Año 7 Nº 46 Julio de 2023

Revista SEGURIDAD .Online

LA PRINCIPAL PLATAFORMA DE INFORMACIÓN DE SEGURIDAD EN LATINOAMÉRICA

& DEFENSA

SHOT FAIR BRASIL 2023
La mayor muestra de tiro deportivo y el mundo táctico

VIGILANCIA CON IA
Una propuesta que llega a Chile

TRÁFICO DE DROGAS HACIA EUROPA
La batalla por los contenedores y la guerra por los puertos

Cámaras Corporales
Próxima incorporación masiva

REDSEG

RED LATINOAMERICANA DE EMPRESAS Y PROFESIONALES EN SEGURIDAD TECNOLÓGICA

REGÍSTRESE, ES GRATIS.

www.redseg.org

SOLICITE SU MEMBRESÍA OFICIAL

planes.redseg.org

PATROCINANTES OFICIALES

Revista SEGURIDAD

DIGITALX C.A
INNOVACIÓN AL LÍMITE
RIF: J40985476-0

GRUPO RAM´S
Seguridad Integral

Asistencia Telefónica: +58 412 4980135 info@redseg.org

EDITORIAL

Nº46 Julio de 2023

Muchos ciudadanos han tomado la desición de evitar ver las informaciones en las mañanas o simplemente cambiar de canal, lo cual representa la mejor demostración del hastío ciudadano, ante la creciente proliferación de asaltos, encerronas, salidas de banco, homicidios, y persecuciones que terminan en horribles accidentes o en víctimas inocentes.

Nos encontramos ante un verdadero espiral de violencia frente al cual no queda claro cuáles son las verdaderas propuestas por parte de la autoridad; más bien somos testigos de una suerte de manejo comunicacional, como si este tipo de hechos pudieran ser explicados mediante la exposición de estadísticas, gráficos, porcentajes de delitos y por último, una que otra comparación con países cuya realidad dista enormemente de la nuestra.

Si bien el crimen organizado es un fenómeno en expansión, el tratamiento y la manera en que este se debe enfrentar constituye una prerrogativa a nivel de cada país.

Chile enfrenta una situación de anomia, en la cual conceptos como la autoridad son debatidos y relativizados, olvidando que toda sociedad civilizada dispone de instituciones a cargo de velar por el orden y la seguridad, los cuales deben contar con el irrestricto apoyo por parte de las autoridades, el cual más allá del aporte en materia presupuestaria, debe manifestarse claramente respecto de un elemento rector en toda sociedad, como es el respeto a la autoridad legítimamente facultada por el estado para imponer el orden y la seguridad ciudadana.

La seguridad es, y será siempre, una prioridad país, por lo anterior resulta doblemente lamentable ver como las autoridades han centrado su agenda comunicacional por casi un mes en discutir problemas derivados de escandalosas situaciones de corrupción, las cuales por importante que sean, no pueden detener, ni distraernos con respecto a nuestras reales prioridades como país.

Robert Gutter Boim
Director

CONTENIDO

www.revistaseguridad.cl
E mail: info@revistaseguridad.cl - revseguridad@gmail.com

AÑO 7 N° 46 Edición Julio 2023

Revista Seguridad Online es una edición de Producciones Gótica Ltda.

Revista Seguridad Online
Director: Robert Gutter Boim
Fotografía Portada: Image by fxquadro on Freepik
Dirección Creativa: Gótica Ltda
Ventas de Publicidad: +56 9 98246696
revistaseguridadonline@gmail.com - ventas@revistaseguridad.cl

Cámaras corporales
Su próxima incorporación masiva

Las recientes indicaciones al proyecto de ley, que establece el deber de efectuar registros audiovisuales de las actuaciones policiales en el procedimiento penal o, mejor conocido como "Proyecto de Ley de Camaras corporales" han llevado a nuestro medio a abordar en detalle las principales características, ventajas y aprehensiones con respecto de este importante implemento, gracias al cual todo procedimiento policial puede ser registrado y respaldado para eventuales indagatorias posteriores

Las cámaras corporales o "body cams" son dispositivos de grabación de video que se utilizan generalmente en la indumentaria o equipo de seguridad de policías, agentes de seguridad, socorristas, personal militar y otros profesionales que trabajan en situaciones potencialmente peligrosas, o que requieren documentación de eventos en tiempo real.

Estas cámaras se diseñan para grabar desde el punto de vista del usuario, capturando imágenes y audio del entorno en el que se encuentran. Por lo general, se utilizan para obtener evidencia objetiva de incidentes, interactúan con el público y, en general, para mejorar la transparencia y responsabilidad en el desempeño de sus funciones.

Beneficios de las cámaras corporales:

1. Evidencia objetiva: Ayudan a obtener una representación imparcial de lo que sucedió durante una interacción o incidente.

2. Protección y seguridad: Pueden ser una herramienta de protección tanto para el usuario, como para las personas con las que interactúan.

3. Responsabilidad y transparencia: Fomentan la responsabilidad entre los profesionales que las utilizan, ya que saben que sus acciones están siendo grabadas.

4. Capacitación y mejora: Las grabaciones pueden ser utilizadas para la formación del personal y la mejora de los procedimientos, en base a experiencias pasadas.

5.Recopilación de pruebas: Pueden utilizarse en casos judiciales o investigaciones para presentar pruebas visuales.

Es importante señalar que el uso de las cámaras corporales también plantea cuestiones relacionadas con la privacidad y el manejo adecuado de los datos grabados, por lo que suele haber regulaciones y políticas específicas para su utilización.

En las labores policiales, las cámaras corporales son dispositivos de grabación de video que se utilizan como parte del equipo estándar en muchas jurisdicciones. Estas cámaras son usadas por los oficiales para capturar imágenes y audio de sus interacciones con el público y eventos que ocurren durante su servicio.

El uso de cámaras corporales en la policía tiene varios propósitos y beneficios:

1.Evidencia objetiva: Las grabaciones de video proporcionan una representación imparcial de los incidentes, lo que puede ser crucial en la investigación y enjuiciamiento de casos.

2.Responsabilidad y transparencia: La presencia de cámaras puede fomentar la responsabilidad en los oficiales, ya que saben que sus acciones están siendo grabadas, lo que puede conducir a un comportamiento más profesional y ético.

3.Protección para el oficial y el público: Las body cams pueden servir como una herramienta para proteger a los oficiales de acusaciones falsas o infundadas y, al mismo tiempo, proteger los derechos de los ciudadanos durante los encuentros con la policía.

4.Capacitación y mejora: Los videos grabados pueden ser utilizados para la formación y evaluación de los oficiales, ayudando a mejorar las tácticas y prácticas policiales.

5.Resolución de conflictos: Las grabaciones de video pueden ayudar a resolver disputas y aclarar hechos, en situaciones de confrontación.

Es importante mencionar que el uso de cámaras corporales en la policía también plantea desafíos relacionados con la privacidad de las personas grabadas, la retención y el acceso a los datos, así

como la capacitación adecuada para los agentes, sobre el uso apropiado de estas cámaras.

Las políticas y regulaciones sobre el uso de cámaras corporales varían según las jurisdicciones, y muchos departamentos policiales tienen pautas específicas para determinar cuándo y cómo deben ser activadas y desactivadas las cámaras, así como la retención y acceso a las grabaciones. Estos aspectos son fundamentales para equilibrar los beneficios de la transparencia y la rendición de cuentas con la protección de la privacidad individual.

Ventajas de las cámaras corporales

Las cámaras corporales ofrecen diversas ventajas en diferentes contextos y situaciones. Algunas de las principales ventajas de su uso son:

1.Evidencia objetiva: Las grabaciones de video proporcionan una representación imparcial y objetiva de los eventos y las interacciones, lo que puede ser valioso en investigaciones y juicios. Ayudan a evitar la distorsión de los hechos y las versiones contradictorias, al tener un registro visual directo de lo que sucedió.

2.Transparencia y responsabilidad: El uso de cámaras corporales fomenta la transparencia en las acciones de los individuos o profesionales que las llevan. Saber que están siendo grabados puede aumentar la responsabilidad y disuadir comportamientos inapropiados.

3.Protección para los implicados: Las cámaras corporales pueden proteger tanto a los usuarios de las cámaras, como a las personas con las que interactúan. Las grabaciones pueden ser útiles para demostrar que los oficiales o profesionales actuaron adecuadamente, en situaciones de confrontación.

4.Resolución de disputas: Las grabaciones en video pueden ser utilizadas para resolver disputas o conflictos entre las partes involucradas. Al contar con una evidencia visual, se pueden aclarar malentendidos y discrepancias en versiones de los eventos.

5.Mejora de la capacitación: Las grabaciones de las cámaras corporales pueden ser utilizadas para la formación y evaluación del personal. Los videos pueden servir como material de capacitación para mejorar las tácticas y prácticas en diversos campos, como la policía, los servicios de emergencia, entre otros.

6.Reducción de quejas y demandas: La presencia de cámaras corporales puede llevar a una disminución en las quejas y demandas contra los profesionales que las usan, ya que las grabaciones pueden aclarar situaciones y prevenir acusaciones falsas.

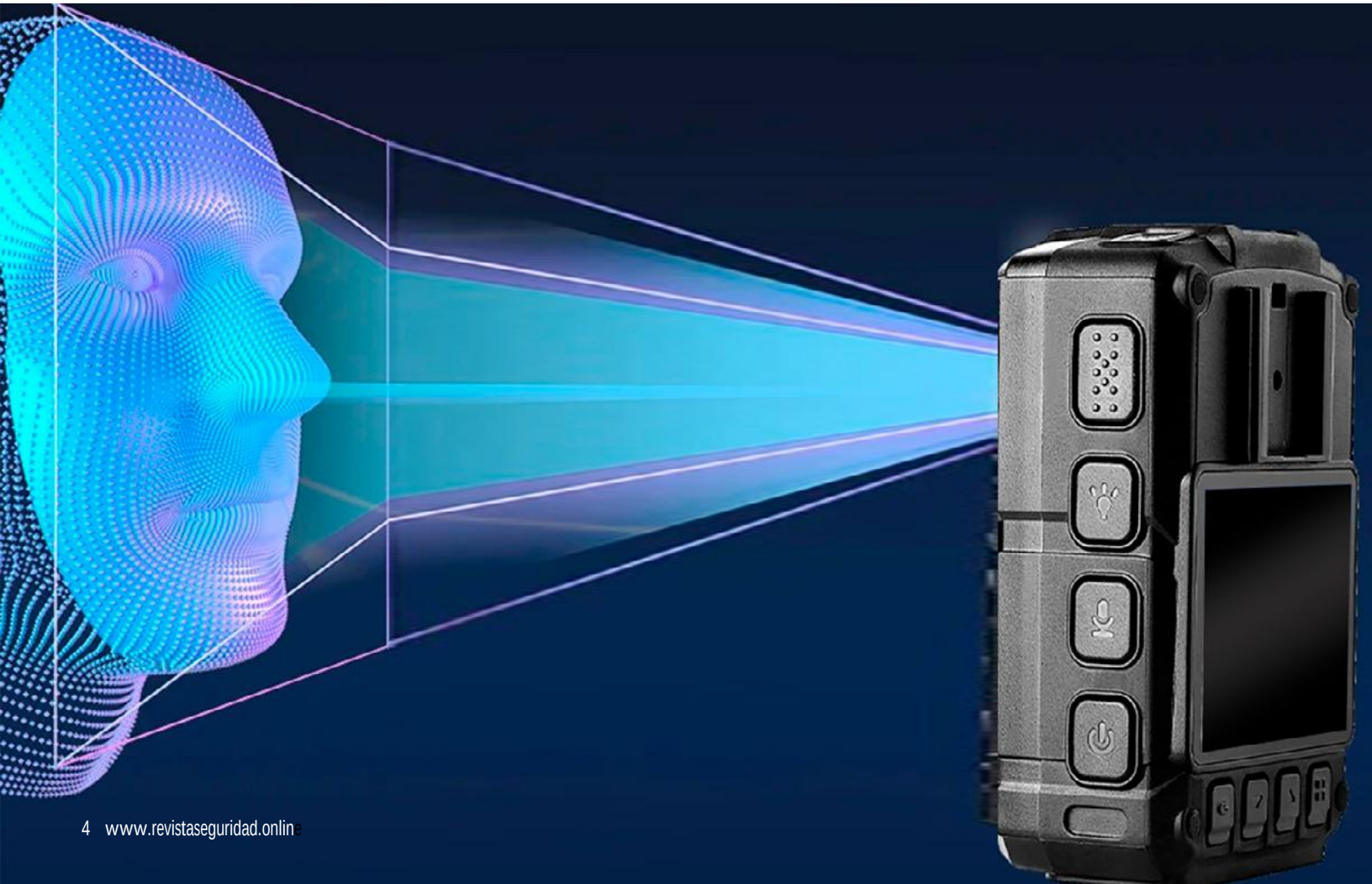
7.Documentación de eventos importantes: Las cámaras corporales permiten documentar en tiempo real eventos relevantes que pueden ser útiles para posteriores investigaciones, o revisiones.

8.Uso en contextos profesionales y recreativos: Además de los campos profesionales, como la seguridad y la policía, las cámaras corporales también se utilizan en actividades recreativas y deportivas extremas para capturar momentos emocionantes desde la perspectiva del usuario.

Es importante tener en cuenta que, si bien las cámaras corporales ofrecen numerosas ventajas, también plantean desafíos éticos y de privacidad en términos de cómo se recopilan, almacenan y acceden a las grabaciones. Es esencial establecer políticas claras y regulaciones, para garantizar un uso adecuado y responsable de estas cámaras.

Peligros y desafíos en el uso de las cámaras corporales

El uso de cámaras corporales también conlleva ciertos peligros y desafíos, que deben ser considerados para garantizar un equilibrio adecuado entre los beneficios y las preocupaciones relacio-



nadas. Algunos de los peligros más importantes son los siguientes:

1.Privacidad y derechos civiles: Las cámaras corporales pueden capturar imágenes y audio de personas y lugares sin su consentimiento, lo que puede plantear cuestiones de privacidad y violación de los derechos civiles. Es esencial establecer políticas claras sobre cuándo y dónde se pueden utilizar las cámaras para evitar abusos o la invasión de la privacidad.

2.Uso indebido: Existe el riesgo de que las cámaras corporales puedan ser utilizadas de manera inapropiada o para propósitos no autorizados, como la vigilancia injustificada o el acoso. Un control adecuado y normas estrictas sobre el uso de las cámaras son cruciales para prevenir posibles abusos.

3.Manipulación de grabaciones: Si no se protege adecuadamente el acceso y la integridad de las grabaciones, existe la posibilidad de que sean manipuladas o editadas, lo que podría comprometer la veracidad de la evidencia presentada en juicios o investigaciones.

4.Desconfianza y relaciones comunitarias: Aunque las cámaras corporales pueden aumentar la transparencia y la rendición de cuentas, algunas comunidades pueden sentir que su privacidad está siendo invadida y que la presencia constante de cámaras, genera desconfianza hacia las fuerzas de seguridad o profesionales que las utilizan.

5.Costos y logística: La implementación y mantenimiento de sistemas de cámaras corporales puede ser costosa, especialmente para organismos gubernamentales o empresas con recursos limitados. También implica una logística adicional para almacenar y gestionar grandes cantidades de datos de video.

6.Distracción y seguridad del usuario: Las cámaras corporales pueden convertirse en una distracción para el usuario en ciertas situaciones críticas o peligrosas. Los profesionales que las usan deben asegurarse de que el dispositivo no interfiera con sus responsabilidades, o ponga en riesgo su seguridad.

7.Dificultad en situaciones de alta tensión: En algunas situaciones de alta tensión o confrontación, los oficiales pueden olvidar activar o desactivar adecuadamente las cámaras, lo que puede resultar en la pérdida de información crucial.

8.Limitaciones técnicas: Las cámaras corporales pueden tener limitaciones en cuanto a calidad de video, ángulo de visión y duración de la batería, lo que puede afectar la utilidad de las grabaciones en ciertos escenarios.

Para mitigar estos peligros, es esencial establecer políticas claras y específicas sobre el uso de cámaras corporales, proporcionar capacitación adecuada al personal sobre su uso apropiado y respetar los derechos individuales y la privacidad de las personas grabadas. También se debe garantizar un almacenamiento seguro y una gestión responsable de las grabaciones para evitar su mal uso, o acceso no autorizado.

Cámaras corporales online

Las cámaras corporales pueden referirse a dos conceptos diferentes:

1. Cámaras corporales con transmisión en vivo:

Algunas cámaras corporales están diseñadas para transmitir en tiempo real las imágenes y el audio que capturan a través de una conexión a Internet. Estas cámaras permiten a los usuarios o autoridades ver y supervisar las imágenes en tiempo real desde una ubicación remota. Esta funcionalidad puede ser útil en situaciones en las que se necesita una respuesta rápida o cuando se requiere supervisión en tiempo real de las acciones del usuario.

2.Acceso en línea a grabaciones de cámaras corporales:

También puede referirse a la posibilidad de acceder en línea a las grabaciones almacenadas en las cámaras corporales después de que se hayan realizado. Esto puede implicar que las grabaciones se carguen en un servidor seguro y se acceda a ellas mediante una plataforma en línea con las credenciales de acceso adecuadas. Esto es útil para administrar y revisar las grabaciones, especialmente en organizaciones o departamentos que requieren un seguimiento y análisis posterior de las interacciones y eventos registrados.

En ambos casos, el acceso en línea a las cámaras corporales plantea desafíos adicionales en términos de seguridad, privacidad y protección de datos. Es esencial asegurarse de que las transmisiones en vivo o las grabaciones almacenadas estén protegidas de accesos no autorizados y se gestionen de acuerdo con las regulaciones de privacidad y protección de datos aplicables. También se debe garantizar que el acceso a estas grabaciones esté restringido solo a personas autorizadas y que se implementen medidas adecuadas para evitar el mal uso o la manipulación indebida de las imágenes, y el audio capturados.

Cámaras corporales en procedimientos policiales: las imágenes aumentan la confianza entre agentes y comunidad

• Es una tendencia en el mundo que las policías se modernicen y busquen tecnologías de punta para proteger a su personal en terreno. Pero no solo por la necesidad de avanzar en materia de transparencia y confianza mutua con la comunidad, sino también para que los procesos sean más eficientes y la justicia pueda contar con evidencia y pruebas concretas.

• Uno de los elementos diferenciadores de las cámaras corporales de Motorola Solutions es que la información capturada no se puede manipular, editar o compartir en dispositivos externos. El material se puede reproducir las veces que sea necesario, de manera controlada, para revisar evidencia crítica y hacer un análisis posterior al incidente, guardar la información valiosa y desechar lo que no es útil.

Octubre de 2022. Estados Unidos. El Departamento de Interior informa que todas las fuerzas de seguridad que patrullen las calles y estén en contacto con los ciudadanos, deberán portar cámaras corporales. En un comunicado, la autoridad dio a conocer las nuevas normas, cuyo objetivo declarado es mejorar la seguridad, la transparencia y la rendición de cuentas. En la última línea, incrementar la confianza entre los agentes y los ciudadanos.

Marzo de 2023. Nashville. La Policía de esa ciudad, en el Estado de Tennessee, divulga las imágenes captadas por la cámara corporal de uno de sus agentes, las que muestran, segundo a segundo, el procedimiento policial que se llevó a cabo para neutralizar a la tiradora que atacó a tres niños que estudiaban en The Covenant School. El mundo pudo enterarse del proceder de la policía y del modus operandi de la atacante. La noticia recorrió el orbe por su crudeza, pero sin espacio para subjetividades ni versiones encontradas.

Los hechos hablan muy fuerte: Las cámaras corporales —que pueden ser usadas por agentes de seguridad, emergencias, de tránsito y bomberos, incluso en ambientes industriales y empresariales — permiten la documentación de eventos en tiempo real, antes, durante y después de un incidente. Así, actúan como otros "ojos" que cuidan y registran que se cumpla la ley. Brindan transparencia en su material documentado, protegen la cadena de custodia y operan como evidencia de alto valor en cualquier proceso judicial. Esto se traduce, en la práctica, en más confianza ciudadana.

En el caso de Francia —otro país donde los procedimientos policiales hacen noticia de manera recurrente—, el Gobierno también decidió abordar la transparencia y mejorar el accountability a través de la tecnología. A partir de 2021, el Ministerio del Interior francés dotó a sus fuerzas de seguridad de un stock de más de 30.000 cámaras corporales Motorola. La Policía de Bélgica, Rumania y varias fuerzas policiales del Reino Unido también han avanzado en esa dirección.

Claramente, es una tendencia en el mundo que las policías se modernicen y busquen tecnologías de punta para proteger a su personal en terreno. Pero no solo por la necesidad de avanzar en materia de transparencia, sino también para que los procesos sean más eficientes y la justicia pueda contar con evidencia y pruebas concretas.

