los vehículos con la nomenclatura en la que los fabricantes certifican sus materiales, donde nuevamente es más común certificar bajo las normas NIJ y CEN.

Esto no es casualidad, por ejemplo, en Brasil los productos destinados al blindaje de vehículos siguen una norma única para todos los modelos de blindaje, la llamada ABNT NBR 15000, guiada por directrices específicas para garantizar la mejor protección de los vehículos. Esta regulación tiene su fundamento en la norma NIJ. Según las recomendaciones de las normas balísticas autorizadas en el territorio brasileño, los vidrios blindados deben tener registros con el ejército brasileño y solo se autoriza su comercialización cuando pasan por pruebas rigurosas de materiales.

El desconocimiento por parte de los compradores ha hecho que se generalice la compra de los llamados niveles plus, los clientes difícilmente tienen conocimientos de balística y aquí es donde la misma industria se ha encargado de generar, difundir y tolerar la mala información, argumentando que lo que se busca es adaptar la protección a los calibres más usados por la delincuencia en México. Nada más falso, si se hace una revisión más seria al fenómeno de la delincuencia, veríamos que no es necesario abrir un abanico de todas las posibilidades balísticas habidas.

A manera de conclusión, se puede afirmar que es necesaria y urgente una revisión a toda la reglamentación del blindaje en México, con una sola norma que regule a toda la industria como el caso brasileño.

En el blindaje no hay trajes a la medida, existen materiales de resistencia probada que se seguirán usando por su calidad y durabilidad, probados bajo normas ya establecidas, no hay que "descubrir el hilo negro". Lo que sí se puede hacer es hablar con la verdad a los compradores y decirles que sus vehículos están protegidos con materiales probados científicamente no por los votos de la fe humana en el caso de los plus.

Ricardo Guzmán
Director de operaciones en Vínculo Estrategas Comerciales. Amplia experiencia en el ámbito del blindaje automotriz y colaborador comecial a nivel gerencial y directivo en las más importantes blindadoras de México
rguzman@vinculoec.com.mx
México
Articulista Invitado

Nuevo AXIS COMMUNICATIONS Q1686-DEL, dispositivo de fusión radar-video

- *Combina dos potentes tecnologías en un único dispositivo.*

- *Ofrece excelentes capacidades de zoom, video nítido de alta resolución en detalle.*

La empresa de soluciones en videovigilancia Axis Communications presentó dispositivo de fusión radar-video todo en uno diseñado para la monitorización del tráfico. Cuando se combina con el software de reconocimiento de matrículas, este potente dispositivo puede conectar la velocidad de un vehículo a una matrícula.

Fácil de instalar, configurar y ajustar, AXIS Q1686-DLE Radar-Video Fusion Camera combina dos potentes tecnologías en un único dispositivo. Permite controlar de forma fiable velocidades de vehículos de hasta 200 km/h (125 mph), 24/7. Cuando se combina con un software de reconocimiento de matrículas como AXIS License Plate Verifier o un software de terceros, conecta una velocidad a una matrícula para identificar de forma fiable un vehículo.

Este dispositivo inteligente también puede detectar la conducción en sentido contrario, incluso a altas velocidades. Mediante el software de reconocimiento de matrículas, puede identificar de forma precisa una matrícula y localizar el vehículo infractor.

El escenario de cruzamiento de varias líneas aumenta la precisión, ya que el mismo objeto debe cruzar dos líneas virtuales para activar una alarma, lo que hace que las notificaciones sean más fiables. Con una baja tasa de falsas notificaciones, la policía puede reaccionar a las alarmas y detener rápidamente los vehículos que circulan en sentido contrario.

Este dispositivo de fusión ofrece excelentes capacidades de zoom, video nítido de alta resolución en detalle, así como imágenes con la densidad de píxeles necesaria para el reconocimiento de matrículas. Gracias a un kit de iluminación por infrarrojos optimizado para el tráfico, permite capturar imágenes de matrículas en entornos de oscuridad total a una distancia de hasta 50 m (164 pies). Además, los metadatos generados se pueden recopilar y visualizar en un panel de control para obtener información valiosa.

Basada en una plataforma abierta, AXIS Q1686-DLE es compatible con varios sistemas y plataformas de gestión de video. También puede activar otros dispositivos, por ejemplo, una luz estroboscópica para advertir y disuadir, por ejemplo, a los conductores que circulan en sentido contrario. Además, la coexistencia inteligente permite instalar hasta ocho dispositivos situados cerca los unos de los otros.

Funciones clave:

- Dos potentes tecnologías en un único dispositivo
- Conexión de la velocidad del vehículo con una matrícula
- Control de velocidades de vehículos hasta 200 km/h (125 mph)
- Detección y reconocimiento de vehículos que circulan en sentido contrario
- Funciones de ciberseguridad integradas con Axis Edge Vault

Este innovador y rentable dispositivo combina una cámara Axis Q-line superior con un radar de 60 GHz. Ofrece una instalación sencilla y se suministra calibrado de fábrica con la cámara y el radar perfectamente alineados. Con una selección de perfiles de escena, es posible adaptar automáticamente el ajuste de la imagen para adaptarse a propósitos específicos. Además, el asistente de captura de matrículas integrado garantiza una configuración sencilla y un rendimiento óptimo.

Seguridad en el sector automotriz

▪ Un aliado clave para proteger la seguridad en ataques en el sector automotriz:TISAX ®

▪ Con México reafirmando su presencia en el sector automotriz, y las filtraciones, hackeos, amenazas a la nube y los ataques a dispositivos conectados en aumento, resulta imperante aumentar la protección y agregar filtros de control en este sector.

A medida que la tecnología avanza rápidamente y la transición hacia procesos digitales se vuelve inevitable, los riesgos cibernéticos se vuelven cada vez más evidentes. Y es que, de acuerdo con el estudio, Digital Trust Insights 2024 de PwC, cinco de cada 10 empresas mexicanas tuvieron pérdidas de hasta 999 mil dólares como resultado de una filtración en los últimos tres años, además de que 26% destacó daños económicos de un millón y hasta más de 20 millones de dólares en el mismo periodo.

"México vive un constante crecimiento en el sector automotriz, pues es el séptimo mayor fabricante de automóviles en el mundo y líder latinoamericano de producción y exportación, enfrenta retos y áreas de oportunidad como el desarrollo tecnológico y la necesidad de adaptarse a los cambios del entorno. Reducir estos riesgos será crucial a medida que más ciberdelincuentes busquen capitalizar las vulnerabilidades del sector", afirmó Yonathan Parada, socio de Cybersecurity Risk and Regulatory.

La industria automotriz, podría enfrentar peligros particularmente significativos este año, ya que de acuerdo con el Global Automotive Cybersecurity Report de Upstream, la proporción de incidentes con un impacto "alto" o "masivo" en la industria, se duplicó de 2022 a 2023, representando casi el 50% de estos.

Hoy los ataques en el espacio automotriz pueden afectar no solo a los fabricantes de automóviles, sino también a las flotas de automóviles y los consumidores. En el caso de los fabricantes de autos, destacan los riesgos de propiedad intelectual, afectación en la cadena de valor y suministro derivados de los procesos de fabricación conectados – convergencia en las redes de TI/TO[1]– los cuales aumentarán a medida que se sigan implementando estos sistemas y la alta dependencia de terceros involucrados en los procesos productivos.

PwC México apunta que, ante el aumento de ciberataques esperado por las empresas mexicanas, el estándar Trusted Information Security Assessment Exchange (TISAX®) es un aliado clave para la proteger la información en el sector automotriz, además de que está siendo exigido cada vez en mayor medida por las ensambladoras a sus proveedores y/o fabricantes de equipos originales (OEMs).

Y es que, según los resultados del reporte antes mencionado, en 2023, el 67% de las actividades maliciosas tuvieron un impacto "alto" o "masivo", y el 58% de las actividades involucraron múltiples OEMs o tuvieron un alcance global[2]. De ahí que sea de suma importancia implementar controles y procedimientos de seguridad que refuercen un plan de respuesta a incidentes, contribuyendo de esta manera a fortalecer resiliencia y confianza.

Esto incluye a los actores de la industria de automóviles, quienes tienen un área de oportunidad para transmitir información de forma segura en procesos tan importantes como el diseño de desarrollo y producción, el manejo de prototipos, la seguridad funcional de los procesos de fabricación, los canales de distribución y ventas, y más.

"El sello de confianza TISAX® se vuelve una pieza clave. Este mecanismo de evaluación e intercambio de información permite a las empresas automotrices evaluar y certificar la seguridad de la información de sus proveedores. Esto es especialmente importante en un mundo cada vez más digitalizado, donde la protección de los datos y la confidencialidad son fundamentales", declaró el experto.

TISAX® es un sello de confianza desarrollado por la organización ENX Association, para establecer un marco común de evaluación y certificación de la seguridad de la información en la cadena de suministro automotriz, es un sistema que permite a las empresas automotrices evaluar y certificar la seguridad de la información de sus proveedores.

Referencia:

[1] Convergencia TI/ TO: integración de los sistemas de tecnología de la información (TI) con sistemas de tecnología operativa (TO).
[2] Global Automotive Cybersecurity Report, Upstream

GRUPO ALEM

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

¡Garantizamos su tranquilidad!

Guardias intramuros: Capacitados en diferentes modalidades (condominios, plazas comerciales, fábricas, etc)

Escoltas: Entrenados constantemente y especializados de acuerdo a la actividad del protegido

Custodias: Para todo tipo de transporte de mercancías en tránsito

Rastreo satelital: Vehículos particulares, carga o flotillas

Videovigilancia: Fija, móvil y remota

Análisis de riesgos y vulnerabilidades: Desarrollado por expertos en seguridad física y patrimonial

www.grupoalem.mx

edgar.seguridad.integral@gmail.com

+52 564705 2246

Convergencia: tecnología y sostenibilidad

Parte 2

▪ Las organizaciones deben navegar por una compleja red de regulaciones y estándares que rigen tanto la tecnología como la sostenibilidad.

En la primera parte de este artículo, hablé sobre como la convergencia de tecnología y sostenibilidad se ha vuelto inherente para las compañías que buscan destacarse en el desempeño Ambiental, Social y de Gobernanza (ESG), y de como el acelerado cambio climático nos llevó globalmente a tener un enfoque de acción mediático en este tópico. Por lo que es importante movernos a esta convergencia entre tecnología y sostenibilidad en una visión holística como objetivo estratégico en nuestras organizaciones sin importar la industria a la que nos dedicamos.

La tecnología sirve como catalizador para el desarrollo sostenible, ofreciendo soluciones innovadoras para abordar los desafíos ambientales, sociales y económicos. Desde sistemas energéticamente eficientes e infraestructuras inteligentes hasta análisis de datos y tecnología blockchain, las organizaciones pueden aprovechar los avances tecnológicos para optimizar la utilización de recursos, mejorar el bienestar social y garantizar prácticas de gobernanza ética. Al integrar consideraciones de sostenibilidad en las estrategias tecnológicas, las organizaciones pueden minimizar el impacto ambiental, promover la responsabilidad social y lograr una viabilidad económica a largo plazo.

En el panorama regulatorio actual, las organizaciones deben navegar por una compleja red de regulaciones y estándares que rigen tanto la tecnología como la sostenibilidad. El cumplimiento normativo es esencial para mitigar riesgos, garantizar transparencia y aumentar la confianza de los interesados.