En Chile, la autoridad comienza a dar pasos en la misma dirección. Este año, de hecho, el ministro de Hacienda anunció recursos adicionales por US$1.500 millones para seguridad, recursos que se destinarán, entre otras cosas, a fortalecer las capacidades de las policías mediante la adquisición de equipamiento y material de transporte, implementos de protección y, específicamente, cámaras corporales que incrementen la confianza entre los agentes y la comunidad.

Para Mauricio Bórquez, experto en seguridad de Motorola Solutions, avanzar en esta dirección debe ser un elemento clave en el proceso de fortalecimiento de las policías chilenas: "Las imágenes captadas a través de distintos dispositivos no solo mejoran la confianza entre las policías y las comunidades, sino que también constituyen la evidencia más potente e incomparable para mostrar una verdad. ¿Cualquier imagen?, claramente no. Las imágenes son valiosas en la medida que mantengan su pureza y primitiva conservación, de modo de mostrar la realidad no manipulada ni maquillada".

El ejecutivo agrega: "En Motorola Solutions sabemos que disponer de una cadena de custodia segura es condición sine qua non para que los intervinientes del proceso penal puedan considerar este tipo de evidencias como elementos plenamente válidos. Tenemos la tecnología necesaria para responder a lo que las policías modernas y los tribunales de garantía exigen: una solución de continuidad en el proceso de manejo de la evidencia, desde que es detectada hasta que se da inicio a la cadena de custodia, la que no puede ser interrumpida. Es lo que hoy se conoce como virtualización de la cadena de custodia de la evidencia, contemplada en el CPP, fundamental para garantizar el Proceso Penal"

Cámaras y sensación de seguridad

Las cámaras corporales se han posicionado como una herramienta fundamental en la captura y registros de incidentes. De allí que más del 60% de los ciudadanos aseguran sentir mayor sensación de seguridad en sociedad cuando se utilizan tecnologías avanzadas de video, según el estudio "Consenso por el cambio" de Motorola Solutions.

Tal como indica Mauricio Bórquez, de Motorola Solutions, la posibilidad de grabar los hechos y las interacciones que se presentan en un procedimiento a través de cámaras corporales, permite que la información sea compartida con centros de comando y control, y se utilice para la toma de decisiones. De esta manera, aporta mayor conocimiento situacional para que la policía tome decisiones de manera ágil, eficiente y certera.

Uno de los elementos diferenciadores de la tecnología de Motorola Solutions, es que la información capturada por estas cámaras no se puede manipular, editar o compartir en dispositivos externos, para mayor seguridad y protección. El material se puede reproducir las veces que sea necesario, de manera controlada, para revisar evidencia crítica y hacer un análisis posterior al incidente, guardar la información valiosa y desechar lo que no es útil.

Claramente, la tecnología de Motorola Solutions supone un salto importante en materia de confianza para policías y comunidades y una oportunidad para la administración de justicia con evidencia de calidad.

Líderes a nivel global

Con más de 100 mil clientes, en 100 países alrededor del mundo, Motorola Solutions es el líder global en el campo de las comunicaciones y la video seguridad. Fue la creadora de los equipos que transmitieron las primeras palabras de Neil Armstrong desde la luna, en 1969, y hoy trabaja con la mayoría de las policías más prestigiosas y profesionales del mundo.

En el caso de Chile, Motorola Solutions es proveedor de las principales agencias de seguridad y protección civil y, gracias a esa confianza y calidad de sus soluciones, pudo proporcionar—mediante licitación— un conjunto de 300 cámaras corporales para Carabineros, en abril de 2020.

La tecnología de cámaras corporales de Motorola Solutions, está diseñada para cumplir con el alto estándar de seguridad del Ministerio del Interior de Francia, La Policía y Guardia fronteriza de Rumania y la Policía de Lituania, por citar algunos ejemplos.

El hardware y el software de video incluyen el seguro algoritmo de cifrado, AES-256, utilizado ampliamente en aplicaciones gubernamentales y militares para ayudar a garantizar que el sistema esté a prueba de manipulaciones. Mediante este sistema nada se puede ver, modificar o eliminar, sin el conocimiento del propietario del sistema y las cámaras no tienen memoria extraíble, lo que evita la recuperación de imágenes de dispositivos perdidos o robados.

"Grabar los hechos y las interacciones que se presentan en un procedimiento a través de cámaras corporales permite que la información sea compartida con centros de comando y control y se utilice para la toma de decisiones"

"En Motorola Solutions sabemos que disponer de una cadena de custodia segura es condición sine qua non para que los intervinientes del proceso penal puedan considerar este tipo de evidencias como elementos plenamente válidos".

CÁMARA CORPORAL PARA SEGURIDAD PÚBLICA

CAPTURE EVENTOS CON TOTAL PRECISIÓN

MOTOROLA SOLUTIONS

F01, más que una cámara corporal una plataforma para responder a emergencias

De la mano de la empresa nacional Begoo, llega a chile la camara corporal F01, fabricada por la reconocida empresa taiwanesa RTS. Es importante recordar que la serie RT Stream RTS F01 y el Sistema de respuesta de emergencia móvil (MERS) fueron nominados para los Premios a la innovación CES 2022 en la categoría de productos de tecnologías portátiles en función del esquema sobresaliente, y el diseño innovador del producto de ingeniería.

Disponer de la posibilidad de Comandar y coordinar acciones policiales, de seguridad o de desastre, requieren de la incorporación de dispositivos de transmisión de imagen y audio en tiempo real los cuales permitirán al supervisor remoto poder ver, oír, hablar, localizar y enviar notificaciones de alerta en cuestión de segundos.

F01 es una cámara corporal de transmisión en tiempo real 5G, diseñada para el ejército, la policía, extinción de incendios, investigación e inspección de campo, operaciones peligrosas y otras aplicaciones especiales. Equipado con funciones de red Wi-Fi y LTE 4G y 5G, la exclusiva tecnología de codificación de video proporciona un tiempo de transmisión rápido.

La memoria eMMC de 64 MB incorporad,a puede almacenar el video. Además, la plataforma del servidor en la nube iCommander y el cliente proporcionan una solución total de las funciones de la aplicación.

Incorporado con SOC de compresión de video Ambarella S5 y sensor SONY imx385 Micro-starlight.

El sistema de respuesta de emergencia Mobile, consiste en una cámara multifunción móvil portátil / alimentada por batería de litio / 5G de transmisión en vivo inalámbrica, la cual proporciona las mejores capacidades de comando y acción visual habilitadas para audio.

Puede proporcionar video en tiempo real, walkie talkie grupal, posicionamiento y alertas que salvan vidas. Cuando los comandantes ven y hablan al mismo tiempo, es fácil conocer la situación de forma remota para reducir o evitar la pérdida de vidas y el mando en tiempo real.

Cámara corporal F01 5G

Directamente a través del 5G incorporado o wifi, para proporcionar funciones todo en uno de audio / video / alarma en tiempo real. Hay 2 canales de baja lux. Video HD, charla grupal y broadcast, posicionamiento, salvamento y gestión de tareas.

La cámara corporal RTS F01 proporciona compresión dinámica de video / audio, compresión optimizada de acuerdo con el tamaño de ancho de banda 4G / 5G, transmisión en tiempo real de video HD y conversaciones de muchos a muchos con la latencia más baja, y al mismo tiempo, el F01 almacena localmente en EMM,C con la mejor calidad de video y ancho de banda de 1080p

* Batería de litio miniaturizada incorporada, admite varias formas de desgaste

* Soporte de batería de litio Large 6000mAH para funcionamiento completo hasta 4.5 horas, red continua 4G y transmisión de video HD en tiempo real, llamadas de múltiples partes, alertas que salvan vidas, posicionamiento y gestión de tareas.

* Las llamadas grupales PTT (Push To Talk) se pueden hacer con F01, comandante in situ y supervisor en la nube.

* El F01 proporciona visión nocturna a todo color bajo la luz extremadamente baja, sin necesidad de encender la luz infrarroja. En el caso de oscuridad completa, la luz infrarroja se puede encender automáticamente para video en blanco y negro, y cuando se cambia a luz de estrellas, puede volver automáticamente a imágenes a todo color.

La "cámara multifunción 5G portátil" con transmisión 5G y sistema altamente integrado reduce la carga y garantiza la seguridad. También logra las funciones todo en uno más completas y minimizadas en un solo dispositivo F01. Con el servidor de plataforma en la nube iCommander y el control de aplicaciones, todos transmiten video, audio y alarmas a través de 4G o wifi para proporcionar cinco funciones todo en uno, en tiempo real.

Grabación y reproducción de vídeo/audio local y en la nube

Cuando el personal enciende el dispositivo RTS-F01, además de transferir instantáneamente imágenes HD al servidor y almacenarlas, graba inmediatamente las imágenes de alta calidad de 1080p en el almacenamiento RTS-F01 eMMC para su posterior reproducción, comparación y rastreo, y para evitar el uso de tarjetas micro

SD para el almacenamiento, que se dañarán (big problemascomo pistas, grabaciones perdidas e intercambios intencionales).

Monitoreo en tiempo real de video HD nocturno a todo color

RTS-F01 2CH cámara nocturna a todo color, siempre que haya una luz estelar débil, puede obtener video en color sin luz infrarroja. El centro de control y los comandantes in situ, pueden mantener un estrecho contacto con el personal de primera línea en cualquier momento, garantizar el envío en tiempo real, la ambulancia y el apoyo de emergencia en tiempo real.

Controle completamente la situación en tiempo real al mejorar la eficiencia frente a desastres, permitiendo garantizar la seguridad y la vida de las personas, mejorar la eficiencia de socorro en casos de desastre, eficiencia en el trabajo reduciendo la ocurrencia de desastres

Escucha en tiempo real

El comandante puede configurar una sola escucha F01, grupo F01 PTT hablando y todos los F01 PTT hablando en cualquier momento a través de la aplicación

Adicionalmente el sistema proporcionaconversaciones grupales en tiempo real.

Se puede utilizar como segunda vía además de walkie-talkies, debido a la radiación de calor y la a menudo incapacidad para comunicarse en el edificio, lo anterior es posible gracias a la tecnología exclusiva de cableado dinámico para garantizar un paquete de voz uno a uno, asegurando un flujo mínimo de archivos de audio.

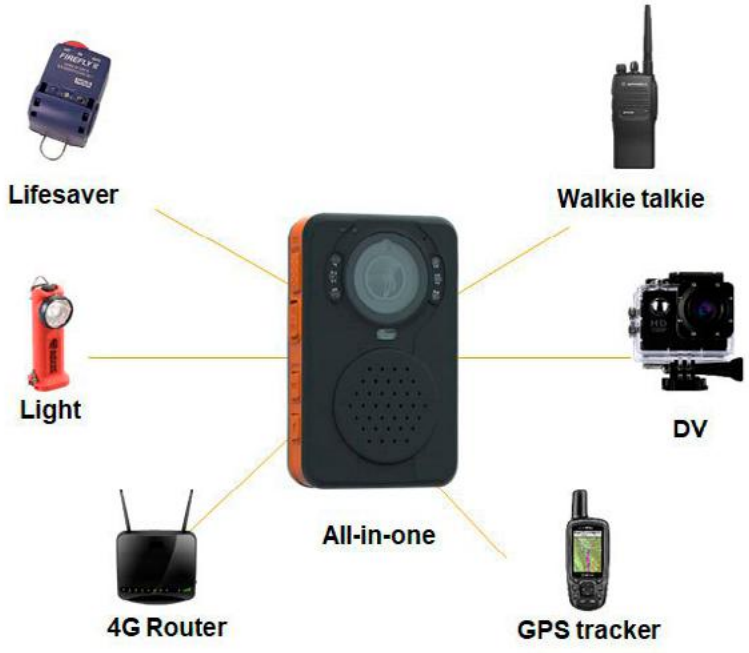
GPS, WIFI, posición LBS

RTS-F01 y APP pueden proporcionar posición en tiempo real a través de GPS, WIFI y LBS de manera triple para evitar la situación cuando el GPS ingresa al edificio sin conexión con un satélite artificial y hacer que el posicionamiento a menudo sea imposible. Combinamos GPS y capturamos routers WIFI cercanos y estaciones base 4G, y realizamos operaciones para obtener información de posicionamiento, asegurándonos de obtener la ubicación y el estado de forma correcta y precisa.

El sistema MERS utiliza las cámaras corporales profesionales F01, tienen la capacidad de descargar online las grabaciones de video realizadas, en el servidor que el cliente defina, usando las redes 3G, 4G, 5G y WiFi. No usa Dock Station. No usar dock station en un proyecto significa un gran ahorro de dinero y tiempo, en la puesta en servicio de las F01.

Las instalaciones de éstas traen consigo problemas de disponibilidad de enchufes eléctricos, puertas ETH, cables, router, transporte de equipos y técnicos por cada localidad en que se usan las cámaras.

También, la mantención es más sencilla considerando que todas las redes son inalámbricas, descartando fallas de HW y solucionando los problemas en línea de manera expedita Adicionalmente, la puesta en servicios de cada F01 es rápida y facilita la distribución de los equipos en todo el país.



Servidor de plataforma en la nube, proporcionando las siguientes funciones: Software de plataforma de servidor (basado en Linux),

Mayores informaciones: www.begoo.cl

Consideraciones al seleccionar una metodología de análisis de riesgos

Foto de Tima Miroshnichenkpexels.com

Los riesgos de seguridad son aquellos que pueden afectar negativamente a la integridad, confidencialidad o disponibilidad de la información u otros activos de una organización. Para gestionar estos riesgos, es necesario realizar un análisis que permita identificarlos y evaluarlos de forma adecuada.

Una metodología de evaluación de riesgos es un enfoque sistemático para llevar a cabo este proceso. Sin embargo, no existe una única metodología que sea válida para todos los casos, sino que se debe seleccionar la más apropiada en función de diversos factores.

Algunos de los factores a considerar al seleccionar una metodología de evaluación de riesgos incluyen:

El objetivo del análisis de riesgos.

¿Qué se pretende conseguir con el análisis? ¿Qué tipo de decisiones se van a tomar en base a sus resultados? ¿Qué nivel de detalle se requiere? El objetivo determina el alcance y la profundidad del análisis, así como los criterios de evaluación y tratamiento de los riesgos. Por ejemplo, si el objetivo es cumplir con una normativa o estándar específico, se deberá elegir una metodología que sea compatible con sus requisitos y que proporcione evidencias suficientes para demostrar el cumplimiento. Si el objetivo es mejorar la gestión de la seguridad, se deberá elegir una metodología que permita identificar las áreas más críticas, y las medidas más efectivas para reducir los riesgos.

El contexto del análisis de riesgos.

Las organizaciones más grandes y complejas pueden requerir una metodología de evaluación de riesgos más sofisticada que las organizaciones más pequeñas y simples. ¿Qué características tiene la organización que realiza el análisis? ¿Qué tipo de activos se van a analizar? ¿Qué amenazas y vulnerabilidades se enfrentan? ¿Qué requisitos legales, contractuales o éticos se deben cumplir?

El contexto influye en el nivel de riesgo aceptable, así como en las fuentes de información y los métodos de recogida de datos que se pueden utilizar. Por ejemplo, si la organización tiene una alta dependencia de la tecnología, se deberá elegir una metodología que contemple los riesgos asociados a los sistemas informáticos y las redes. Si la organización tiene una gran diversidad de activos, se deberá elegir una metodología que permita clasificarlos y priorizarlos según su importancia.

Apetito de riesgo de la organización.

El apetito de riesgo de la organización, es la cantidad de riesgo que está dispuesta a aceptar. La metodología de evaluación de riesgos debe ser capaz de identificar y evaluar los riesgos que están dentro del apetito de riesgo de la organización.

Recursos disponibles para el análisis de riesgos.

¿Qué tiempo, dinero y personal se puede dedicar al análisis? ¿Qué nivel de conocimiento y experiencia tienen los participantes? ¿Qué herramientas o técnicas se pueden emplear? El recurso condiciona la viabilidad y la calidad del análisis, así como el grado de involucración y compromiso de los interesados. Por ejemplo, si el recurso es limitado, se deberá elegir una metodología que sea sencilla y rápida de aplicar, pero que no comprometa la validez y la fiabilidad de los resultados. Si el recurso es amplio, se podrá elegir una metodología más compleja y rigurosa, pero que requiera más capacitación y coordinación.

Requisitos reglamentarios de la organización.

Es posible que se requiera que la organización cumpla con ciertos requisitos reglamentarios, como los exigidos por la Ley Sarbanes-Oxley o la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA), entre otros. La metodología de evaluación de riesgos debe ser capaz de abordar estos requisitos.

Además de estos factores, la organización también debe considerar lo siguiente al seleccionar una metodología de evaluación de riesgos:

Facilidad de uso de la metodología.

La metodología debe ser de fácil comprensión y uso por parte del personal de la organización.

Flexibilidad de la metodología.

La metodología debe ser lo suficientemente fle-

xible para adaptarse a las necesidades específicas de la organización.

Precisión de la metodología.

La metodología debe ser capaz de producir resultados precisos y confiables.

Costo de la metodología.

El costo de la metodología debe ser razonable y asequible para la organización.

Estos son solo algunos ejemplos de los factores que se deben tener en cuenta para seleccionar una metodología en análisis de riesgos de seguridad. No obstante, existen otros elementos que pueden ser relevantes según el caso concreto, como la cultura organizacional, las expectativas de los clientes o las tendencias del mercado.

Tipos de metodologías de evaluación de riesgos

Existen dos tipos principales de metodologías de evaluación de riesgos: cualitativas y cuantitativas. Las metodologías cualitativas utilizan el juicio subjetivo para evaluar los riesgos, mientras que las metodologías cuantitativas utilizan datos numéricos para evaluar los riesgos.

Algunos ejemplos de metodologías cualitativas de evaluación de riesgos incluyen:

Modelado de amenazas: identifica y evalúa las amenazas a las que se enfrenta una organización.

Análisis de impacto comercial: identifica los activos críticos de una organización y evalúa el impacto de una interrupción en esos activos.

Análisis FODA: El análisis FODA identifica las fortalezas, debilidades, oportunidades y amenazas que enfrenta una organización.

Algunos ejemplos de metodologías de evaluación de riesgos cuantitativos incluyen:

Simulación de Monte Carlo: utiliza números aleatorios para generar una distribución de posibles resultados. Esta distribución se puede utilizar para estimar la probabilidad de que ocurra un riesgo y el impacto potencial de ese riesgo.

Análisis de árbol de fallas: identifica las posibles causas de un evento en particular.

Análisis del árbol de eventos: el análisis del árbol de eventos identifica las posibles consecuencias de un evento en particular.

El mejor tipo de metodología de evaluación de riesgos para una organización dependerá de las necesidades específicas de la organización. Si la organización necesita producir resultados precisos y confiables, entonces una metodología cuantitativa puede ser la mejor opción. Sin embargo, si la organización necesita una metodología que sea fácil de usar y flexible, entonces una metodología cualitativa puede ser una mejor opción.

La selección de una metodología de evaluación de riesgos es una decisión importante que debe tomarse con cuidado. La organización debe considerar todas sus necesidades y requisitos, al hacerlo, puede asegurarse de que está seleccionando la mejor opción para su situación específica.

Autor:
Alfredo Yuncoza
Presidente del Hispanic Advisory Board de IFPO.

En plena era del IoT y las smart home ¿Son realmente seguras las cámaras de videovigilancia?

Piezas fundamentales para proteger los perímetros hogareños, estos dispositivos son cada vez más importantes para obtener registros de la actividad sospechosa en los alrededores. Sin embargo, al estar conectados, se transforman en una posible entrada para los ciberdelincuentes.

Las podemos ver a menudo en las afueras de casas, locales, empresas, instituciones y hasta en jardines infantiles y colegios. Símbolos de la seguridad, más que una medida preventiva para evitar robos y un elemento disuasorio, las cámaras de seguridad sirven para tener registros visuales frente a hechos de delincuencia y actividad sospechosa.

Sin embargo, si bien desde hace algunos años estamos viviendo el auge de los dispositivos conectados a internet en el hogar como televisores, refrigeradores y hasta lavadoras, aún no existe noción del riesgo que implica tener una cámara IP. Lo cierto es que, conectada inherentemente a la red (cableada o inalámbrica), es un foco de vulnerabilidad.

"Cómo política de Estado y de varios gobiernos, la conectividad del país crece satisfactoriamente. No obstante, aquello no está ligado a políticas de ciberseguridad básicas. Y esto es aún más crítico en los hogares. Por lo tanto, es difícil saber si los dispositivos de grabación son infalibles. Cumplen un rol fundamental, pero son una puerta de entrada y brecha donde hay que poner mucho cuidado", explica Walter Montenegro, gerente de ciberseguridad para Cisco Chile.

En los últimos años, las soluciones de videovigilancia han evolucionado rápidamente gracias a la tecnología, inteligencia artificial y machine learning. Es una combinación que permite que la supervisión ofrezca grandes ventajas en el reconocimiento facial y de objetos, en condiciones poco favorables como la baja luminosidad o un clima complejo.

"Se ha avanzado mucho con la incorporación de la nube y soluciones de automatización, ya que la grabación de grandes cantidades de información requiere del complemento tecnológico. Por lo tanto, aunque en Chile no es una alerta crítica, debemos poner atención en los riesgos cibernéticos. Si bien las personas usan estos dispositivos para garantizar su seguridad física, la pregunta sobre si estos productos son buenos en materias de ciberseguridad, es un signo de interrogación importante", precisa Montenegro.

Según datos de Allied Market Research, el tamaño del mercado global de AI CCTV, se valoró en $14,83 mil millones en 2020, y se proyecta que alcance los $55,22 mil millones para 2030, registrando una CAGR del 14,9% de 2021 a 2030.

Inteligencia vulnerable

Hoy, podríamos decir, los proveedores de IoT fallan en la implementación de controles de ciberseguridad. El concepto de smart cities y smart home toman cada vez más fuerza, por lo que si no se toman las precauciones correspondientes, los hogares pueden ser entrada para ataques cibernéticos.

"Hay muchas opciones de cámaras de seguridad y proveedores, pero son imposibles de examinar por completo. Además, aún no somos conscientes de la delincuencia digital y, en este caso particular, las personas no piensan que la cámara puede ser foco de vulnerabilidad, solo quieren tener un dispositivo en el exterior que les entregue visibilidad cuando están o no en sus casas", detalla el ejecutivo.

Calidad, definición, durabilidad, almacenamiento, monitoreo desde aplicaciones en línea, entre otros, son los factores a considerar por lo general.

Pero hay que poner atención en que, además, tengan la calificación de seguridad.

"Ciertamente, las cámaras de videovigilancia entregan la sensación de seguridad a las personas al tiempo que ofrecen registro visual de lo que sucede. Pero es importante que tomemos conciencia de que estamos arriesgando la privacidad, violación de datos y seguridad en línea. En ese sentido, tenemos que empezar a exigir proveedores que ofrezcan un buen tratamiento al respecto", sentencia Montenegro.

Detectar y acabar con posibles "intrusos digitales", también es tarea de los ciudadanos. Las cámaras de videovigilancia están por todos lados: bancos, autopistas, calles, avenidas, supermercados, comercio, entre otros, por lo que es clave concientizar y entender que hay salvaguardar los hogares, ya que una vulneración de datos puede generar un gran daño.

Image by Gerd Altmann from Pixabay

Walter Montenegro, gerente de ciberseguridad para Cisco Chile.

La feria de hidrogeno verde más importante del mundo llegó a chile

Por primera vez se realizó en nuestro país, Hyvolution, el encuentro más grande a nivel mundial. ¿Por qué nuestro país es tan importante como actor clave para el hidrogeno verde? Acá te lo contamos.

Hyvolution llegó a Chile con el objetivo de reunir en un solo espacio al ecosistema, con actores nacionales e internacionales para la promoción, relacionamiento y fortalecimiento de la cadena de valor, que incluye la producción, almacenamiento, distribución, usos, servicios técnicos y financieros, entre otros. En ese marco, empresas lideres en soluciones de seguridad como ZKTeco estuvieron presentes con un stand que caracteriza los lazos colaborativos con sus distribuidores mayoristas, en este caso con Estec. En el lugar más de mil empresas estuvieron presentes.

Con la presencia del ministro de Energía, Diego Pardow; el subsecretario del Ministerio de Transportes y Telecomunicaciones, Jorge Daza; el Director General de ProChile, Ignacio Fernández; y la Directora de InvestChile, Karla Flores, se dio inicio a esta importante feria de Hidrógeno Verde, que fue el punto de encuentro comercial para más de 3.500 ejecutivos y tomadores de decisión de las más de mil empresas participantes, expositores y visitantes, quienes participaron de las áreas de exhibición, congreso internacional y zonas de networking comercial.

El ministro de Energía, Diego Pardow, comentó que "estamos trabajando con una empresa que ya está utilizando estas nuevas tecnologías para reemplazar el funcionamiento del sector portuario de Valparaíso. Este tipo de noticias son bienvenidas. El corazón de nuestra política pública es aprovechar esta oportunidad de exportación de hidrogeno para acompañar el proceso de descarbonización inicial chileno, para también construir una oportunidad distinta en otras áreas y que permitan el mejoramiento de los trabajos. Todas esas son oportunidades para nuestro país"

Esta es la sexta versión de la feria y su primera vez en nuestro país. La esencia de Hyvolution es trabajar juntos hacia esta transición al futuro y Chile tiene una oportunidad única de trabajar con energías limpias, en ese sentido, todos los presentes destacaron que estarán ahí para colaborar en proyectos que requieran de estas nuevas energías.

En esa línea, Miguel Valenzuela, Market Manager de Seguridad Electrónica de Estec, resaltó que "para nosotros es fundamental estar en Hyvolution ya que la tendencia de las nuevas plantas que se desarrollarán en Chile va en ese sentido y así nosotros podamos ofrecer nuestro portafolio de soluciones en comunicaciones y puntualmente en seguridad electrónica. Sobre la perspectiva de esta industria es muy importante el ser parte de esto junto a nuestro partner estratégico que es ZKTeco".

Rodrigo Barrios, gerente comercial de TNS Chile puntualizó que "el uso de tecnologías en general qué nos permitan integrar sistemas, siempre será una solución para poder hacer las cosas de manera más rápida y automatizada. Muchas de estas producciones requieren accesos de forma remota, todo eso aplicado a la tecnología de control de acceso permite automatizar y eso hace que las cosas sean más eficientes y mucho más económica que se hace hoy. Por ejemplo, en vez de tener a una persona en una estación de monitoreo, perfectamente se te podría reemplazar por una autorización remota de alguien que esté conectado al sistema. Ese tipo de soluciones harán que los sistemas sean más automatizados".

Rodrigo Valenzuela, gerente de Hyvolution Chile,

Rodrigo Barrios Sánchez , Gerente Comercial en TNS Chile

comentó sobre la relevancia de este encuentro en el país: "Es la primera edición en Chile, no así a nivel global -es la sexta edición-. Esta es una feria francesa que se desarrolla en París y nosotros como grupo Hyvolution la hemos traído. La feria pretende conectar comercialmente todo lo que está pasando en Europa, todos estos desarrollos tecnológicos, con Latinoamérica, siendo Chile el punto de encuentro comercial. En esa lógica, pretendemos conectar toda la cadena de valor del hidrógeno, desde la producción hasta la exportación, pasando por los proveedores, el financiamiento, almacenamiento, etcétera".

Rodrigo Valenzuela, Gerente Hyvolution Chile/Development & New Global Business Manager en FISA

Por su parte, Gustavo Maluenda, CEO de ZKTeco en Chile, manifestó su conformidad con la jornada en la que no solo expusieron su gama de productos, referentes en materia de control de acceso, sino también en la relevancia de potenciar la integración para dar soluciones precisas, ajustadas, reales y eficientes a los clientes. En esta misma línea comentó que "hoy tenemos las soluciones tecnológicas que están a la altura de este mercado en expansión, y digo hoy porque hace no mucho, realizamos el lanzamiento oficial de Armatura en Chile y que viene de la mano con productos de alta gama a precios competitivos del mercado, para ser la solución integral a los diferentes requerimientos de seguridad. Nuestra fábrica de Tailandia, donde se manufactura Armatura, ha trabajado en incorporar altos estándares de mercado y procedimiento en la línea de manufactura y protocolos estandarizados a las soluciones, como es la encriptación AES 256, certificados TLS, comunicación; BacNet, OPC y Modbus por nombrar algunos".

Gustavo Maluenda, CEO de ZKTeco Chile

Equipos de ZKTeco y Estec, Stand 246 de Hyvolution 2023

Omar Martínez, Head of Sales de ZKTeco junto a Diego Pardow, Ministro de Energía

Gustavo Maluenda, CEO de ZKTeco junto a Miguel Valenzuela,Market Manager Seguridad Electronica y Manuel Vera, Market Manager Mineria de Estec

El impacto a nivel nacional de la alianza estec – zkteco en materia de seguridad electrónica

Tras esta alianza con zk ya estamos pensando siempre en la vanguardia para nuestros clientes cuentan desde estec.

Durante el mes de junio se realizó el que podría catalogarse como uno de los hitos más importantes en materia de seguridad electrónica en nuestro país. Y es que ZKTeco consolidó fuerzas, como suele hacerlo con varias marcas, con Estec, uno de los lideres en provisión de materiales, equipos y herramientas a la hora de enfrentar proyectos de cableado, estructurado, fibra óptica y ley de ducto. Con presencia en Chile y Perú, Estec participa también en las principales industrias de la minería, salud, retail, telecomunicaciones, banca y construcción, entre otras.

De ahí que nace el lazo con ZKTeco que también trabaja a codo en todas estas áreas. En pleno 2023 las nuevas tendencias en sistemas de control de acceso fueron parte de este importante lanzamiento, en donde también estuvieron presentes importantes empresas del mercado como Rom Mayer, SPC Chile, IIA entre otras.

Para Pablo Valenzuela, subgerente de Negocios de Estec, este tipo de instancias son muy importantes. "Lo primero es la cercanía con el cliente, cómo a partir de una actividad como esta logras eso para apoyar y entregarle más valor al cliente. La alianza con ZKTeco nos da un plus, porque muchos de nuestros clientes no tienen la capacidad de tener un área de innovación y nosotros asumimos ese rol para ayudarlos en sus soluciones en la minería, por ejemplo. Somos un área de innovación externa para nuestros clientes porque ahí ellos dicen que esta no es solo una empresa distribuidora de productos sino que somos una empresa que los estamos apoyando para que sigan creciendo"

ZKTeco nace en 1998, anteriormente ZKSoftware (1985), empresa de renombre mundial siendo líder en desarrollo de tecnología biométrica, brindando soluciones a empresa y usuarios finales tanto en sector público y privado. Cuenta con varios centros de desarrollo, diseño e innovaciones en USA, Europa, India, en China en las ciudades de Dongguan, Xiamen y Dalian. En la actualidad, la mayoría de las 500 principales empresas globales han aplicado las técnicas y terminales inteligentes de ZKTeco, teniendo presencia en más de 100 países y regiones. Sus tecnologías de verificación incluyen huella digital, reconocimiento facial, de venas y de palmas.

Giovanni Pinchetti, Subgerente de Ventas de Estec cuenta que "esta presentación nos hace crecer como exponentes relevantes en área de seguridad electrónica. ZK parea nosotros es el líder del mercado nacional y uno de los lideres a nivel mundial. Dicho eso, para nosotros tener una alianza con ellos es demasiado importante porque nos da un status distinto con nuestros clientes"

En Estec cuentan que quieren enfocarse en soluciones como por ejemplo las barreras en los edificios residenciales, los torniquetes hasta las cámaras de seguridad, los controles de acceso, las cerraduras de las puertas, las barreras de control de acceso para los vehículos. Hay soluciones para distintas industrias, por ejemplo, para la minería el standard es otro, para el mundo de los salmones y del retail también. La gracia de contar con ZK es que ponemos a disposición de los clientes todas esas herramientas que ellos ya tienen.

ESTEC y ZKTeco a nivel nacional

Una actividad que cierra un primer ciclo iniciado en diferentes regiones. "Logramos acercarnos más a muchas empresas integradoras que no habían tenido el soporte en su momento y la atención adecuada para que puedan abordar sus proyectos, un ejemplo fue en Concepción en donde se mostró el equipamiento y soluciones a clientes finales, de ellos muy agradecido por nuestra visita y por la realización de actividades locales.

"Solicitudes de Certificaciones en cada región. Esto es algo que se está planificando quedaron a la espera de que se puedan concretar y de esta forma no tener que estar viajando a Santiago para poder certificarse", explica Maureen Órdenes, integrante del staff de la fábrica asiática que se desplegó junto al equipo en los diferentes territorios.

Conversamos con los diferentes jefes de sucursales de Estec y esto fue lo que nos dijeron

respecto a la sinergia generada en cada encuentro:

Diego Novoa,Subgerente de Sucursales Regiones ESTEC

¿Cuál es el valor agregado para las regiones el tener espacios directos con los clientes?

Nos permiten iniciar conversaciones que son muy relevantes para conocer y entender el negocio de vuestros clientes, y así emprender una relación comercial de largo plazo a través del servicio y asesoría constante en el tiempo. Un cliente actualizado en las nuevas tecnologías de ZKTeco, consigue que se abran más puertas para su negocio, donde podrá entregar e implementar soluciones más integrales.

¿Cómo evaluaría estos encuentros en alianza con ZKTeco?

Nos acercan cada vez más a los clientes, quienes agradecen mucho estas iniciativas, les permite fortalecer sus conocimientos y expectativas de rentabilidad. Asimismo al estar respaldados por la marca y el equipo Estec, pueden trasmitir más confianza y seguridad para consolidar su servicio a sus clientes finales.

Por su parte Nicolás Fernández, jefe de la sucursal de Temuco precisa:

¿Cuál es el beneficio e impacto en su región el que se realicen las actividades informativas con los clientes?

Es de alto impacto para la novena región ya que no existen proveedores de ZK en Temuco. La implementación de actividades en conjunto a través de Estec nos debería posicionar sobre otras opciones que ofrecen nuestros competidores. Hoy por hoy contamos con parte del mix ZK/Estec para entrega inmediata en Temuco y el número de conversaciones sobre esta línea de negocio va en aumento con nuestros clientes.

En tanto, Luis Labrador, jefe de la sucursal de Coquimbo asevera: "Hoy en día estar actualizado de las nuevas tecnologías es clave para entregar soluciones oportunas, y ser referentes de estas tendencias, te permite interactuar con quienes entregan un servicio. Las actividades informativas dentro del mundo comercial son claves para captar nuevos integradores, quienes juegan un papel vital en el desarrollo y asesoría en las instalaciones en la zona". Y agrega: "En la región de Coquimbo, ha aumentado en los últimos años la instalación de sistemas de control de acceso. El año pasado tuvimos el evento Estec-ZKTeco, que nos permitió conectarnos con nuestros integradores y conocer el valor agregado a través de la marca. Las instituciones de

ESTEC sucursal Talca

ESTEC sucursal Coquimbo

ESTEC sucursal Viña del mar

ESTEC sucursal Concepción

enseñanza, minería, terminales, hotelería y casinos en la región, están buscando soluciones que les permita no solo incrementar el nivel de seguridad, también regular entrada/salida del personal de la empresa para hacer más eficiente el uso de los recursos. Estos rubros son el foco de trabajo para este año 2023, donde buscamos capacitar a nuestros integradores de la zona, y potenciar la presencia de la marca".

En lo que respecta a la región de Valparaíso, Aquiles Pandelaria, jefe de la sucursal de Viña del Mar de Estec asegura que: "Nuestros clientes agradecen que se realicen actividades informativas, capacitaciones y eventos tecnológicos que muestren diferentes soluciones, características o ventajas de la marca ZKTeco, se sienten apoyados en sus proyectos y lo consideran como un valor agregado importante que impacta positivamente en sus negocios. El mercado de seguridad electrónica ha tenido una fuerte alza en el último tiempo a nivel nacional y en la región, junto a nuestros clientes hemos desarrollado variados proyectos entregando soluciones de seguridad electrónica para diferentes segmentos como hoteles, hospitales, industria, retail, entre otros. Nuestro objetivo es seguir trabajando para dar solución a problemas de seguridad con esta tecnología avanzada".

En representación de la zona sur, específicamente en la ciudad de Puerto Montt, Patricio Jacob, agrega: "Es muy relevante el posicionamiento que hemos hecho en conjunto a la marca ZK, los clientes de la zona sur no estaban acostumbrados a que se realicen eventos informativos sobre marcas, y lo que hemos realizado hasta el momento en conjunto a la marca rompe ese paradigma, estamos dando herramientas elementales para que los proyectos locales tengan mano de obra calificada. El impacto es muy claro: estamos siendo pioneros en informar y capacitar a integradores de Seguridad electrónica en localidades tan extremas como: Chiloé, Coyhaique, Aysén o Punta Arenas. Estec y ZK en alianza generan una extraordinaria simbiosis para las pymes de la región, agregando valor agregado y distintivo al contratista local de las regiones X, XI,XII Y XIV

Para Jahleet Burgos, jefe de sucursal de Concepción, estos encuentros han permitido un mejor conocimiento de la marca, "las actividades informativas ayudan a crear conciencia y aumentar el conocimiento de la marca ZKTeco en la región. Los clientes potenciales y existentes pueden aprender sobre los productos que ofrece la marca, lo que puede generar un mayor interés y una mayor consideración al momento de tomar decisiones de compra.

Educación y capacitación:

Estas actividades permiten educar a los clientes sobre las soluciones y tecnologías ofrecidas por ZKTeco mediante demostraciones, talleres, presentaciones o desayunos tecnológicos, los clientes pueden entender cómo utilizar los productos de manera efectiva y aprovechar al máximo sus características. Esto contribuye a mejorar la experiencia del cliente y su satisfacción, tanto con Estec como la propia marca ZKTeco". Y puntualiza respecto al fortalecimiento con los clientes finales: "Generación de confianza: Al proporcionar información detallada sobre la marca ZKTeco, calidad de productos y compromiso con la seguridad y la innovación, se puede generar confianza en los clientes. Esto es especialmente importante en el caso de soluciones de seguridad y control de acceso, donde la confianza en el proveedor (Estec) es fundamental. En resumen, las actividades informativas con los clientes sobre la marca ZKTeco pueden tener un impacto positivo al aumentar el conocimiento de la marca, el educar a los clientes con conocimiento, y generar confianza en ellos para con nosotros como proveedor de la marca".

Para cerrar este recorrido a nivel nacional, Elías Novoa, jefe de la sucursal de Talca, asegura que los clientes tienen mayor conocimiento y se van con dudas clarificadas en conjunto con los especialistas, "de esta manera están más relacionados con las marcas y productos que trabajamos. Al momento incrementaron las cotizaciones de seguridad electrónica donde nuestros clientes están entregando soluciones ZKTeco a sus mandantes".

Gustavo Maluenda, CEO de ZKTeco Chile

Gustavo Maluenda, CEO de ZKTeco, agrega que "esta alianza en miras del mercado viene reforzada de nuestro lado con la incorporación de nuevas personas a nuestro equipo de trabajo, en especial de Teddy Cabrera, nuestro nuevo BDM Zona Sur, quien estará apoyando a nuestro mercado desde Talca hasta Puerto Montt"

Teddy Cabrera, Business Development Manager Región del Maule hasta Puerto Montt, ZKTeco Chile

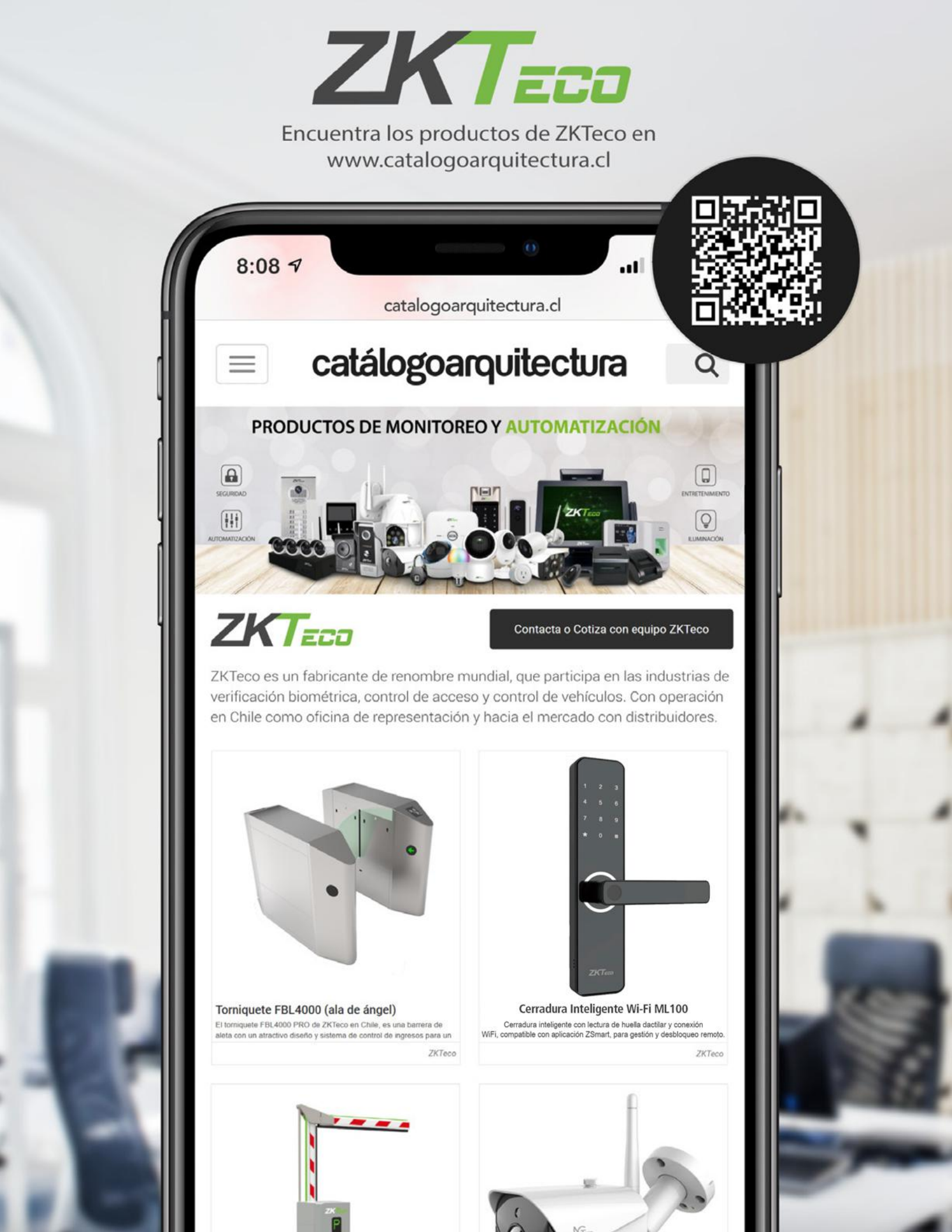
Por su lado Teddy Cabrera, quien se ha sumado al equipo de ZKTeco con la finalidad de reforzar la propuesta de valor hacia el mercado, agrega que: "Dentro de mis tareas está la de brindar apoyo en la gestión de negocios de nuestros distribuidores mayoristas en el sur del país, desde Talca a Puerto Montt.