Normas como la ISO 27001 para la gestión de la seguridad de la información y las certificaciones de sostenibilidad proporcionan marcos estructurados para que las organizaciones alineen sus prácticas con las mejores prácticas globales. Al adherirse a los requisitos regulatorios y a los estándares como la ISO 26000 que se centra en la responsabilidad social y proporciona a las organizaciones orientación sobre cómo puede operar de manera ética y socialmente responsable, considerando el impacto en sus decisiones y actividades en la sociedad y el medio ambiente adicional que, contribuye directamente al cumplimiento de los objetivos de desarrollo sustentable de las Naciones Unidas.

Como se mencionó anteriormente, no solo es importante el rol que tiene el responsable del área de "compliance", sino también de todos en la organización, ya que es fundamental para el cumplimiento de los objetivos de ESG. El papel de los gerentes de seguridad física, responsables de TI (por mencionar algunos) es crucial en el fortalecimiento del desempeño y la reputación ESG de una organización. Al integrar el cuidado del medio ambiente, responsabilidad social y los principios sólidos de gobernanza en las estrategias y prácticas de seguridad, y pueden contribuir considerablemente a los objetivos de sostenibilidad más amplios.

A través de iniciativas como iluminación energéticamente eficiente, controles de acceso, sistemas de vigilancia y gerentes de seguridad física pueden minimizar el impacto ambiental, mejorar la protección en el lugar de trabajo y garantizar el cumplimiento normativo. Además, al colaborar con los interesados y adoptar enfoques basados en el riesgo, los administradores de defensa física pueden mejorar la resiliencia organizacional y contribuir a objetivos de sostenibilidad a largo plazo.

Aunque la ISO 26000 y la ISO 27001 abordan aspectos diferentes de la gestión empresarial, pueden complementarse entre sí para promover prácticas empresariales más éticas, responsables y seguras. La integración de ambas normas puede ayudar a las organizaciones a avanzar hacia sus objetivos de responsabilidad social y seguridad de la información de manera coherente y eficaz.

A medida que las organizaciones navegan por las complejidades del panorama empresarial moderno, integración de tecnología y sostenibilidad se ha vuelto imperativa para impulsar el desempeño ESG y el éxito organizacional. Al aprovechar los avances tecnológicos, navegar por los marcos regulatorios e integrar enfoques como la ISO 27001, las organizaciones pueden maximizar su impacto ambiental, social y de gobernanza, fomentando resiliencia, innovación y creación de valor a largo plazo para los interesados.

En una era definida por desafíos y oportunidades globales, las organizaciones deben adoptar estrategias integradas que prioricen la sostenibilidad y la gobernanza ética como componentes integrales de su visión estratégica y prácticas operativas.

Si eres una empresa certificada en la ISO 27001 o estas en proceso de certificación, es importante que implementes prácticas y métricas de sustentabilidad. ¡Hasta la próxima!

Gigi Agassini, CPP
Principal Consultant, GA Advisory y socia activa de Amexsi
México

Articulista Invitada

CRNOVA SECURITY

Custodia de Mercancía

Guardia Intramuros

Monitoreo y Rastreo

ISO 9001 | ISO 28000 | BASC | ISO 18788 | ISO 37001

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

crnovaoficial

crnovasecurity

www.crnova.com.mx

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

Implementación de **tecnología** en las empresas de **seguridad privada**

▪ Fundamental es que los empresarios de seguridad vean estas herramientas como aliados en lugar de enemigos tecnológicos.

En México, las empresas de seguridad privada enfrentan desafíos significativos, como la escasez de personal, la alta rotación (sin mencionar las pérdidas económicas asociadas), y la falta de empatía de algunos clientes ante los costos derivados de las regulaciones actuales. Estos factores representan un reto aparentemente insuperable para el sector. A menudo, los presupuestos asignados por los clientes finales no contemplan los aumentos necesarios para garantizar el servicio requerido, lo que impacta directamente en la rentabilidad de las empresas.

¿Cómo enfrentar estos retos?, ¿cómo optimizo la permanencia de mi personal y disminuyo la rotación? Aunque las estrategias implementadas por empresas de calidad son efectivas, en la actualidad no son suficientes. Aquí es donde la tecnología puede marcar la diferencia de manera positiva tanto para los empresarios de seguridad privada como para sus clientes. La rentabilidad de los servicios puede aumentar en más del 30%, dependiendo de la eficiencia y calidad de la tecnología implementada. Cada cliente es único y requiere soluciones personalizadas.

En la era tecnológica actual, la implementación adecuada de herramientas puede ofrecer resultados sorprendentes. Hoy son pocas las soluciones que no se pueden llevar a cabo. La integración de diversas marcas y equipos por parte de fabricantes y desarrolladores de tecnología ha permitido crear soluciones específicas para cada cliente. Por ejemplo, la implementación de un "guardia virtual" puede realizar una variedad de funciones con una eficiencia extraordinaria, como controles de acceso, validaciones de identidad, comunicaciones con centros de monitoreo, entre otros.

Las opciones de implementación son infinitas. Cabe recalcar esta pregunta que siempre hacemos: ¿esto sustituye al factor humano?, la respuesta es "NO" pero la integración del factor humano con la tecnología genera servicios más eficientes y efectivos.

Es fundamental que los empresarios de seguridad vean estas herramientas como aliados en lugar de enemigos tecnológicos. Siempre habrá un profesional Amexiano disponible para asesorar en este ámbito. Recordemos que "si fuera fácil, cualquiera lo haría". Por tanto, es fundamental apreciar la visión y la valentía requeridas para avanzar en esta dirección. Estoy seguro de que, si estás leyendo este artículo, es porque tienes la visión de dar ese paso. ***#SILOCREESLOCREAS***

Carlos Román Martínez Sánchez,
DSE Presidente del Comité ALAS México y CSO Tedee México.
México

Articulista Invitado

PROTEGE calidad, profesionalismo y **desarrollo de habilidades** con expertos

▪ *Empresa con soluciones conformadas con Inteligencia Artificial y análisis de riesgos dentro de la cadena de suministro.*

Ofrecer valor agregado en el servicio es la respuesta para sumar más y nuevos clientes al negocio, lo que se proyecta en crecimiento y expansión en el mercado de la seguridad privada, nicho que cada vez se vuelve más competido, pero donde solo los profesionales permanecen. Ese es el reto.

Servicios de Seguridad Privada, Protege, es una firma con más de dos décadas de experiencia en seguridad armada, con servicios en las 32 entidades federativas de la República Mexicana, especializada en la vertical para el traslado de bienes y valores, custodia y de mercancía de alto valor, así como protección de bienes con elementos civiles y armados. La empresa cuenta con soluciones conformadas con Inteligencia Artificial y análisis de riesgos dentro de la cadena de suministro, *core* de la compañía.

"De los sectores que atendemos y de más vulnerabilidad en el día a día son medicamento, tecnología, marcas de ropa de alta gama y accesorios -femeninos y de caballero-, es lo que está teniendo mayor riesgo dentro de la cadena de suministro, así como vinos y licores", comenta el Comandante Juan Manuel García Coss, presidente ejecutivo de Protege.

Para satisfacer los servicios especializados, cuenta con oficinas en Tabasco, Jalisco, Ciudad de México, Baja California, Nuevo León y Estado de México. Hoy, enfocado en la región del Pacífico, refuerza la ruta en su totalidad con inicio y término en Baja California y Ciudad de México, con una oficina intermedia en Jalisco; esto con la intención de apoyar en cualquier capacidad, necesidad y requerimiento de los clientes.

"Para atender la demanda de servicios, contamos con un promedio de 900 elementos armados y 300 sin armas", refiere el directivo.

La empresa de seguridad privada ofrece valor agregado en el servicio, prueba de ello es la respuesta de sumar más clientes, debido a las buenas referencias que hablan de la compañía en los últimos años en temas de integración de seguridad privada a diferentes negocios para su eficiente cobertura y protección de activos.

"Además de servicio armado, contamos con un centro de seguimiento y monitoreo, un C4 dedicado a todos nuestros servicios como lo es el monitoreo de las unidades y servicios de guardias en cada una de las instalaciones de los clientes; así como el uso de la tecnología con Inteligencia Artificial, para colaborar en cuanto a la identificación de posibles riesgos dentro de las custodias y cobertura al interior de nuestras plantillas de guardias en las diferentes entidades federativas", resalta el Comandante García Coss.

El siguiente paso… proyección del negocio

La generación que actualmente dirige a la empresa, ha logrado consolidar su posicionamiento en el mercado nacional por dos décadas, y lo que sigue es despuntar de la mano de las nuevas generaciones, a través de la sucesión en la dirección del negocio desde Baja California con la expansión hacia Centroamérica, en específico Perú y Honduras.

Pertenecer a diferentes asociaciones, en específico con ASIS desde hace 19 años, le ha permitido al consorcio estar en contacto directo con profesionales de la seguridad a nivel mundial, y hoy nutre sus conocimientos a través de conversaciones y de las diferentes comisiones que integran la asociación.

"Esto es una capacitación del día a día con profesionales del mismo ramo y que a final de cuentas, lejos de tener competencia, tenemos unión, refiere el presidente ejecutivo Juan Manuel García Coss.

"Además, estamos en AMESP, organización de profesionales de la seguridad de la cual tenemos también el apoyo; organizaciones para mejorar continuamente nuestra calidad en el servicio y colaboración con la cadena de suministro, aunado a nuestras certificaciones de ISO y de BASC, en donde potenciamos como fortaleza nuestra estrategia de selección y reclutamiento de colaboradores, ya que una de las principales necesidades que tenemos es la confiabilidad, valores y discreción de la información. Eso ha sido un diferenciador importante para tener un crecimiento constante", afirma.

A lo largo de estos 20 años, reconoce que las competencias son buenas, pero competir contra sí mismo, es mejor, esto con la intención de cumplir con las necesidades que el cliente requiere, lo que se refleja en el crecimiento económico constante que han tenido (del 8 al 12%) de manera anual.

La compañía pertenece a un holding empresarial conformado por las compañías Grupo Corporativo de Prevención, que inició operaciones hace 21 años, Protege, Servicios de Seguridad Privada que se integró hace seis, y Logística y Transporte GCP con 12 años en el mercado. Asimismo, anunció la incorporación de una nueva línea de negocio familiar que vendrá a fortalecer la capacidad de respuesta que hoy tiene para los clientes.

"Compartir con todo el gremio de la seguridad nos da la satisfacción de saber que estamos siendo reconocidos como una de las actividades primordiales para el desarrollo de nuestra sociedad, así como el de pertenecer al Consejo Nacional de Seguridad Privada, donde somos consejeros desde hace algunos años y que obviamente nos da una gran satisfacción, puesto que el mercado de la seguridad está abierto para quien desee trabajar y esforzarse por brindar algo de lo que la sociedad nos ha brindado", finaliza Juan Manuel García Coss.

Juan Manuel García Coss
presidente ejecutivo Protege

FEPASEP realizó en México edición 17 Congreso Panamericano de Empresas de Seguridad Privada

▪ En él se presentó una amplia variedad de conferencias magistrales, paneles de discusión y presentaciones sobre temas clave para la seguridad privada.

▪ Contó con un programa de alta calidad, con renombrados especialistas internacionales y nacionales.

La Asociación Mexicana de Empresas de Seguridad Privada, AMESP, junto con la Federación Panamericana de Seguridad Privada (FEPASEP), llevó a cabo en la Ciudad de México el 17 Congreso Panamericano de Empresas de Seguridad Privada. Cabe destacar que la industria de la seguridad privada en México, ha experimentado un crecimiento significativo de un 25% en los últimos cinco años y representa el 1.8% del PIB nacional, al ser la sede de tan relevante encuentro regional.