El mercado de seguridad electrónica en Chile día a día obtiene mayor necesidad de mejoras, mayores requerimientos con más y mejores productos que junto a ZKTeco podemos proporcionar, pero para que esta cadena funcione cada eslabón debe estar preparado, es decir, tanto el equipo de ventas del mayorista, del distribuidor, del reseller y también el integrador. Es por esto que debemos estar enfocados en realizar actividades informativas a nuestros integradores y clientes en general, generaremos valor agregado al producto final".

Teddy es el actual Business Development Manager desde la Región del Maule hasta Puerto Montt.

ZKTeco

Encuentra los productos de ZKTeco en
www.catalogoarquitectura.cl



Filtración de credenciales y datos personales

Image by Gerd Altmann from Pixabay

El año 2023, ha sido particularmente un año en que los investigadores de ciberseguridad y los fabricantes de tecnologías en esta materia, han podido evidenciar un aumento significativo en las campañas de publicidad maliciosa, las cuales tiene por finalidad infiltrar software del tipo malicioso "malware" para obtener información y datos de cuentas de email, datos bancarios, tarjetas de créditos y en especial de credenciales de accesos de usuarios.

En este sentido, "Info-Stealer Vidar" es uno de los malware de mayor visibilidad debido a la gran cantidad de usuarios comprometidos a nivel mundial, no siendo Chile una excepción a este patrón de comportamiento.

Info-Stealer Vidar, se encuentra comercializado en el mercado negro tecnológico, también conocido como Deep Web y Dark Web, como son por ejemplo XSS, Breached, Ramp, Exploit In, Altenen o simplemente estos se encuentran distribuyéndose gratuitamente en múltiples canales de plataformas de mensajerías como Telegram, utilizando un modelo de Malware As a Service.

El modo de funcionamiento de este malware que captura datos desde los sistemas de las víctimas, se basa en la necesidad de los usuarios que requieren de utilizar herramientas y software disponibles en los distintos buscadores como por ejemplo Google, en donde un usuario busca descargar un aplicativo como son AnyDesk, Zoom, Notepad++, Foxit, Photoshop y estos se despliegan como anuncios, los cuales redirigen a sitios maliciosos, sin que el usuario se entere.

En la columna de hoy, proporcionaremos una mirada de alto nivel a las campañas que existen, centrándose específicamente en la entrega del malware Vidar Info-stealer.

Lo primero que se debe tener presente es como se logra infiltrar y comprometer el equipo que cuenta con las credenciales y datos relevantes que el atacante desea conocer, para esto es importante tener presente que el principal medio es la utilización de anuncios de uso de software legitimo pero estos no cuentan con información visible sobre su editor (falsos).

En segundo lugar cuando el usuario ingresa al anuncio, este lo dirigirá al sitio web que lo comprometerá. Esto sucederá una vez el usuario seleccione la versión deseada del software, el sitio presentará un botón de descarga al visitante.

En tercer lugar e invisible para el usuario, al hacer clic en descargar, independientemente de la versión seleccionada, el tráfico se redirige al sitio de malware, desplegando un archivo generalmente del tipo zip, con el nombre del instalador.

En cuarto lugar tras la extracción, el archivo tendrá un tamaño de archivo estándar para software, este aspecto es importante, ya que el tamaño se atribuye a la inclusión de un número excesivo de bytes nulos, que sirven para evitar que el archivo sea escaneado por algún antivirus y subido a plataformas de análisis de malware, que tiene un límite de tamaño de archivo de 650 megas.

En quinto lugar después de la ejecución, el malware establece rápidamente una conexión que dependerá del medio de compromiso, pudiendo ser, este por ejemplo, un canal de Telegram para adquirir su dirección de comando y control. En caso de que Telegram no esté disponible, el malware intentará conectarse a un perfil en la plataforma que tenga disponible, en cuyo caso utilizará otras direcciones.

En sexto y relevante etapa, se procederá a registrar y obtener el archivo de configuración y, posteriormente, descarga un archivo que contiene varias bibliotecas DLL legítimas, que se utilizan para extraer información y contraseñas guardadas de varias aplicaciones y navegadores.

Como se ha presentado, podemos decir que la reciente proliferación de campañas de publicidad maliciosa, que emplean los ciberdelincuentes para distribuir malware, se ha convertido en un importante motivo de preocupación para las personas y organizaciones de todo tipo.

A diferencia de los vectores de infección más tradicionales, como el correo electrónico, es más difícil protegerse contra la publicidad maliciosa. Además, el uso de técnicas de relleno para inflar el tamaño de las cargas de malware puede dificultar la detección y el análisis que las plataformas de antivirus y malware.

Por este motivo, se sugiere y propone para mitigar el riesgo de ser víctima de este tipo de ataques, tener la precaución al interactuar con anuncios en línea, específicamente, es recomendable evitar ingresar a los anuncios mientras busca software gratuito en los motores de búsqueda, en su lugar, descargar programas directamente de fuentes oficiales.

Este enfoque puede reducir la probabilidad de descargar malware de fuentes no confiables, sin darse cuenta.

Finalmente utilización de software de bloqueo de anuncios, ya que la implementación de un bloqueador de anuncios puede proporcionar una capa adicional de protección contra las campañas de publicidad maliciosa y mejorar la ciberseguridad general. Esto sumado al uso de un segundo factor de autentificación en todos los sistemas, es vital para reducir el compromiso de información.

Autor: Carlos Villagra
Ingeniero en Telecomunicaciones de la universidad tecnológica de Chile, Magister en Ciberseguridad, con más de 20 años de experiencia laboral en las áreas de Seguridad de la Información, docente de post grado de la universidad UNIACC

Probabilidad objetiva, subjetiva y aleatoriedad

Image by JEI CREATIVO from Pixabay

¿Conoces la diferencia entre probabilidad objetiva y subjetiva que son ampliamente utilizadas en el análisis de riesgos? ¿Conoces también la relación entre aleatoriedad y probabilidad? En la mayoría de las ocasiones en la escuela se enseña la probabilidad objetiva en cuanto al cálculo de la frecuencia, pero también en la mayoría de las ocasiones en la vida real nos enfrentamos a problemas donde el cálculo de la frecuencia no es posible porque las situaciones que planteamos, no cumplen las premisas de los experimentos aleatorios.

Para ayudar a aclarar estos tres conceptos, empezamos a continuación con dos posibles ejemplos en el día a día de empresas, uno en el que podemos calcular probabilidades de forma objetiva y otro en el que tenemos que hacerlo de forma subjetiva.

Probabilidad Objetiva

Un ejemplo puede ser la predicción de fallas en una red eléctrica. Imagina una empresa de distribución de energía eléctrica que opera una extensa red de transmisión y distribución.

Con base en datos históricos de fallas, información sobre el estado de los equipos, análisis de desgaste y mantenimiento preventivo, es posible calcular objetivamente la probabilidad de fallas en diferentes componentes de la red, como transformadores, cables o postes. La empresa puede utilizar métodos estadísticos avanzados, como el análisis de confiabilidad de sistemas, para identificar patrones y estimar la probabilidad de fallas, en determinados intervalos de tiempo.

Este enfoque objetivo permite una planificación adecuada del mantenimiento, asignación de recursos y reducción de los riesgos operativos.

Probabilidad Subjetiva

Un ejemplo de probabilidad subjetiva es la evaluación de riesgos geopolíticos en una organización global. Considera una empresa multinacional que opera en varios países con entornos políticos y sociales complejos y en constante cambio. En este caso, calcular probabilidades objetivas basadas en datos históricos, puede ser desafiante debido a la falta de patrones claros, o a la falta de información confiable.

En cambio, la organización debe recurrir a la evaluación subjetiva de los riesgos geopolíticos, teniendo en cuenta análisis de expertos en política internacional, información de agencias de inteligencia, análisis de escenarios y percepciones regionales.

Este enfoque subjetivo permite que la empresa tome decisiones estratégicas con más confianza, como ingresar a nuevos mercados o asignar recursos en regiones con mayor o menor estabilidad política.

Estos ejemplos demuestran cómo la gestión de riesgos puede abordarse de maneras distintas, según la disponibilidad de datos y la naturaleza de los eventos analizados.

Aleatoriedad

Cuando lazamos un dado no sabemos qué número va a salir; sin embargo, si lanzamos una piedra al aire estamos seguros de que caerá al suelo.

Es decir, en algunos experimentos podemos saber lo que va a ocurrir y en otros no.

- A los experimentos en los cuales no sabemos lo que va a ocurrir se les llama experimentos aleatorios.

- A los otros, aquellos en los que sí podemos decir lo que va a ocurrir, se les llama experimentos deterministas. Solo para hacer más comprensible los dos ejemplos iniciales, consideramos necesario aclarar cuáles son las premisas mínimas para que los experimentos se consideren aleatorios:

1. **Repetibilidad:** El experimento debe ser repetible, es decir, es posible realizar el mismo experimento varias veces bajo condiciones similares;

2. **Independencia:** Los resultados de un experimento no deben influir en los resultados de otros experimentos. Cada experimento debe ser realizado de forma independiente;

3. **Equi-probabilidad:** Cada resultado posible del experimento debe tener la misma probabilidad de ocurrir. Esto significa que todos los resultados tienen las mismas posibilidades de obtenerse;

4. **Resultados mutuamente excluyentes**: Los resultados posibles del experimento deben ser mutuamente excluyentes, lo que significa que solo un resultado puede ocurrir en cada intento

del experimento;

5. **Determinismo:** Las premisas de aleatoriedad deben aplicarse antes de que ocurra el experimento, es decir, no debe haber ningún factor determinista conocido, que influya en el resultado del experimento.

Es importante destacar que no todos los eventos de la vida real cumplen con estas premisas, lo que hace que el cálculo objetivo de frecuencias sea inviable en muchos casos.

En estas situaciones, el enfoque subjetivo puede ser más apropiado para evaluar y gestionar riesgos.

A los experimentos en los cuales no sabemos lo que va a ocurrir se les llama experimentos aleatorios. Además de las cinco premisas mencionadas anteriormente, existen otras premisas que se pueden considerar al evaluar si un experimento se considera aleatorio.

Si bien puede haber diferentes perspectivas sobre qué premisas son necesarias, algunas adicionales pueden incluir:

6. **Igualdad de condiciones iniciales:** Los experimentos deben realizarse en condiciones iniciales similares o iguales. Esto garantiza que no haya sesgo en las condiciones iniciales, que puedan afectar los resultados del experimento.

7. **Ausencia de sesgo de selección**: Los participantes o muestras seleccionados para el experimento deben ser elegidos de manera aleatoria e imparcial, sin ningún sesgo o preferencia. Esto es importante para garantizar que la muestra sea representativa de la población en estudio.

8. **Aleatoriedad en la asignación:** En experimentos donde hay asignación de tratamientos o grupos de forma aleatoria, es necesario garantizar que la asignación sea verdaderamente aleatoria, sin ningún sesgo o influencia externa.

9. **Ausencia de influencias externas significativas**: Los resultados del experimento deben verse mínimamente afectados por factores externos que no se estén controlando, o considerando en el contexto del experimento.

Estas premisas adicionales pueden variar según el campo de estudio y el tipo de experimento en cuestión. Es importante considerar el contexto específico del experimento al evaluar si cumple con los criterios de aleatoriedad.

A los experimentos en los cuales no sabemos lo que va a ocurrir se les llama experimentos aleatorios. En conclusión, la distinción entre probabilidad objetiva y subjetiva desempeña un papel fundamental en la gestión de riesgos.

Mientras que la probabilidad objetiva se basa en premisas de experimentos aleatorios, cálculos de frecuencias y datos históricos, la probabilidad subjetiva surge cuando estas premisas no pueden cumplirse.

Es importante reconocer que no todos los eventos de la vida real se ajustan a las condiciones ideales para el cálculo objetivo de probabilidades. Por lo tanto, el enfoque subjetivo, que incorpora conocimiento especializado, análisis de escenarios y percepciones individuales, desempeña un papel crucial, en la toma de decisiones en situaciones complejas e inciertas.

La gestión de riesgos efectiva requiere una comprensión adecuada de estos conceptos y la aplicación adecuada de enfoques objetivos y subjetivos, adaptándose al contexto específico de cada organización y desafío.

Autor:
Tácito Augusto Silva Leite
MBA en Gestión estratégica de seguridad empresarial
con posgrado en Dirección de seguridad
en empresas y Gestión de recursos de defensa.
Certificación de Gestión de riesgos
Autor de diversos lbros del área de la seguridad

¿Qué son las salas de control y para qué sirven?

Centros o Salas de Control, son los espacios especialmente diseñados para atender y resolver las situaciones de emergencia, principalmente en entidades de gobierno o empresas privadas de los sectores de energía, salud, seguridad y vialidad. Por ello, su conceptualización y diseño se basan en función de llevar a cabo todas estas tareas de forma óptima, para que la visualización, el control de procesos y la gestión, sean los más adecuados y eficientes.

Estos centros están siempre diseñados a partir de un estudio del espacio físico, destinado para su funcionamiento. Además, irán en combinación y armonía perfecta con el número de operadores, el tipo de trabajo y las tareas a realizar, y su función como parte de un sistema integrado.

Asimismo, el tener una Sala de Control de alto rendimiento, con elementos únicos que permita a los operadores realizar funciones de monitoreo, seguimiento, análisis y toma de decisiones ante situaciones críticas, durante las 24 horas al día, los siete días de la semana y los 365 días del año, es lo que cualquier entidad pública o privada requiere para tener el mejor funcionamiento.

Por ejemplo, las salas de control de una comisaría de policía, de una refinería o de una organización de procesos intensivos, los operadores requieren acceso a la información en tiempo real y con la mayor seguridad. Para ello, contar con los mejores sistemas que permitan un flujo de trabajo eficiente, con un retorno de inversión apropiado y con la mayor seguridad durante su operatividad, es indispensable.

Así, cuando los sistemas que se utilizan tienen detrás de sí un gran desarrollo tecnológico, se puede confiar en que la visualización de los diferentes objetivos será la mejor y podrá incidir en la mejor toma de decisiones. De esta manera tener un mural de video con la mejor calidad de imagen, es una buena inversión, al optimizar los procesos en las salas de control.

¿Qué requerimos para diseñar una Sala de Control?

Aunque muchos extraños verían las salas de control como entornos bastante estáticos, el mercado en realidad ha pasado por muchos cambios en los últimos años, principalmente ante el aumento exponencial de las fuentes disponibles, lo que ha causado muchos desafíos, tanto para el personal, como para la infraestructura.

Así, el implementar un centro o Sala de Control requiere considerar varios aspectos:

- El espacio disponible
- La ergonomía para los operadores
- El entorno tecnológico que permita el flujo de trabajo adecuado
- Los procesos operativos que permitan responder de inmediato en situaciones críticas.
- La seguridad cibernética

Por lo tanto, la conceptualización y el diseño de los espacios destinados a las salas de control depende de las necesidades del trabajo, considerando en primera instancia a los operadores, donde la tecnología siempre estará en función del servicio a éstos y a la facilidad para realizar su trabajo.

¿Qué tecnología requiere la Sala de Control?

La ergonomía del espacio destinado –principalmente- a la visualización de espacios, procesos y/o de infraestructura, requiere un videowall, uno o varios procesadores de video que permitan al operador el manejo de los datos desde su equipo de cómputo o servidor, además de un software que permita la seguridad del flujo de la información y la comunicación adecuada entre los equipos.

Los mejores avances tecnológicos permitirán a los usuarios visualizar imágenes con la mejor calidad en monitores desarrollados para ello, como los diseñados por Barco, que pueden ser de proyección láser o de pantallas planas LCDs o LED directo. De estos últimos, el más reciente avance son los murales de la Serie TruePix, videowalls LED, cuyo funcionamiento continuado durante toda la vida útil del producto, sin tiempos de inactividad, es posible. Además, True Pix se calibra automáticamente y, aunque se cambien los módulos, el resto del videowall sigue funcionando.

Asimismo, EssentialCare y SmartCare de Barco, son paquetes de servicios que le proporcionan la tranquilidad necesaria durante el funcionamiento de su videowall LED TruePix, como cualquier otro equipo de la marca. Son la mejor garantía, no sólo para mantener su videowall operativo durante todo el ciclo de vida de la inversión, sino también para asegurar un presupuesto predecible. De esta forma optimizará su retorno de inversión (ROI, por sus siglas en inglés).

Confianza en Barco

Junto a nuestra amplia oferta de servicios, también juega un factor adicional menos cuantificable pero extremadamente importante: la marca Barco. Fundada en 1934, contamos con una rica historia de casi 90 años y llevamos más de 20 liderando los mercados de LED y el software que requieren para su mejor operación. Esto significa que no sólo contamos con los conocimientos y la experiencia necesarios para diseñar e implantar soluciones LED de forma óptima, sino que también somos una empresa consolidada con un equipo sólido, y una red mundial de oficinas regionales de asistencia.

Por tanto, la consistencia en el servicio y la disponibilidad de piezas de repuesto están garantizadas. Además, gozamos de una excelente reputación y nos dedicamos a realizar negocios honestos y transparentes, (proporcionando información correcta y verificable sobre las especificaciones). Calidad y fiabilidad son las palabras clave de toda nuestra cartera. Un ejemplo de ello es el riguroso control de calidad durante las pruebas de aceptación en fábrica.

Autor: Manuel Navarrete Pérez, LVX Leader Latinoamérica en Barco

Ciberseguridad en Vehículos de Protección Ejecutiva

En el año 2005 ingresé a trabajar como instructor de tiro para el personal de seguridad, (oficiales de seguridad y escoltas) de la mayor empresa de producción de alimentos de Venezuela, en el año 2007 ascendí a supervisor general de seguridad de dicha organización, recuerdo cuando en el año 2008 vino a Venezuela la princesa de Tailandia, a entregar un premio a dicha corporación por la utilización del vetiver en la producción de algunos productos.

Allí fue cuando tuve mi primera experiencia en el estudio, planificación y ejecución de avanzadas móviles en la protección ejecutiva, los profesionales que están leyendo y que se dedican a esta rama de la seguridad sabrán que al realizar una avanzada de un punto A a un punto B, son muchísimas las variantes a evaluar, entre estas podría nombrar:

· Tránsito automotor
· Vías terrestres
· Puntos donde falla la señal de telefonía
· Solicitar en el destino u hotel la identificación del personal que labora en dicha espacio: gerente nocturno, gerente diurno, entre otros
· Buscar una habitación que esté al final del pasillo, que no tenga accesos por ventanas.

Son muchas variantes que les pudiera mencionar pero de nada valdría porque éstas, a su vez, no son estrictas o fijas ya que siempre variarán de acuerdo al momento y circunstancia, lo interesante de todo esto es mantenerse siempre a la vanguardia y no tener estructuras de seguridad rígidas, ya que como dice Iván Ivánovich en su libro: Protección Ejecutiva en el siglo XXI: La Nueva Doctrina: "Tenemos que saber quiénes son, como ellos saben quiénes somos, tenemos que saber dónde están, como ellos saben dónde estamos, tenemos que seguirlos, como ellos nos siguen a nosotros, tenemos que sorprenderlos, como ellos nos quieren sorprender a nosotros".