El Congreso tiene como misión principal, promover un intercambio entre empresarios, autoridades y clientes de la región latinoamericana para actualizar la oferta de servicios de seguridad privada, a través de la incorporación de nuevas tecnologías y estándares de profesionalización.

Gabriel Bernal Gómez, presidente de la Asociación Mexicana de Seguridad Privada (AMESP), destacó en su mensaje que la seguridad privada se ha convertido en un pilar esencial para el entorno empresarial frente a la situación de seguridad pública que enfrenta el país.

Asimismo recalcó la necesidad imperante de reformar la Ley de Seguridad mexicana, citando que la legislación vigente no satisface las demandas contemporáneas y padece de una falta de sintonía con los avances tecnológicos y los métodos cada vez más complejos utilizados por el crimen organizado.

También expuso las complicaciones que la diversidad legislativa actual implica para las empresas de seguridad privada, las cuales deben obtener múltiples permisos para operar a través de las fronteras estatales.

Para esta edición del Congreso, el equipo organizador de AMESP preparó un programa de alta calidad, con renombrados especialistas internacionales y nacionales que compartirán su expertise, conocimientos y mejores prácticas. Esta edición propuso un enfoque de servicio híbrido que integra guardias altamente capacitados con soluciones tecnológicas avanzadas con Inteligencia Artificial (IA), hasta patrullajes con drones + GPS.

El Congreso reunió expertos y líderes del sector, quienes intercambiaron conocimientos y mejores prácticas. Asimismo, contó con una amplia variedad de conferencias magistrales, paneles de discusión y presentaciones sobre temas clave para la seguridad privada. Además, se ofrecieron diversas oportunidades de networking, donde se establecieron contactos con otros profesionales destacados del sector.

La realización del Congreso, fue enfocar esfuerzos en el intercambio de estrategias y prácticas innovadoras, así como reforzar la posición de la seguridad privada como uno de los principales empleadores en México, con más de 800 mil trabajadores, abogando por normativas que reflejen realidad y necesidades actuales.

Con la asistencia al Congreso de los miembros y asociaciones en la región panamericana, añade Gabriel Bernal Gómez, permitirá fortalecer los lazos de colaboración y cooperación entre las organizaciones.

Gabriel Bernal Gómez
presidente de la Asociación Mexicana de Empresas de Seguridad Privada, AMESP

Expertos en **soluciones menos lesivas**

APRINSA

100 Aprinsa

200 Aprinsa

Modelos: 100 y 200

Equipo de control electronico inteligente

Estan preparadas para detener actividades violentas e ilegales de individuos, mientras no causa efectos mortales al sospechoso. Ideal para ser usado en recorridos de vigilancia en las calles y estaciones de tráfico, hospitales, cortes de justicia, prisiones, etc.

- **Seguro de usar:** Tecnología probada durante décadas sin efectos mortales
- **Rapido de usar:** Efectivamente controla al sospechoso inmediatamente
- **Fácil de usar:** Paraliza al sospechoso por contacto o a distancia al apretar el gatillo, apuntando el láser
- **Listo para usar:** Precio razonable

@seguridad1 33 3700 7721

direccion@aprinsa.net

Certificados apócrifos; desafío de los equipos balísticos

▪ En México 30% de las blindadoras carecen de certificaciones de sus productos y existe un aumento en la edición o falsificación de certificados para concursar en licitaciones.

En un escenario donde la seguridad es una prioridad, los certificados de los materiales balísticos son pilares fundamentales para asegurar la eficacia y fiabilidad de los productos blindados, sin embargo, en México la existencia de certificados apócrifos representa una seria preocupación. Ante este desafío, el Consejo Nacional de la Industria de la Balística (CNB) informa la práctica de algunas empresas que editan los certificados balísticos para ganar licitaciones por lo que promueve la certificación confiable.

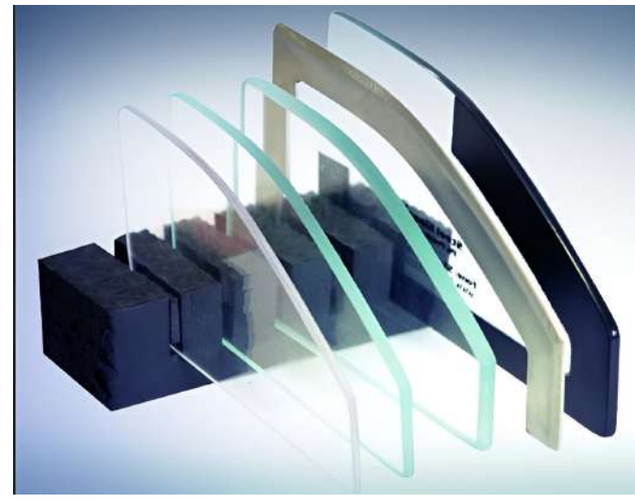
México es uno de los principales mercados de equipos de seguridad en América Latina, lo que subraya la importancia de garantizar la autenticidad de los certificados balísticos en materiales como: el acero, vidrio, cerámicas y las fibras o textiles (como aramidas y polietilenos) para la instalación en el blindaje ya sea automotriz, arquitectónico, corporal y táctico.

Las pruebas y certificados de materiales balísticos desempeñan un papel crítico al proporcionar garantías sobre la calidad y capacidad de los productos, lamentablemente, la proliferación de documentos apócrifos ha provocado desconfianza en la autenticidad de estos, poniendo en riesgo la seguridad de quienes dependen de los equipos.

Estos certificados apócrifos representan una amenaza para el mercado y también pueden llegar a conducir a consecuencias devastadoras.

"Es importante asegurar a los usuarios que las materias primas con las que se trabajó su blindaje tengan un alto desempeño balístico para su protección, porque confían en que estarán protegidos contra cualquier amenaza", indicó, Gadi Mokotov, presidente del Consejo Nacional de la Industria de la Balística (CNB), además mencionó que es crucial promover estándares de calidad y seguridad en la fabricación y uso de materiales balísticos mediante la colaboración con las autoridades reguladoras.

"En el sector, esta situación se ha hecho cada vez más común, en el Consejo Nacional de la Industria Balística nos preocupa que engañen a los clientes diciendo que son materiales y productos de procedencia lícita y trabajamos día con día para fortalecer los procesos de seguridad porque nuestra prioridad es la vida de las personas", aseguraron Daniela Yoshikuma y Gustavo Estrada, delegados de la Comisión de Fabricantes y Comercializadores de Materiales Balísticos del CNB.



Es importante mencionar que en México aunque exista la Norma Oficial Mexicana (NOM) no hay laboratorios que otorguen certificaciones, sin embargo, los que marcan la diferencia en la actualidad son Chesapeake Testing, National Institute of Justice en Estados Unidos, y Beschussamt München en Alemania entre otras internacionales.

"Para nosotros es muy importante interpretar las normas, ya que una mala interpretación puede generar una expectativa diferente con los clientes, así mismo es crucial que tanto los fabricantes como los usuarios finales reconozcan la importancia de estos certificados y apoyen el trabajo", finalizó Germán Padilla, presidente de la Comisión de Fabricantes y Comercializadores de materiales basálticos del CNB.

ASIS INTERNATIONAL™
WOMEN IN SECURITY

"Protegiendo el presente, facilitando el futuro"

V FORO WOMEN IN SECURITY LATAM & CARIBBEAN 2024

01 Y 02 DE AGOSTO 2024

PANAMA

www.wislatam.org

EJES TEMÁTICOS

Conflictos Geopolíticos y Sociales
Innovación y Ciberseguridad
Liderazgo y Resiliencia
Sostentabilidad y Seguridad Humana

ASIS INTERNATIONAL | Women in Security Community

V FORUM WOMEN IN SECURITY LATAM & CARIBBEAN
PANAMA – 2024

ASIS INTERNATIONAL
Advancing Security Worldwide™
www.asisonline.org
Panama Chapter 235

Gestión de proyectos de seguridad, decálogo de errores

▪ Gerentes de proyectos deben adoptar un enfoque proactivo y estratégico para superar errores, lo que incluye establecer procesos de planificación rigurosos, realizar evaluaciones de riesgos detalladas, invertir en la capacitación del equipo, entre otras más.

Caracas, Venezuela.- La gestión eficaz de proyectos de seguridad es un aspecto crítico en protección de activos y prevención de incidentes que pueden comprometer la integridad de una organización. Los gerentes de proyectos que se especializan en seguridad deben ser meticulosos en su enfoque y estar siempre alertas a las variables que pueden afectar el resultado de sus proyectos. A continuación, se detallan los 10 errores más comunes en la gestión de proyectos de seguridad y cómo pueden impactar negativamente en los resultados.

- **Primero.** una definición poco clara del alcance del proyecto. Sin un entendimiento preciso de lo que se debe lograr, es fácil desviarse del objetivo principal, lo que puede resultar en un desperdicio de recursos y en la entrega de un proyecto que no cumple con las necesidades de seguridad requeridas.

- **Segundo.** no realizar una evaluación de riesgos exhaustiva. La seguridad es un campo donde los riesgos no identificados pueden tener consecuencias graves. Una evaluación de riesgos superficial puede dejar vulnerabilidades sin detectar que podrían ser explotadas posteriormente por las amenazas.

- **Tercero.** carecer de un equipo de proyecto adecuadamente capacitado. La seguridad es un área técnica que requiere conocimientos especializados. Un equipo que no posee las habilidades necesarias no podrá implementar las soluciones de seguridad de manera efectiva.

- **Cuarto.** no mantener una documentación adecuada a lo largo del proyecto. La documentación es esencial para la trazabilidad de decisiones, cambios y progreso. Sin ella, es difícil mantener continuidad y responsabilidad dentro del equipo de proyecto.

- **Quinto.** ausencia de métricas de éxito claras. Sin indicadores de rendimiento bien definidos, es difícil medir el éxito del proyecto y saber si los objetivos de seguridad se están cumpliendo efectivamente.

- **Sexto.** no tener un plan de comunicación efectivo. La comunicación es clave en la gestión de proyectos, especialmente en el ámbito de la seguridad, donde la información debe fluir de manera oportuna y precisa para evitar malentendidos que podrían resultar en brechas de seguridad.

- **Séptimo.** gestión ineficaz del cambio. Los proyectos de seguridad pueden requerir adaptaciones debido a cambios en el entorno de amenazas o en los requisitos reglamentarios. La resistencia al cambio puede hacer que el proyecto se vuelva obsoleto antes de su finalización.

- **Octavo.** carencia de un plan de contingencia. Los imprevistos ocurren, y sin un plan de contingencia, un proyecto puede descarrilarse rápidamente ante el primer signo de problemas, poniendo en riesgo la seguridad de la organización.

- **Noveno.** no involucrar a todas las partes interesadas en el proceso de toma de decisiones. La seguridad afecta a toda la organización, y las decisiones tomadas sin la entrada de todas las partes interesadas pueden resultar en soluciones que no son aceptables o efectivas para todos.

- **Décimo.** no realizar revisiones y actualizaciones periódicas. El entorno de seguridad es dinámico, y lo que era adecuado al inicio del proyecto puede no serlo al final. Las revisiones periódicas aseguran que el proyecto se mantenga relevante y efectivo.

Para superar estos errores, los gerentes de proyectos deben adoptar un enfoque proactivo y estratégico. Esto incluye establecer un proceso de planificación riguroso, realizar evaluaciones de riesgos detalladas, invertir en la capacitación del equipo, mantener una documentación completa, definir métricas de éxito claras, establecer canales de comunicación efectivos, gestionar el cambio de manera flexible, preparar planes de contingencia sólidos, involucrar a todas las partes interesadas y realizar revisiones periódicas del proyecto.