Tomando en consideración este punto donde se les sugiere que debemos mantenernos a la vanguardia de las nuevas tendencias o doctrinas, el área tecnológica no escapa de esto, el personal de seguridad y protección ejecutiva debe estar alineado y conocer las tendencias de ciberseguridad para prestar un servicio acorde con los nuevos tiempos.

El año pasado recibí una llamada telefónica de un colega venezolano radicado en Perú, quien presta protección a una de las cantantes de reggaetón de moda, el cual tenía un inconveniente con su equipo de operadores de protección ya que se había filtrado la información del lugar de estadía donde esta cantante estaría un fin de semana con su pareja, al filtrarse la información un cúmulo de fanáticos se acercaron a recibir en el aeropuerto a la cantante, y el doble de personas estuvieron atentos al arribo de la misma en el hotel destino, ella molesta le reclamó a su equipo de seguridad ya que solo 5 personas conocían este itinerario.

Al realizar las técnicas correspondientes determiné que uno de estos escoltas, días previos al viaje, había ingresado a una página pornográfica utilizando su teléfono móvil celular descargando un malware por el cual se filtró la información, evidentemente un cantante no es el tipo de objetivo que busquen asesinar, tal vez extorsionar como posiblemente fue esta la ocasión, y al no concretarse la misma fue expuesta la privacidad de la cantante.

Pongo esto como ejemplo para entrar en contexto sobre la seguridad informática y la seguridad de la información que debe tener un equipo de protección y más si hablamos sobre la ciberseguridad en los vehículos de protección ejecutiva, como bien saben ya los automóviles dejaron de ser vehículos con computadoras, ahora son computadoras hechas vehículos.

Computadoras que son vehículos

Solo tenga esto en consideración, si existe un altercado donde un atacante intenta detener el vehículo de un VIP mediante disparos a los neumáticos, estos van a resistir y continuar la marcha ya que cuentan con el dispositivo Run Flat el cual no es más que un neumático macizo de caucho dentro del neumático convencional, si bien es cierto que la huida o marcha no será a gran velocidad nos sacará del apuro al continuar la marcha sin detenerse.

Pero en los vehículos modernos la situación cambia ya que si este altercado ocurriera, los sensores van a reconocer la falla y la computadora ordenará que el vehículo se detenga exponiendo to-

talmente al PMI y a la operación en sí, es por esto que conocer de ciberseguridad en los vehículos de protección ejecutiva es vital.

De acuerdo al Informe de Ciberseguridad Automotriz Global 2023 la industria automotriz se está expandiendo rápidamente hacia un vasto ecosistema de movilidad inteligente, introduciendo nuevos niveles de sofisticación cibernética y vectores de ataque.

Dice este informe que los nuevos vectores de ataque redefinirán la ciberseguridad automotriz ya que han transformado dicha industria en un ecosistema de movilidad inteligente más, sin embargo, con la transformación hay nuevos riesgos de seguridad informática que deben abordarse, como, por ejemplo, el aumento exponencial de los ataques cibernéticos tanto en su magnitud, frecuencia y sofisticación.

En los primeros 6 meses de este año, las predicciones se han hecho realidad, por ejemplo: los ataques y manipulaciones en la infraestructura EV, los ataques basados en API han aumentado drásticamente lo que permite a los adversarios expandir el impacto a una escala mayor de vehículos, incluso flotas enteras.

Pero no todo es malo, ya que las empresas o instituciones han tomado en cuenta todas estas problemáticas y han comenzado a implementar y mejorar por medio de normativas para proteger los activos de movilidad inteligente, y garantizar la confianza y seguridad de los conductores y operadores de protección ejecutiva.

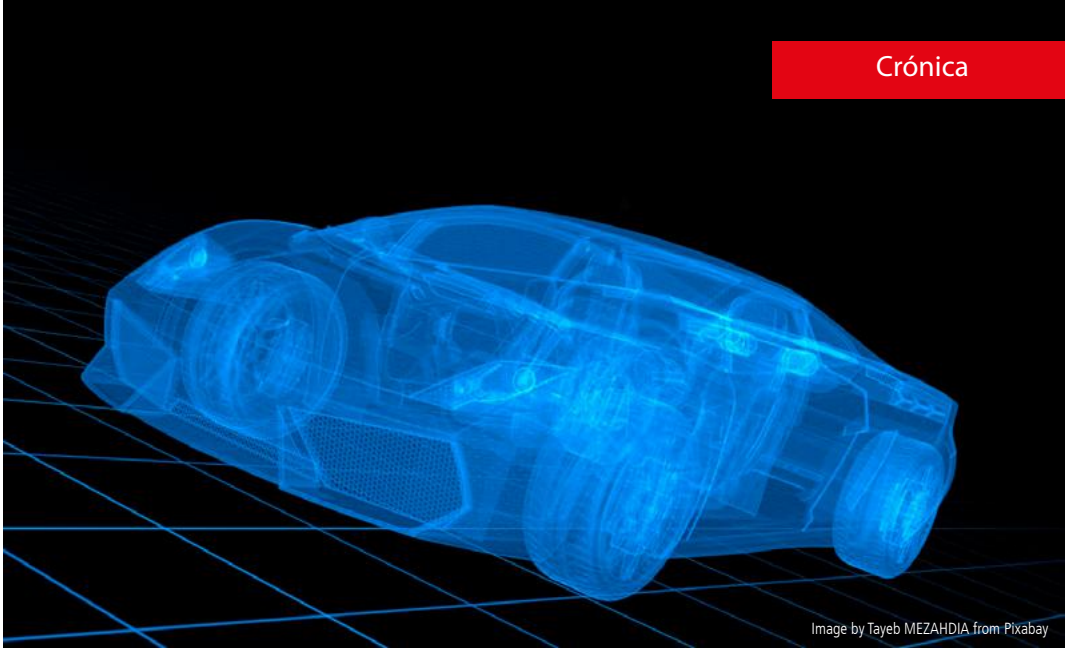


Image by Tayeb MEZAHDIA from Pixabay

Existen normas como la ISO/SAE 21434, la UNECE WP.29 R155 y R156, esta última entró en vigor en el año 2021, presentó su primer hito en el año 2022 y en este año 2023 tuvo una de las mejores actualizaciones que ha recibido, aplicándose a todos los tipos de vehículos nuevos.

Los distintos equipos de profesionales dedicados a la ciberseguridad tienen la tarea de enfrentar las amenazas que van más allá de los ataques directos contra los vehículos, apuntando a flotas, aplicaciones y servicios de movilidad e incluso a las estaciones de carga de vehículos eléctricos ya que estos representan actualmente el 4% de los ataques o incidentes a E.V. lo cual sin duda seguirá en aumento durante este año.

Los profesionales de la ciberseguridad nos hemos dedicado a fortalecer las distintas ramas de la seguridad, pero también lo han hecho los ciberdelincuentes, por lo cual los operadores de protección ejecutiva deben permanecer cada vez más atentos y en constante capacitación para garantizar que se puedan cumplir los objetivos y servicios trazados.

A medida que los vectores de ataques crecen y se vuelven más complejos, la ciberseguridad de IT centrada en vehículos de protección ejecutiva se entrelaza cada vez más.

Adolfo M. Gelder
Fuentes:
Google
UPStream

Sistemas de vigilancia con inteligencia artificial

Una propuesta que llega a Chile

En su segunda cuenta pública ante el Congreso Pleno, el presidente Gabriel Boric anunció la implementación de un sistema de vigilancia con inteligencia artificial (IA) en Chile, con el objetivo de combatir la delincuencia y brindar mayor seguridad a la ciudadanía. Más allá de importante anuncio resulta de alto interés conocer mayores antecedentes con respecto a este tipo de soluciones tecnológicas en seguridad.

El beneficio de la Inteligencia Artificial

La aplicación de videovigilancia en red en conjunto con análisis inteligente, cobra vital relevancia para pensar en las diversas oportunidades de aprovechamiento de la tecnología de análisis con otras tendencias del sector. La Inteligencia Artificial, es percibida como la tecnología que aumentará y mejorará el rendimiento humano en muchos sectores y la industria de la videovigilancia no es una excepción.

El análisis basado en IA se utiliza cada vez más para procesar rápidamente grandes cantidades de datos y desencadenar acciones, además es la tendencia de seguridad más importante para el desarrollo de las ciudades. Estas funciones ayudan a respaldar a un equipo de seguridad al monitorear escenas grandes y cambiantes, como en una autopista o perímetros, identificando objetos de interés y marcando aquellos que requieren una acción.

Hoy se vislumbra una fusión entre la visión de la cámara (que ya no es solo una lente), y las tecnologías de aprendizaje profundo que permiten que el análisis de video sea más preciso en la extracción, clasificación y catalogación de metadatos, más inteligente en el seguimiento de patrones y tendencias demográficas, la cual, brinda una oportunidad muy grande para el mejoramiento de los servicios ofrecidos en una ciudad.

Sistemas de cámaras de vigilancia con Inteligencia artificial

Los sistemas de cámaras de vigilancia con inteligencia artificial (IA) son una innovadora tecnología que combina cámaras de seguridad tradicionales con algoritmos de aprendizaje automático y técnicas de visión por computadora para proporcionar un nivel más avanzado de monitoreo y análisis de video. Estos sistemas utilizan la inteligencia artificial para detectar, analizar y responder a eventos en tiempo real, lo que mejora significativamente la eficiencia y precisión de la vigilancia.

Aquí hay algunas características clave de los sistemas de cámaras de vigilancia con inteligencia artificial:

1. Detección de objetos y personas: Los algoritmos de IA permiten a las cámaras identificar automáticamente objetos, personas y vehículos en el video, en tiempo real. Esto es útil para detectar actividades sospechosas, intrusos o comportamientos anómalos.

2. Reconocimiento facial: La IA puede realizar el reconocimiento facial para identificar individuos específicos, lo que resulta valioso en entornos como aeropuertos, estaciones de transporte público, centros comerciales y otros lugares donde se requiere un alto nivel de seguridad.

3. Análisis de comportamiento: Los sistemas de IA pueden analizar patrones de comportamiento para identificar situaciones anómalas o peligrosas. Por ejemplo, pueden detectar un objeto abandonado, altercaciones, colisiones o movimientos erráticos.

4. Detección de intrusiones y perímetros: La IA puede ser utilizada para establecer zonas o límites de seguridad y detectar intrusiones en áreas restringidas.

5. Reconocimiento de matrículas: Los sistemas de IA pueden identificar y registrar matrículas de vehículos, lo que resulta útil en el control del tráfico, estacionamientos y aplicaciones de seguridad vial.

6. Alertas y notificaciones: Los sistemas pueden enviar notificaciones o alertas en tiempo real a través de mensajes de texto o correos electrónicos cuando se detectan eventos importantes.

7. Búsqueda y recuperación de video inteligente: La IA facilita la búsqueda de eventos específicos

en grandes cantidades de metraje de video mediante el etiquetado y la indexación automática.

8. Análisis de emociones: Algunos sistemas de IA pueden detectar expresiones faciales y analizar las emociones de las personas en el video, para proporcionar información adicional sobre el comportamiento observado.

9. Mejora de la precisión y reducción de falsos positivos: La inteligencia artificial puede adaptarse y mejorar continuamente su capacidad de detección, lo que ayuda a reducir los falsos positivos y negativos.

10. Integración con otras tecnologías: Estos sistemas de cámaras de vigilancia con IA pueden integrarse con otras tecnologías de seguridad, como sistemas de acceso, sistemas de alarma y dispositivos de control, para crear soluciones de seguridad más completas y efectivas.

Es importante tener en cuenta que, como con cualquier tecnología de vigilancia, el uso de sistemas de cámaras de vigilancia con inteligencia artificial debe llevarse a cabo de manera ética, y cumpliendo con las regulaciones y leyes de privacidad aplicables en cada región. El uso responsable de esta tecnología garantiza que se aprovechen sus beneficios sin comprometer los derechos y la privacidad de las personas.

Principales riesgos de utilizar sistemas de cámaras de vigilancia con Inteligencia artificial

Si bien los sistemas de cámaras de vigilancia con inteligencia artificial ofrecen beneficios significativos en términos de seguridad y monitoreo, también presentan una serie de riesgos y desafíos que es importante considerar:

1. Privacidad y derechos individuales: La principal preocupación con los sistemas de vigilancia con IA es la invasión de la privacidad. Estos sistemas pueden recopilar y analizar datos personales sin el conocimiento o consentimiento adecuado de las personas, lo que podría infringir sus derechos individuales.

2. Uso indebido y vigilancia masiva: Los sistemas de vigilancia con IA podrían ser utilizados para fines indebidos, como la vigilancia masiva o la discriminación por perfiles étnicos o sociales. Esto puede llevar a la creación de una sociedad de vigilancia excesiva y erosionar la libertad individual.

3. Vulnerabilidades de seguridad: Los sistemas de vigilancia con IA pueden ser vulnerables a ataques cibernéticos, lo que podría permitir a los hackers acceder a las cámaras y obtener imágenes en tiempo real, deshabilitar la vigilancia o manipular los datos.

4. Precisión y sesgo: Los algoritmos de IA utilizados en los sistemas de vigilancia pueden tener problemas de precisión y sesgo. Por ejemplo, pueden cometer errores al identificar a personas, etiquetar actividades como sospechosas cuando no lo son, o mostrar sesgos basados en características demográficas.

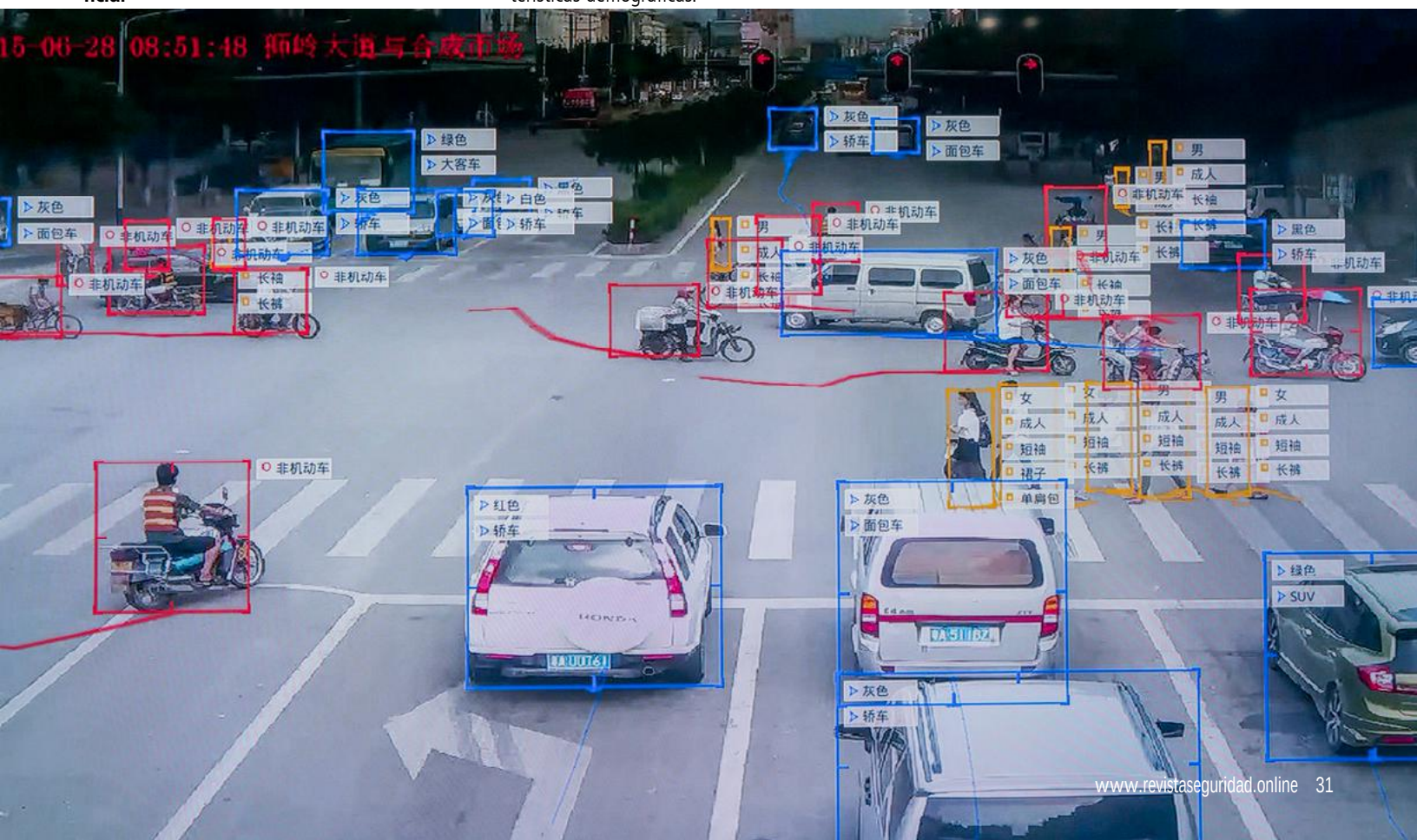
5. Dependencia de la tecnología: Confiar en la inteligencia artificial para la seguridad puede llevar a una dependencia excesiva de la tecnología, lo que podría dejar a las personas desprotegidas si hay fallas en el sistema o interrupciones de energía.

6. Consentimiento y transparencia: En muchos casos, las personas no están al tanto de la presencia de sistemas de vigilancia con IA o de cómo se utilizan los datos recopilados. Es esencial garantizar el consentimiento informado y la transparencia en el uso de esta tecnología.

7. Regulaciones y marco legal: La rápida evolución de la tecnología de vigilancia con IA puede superar la capacidad de los marcos legales y regulatorios para abordar adecuadamente los desafíos que presenta. Es importante contar con una legislación adecuada que proteja los derechos y la privacidad de las personas.

8. Error y decisiones automáticas: Si los sistemas de IA toman decisiones críticas basadas en la información de las cámaras, existe el riesgo de que puedan cometer errores o interpretar erróneamente situaciones, lo que podría tener consecuencias graves.

9. Falta de supervisión humana: Una excesiva dependencia de la IA en el proceso de toma de decisiones, podría llevar a la falta de supervisión humana y la pérdida de la capacidad de discernimiento ético y contextual.



Para abordar estos riesgos, es fundamental implementar estas tecnologías de forma responsable y ética. Esto incluye garantizar el cumplimiento de las regulaciones de privacidad, obtener el consentimiento informado, garantizar la seguridad cibernética, realizar pruebas exhaustivas para reducir el sesgo y permitir la supervisión y toma de decisiones humanas en situaciones críticas. También es importante involucrar a múltiples partes interesadas, como expertos en ética, juristas, defensores de la privacidad y el público en general, para crear un equilibrio adecuado entre seguridad y protección de los derechos individuales.

Países con Sistemas de cámaras de vigilancia con Inteligencia artificial

La implementación de sistemas de cámaras de vigilancia con inteligencia artificial está en constante expansión en todo el mundo. Es una tecnología en crecimiento que se utiliza en diferentes países para mejorar la seguridad y el monitoreo en diversas áreas. Algunos de los países que han adoptado activamente sistemas de cámaras de vigilancia con inteligencia artificial incluyen:

1. China: China es uno de los líderes mundiales en la implementación de sistemas de vigilancia con inteligencia artificial. Ha desarrollado una red masiva de cámaras de vigilancia que utilizan tecnología de reconocimiento facial y otras capacidades de IA en ciudades y áreas públicas.

2. Estados Unidos: Los sistemas de cámaras de vigilancia con IA también se han desplegado ampliamente en los Estados Unidos, tanto en áreas urbanas como en infraestructuras críticas como aeropuertos, estaciones de tren y edificios gubernamentales.

3. Reino Unido: El Reino Unido ha utilizado sistemas de vigilancia con IA para monitorear calles y áreas públicas, especialmente en ciudades importantes.

4. Emiratos Árabes Unidos: Los Emiratos Árabes Unidos han invertido significativamente en tecnologías de vigilancia con IA para mejorar la seguridad y el control en sus ciudades.

5. Singapur: Singapur ha implementado sistemas de cámaras de vigilancia con IA en diversos lugares, como aeropuertos, puertos y zonas urbanas, para mejorar la seguridad y la gestión del tráfico.