Al centrarse en estas áreas clave, los gerentes de proyectos pueden minimizar los riesgos y maximizar la efectividad. La gestión de proyectos de seguridad es una tarea desafiante, pero con la atención adecuada a los detalles y un enfoque en la prevención de errores comunes, es posible lograr resultados que no solo cumplan con los objetivos, sino que también fortalezcan la postura de seguridad general de la organización. En última instancia, el éxito en la gestión de proyectos de seguridad se basa en la capacidad de anticipar problemas, adaptarse a nuevas situaciones y aprender de cada experiencia para mejorar continuamente los procesos y resultados.

Alfredo Yuncoza
Presidente del Consejo Consultivo Latino de IFPO.
Email: ayuncoa@gmail.com.
Instagram y Twitter: @alfredoyuncoza
Venezuela

Articulista Invitado

Inteligencia Artificial y protección: un binomio virtuoso

▪ La IA llega a ser un catalizador que engloba sistemas y máquinas que imitan la inteligencia humana, permitiendo a las máquinas aprender de la experiencia, adaptarse a nueva información y realizar tareas humanas.

Quito, Ecuador.- La intersección de la Inteligencia Artificial (IA) y la protección está transformando la forma en que las sociedades se protegen contra una variedad de amenazas. No solo mejora la capacidad de prever, detectar y responder a riesgos, sino que también optimiza los recursos y proporciona soluciones innovadoras a desafíos antiguos y emergentes. Con este artículo deseo explorar cómo la IA está revolucionando los campos de la protección, los beneficios de esta integración y los desafíos y consideraciones éticas que surgen.

La protección física ha sido tradicionalmente una combinación de vigilancia humana, barreras físicas y tecnologías básicas como alarmas y cámaras de vigilancia. Estos métodos, aunque efectivos en su tiempo, han enfrentado limitaciones en alcance, tiempo de respuesta y capacidad de análisis. Con el auge de la digitalización, la seguridad cibernética ha ganado importancia crucial. Proteger los sistemas informáticos y los datos sensibles de ataques cibernéticos se ha vuelto esencial para organizaciones y gobiernos. Las amenazas cibernéticas incluyen malware, phishing, ransomware y ataques de denegación de servicio.

Es así que actualmente, las amenazas modernas a menudo combinan elementos físicos y digitales, requiriendo una estrategia de protección holística. La convergencia de estos ámbitos demanda soluciones avanzadas que puedan gestionar ambos tipos de amenazas simultáneamente.

La Inteligencia Artificial llega a ser un catalizador que engloba sistemas y máquinas que imitan la inteligencia humana, permitiendo a las máquinas aprender de la experiencia, adaptarse a nueva información y realizar tareas humanas. Sus capacidades clave incluyen el aprendizaje automático (machine learning), el procesamiento del lenguaje natural, la visión por computadora y la robótica.

Este aprendizaje automático permite a los sistemas de IA mejorar su precisión analizando grandes volúmenes de datos. En protección, esto significa que los sistemas pueden prever futuras amenazas basándose en patrones históricos. Esta capacidad permite a las máquinas entender e interpretar el lenguaje humano, útil en la protección para analizar comunicaciones electrónicas y detectar señales de amenazas, siendo por ejemplo la visión por computadora la que permite a los sistemas de IA interpretar imágenes y videos, mejorando la vigilancia y la detección de actividades sospechosas en tiempo real.

De la misma forma, la robótica impulsada por IA permite la creación de dispositivos autónomos para tareas de patrullaje y respuesta a emergencias.

Las aplicaciones de la IA en temas de protección van desde:

Vigilancia y monitoreo

- **Análisis en tiempo real:** Los sistemas de visión por computadora pueden analizar transmisiones de video en tiempo real para detectar comportamientos sospechosos.
- **Reconocimiento facial:** Identifica personas de interés en tiempo real.

- **Monitoreo proactivo:**
Los algoritmos de IA pueden predecir incidentes basándose en patrones de comportamiento.

Seguridad cibernética

- **Detección de amenazas:**
Análisis de grandes volúmenes de tráfico de red para identificar actividades anómalas.
- **Respuesta automática:**
Respuestas automatizadas a ciertas amenazas, como aislar sistemas infectados.
- **Autenticación segura:**
Mejora de sistemas de autenticación mediante el uso de IA.

Protección de Infraestructuras Críticas

- **Mantenimiento predictivo:**
Prevención de fallos en equipos y sistemas.
- **Análisis de riesgos:**
Identificación de riesgos potenciales y vulnerabilidades.

- **Coordinación de respuesta:**
Optimización de la asignación de recursos durante crisis.

Aplicaciones en el entorno corporativo

- **Protección física en instalaciones:**
Monitoreo de entradas y salidas.
- **Protección de datos sensibles:**
Detección y respuesta a accesos no autorizados.
- **Ciberseguridad corporativa:**
Protección contra ataques cibernéticos mediante análisis predictivo.

En este contexto, diremos que la IA mejora la eficiencia y precisión de las operaciones mediante la automatización de tareas repetitivas y proporcionando análisis detallados en tiempo real, reduciendo la necesidad de supervisión humana constante y disminuyendo los costos operativos. Permite un enfoque proactivo de la protección, identificando y mitigando riesgos antes de que se conviertan en problemas, de igual forma pueden adaptarse y escalarse fácilmente para enfrentar nuevas amenazas y desafíos, así como proporcionar información y análisis detallados que mejoran la toma de decisiones en situaciones complejas.