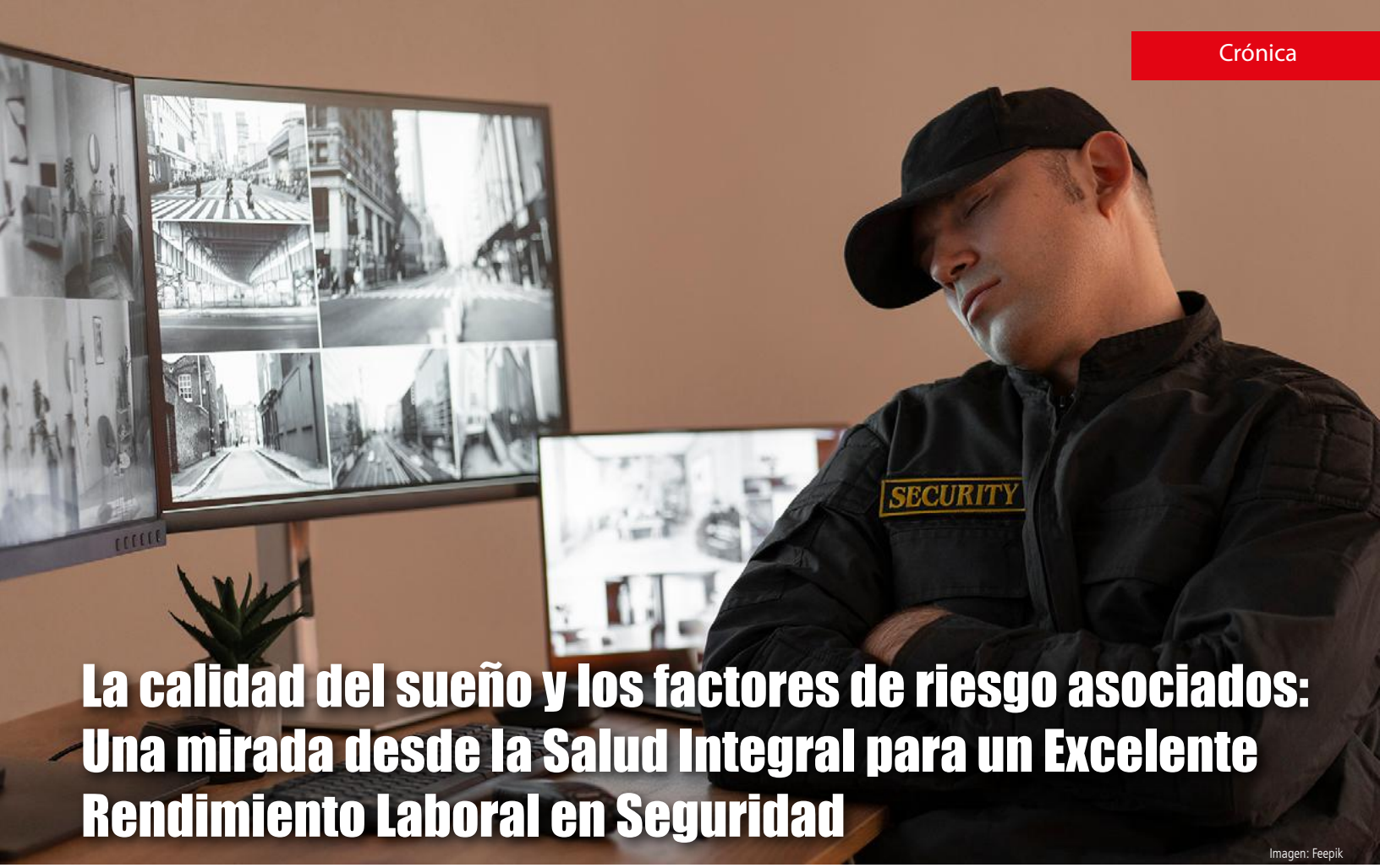
6. Corea del Sur: Corea del Sur ha adoptado tecnologías de vigilancia con IA para mejorar la seguridad en espacios públicos y en el transporte público.

7. Alemania: En Alemania, también se han utilizado sistemas de vigilancia con IA en ciudades y áreas públicas para mejorar la seguridad y el control del tráfico.

8. Australia: Australia ha implementado sistemas de vigilancia con IA en aeropuertos, estaciones de transporte público y otras áreas críticas para fortalecer la seguridad y la gestión.
9. Japón: Japón ha utilizado la inteligencia artificial en sistemas de cámaras de vigilancia para monitorear áreas urbanas y mejorar la seguridad pública.

Es importante tener en cuenta que la implementación de estos sistemas de vigilancia con IA puede variar significativamente en diferentes países debido a las diferencias culturales, regulaciones de privacidad y políticas de seguridad. Además, algunos países pueden tener mayores preocupaciones éticas y legales sobre el uso de estas tecnologías, lo que puede influir en su implementación y alcance.

Image by Freepik



La calidad del sueño y los factores de riesgo asociados: Una mirada desde la Salud Integral para un Excelente Rendimiento Laboral en Seguridad

Imagen: Feepik

El sueño es una función vital para el bienestar humano, y su importancia se ha reconocido cada vez más en el ámbito de la salud integral. Un sueño de calidad es fundamental para el bienestar físico y mental de las personas. Durante el sueño, el cuerpo y la mente se recuperan y se preparan para enfrentar un nuevo día. Sin embargo, la encuesta nacional de Salud en Chile 2016-2017, señala que el 48% de las mujeres y 39,4% de los hombres existe sospecha de algún tipo de alteración del sueño. La deficiencia de sueño puede tener consecuencias negativas a la salud ya que, tiene diversos factores de riesgo que pueden afectar negativamente la calidad y la duración del sueño, lo que tiene implicancias significativas para la salud y el funcionamiento diario de las personas, tales como; dificultades cognitivas, alteraciones del estado de ánimo, disminución del rendimiento laboral y/o académico, ganancia de peso excesiva, obesidad y alteraciones metabólicas, entre otras.

Es por ello que un sueño "saludable" promueve el bienestar emocional, la memoria y la atención, así como el adecuado funcionamiento del sistema inmunológico, entre otras. Existe una relación entre el funcionamiento del sistema circadiano, la alimentación y la regulación metabólica, esta alteración de la ritmicidad circadiana a partir de alteraciones genéticas, conductuales y alimentarias generaría algún tipo de condición de salud en general, o bien de salud mental.

Los ritmos circadianos en la fisiología humana.

Distintos estímulos externos como la luz, la comida o la actividad física influyen en el organismo generando unas respuestas fisiológicas endógenas cíclicas, que están marcadas por unos relojes internos. En el cuerpo humano existe un reloj principal que se localiza en el sistema nervioso central (SNC) y unos relojes periféricos que se pueden encontrar en casi todas las células y tejidos del organismo. A su vez, el SCN mantiene la sincronía de los relojes periféricos, mediante inervación autónoma y /o señales humorales. Toda esta sincronía circadiana finalmente se ve reflejada en distintos procesos fisiológicos y comportamentales. Referencia Bibliográfica: Calvo Fernández, J. R., & Gianzo Citores, M. (2018). Los relojes biológicos de la alimentación. Nutrición hospitalaria, 35(SPE4), 33-38.

Recordemos que el reloj biológico es aquel que establece la mantención de los ritmos o comúnmente se le conoce como ciclos circadianos en mamíferos, los cuales los ritmos biológicos tienen una duración cercana a 24 horas, un ejemplo de ello es su influencia en el ciclo de actividad-reposo, el ciclo sueño-vigilia o el perfil de secreción de diversas hormonas. Actualmente, se reconoce como un sistema circadiano de organización jerárquica conectada a nivel central y periférico en el organismo.

Entre los factores más relevantes que contribuyen a un desajuste circadiano, se encuentran:

1.Estrés y Ansiedad

Son factores de riesgo comunes que pueden afectar negativamente el sueño. Las preocupaciones, las responsabilidades y las presiones de la vida cotidiana pueden generar dificultades para conciliar el sueño y mantenerlo durante la noche. Además, la falta de sueño adecuado puede aumentar los niveles de estrés y ansiedad, creando un ciclo perjudicial para la salud mental.

Un ejemplo de ello son los horarios de trabajo extensos, entre ellos se encuentra el personal de seguridad pública-privada y personal de salud, entre ellos de urgencias y/o emergencias, a menudo trabajan en turnos rotativos o en horarios nocturnos. Esto puede provocar una desregulación del ciclo circadiano, dificultando la conciliación y el mantenimiento del sueño adecuado.

El desajuste en los patrones de sueño-vigilia puede llevar a problemáticas de insomnio y fatiga crónica entre otras, afectando negativamente la salud mental y el rendimiento laboral de un vigilante o encargado de la labor de seguridad de un recinto o protección de personas importantes,

Recomendaciones para tener un sueño saludable (Modificado World Sleep Society).

El sueño es una función vital para el bienestar humano, y su importancia se ha reconocido cada vez más en el ámbito de la salud integral. Un sueño de calidad es fundamental para el bienestar físico y mental de las personas. Durante el sueño, el cuerpo y la mente se recuperan y se preparan para enfrentar un nuevo día. Sin embargo, la encuesta nacional de Salud en Chile 2016-2017, señala que el 48% de las mujeres y 39,4% de los hombres existe sospecha de algún tipo de alteración del sueño. La deficiencia de sueño puede tener consecuencias negativas a la salud ya que, tiene diversos factores de riesgo que pueden afectar negativamente la calidad y la duración del sueño, lo que tiene implicancias significativas para la salud y el funcionamiento diario de las personas, tales como; dificultades cognitivas, alteraciones del estado de ánimo, disminución del rendimiento laboral y/o académico, ganancia de peso excesiva, obesidad y alteraciones metabólicas, entre otras.
Es por ello que un sueño "saludable" promueve el bienestar emocional, la memoria y la atención, así como el adecuado funcionamiento del sistema inmunológico, entre otras. Existe una relación entre el funcionamiento del sistema circadiano, la alimentación y la regulación metabólica, esta alteración de la ritmicidad circadiana a partir de alteraciones genéticas, conductuales y alimentarias generaría algún tipo de condición de salud en general, o bien de salud mental.

Los ritmos circadianos en la fisiología humana.

Distintos estímulos externos como la luz, la comida o la actividad física influyen en el organismo generando unas respuestas fisiológicas endógenas cíclicas, que están marcadas por unos relojes internos. En el cuerpo humano existe un reloj principal que se localiza en el sistema nervioso central (SNC) y unos relojes periféricos que se pueden encontrar en casi todas las células y tejidos del organismo. A su vez, el SCN mantiene la sincronía de los relojes periféricos, mediante inervación autónoma y /o señales humorales. Toda esta sincronía circadiana finalmente se ve reflejada en distintos procesos fisiológicos y comportamentales. Referencia Bibliográfica: Calvo Fernández, J. R., & Gianzo Citores, M. (2018). Los relojes biológicos de la alimentación. Nutrición hospitalaria, 35(SPE4), 33-38.

Recordemos que el reloj biológico es aquel que establece la mantención de los ritmos o comúnmente se le conoce como ciclos circadianos en mamíferos, los cuales los ritmos biológicos tienen una duración cercana a 24 horas, un ejemplo de ello es su influencia en el ciclo de actividad-reposo, el ciclo sueño-vigilia o el perfil de secreción de diversas hormonas. Actualmente, se reconoce como un sistema circadiano de organización jerárquica conectada a nivel central y periférico en el organismo.

Entre los factores más relevantes que contribuyen a un desajuste circadiano, se encuentran:

1.Estrés y Ansiedad

Son factores de riesgo comunes que pueden afectar negativamente el sueño. Las preocupaciones, las responsabilidades y las presiones de la vida cotidiana pueden generar dificultades para conciliar el sueño y mantenerlo durante la noche. Además, la falta de sueño adecuado puede aumentar los niveles de estrés y ansiedad, creando un ciclo perjudicial para la salud mental.

Un ejemplo de ello son los horarios de trabajo extensos, entre ellos se encuentra el personal de seguridad pública-privada y personal de salud, entre ellos de urgencias y/o emergencias, a menudo trabajan en turnos rotativos o en horarios nocturnos. Esto puede provocar una desregulación del ciclo circadiano, dificultando la conciliación y el mantenimiento del sueño adecuado.

El desajuste en los patrones de sueño-vigilia puede llevar a problemáticas de insomnio y fatiga crónica entre otras, afectando negativamente la salud mental y el rendimiento laboral de un vigilante o encargado de la labor de seguridad de un recinto o protección de personas importantes, entre otras actividades propias de la seguridad privada.

El personal de seguridad pública está expuesto a altos niveles de estrés laboral, lo que puede llevar al síndrome de burnout, caracterizándose por una sensación de agotamiento físico y emocional, lo cual puede interferir significativamente con el sueño y el descanso adecuado.

Esto que pareciera ser una trivialidad, no lo es y cobra una relevancia estratégica debido a que la

falta de dormir se traduce en un descanso insuficiente que afectará las funciones laborales de vigilancia e incluso puede condicionar en un trabajador de la seguridad a una respuesta inadecuada o contraria a los protocolos producto de la falta de descanso. Es imprescindible que las empresas dedicadas a la seguridad privada aborden esta problemática con programas preventivos y de educación para su personal, esto aportará significativos beneficios al desempeño de sus funciones.

2.Trastornos del Sueño

La apnea del sueño y el insomnio entre otras, representan otro factor de riesgo significativo. Estos trastornos pueden interferir con la calidad y la cantidad del sueño, lo que lleva a una sensación de cansancio crónico y afectando la capacidad cognitiva y el rendimiento en general. Es crucial que los profesionales de la salud pública promuevan la consciencia y el acceso a la detección y tratamiento adecuado de estos trastornos.
3.Diferenciación de Diagnóstico de la Depresión

La depresión y el sueño están estrechamente relacionados. La depresión puede alterar el patrón de sueño, causando insomnio o hipersomnia. Por otro lado, la deficiencia de sueño puede aumentar el riesgo de desarrollar o agravar los síntomas depresivos. Es importante abordar tanto la depresión como los problemas de sueño de manera interdisciplinaria para un tratamiento clínico adecuado. Es vital tener esta consideración en el mundo de la seguridad, toda vez que podría ser un riesgo mayor el que un trabajador dedicado a la seguridad estuviera en funciones y no haya sido diagnosticado, las consecuencias podrían ser impredecibles.

Es importante reconocer cuándo los problemas de sueño requieren la intervención de un profesional de la salud. Si los problemas de sueño persisten durante un período prolongado e interfieren con las actividades diarias, causan malestar emocional significativo o bien afectan negativamente la calidad de vida, es recomendable buscar la ayuda de un profesional de la salud especializado en trastornos del sueño.

4.Estilos de vida poco Saludables, Hábitos de Sueño y Entornos Inadecuados

La salud pública es una disciplina que se preocupa por el bienestar colectivo de la población y busca abordar los factores que deterioran la salud de manera global. La higiene del sueño se refiere a las prácticas y hábitos que favorecen una buena calidad del sueño. Dormir es una función esencial para el organismo, durante la cual ocurren procesos de reparación celular, consolidación de la

Autora: Ximena Abarca Piña
Magister Salud Pública de la Universidad Andrés Bello
Diplomada en salud en universidades nacionales y extranjeras
Jefa del Proyecto A-System en Cie-Latam
ximena.abarca@cie-latam.cl
www.cie-latam.cl

Campaña de Fraude

"Aviso de notificación de la DEHÚ:

Un phishing bien diseñado

En el mundo hispanohablante históricamente hemos tenido una ventaja a la hora de enfrentarnos a los fraudes online: Muchos de estos fraudes son diseñados para el mercado angloparlante, y/o por grupos de ciberdelincuencia que no hablan nuestro idioma. Por ende, partían con desventaja a la hora de engañarnos, ya que probablemente, a poco que nos fijemos en su legibilidad, algo no funcionaba.Sin embargo, de un tiempo a esta parte la industria del cibercrimen ha crecido tanto que ya es muy habitual encontrarse ante campañas de phishing muy bien elaboradas y localizadas al mercado en cuestión. Este es el caso de la que quería hablar hoy, y que he recibido recientemente: El fraude del aviso de notificación de la DEHÚ.

Primero de todo: ¿ Qué es eso de la DEHU?

DEHÚ es la plataforma de notificación del gobierno de España. Desde hace unos años, y en ese proceso continuo de transformación digital, cada vez más notificaciones se reciben de forma telemática, y para ello, los diferentes ministerios españoles se han ido sumando a la plataforma.

Por tanto, es muy probable que si tienes un requerimiento de Hacienda, o esté esperando alguna subvención, o haya participado en alguna licitación, o simplemente tiene una empresa a su nombre y cuente, por supuesto, con un certificado digital o algún sistema de acceso telemático a servicios gubernamentales, o haya tenido que usar (y pegarte, todo sea dicho) con DEHÚ.

Que no sé usted, pero yo, cada vez que recibo un aviso de notificación de DEHÚ, me pongo nervioso.

En la mayoría de las ocasiones, se trata de una alerta de algún tema relacionado con el ministerio de transformación digital, por eso de que CyberBrainers es una entidad acogida al programa de agente digitalizador del Kit Digital, y este programa, como tantos otros, utiliza DEHÚ como plataforma de notificación.

Pero claro, cuando usted mira el email que te envían, no tiene ni idea de si se trata de algo bueno o malo, siendo esto último lo más habitual.Incluso con el Kit, ya van varias notificaciones que han supuesto tener que volver a enviar más documentación para seguir siendo agentes digitalizadores, por eso de que el gobierno saca programas y luego, con el tiempo, va cambiando a su antojo los requerimientos para estar adscritos, teniendo los digitalizadores que perder nuevamente tiempo documentando otra vez lo que ya habíamos documentado, y nos habían aceptado, previamente.

Y no solo, sino que, como les decía, DEHÚ es la plataforma que también usa la Agencia Estatal de Administración Tributaria. Y ya sabes que siempre que recibe una notificación de Hacienda, es para mal.

A un servidor, por ejemplo, este año le han hecho dos inspecciones: Una a título personal, y otra a título de la empresa. En ambas he podido salir airoso (lo tengo todo regularizado), pero ya sabe cómo va la cosa: Aunque haya hecho todo bien, puede que no se lo acepten, como le pasó a Èlia hace ya un par de años con otra inspección, en la que incluso le echaron para atrás viajes de ida y vuelta para dar conferencias, ya que según el inspector asignado, eso no era por trabajo, es por ocio (claro, te vas un día a la otra punta del mundo, das una conferencia y presentas pruebas de ello, y vuelves al día siguiente, porque te gusta viajar en avión…).

En fin, que sea como fuere, ahora, que estamos en fechas de presentar la Renta, los cibercriminales están lanzando ya campañas de fraude haciéndose pasar por Hacienda.Y la que he recibido yo la semana pasada, perfectamente podría haber pasado por verídica.

¿Cómo funciona el fraude del aviso de notificación de la DEHú?

Echas las presentaciones anteriores, paso a definir cómo fue el ataque, y por qué estuve a puntito de picar.

Pero antes, una matización: Al menos a un servidor siempre que recibo una notificación de la DEHÚ, la suelo recibir por duplicado, supongo que porque tengo dos correos (personal y corporativo) asociados.Por eso, me sorprendió que un día como hoy, a la tarde, recibiera una única notificación de la DEHÚ al correo corporativo.

Sin embargo, daba la casualidad que ese mismo día, a la mañana, había recibido varias, por lo que perfectamente podría tratarse o de un email que se envió más tarde de lo previsto, o de otra nueva notificación.

Así que, cómo no, corrí a abrirlo, y me encontré

Aviso de notificación de la DEHú contacto@cyberbrainers.com Recibidos ×

DEHú notificaciones@dehu.com a través de rsvehicleimports.com.au jue [redacted] (hace 4 días)
para contacto

ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN ELECTRÓNICA.

Le informamos que está disponible una nueva notificación para contacto@cyberbrainers.com como Titular con los siguientes datos:

- Titular contacto@cyberbrainers.com
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: L02000050
- Identificador: 51[redacted]
- Concepto: Notificación -- Expediente 46[redacted]SIA 2087160, Serie SF0249)
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://agenciatributaria.gob.es

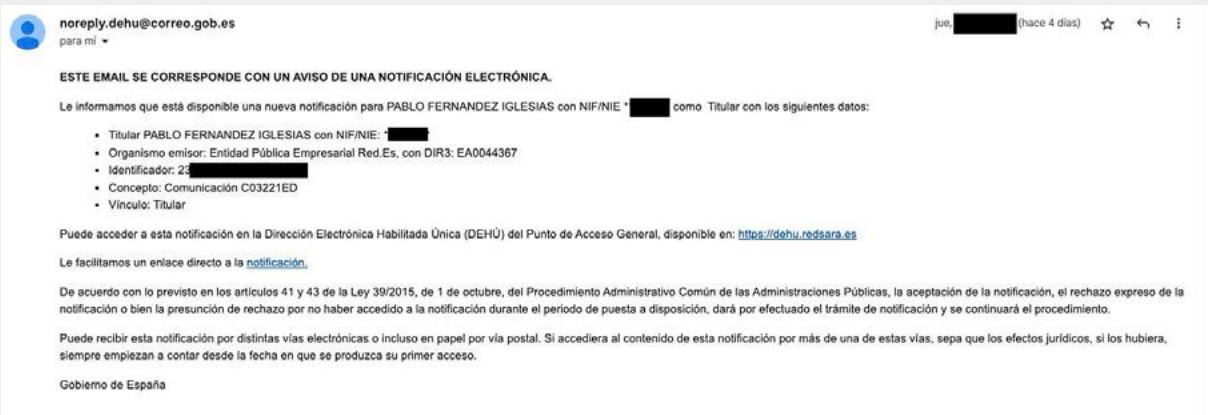
Le facilitamos un enlace directo a la notificación.

De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la aceptación de la notificación, el rechazo expreso de la notificación o bien la presunción de rechazo por no haber accedido a la notificación durante el periodo de puesta a disposición, dará por efectuado el trámite de notificación y se continuará el procedimiento.

Puede recibir esta notificación por distintas vías electrónicas o incluso en papel por vía postal. Si accediera al contenido de esta notificación por más de una de estas vías, sepa que los efectos jurídicos, si los hubiera, siempre empiezan a contar desde la fecha en que se produzca su primer acceso.

Gobierno de España

Ejemplo de campaña de phishing de la DEHÚ bien diseñada



noreply.dehu@correo.gob.es jue [redacted] (hace 4 días)
para mí

ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN ELECTRÓNICA.

Le informamos que está disponible una nueva notificación para PABLO FERNANDEZ IGLESIAS con NIF/NIE *[redacted] como Titular con los siguientes datos:

- Titular PABLO FERNANDEZ IGLESIAS con NIF/NIE: *[redacted]
- Organismo emisor: Entidad Pública Empresarial Red.Es, con DIR3: EA0044367
- Identificador: 23[redacted]
- Concepto: Comunicación C03221ED
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://dehu.redsara.es

Le facilitamos un enlace directo a la notificación.

De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la aceptación de la notificación, el rechazo expreso de la notificación o bien la presunción de rechazo por no haber accedido a la notificación durante el periodo de puesta a disposición, dará por efectuado el trámite de notificación y se continuará el procedimiento.

Puede recibir esta notificación por distintas vías electrónicas o incluso en papel por vía postal. Si accediera al contenido de esta notificación por más de una de estas vías, sepa que los efectos jurídicos, si los hubiera, siempre empiezan a contar desde la fecha en que se produzca su primer acceso.

Gobierno de España

Ejemplo de correo real y oficial enviado por la DEHÚ

lo siguiente:

Se trata, a todas luces, de exactamente el mismo copy que tienen todos los envíos de la DEHÚ, y por lo que puedo ver, parece ser una notificación de Hacienda (vamos, algo malo…).

Adjunto otro mail, recibido ese mismo día, y que sí es oficial, para que veas las escasas diferencias que tiene esta campaña de phishing, con un correo real de la DEHÚ.

Como pueden apreciar, teniendo uno delante de otro es fácil darse cuenta de que en el primero no se dirigen a mi como titular, sino al correo electrónico. Por supuesto, si fuera oficial o bien pondrían, como ponen, mis datos fiscales personales (nombre completo y algunos de los números del DNI), o bien iría dirigido a la propia empresa, en cuyo caso aparecerían los datos fiscales de la misma (razón social y algunos de los números del CIF). Pero por lo demás, es un calco exacto de las comunicaciones oficiales.

Hay que decir, eso sí, que lo abrí desde el móvil, y como recomiendo hacer siempre en esos tres puntos que identifican a un phishing, para confirmar su legitimidad, lo primero que hice fue ver quién era el emisor del mail, encontrándome con que, en efecto, parecía ser un mail oficial enviado por notificaciones@dehu.es.

De nuevo, algo que parece legítimo… pero que no existe como tal. Las comunicaciones oficiales de la DEHÚ vienen dadas por el dominio oficial de la DEHÚ, que al tratarse de un dominio corporativo, es correo.gob.es.

Otro matiz que de no tener ambos correos (fraudulento y oficial) delante, se nos puede pasar inadvertido.

A la hora de escribir este artículo, no obstante, y ya desde escritorio, veo que aunque en efecto los metadatos de envío estaban correctamente puestos, GMail sí me chiva que el emisor no es esa cuenta, sino otra con un dominio muy poco confiable, como puedes ver a continuación:

Esta información, en la versión móvil, no me aparecía, pensando que en efecto estaba ante una comunicación oficial

Los oficiales, por supuesto, vienen también firmados por correo.gob.es.

Pero recalco, lo estaba mirando desde el móvil, y ahí este indicio no lo tenía, así que, y de nuevo por ser precavido, me da por mirar a dónde llevan esos dos enlaces de la notificación (el tercer punto de los que debemos fijarnos a la hora de identificar fraudes de correos legítimos).

Y aquí es cuando veo que estoy ante un fraude más. Eso sí, con sorpresa incluida.

Ambos enlaces, en vez de llevar a la plataforma de la DEHÚ, llevan a una página dentro del dominio registraalbacete[dot]com. Que ya me dirás qué tiene que ver con la DEHÚ (ni tan siquiera vivo en Albacete), por lo que supongo que simplemente es uno de los dominios que tienen bajo el control los cibercriminales.

La sorpresa viene porque al intentar entrar, me encuentro con que el enlace te redirige a una supuesta página de la Agencia Tributaria, que por lo que puedo ver, están cambiando cada poco (cuando entré la primera vez era una agenciatributaria[dot]online, y ahora veo que redirige a agenciatributaria[dot]hk).

La web en cuestión se parece a la de la Agencia Tributaria, pero es aquí donde el fraude cojea, ya que, que yo sepa, hoy en día no hay manera de acceder a trámites administrativos mediante usuario y contraseña.

O bien lo haces mediante certificado digital, bien mediante Cl@ve, o PIN Permanente. Sistemas que

difícilmente veo cómo pueden robárnoslos los cibercriminales.

Pero oye, igual así cazan los datos de algunas víctimas…

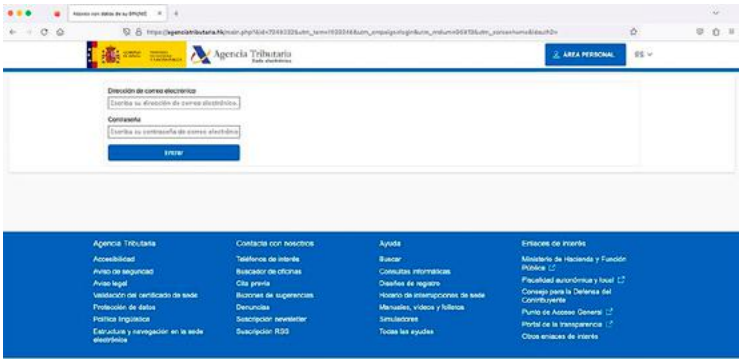
Por cierto, que he probado a poner un usuario y contraseña (inventados, por supuesto), y la web, como era de esperar, me dice que la validación no es correcta y que vuelva a incluirlos.

Ni tan siquiera se han molestado en hacer una redireción a la página oficial…

Y otro apunte:
Desde que me llegó el mail, hasta que he creado este artículo, han pasado 4 días. En estos cuatro días me alegra ver que tanto Chrome como Firefox (los dos navegadores de escritorio que he probado para preparar este tutorial) ya marcaban como potencialmente fraudulento el enlace de Albacete. Y Firefox, además, hacía lo propio con el dominio fake de la AgenciaTributaria (Chrome sí me dejaba entrar a él, sin mostrarme alerta).

Un ejemplo más de los tiempos que manejan estos cibercriminales, que son conscientes de que a las pocas horas de lanzar la campaña, la URL se va a quemar, y tocará volver a lanzar otra campaña.

De hecho, por eso es tan habitual que usen redirecciones que les permitan funcionar durante al menos unas horas más las campañas activas, pudiendo cambiar la URL final del phishing mientras aún no se ha quemado la URL que aparece en el correo, y que redirige al fraude en cuestión.



¿Cómo podemos evitar ser víctimas de este tipo de campañas de phishing?

Como pueden ver, simplemente he aplicado los 3 elementos que delatan a las campañas de phishing o fraude por email.

1. Cerciorarse de quién es quién envía el email realmente
2. Revisar con calma si lo que dice el mail tiene sentido
3. Desconfiar por defecto de los enlaces y de los ficheros adjuntos, estableciendo las medidas de seguridad adecuadas para abrirlos.

Autor: Pablo F. Iglesias

Se describe como un apasionado de la tecnologíaConsultor de Presencia Digital y Reputación Online, presidente de la Consultora de Reputación Online CyberBrainers, y fundador, co-fundador, vocal y vicepresidente de varias startups y asociaciones relacionadas con el mundo de la ciberseguridad, la transformación digital y el marketing.

Con más de una década escribiendo a diario en www.pabloyglesias.com, es uno de los mayores referentes en materia de nuevas tecnologías y seguridad de la información de habla hispana.

Desarrolla labores pedagógicas (online y presencial) sobre Presencia Digital y Seguridad de la Información, intentando concientizar a la sociedad, sobre los riesgos y oportunidades del tercer entorno.

Actualmente asesora a profesionales, PYMES y grandes empresas sobre cómo obtener valor de la información que circula a su alrededor. El punto medio necesario entre marketing, comunicación y seguridad de la información.

La investigación forense
Ciencia y tecnología al servicio de la investigación criminal

El 28 de agosto de este año, el Laboratorio de Criminalística Central de la PDI cumplirá 88 años de vida institucional. Creada solo dos años después de que naciera la Policía de Investigaciones de Chile en 1933, ha sido el área responsable del actual posicionamiento que mantiene la institución como líder en la investigación criminal, y como una de las instituciones más cercanas y confiables para la ciudadanía.

Desde sus inicios, el Laboratorio de Criminalística ha apoyado mediante la aplicación de métodos, técnicas y conocimientos científicos a la función investigativa policial en el esclarecimiento de los delitos, además de colaborar con los Tribunales de Justicia, el Ministerio Público, y los demás actores vinculantes a la persecución penal, efectuando las pericias forenses que se le encarguen.

En la actualidad, el Laboratorio de Criminalística Central de la PDI (LACRIM) es considerado un referente a nivel nacional y regional, debido a la evolución de la administración de justicia, la cual ha puesto en el centro del proceso de persecución penal a la "prueba científica". El Lacrim Central está conformado por 17 secciones, todas y cada una apoyan desde su particular misión a las investigaciones desarrolladas por las diferentes Brigadas de Investigación Criminal, o especializadas del país, a través de la aplicación de técnicas y conocimientos científicos, donde se examinan los indicios recuperados desde la escena del crimen, cuyos resultados se plasman en el informe pericial.

El nivel de equipamiento tecnológico, las capacidades profesionales de su dotación, y el sistema de gestión de calidad, basado en normas nacionales e internacionales, que han determinado la certificación de sus procedimientos, han permitido que el Lacrim Central se imponga como el referente técnico entre los laboratorios forenses de la institución, ofreciendo actualmente un total de 158 servicios periciales certificados, con jurisdicción a nivel regional y nacional, transformándolo en el principal y más completo Laboratorio forense de nuestro país.

El nuevo edificio que alberga al Lacrim Central, inaugurado el 02 de noviembre del año 2021, se ha transformado en un referente latinoamericano en investigación científica forense, pues cuenta con dependencias de estándar mundial para la labor investigativa.

Las actuales exigencias y los profundos cambios socio-policiales, han obligado a la PDI a transformarse en una organización policial de alto rendimiento, capaz de modernizarse y adaptar sus procedimientos hacia la eficiencia y eficacia en su accionar. En cuanto a innovaciones, la implementación de los laboratorios de última generación incluye robots para la extracción de ADN, termocicladores, secuenciadores, tecnología de electroforesis capilar, sistema de PCR en tiempo real, software analizador genético, cámaras reveladores de impresiones dactilares y equipos para la reconstitución de fragmentos dactilares, entre otros instrumentos.

Esta moderna infraestructura es el resultado de un permanente proceso de modernización institucional, el que además incluye una proyección para el segundo semestre del año 2023 en contar con la acreditación legal por la Ley 19.970 que crea el registro nacional de ADN; para el año 2024 contar con la certificación ISO 9.001 y el año 2025 con la acreditación bajo normas ISO 17.025 y la NCH 3249; lo que permitirá alcanzar los más altos estándares de calidad en la pericias forenses tanto a nivel nacional como internacional, sumado al sostenido compromiso del capital humano que se desempeña en esta área, lo que generará una mejora continua y permanente del trabajo científico y del correcto uso de las tecnologías disponibles al servicio de la investigación criminal.

Richard Biernay Arriagada
Relacionador Público
Ingeniero Civil Industrial
Magíster en Educación

Ciberseguridad en la era del Internet de las Cosas (IoT): Protegiendo el futuro conectado

Image by rawpixel.com on Freepik

En la actualidad, el mundo está experimentando una transformación digital sin precedentes. La proliferación del Internet de las Cosas (IoT) ha llevado a una interconexión masiva de dispositivos, desde electrodomésticos inteligentes hasta sensores industriales. Si bien esta revolución tecnológica promete mejorar nuestra calidad de vida y optimizar procesos comerciales, también conlleva riesgos significativos para la ciberseguridad. En esta columna de opinión, se abordará el mundo del IoT y los desafíos de ciberseguridad asociados, junto con las soluciones que deberíamos considerar para salvaguardar nuestro futuro conectado.

El Internet de las Cosas se refiere a la red de dispositivos físicos interconectados que tienen la capacidad de recopilar y compartir datos a través de Internet, sin la necesidad de una interacción humana directa.

Estos dispositivos, conocidos como "cosas" o "dispositivos inteligentes", pueden variar desde termostatos y cámaras de seguridad hasta vehículos autónomos y maquinaria industrial. La clave del IoT radica en la capacidad de estos dispositivos para comunicarse y tomar decisiones basadas en los datos que recopilan, lo que crea un ecosistema conectado y automatizado.

A pesar de los beneficios del IoT, la proliferación de dispositivos conectados también ha abierto un nuevo mundo de vulnerabilidades y desafíos de ciberseguridad. Aquí, destacamos algunos de los riesgos más relevantes:

• Escasa seguridad en los dispositivos: Muchos fabricantes de dispositivos IoT priorizan la funcionalidad y el tiempo de comercialización en lugar de la seguridad, lo que da lugar a dispositivos con vulnerabilidades preexistentes y falta de actualizaciones regulares.

• Identidades no verificadas: Los dispositivos IoT pueden ser blanco de ataques de suplantación de identidad, lo que permite a los ciberdelincuentes acceder a la red y comprometer otros dispositivos.

• Transmisión de datos no segura: La transmisión no cifrada de datos entre dispositivos y servidores podría exponer información sensible, a posibles intercepciones.

• Ataques de denegación de servicio distribuido (DDoS): Un gran número de dispositivos IoT mal protegidos puede ser reclutado para lanzar ataques DDoS masivos, que sobrecargan los sistemas objetivo, dejándolos inoperables.

• Privacidad comprometida: La recopilación masiva de datos por parte de dispositivos IoT puede generar preocupaciones sobre la privacidad, y cómo se utilizan esos datos.

A medida que el IoT continúa expandiéndose y penetrando en prácticamente todos los aspectos de nuestras vidas, es crucial abordar estos desafíos de ciberseguridad para proteger nuestra privacidad, nuestros activos y nuestras infraestructuras críticas. Para lograr esto, se deben tomar medidas concertadas por parte de los fabricantes, los reguladores, las organizaciones y los usuarios finales.

Responsabilidad de los fabricantes:
En primer lugar, los fabricantes de dispositivos IoT deben priorizar la seguridad desde las primeras etapas del diseño. Implementar prácticas seguras de desarrollo de software, realizar pruebas exhaustivas de seguridad y proporcionar actualizaciones regulares de firmware son pasos fundamentales para reducir las vulnerabilidades. Además, establecer estándares de seguridad específicos para el IoT garantizaría una mayor uniformidad en la protección de los dispositivos y fomentaría la confianza del consumidor.

Regulación efectiva:
La ciberseguridad del IoT no puede depender únicamente de las acciones de los fabricantes. Los

gobiernos y organismos reguladores también deben desempeñar un papel activo en la protección de los ciudadanos y las empresas. La implementación de leyes y regulaciones que exijan ciertos niveles de seguridad para los dispositivos IoT, junto con la aplicación de sanciones por incumplimiento, puede motivar a los fabricantes a mejorar la seguridad de sus productos.

Enfoque en la educación y concientización:
Además de las medidas técnicas y regulatorias, la educación y la concientización son esenciales para abordar los desafíos de ciberseguridad del IoT. Los usuarios finales deben ser conscientes de los riesgos asociados con el uso de dispositivos IoT y capacitados para tomar medidas proactivas, como cambiar contraseñas predeterminadas, habilitar la autenticación de dos factores y mantener sus dispositivos actualizados.

Fomentar la colaboración entre la industria:
La colaboración entre fabricantes, investigadores de seguridad y profesionales de ciberseguridad es crucial para abordar las amenazas emergentes. Establecer programas de divulgación responsable, donde los investigadores puedan informar de forma segura sobre vulnerabilidades recién descubiertas, fomentaría la resolución oportuna de problemas de seguridad y ayudaría a mantener a los usuarios a salvo.

El futuro cercano de la ciberseguridad y el IoT

Mirando hacia el futuro, es probable que la ciberseguridad del IoT siga siendo una preocupación apremiante a medida que la tecnología continúa avanzando. La creciente adopción de dispositivos conectados en sectores críticos, como la salud y la energía, aumentará la importancia de proteger estas infraestructuras de ataques maliciosos.

La llegada de la tecnología 5G también abrirá nuevas oportunidades para el IoT, pero también aumentará la superficie de ataque. La latencia ultra baja y la mayor capacidad de conexión, pueden impulsar la adopción de aplicaciones IoT en tiempo real, pero también requerirán un enfoque más sólido en la ciberseguridad para evitar posibles consecuencias catastróficas de fallas de seguridad.

Asimismo, la implementación más amplia de la "computación en el borde" o "edge computing" (metodología de cálculo distribuido que busca llevar la computación y el almacenamiento de datos más cerca de la ubicación donde se necesita) puede descentralizar aún más las operaciones, lo que plantea desafíos adicionales para garantizar una seguridad uniforme y coherente en todos los dispositivos IoT conectados.

El Internet de las Cosas está aquí para quedarse, y su crecimiento continuo no solo mejorará nuestras vidas, sino que también presentará nuevos retos de seguridad. Para asegurar un futuro conectado y protegido, es esencial que los fabricantes, los gobiernos, las organizaciones y los usuarios trabajen juntos para abordar los desafíos de ciberseguridad del IoT.

Algunas sugerencias clave para proteger nuestro futuro conectado incluyen:

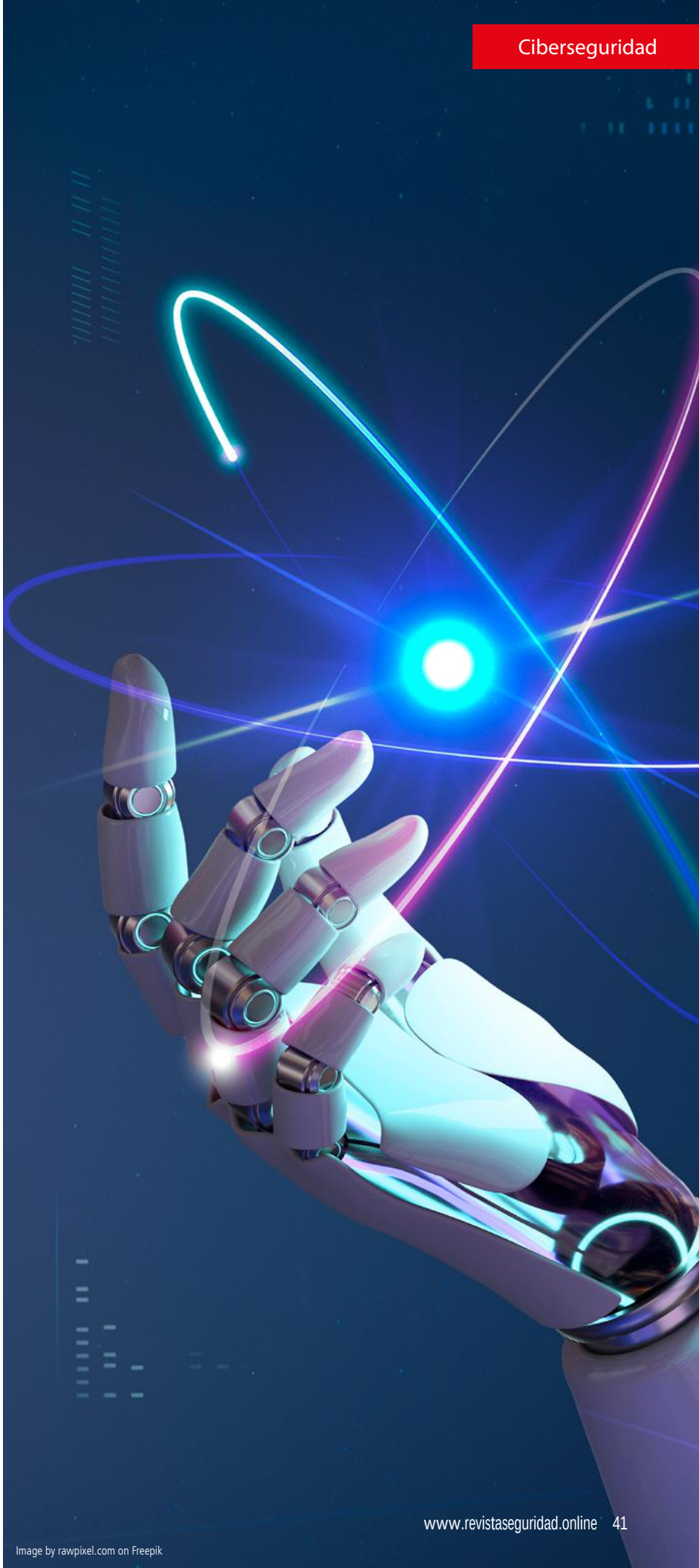


Image by rawpixel.com on Freepik

1. Investigación e innovación continua: La investigación y la innovación, sobre todo en áreas asociadas a la ciberseguridad, deben ser prioritarias para anticipar y contrarrestar las amenazas emergentes. La inversión en tecnologías de seguridad avanzadas, como el análisis de comportamiento y la detección de anomalías, puede ayudar a identificar patrones de actividad sospechosa y prevenir ataques antes de que causen daño.