El uso de IA en vigilancia plantea preocupaciones significativas sobre la privacidad. Es crucial establecer políticas claras y transparentes sobre el uso de datos y garantizar el cumplimiento de regulaciones de privacidad. Los algoritmos de IA pueden perpetuar sesgos si se entrenan con datos históricos sesgados. Es esencial desarrollar algoritmos justos y transparentes, y revisar continuamente su desempeño para mitigar estos riesgos. A medida que se adoptan más soluciones de seguridad basadas en IA, aumenta la necesidad de proteger estos sistemas contra ataques. Implementar medidas robustas de ciberseguridad para proteger los sistemas de IA es fundamental. Una excesiva dependencia de la IA para la protección puede ser problemática si no se dispone de planes de contingencia adecuados. Es importante mantener un equilibrio y garantizar que existan capacidades manuales para intervenir en situaciones críticas.

Finalmente diremos que, es crucial abordar los desafíos y consideraciones éticas asociados con el uso de IA, garantizando privacidad, equidad y seguridad de los sistemas. Con un enfoque equilibrado y responsable, la IA puede desempeñar un papel fundamental en la creación de un mundo más seguro y protegido.

Bibliografía:
1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
2. Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
3. Stallings, W. (2021). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
4. Zhu, H., & Timpano, F. (2019). *Artificial Intelligence and Security Challenges*. Springer.

Edison Cadena Ayala
MSC, CPO, CPOI, CSSM
gerente de la empresa
SEINNATIONAL CIA. LTDA.
Ecuador
Articulista Invitado

Panorama de la seguridad infantil

▪ *Ayudemos a crear conciencia sobre la seguridad de los dispositivos a los que pueden acceder niñas y niños.*

Con la finalidad de promover la seguridad en la niñez en Colombia, la empresa Standars & Engagement llevó a cabo una variedad de sesiones por expertos en la materia sobre la problemática de ingesta de pilas tipo botón en niños y niñas; así como interacción de puntos de vista sobre el panorama general de la seguridad en infantil en el país.

UL Standards & Engagement

El evento promovió estándares que ayuden a crear conciencia sobre la seguridad de los dispositivos a los que pueden acceder niñas y niños, mismos que son susceptibles de ingestión.

SAVE THE DATE!

SEGURIDADEXPO

by Fisa | CHILE

25-27 SEPT. 2024

METROPOLITAN SANTIAGO

PARTICIPA EN ESTA NUEVA VERSIÓN Y CONECTA CON LOS LÍDERES DEL SECTOR

¡Visita nuestro sitio web!

Exhibe tus soluciones en productos, servicios y equipamiento.

¡Hablemos! Y agenda una reunión con nosotros

info@seguridadexpo.cl +56 9 4481 6922

@seguridadexpo

METROPOLITAN SANTIAGO,
San Josemaría Escrivá de Balaguer 5.600,
Vitacura, Santiago - Chile

www.seguridadexpo.cl

ORGANIZA Y PRODUCE
Fisa

EXPO 2024 NAVAL®

Somos el centro de negocios para las industrias de defensa, construcción naval y de seguridad en Latinoamérica.

Participa del principal encuentro profesional del sector, la vitrina perfecta para mostrar tus nuevos desarrollos tecnológicos e innovaciones.

3 - 6 DICIEMBRE

TERMINAL DE PASAJEROS
PUERTO VALPARAÍSO - CHILE

XIII EXHIBICIÓN Y CONGRESO INTERNACIONAL
NAVAL Y MARÍTIMA PARA LATINOAMÉRICA.

Participa como Expositor y/o Auspiciador

[CONGRESO INTERNACIONAL]
Los desafíos para la industria de defensa en el nuevo orden internacional.

[14.500]	[+88]	[+7.000]	[+35]	[+500]
M² de superficie	Empresas Expositoras	Visitas Profesionales	Países Participantes	Reuniones de Negocios

¡Contáctanos! **info@exponaval.cl** **+56 9 4481 6922**

Registro visitantes disponible en www.exponaval.cl

ORGANIZA Y PRODUCE

PATROCINAN

AUSPICIA

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

30 AÑOS PROFESIONALIZANDO

PROGRAMA LATINOAMERICANO DE PREPARACIÓN PARA EL EXAMEN DE CERTIFICACIÓN INTERNACIONAL COMO:

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

COORDINADOR
Lic. J. Rubén Fajardo, CPP, PSP, PCI

PARTICIPANTE	COSTO
Socio ASIS	$24,000 M.N. + IVA $1,500 USD + IVA
No socio	$28,000 M.N. + IVA $1,750 USD + IVA

26 SESIONES
Martes y jueves
17 -21 hrs.

MODALIDAD
Presencial y aula virtual

REPASO
Retiro intensivo
32 hrs.

INICIO
08 DE AGOSTO 2024

MAYOR INFORMACIÓN
(55 1321 1289
socios@asis.org.mx

ESS+®

FERIA INTERNACIONAL DE SEGURIDAD

Altavoz ultra grande
Audio súper alto

30+ AÑOS

Generando oportunidades
para la industria de la seguridad
en Latinoamérica

Exhibición tecnológica *en tiempo real*

Showcase *de innovación*

Pabellón *safety*

Conferencias *y talleres*

Rueda de *negocios*

21-23 AGOSTO 2024

Bogotá, Colombia

EXPERIENCIA · NEGOCIOS · PROGRESO

Seguridad Electrónica | Seguridad Industrial | Seguridad Contra Incendios | Ciberseguridad

REGÍSTRESE COMO VISITANTE

Escanee el código QR
para asistir sin costo todos
los días de la feria

Visite una feria madura, con trayectoria y un propósito superior:

ser parte de la solución

GREMIOS ALIADOS

ASIS · COLADCA · ALAS · UAV

ORGANIZAN

IFEMA MADRID · PAFYC · coferias

MEDIOS ALIADOS

MÁS SEGURIDAD Magazine · GLOBAL DEFENSE MAGAZINE

securityfaircolombia.com