2. Colaboración entre sectores: La ciberseguridad del IoT es un desafío que afecta a múltiples sectores, desde el gobierno y la industria, hasta los consumidores. Es crucial fomentar la colaboración entre estos sectores para compartir información sobre amenazas, mejores prácticas y soluciones de seguridad. El intercambio de conocimientos y experiencias puede mejorar la capacidad de respuesta colectiva ante las amenazas cibernéticas.

3. Enfoque en la educación y capacitación: La capacitación en ciberseguridad debe ser una prioridad tanto para los fabricantes como para los usuarios finales. Los fabricantes deben educar a sus equipos de desarrollo sobre las mejores prácticas de seguridad, mientras que los usuarios finales deben recibir información sobre cómo proteger sus dispositivos y datos. Esto incluye el fomento de prácticas de contraseña sólidas, actuaciones de software regulares y precauciones al compartir información personal.

4. Regulación efectiva y estándares de seguridad: Los gobiernos y organismos reguladores deben establecer y hacer cumplir estándares de seguridad sólidos para los dispositivos IoT. La implementación de regulaciones efectivas puede motivar a los fabricantes a invertir en ciberseguridad y garantizar que los dispositivos que llegan al mercado sean seguros desde el principio.

5. Gestión adecuada de riesgos: Las organizaciones y usuarios deben adoptar un enfoque de gestión de riesgos integral para identificar y abordar posibles amenazas. Esto implica evaluar y clasificar los activos críticos, identificar vulnerabilidades, aplicar controles de seguridad y desarrollar planes de contingencia para mitigar los riesgos identificados.

A medida que avanzamos hacia el futuro, el Internet de las Cosas seguirá siendo una fuerza impulsora en la transformación digital. Sin embargo, también debemos estar preparados para los desafíos de seguridad, que acompañarán a esta revolución tecnológica.

Algunas tendencias y desarrollos que podemos esperar en el futuro cercano incluyen:

1 Integración de IA en la ciberseguridad del IoT: La inteligencia artificial desempeñará un papel cada vez más importante en la detección y prevención de ataques cibernéticos en dispositivos IoT. La IA puede analizar grandes volúmenes de datos en tiempo real, identificar patrones anómalos y responder a amenazas de manera más rápida y efectiva, que los sistemas tradicionales de seguridad.

2. Blockchain para la seguridad del IoT: La tecnología blockchain puede proporcionar una capa adicional de seguridad para los dispositivos IoT, al garantizar la integridad y autenticidad de los datos. Al utilizar registros inmutables y descentralizados, la tecnología blockchain puede prevenir ataques de suplantación de identidad y proporcionar una mayor confianza en la integridad de la información.

3. Regulaciones más estrictas: A medida que aumenten las preocupaciones sobre la ciberseguridad del IoT, es probable que los gobiernos implementen regulaciones más estrictas, para garantizar la protección de los consumidores y la infraestructura crítica. Esto puede incluir normas específicas de seguridad, requisitos de certificación y sanciones más severas para aquellos que no cumplan con los estándares establecidos.

4. Mayor conciencia por parte del consumidor: A medida que los incidentes de seguridad relacionados con el IoT continúen apareciendo, en los titulares, es probable que los consumidores se vuelvan más conscientes de los riesgos y la importancia de proteger sus dispositivos. Esto puede conducir a una mayor demanda de productos y servicios seguros, lo que a su vez presionará a los fabricantes a mejorar la seguridad de sus productos.

El Internet de las Cosas representa una emocio-

Autor: Claudio Escobar
Master in Business Engineering (MBE),
Universidad de Chile; Licenciado
en Informática y Gestión,
Universidad Diego Portales.
Ingeniero en Informática y Gestión,
Universidad Diego Portales.

SHOT FAIR BRASIL
La familia del tiro deportivo y el mundo táctico

Los amantes del tiro deportivo, el mundo táctico y los profesionales de la seguridad se darán cita en la 3ª edición de SHOT FAIR BRASIL los días 2, 3, 4 y 5 de agosto de 2023 , en el Centro de Convenciones y Exposiciones Expoville, en la ciudad de Joinville, Santa Catalina.

El evento, el más grande de América Latina, se ha convertido en una referencia en el segmento de tiro deportivo, con el éxito en el cierre de negocios que se convirtieron en millones de reales, como en las ediciones de 2021 y 2022. SHOT FAIR BRASIL también se ha convertido en un espacio único para el lanzamiento productos, dando una visibilidad sin precedentes a los sectores involucrados.

En 2023, la SHOT FAIR BRASIL tiene como misión mantener unida la familia del tiro deportivo, con integración entre minoristas, importadores, marcas, atletas, instructores y clubes de tiro.

En la tercera edición, el público encontrará una oferta más amplia de expositores, superando el número de ediciones anteriores, además de consolidar el intercambio de conocimientos, con charlas, talleres y jornadas. Una de las novedades para 2023 es el Simposio Comex, con el intercambio de información sobre la importación de PCE – productos controlados por el Ejército.

MUNDO TÁCTICO

Los productos del universo táctico ganan más espacio en 2023. El mundo táctico está formado por productos funcionales y versátiles, utilizados por profesionales que se enfrentan a situaciones desafiantes y amantes de la vida al aire libre y la aventura.

INCLUSIÓN Y AVENTURA

La 3ª edición trae nuevos embajadores Richarlles Ghabriel y Celso Cavallini, que hacen que el nombre de SHOT FAIR BRASIL siga siendo confiable y fuerte.

El tirador deportivo e instructor Richarlles Ghabriel viene a demostrar cuánto el mundo del tiro es sinónimo de inclusión. Richarlles nació sin brazos. Con el apoyo de familiares y amigos, aprendió a disparar con los pies.

Celso Cavallini es uno de los nombres más reconocidos en el mundo táctico y al aire libre. Ha trabajado como reportero de aventuras y juegos extremos en los principales canales de televisión. Junto a importantes marcas, desarrolla productos que garantizan un buen desempeño en situaciones extremas.

Richarlles Ghabriel y Celso Cavallini forman parte del equipo de embajadores formado por el atleta olímpico Felipe Wu, y la coleccionista y tiradora deportiva Aline Kanyo.

La 3ª edición del evento se realiza del 2 al 5 de agosto, en Expoville, en Joinville (SC), y reunirá expositores de equipos tácticos, caza, camping, montañismo, tiro deportivo y aventura.

En SHOT FAIR BRASIL 2023, el público que aprecia el tiro deportivo, las aventuras y experiencias de la vida al aire libre, experimentará una inmersión con las principales marcas de productos y servicios destinados al mundo táctico, caza y pesca, camping, montañismo y otras actividades relacionadas con este robusto segmento.

"SHOT FAIR BRASIL llega a su tercera edición consolidada como el mayor evento nacional del sector.

Reunimos en un mismo entorno excelentes oportunidades de negocio para las empresas, además de experiencias y mucho conocimiento compartido por grandes nombres del panorama nacional e internacional. Además, el evento es un importante espacio de fortalecimiento del sector que impacta la economía, estimula el deporte, valora la cultura y promueve la inclusión", declara el director general de SHOT FAIR BRASIL, Mauro Braga.

Productos y servicios

En SHOT FAIR BRASIL 2023, los visitantes encontrarán una amplia variedad de productos y servicios que incluyen todo tipo de equipos y utensilios tácticos, armas, municiones, cuchillería, cajas fuertes, maletines y estuches, ropa, coleccionables, relojes, accesorios, entre otros.

Como novedad este año, el público encontrará

empresas especializadas en paquetes turísticos de aventura, con itinerarios de caza, además de venta de vehículos especiales como remolques todoterreno.

Para los practicantes de tiro deportivo, además de conocer importantes clubes de tiro de la región, el visitante también podrá vivir momentos de adrenalina y diversión en una cancha de aire suave sin precedentes.

Entre los expositores se encuentran marcas como Mahrte, ASC Guns, Beretta, Springfield Armony Brasil, CBC, Taurus, Detectores Brasil y SOSSul Defender.

También estarán presentes 3Gun Nation, Acero Botas, ADSUMUS Individual Tactical Equipment, Alvos Brasil, Brazilian Savannah Store, Campos Cases, Citerol Uniformes e Ação, Clube Ferrolho de Tiro, Cutelaria Origens, Feasso Brasil, Fire – Sistema de Gestión de Clubes de Tiro, InfiRay Outdoor, Lugano Gramado, Millenium Editora, Rossi Airguns Airsoft, Sociedade Desportiva e Cultural Cruzeiro Joinvillense, Rústico Viajante Adventure, entre otros.

Embajadores

En 2023, la SHOT FAIR BRASIL tiene como misión mantener unida la familia del tiro deportivo, con integración entre empresas, importadores, marcas, instructores, clubes de tiro, coleccionistas, atletas y aficionados.

Para representar a estos públicos, el evento tiene como embajadores al campeón olímpico de tiro, Felipe Wu, ya la atleta, instructora y coleccionista de armas, Aline Kanyo.

Este año, el equipo de embajadores se reforzó al homenajear al tirador deportivo e instructor Richarlles Ghabriel, quien nació sin brazos y, con la motivación de familiares y amigos, aprendió a disparar con los pies; y Celso Cavallini, personalidad del mundo táctico y outdoor, que se ha desempeñado como reportero de aventuras y juegos extremos en los principales canales de televisión.

Día del comerciante

Para ofrecer a los comerciantes la oportunidad de conocer productos y lanzamientos directamente de los fabricantes y representantes, el primer día de SHOT FAIR BRAZIL 2023 (8/2) estará dedicado exclusivamente a este público.

El horario de la mañana, de 10:00 a 12:00 horas, estará reservado para el Seminario para Inquilinos, impartido por el Comandante Diógenes Lucca, que compara Tropas de Élite con empresas de alto rendimiento. La visita a la feria estará

abierta a los comerciantes de 13:00 a 20:00 horas.

Personalidades y capacidades internacionales

La formación también tendrá un espacio especial en SHOT FAIR BRASIL 2023, con un variado programa de conferencias, paneles y clínicas, impartidas por importantes nombres como el norteamericano John Lott Jr., referente en la defensa del uso de armas en el Estados Unidos; la presidenta del Movimento Viva Brasil, especialista en seguridad, armas y municiones, Bene Barbosa; y, por primera vez en el evento, Fabrício Rebelo, jurista, investigador libre en seguridad pública, periodista y escritor.

Uno de los destaques de la grilla de entrenamiento de la SHOT FAIR BRAZIL 2023 será el 1º Simposio de Comercio Exterior de Productos Controlados por el Ejército (PCE), con la participación de representantes de la Receita Federal, el Ejército, representantes del mercado y transitarios. El evento se lleva a cabo el 3 de agosto (jueves), de 10:00 a 12:00.

Entre los otros temas que estarán en la agenda del evento se encuentran el tiro como objetivo educativo, la caza reglamentada en Brasil, la mujer en el mundo del tiro, balística de combate, técnica de tiro, seguridad en las escuelas, armas, números y reglamentos, entre otros.

Venta de boletos

Las entradas para SHOT FAIR BRAZIL 2023 ya se pueden comprar en el sitio web del evento, www.shotfairbrasil.com.br , donde también está disponible la programación completa de conferencias, paneles y clínicas.

Apoyo y realizacion

SHOT FAIR BRASIL 2023 es máster patrocinado por Mahrte (Cuota de presentación); ASC Guns, Beretta, Springfield Armony Brasil, CBC y Taurus (cuota .50 BMG); Detectores Brasil y SOSSul Defender (calibre 5.56 cuota).

Alianza institucional de la Confederación Brasileña de Tiro Práctico, Confederación Brasileña de Tiro Deportivo (CBTE), Asociación CAC Brasil, Asociación Brasileña de Propietarios de Armas de Fuego, Asociación Brasileña de Importadores de Armas y Material Bélico (ABIAMB), Asociación Nacional de la Industria de Armas y Municiones (Aniam), Liga Nacional de Tiro de Defensa Táctica (Liga Nacional TDT), Federación Deportiva de Tiro y Caza de Santa Catarina y Liga Nacional de Tiro al plato. El evento es organizado por Planeventos Eventos Corporativos.

El tráfico de cocaína hacia europa: la batalla por los contenedores y la guerra por los puertos

El tráfico de cocaína y la subsecuente delincuencia organizada es considerada como la única transnacional latinoamericana exitosa que se ha expandido en el mercado mundial tan igual que la transnacional estadounidense de la Coca Cola.

En efecto, el comercio de cocaína ha experimentado un auge inesperado en los últimos años, impulsado por el aumento de la producción.

Ya el 2018 la Global Initiative Against the Transnational Organized Crime, un foro suizo conformado por más de 600 redes de expertos en política criminal internacional, destinado al intercambio de conocimientos y experiencias contra el crimen organizado internacional y orientado a fortalecer las respuestas globales frente a los desafíos de la criminalidad global, podía constatar, como obra en sus informes, que la producción combinada de Colombia, Bolivia y Perú -los tres principales productores de cocaína y países miembros del denominado "triángulo blanco" y exportadores del denominado "oro blanco"- fue más del doble que en 2013, aunque el crecimiento se ha ralentizado recientemente, producto de la pandemia, todavía no hay indicios de que esté alcanzando su punto máximo.

La repercusión de este fenómeno se ha centrado en Estados Unidos y su aparentemente interminable "guerra contra las drogas", sin embargo, hace tiempo que los traficantes inteligentes prefieren Europa, donde hay más potencial de crecimiento que en el mercado estadounidense, ya que es más desarrollado y se obtienen mayores beneficios.

Los mercados de cocaína en Estados Unidos y Europa

En los primeros meses de 2020, Global Initiative Against the Transnational Organized Crime, calculaba que el flujo de droga que entraba o pasaba por Europa se situaba entre 500 y 800 toneladas, de las cuales, solo se han incautado entre el 10 y el 20% del volumen total". Un porcentaje significativo de este flujo está en tránsito hacia otras partes del mundo, los traficantes transportan la droga desde los mercados establecidos de Europa Occidental hasta Rusia y Asia, abasteciendo a todos los países intermedios.

Estados Unidos ha desplegado ingentes recursos en América Latina para combatir el narcotráfico: un ejército de agentes de la Administración para el Control de Drogas (DEA) está sobre el terreno, mientras que otras agencias como el Departamento de Seguridad Nacional y el Servicio de Inmigración y Control de Aduanas de Estados Unidos, así como el Comando Sur del ejército estadounidense, contribuyen a la lucha. En cambio, la presencia y la capacidad europeas en la fase previa son mínimas. Europa sólo ha desplegado un número limitado de agregados policiales u oficiales de enlace en América Latina y cuenta con pocas unidades navales en el Caribe.

A diferencia de Estados Unidos, los problemas de la cocaína en Europa parecen remotos. Europa no sufre el nivel de violencia que padece América Latina, ni la corrupción sistémica que predomina en muchos países latinoamericanos y caribeños.

Mientras Europa luchaba contra la pandemia del coronavirus, la recesión económica, el terrorismo islámico, las tensiones internas y la inmigración irregular, el tráfico de cocaína había quedado muy relegado en la lista de prioridades de los gobiernos del Viejo Continente.

Sin embargo, Europa no está exenta de los daños colaterales del tráfico de cocaína y de los efectos distorsionadores sobre la economía de los miles de millones de euros procedentes de la droga que circulan por los bancos y las economías locales.

En la mayoría de los países europeos se producen también actos violentos relacionados con la droga, existen numerosos ejemplos de corrupción de policías, funcionarios de aduanas y personal de puertos y aeropuertos por parte de organiza-

ciones de narcotraficantes y, lo que es quizá más preocupante, existen pruebas convincentes del fortalecimiento de las mafias europeas gracias a los beneficios generados por el tráfico de cocaína.

La historia del ascenso de la Ndrangheta en Italia y, en todo el mundo, por ejemplo, está estrechamente relacionada con el tráfico de cocaína, mientras que la expansión del poder de las mafias balcánicas también está vinculada a la cocaína. La amenaza que suponen estas estructuras delictivas para la seguridad nacional es clara y creciente. Los daños causados por el tráfico de cocaína en América Latina y el Caribe también deberían preocupar mucho a Europa. Muchos estados europeos tienen antiguas colonias en la región y territorios de ultramar en el Caribe. El desarrollo del régimen venezolano, cada vez más dictatorial y criminal, significa que muchos países europeos con presencia en el Caribe tienen ahora un socio que exporta cocaína y delincuencia, así como emigrantes que huyen del colapso del estado y de una inflación galopante.

El tráfico de cocaína hacia Europa

Para los traficantes, existe una barrera inevitable para el transporte de drogas a Europa, a diferencia de Estados Unidos, no hay puente terrestre, por lo que los traficantes tienen que utilizar rutas marítimas o aéreas. En los últimos diez años han optado en gran medida por las rutas marítimas, concentrándose principalmente en el tráfico de contenedores. Ello ha generado que surja un complejo juego del escondite, ya que los traficantes utilizan diversos métodos para ocultar la cocaína en los millones de contenedores que entran en Europa cada año.

Los narco submarinos

Existen otras formas de introducir cocaína en Europa, a fines de 2019, las autoridades españolas incautaron de un narco submarino que había cruzado el Atlántico con tres toneladas de cocaína, por valor de hasta 100 millones de euros, aunque la policía española cree que este tipo de embarcaciones se utilizan desde hace años, era la primera que se encontraba en aguas europeas, por eso las autoridades hoy en día, prestan especial atención a los contenedores procedentes directamente de países productores de cocaína (Perú y Colombia). En virtud de que la policía y las aduanas europeas están perfeccionando su accionar en el control y vigilancia en los aeropuertos y zonas fronterizas, los traficantes utilizan cada vez más trucos para colar droga entre mercancías legítimas sin que los propietarios sepan que hay cargamentos de cocaína en los contenedores.

Vuelos comerciales, vuelos charter y buques de vela

Aunque las principales rutas para el transporte de cocaína a Europa son los vuelos comerciales, existen casos de vuelos chárter que vuelan directamente de América Latina a Europa transportando grandes cantidades de cocaína.

Los buques de vela también son más fáciles de navegar y controlar, y con el aumento del tráfico entre el Caribe y Europa, esta es una forma cada vez más popular de transportar grandes cargamentos de cocaína. España siempre ha sido el hogar natural de los narcotraficantes latinoamericanos por sus vínculos lingüísticos y culturales, y gracias a una alianza con narcotraficantes gallegos, España se convirtió en la principal puerta de entrada de la cocaína en Europa a finales de la década de 1880.

España, sin embargo, se ha visto eclipsada por Bélgica y los Países Bajos, la eficacia de los mega puertos de Hamburgo en Alemania, Antwerpen en Bélgica y Rotterdam en Holanda, que combinada con la excelente infraestructura de transporte, pudiendo enviar un contenedor a casi cualquier lugar de Europa, ha atraído a los narcotraficantes. El número de incautaciones en esta ruta ha fluctuado en los últimos 20 años, pero hay indicios de que podría estar aumentando de nuevo.

Presencia de mafias europeas en América Latina

Mientras los delincuentes latinoamericanos se desplazaban hacia Europa para vender su producto, algunos mafiosos europeos empezaron a desplazarse hasta Latinoamérica para estar más cerca de las fuentes de producción y conseguir así mejores precios por la cocaína.

Como era de esperar, fue la mafia italiana la que allanó el camino hacia la cima, asegurándose cocaína barata en Colombia y estableciendo una

presencia permanente en América Latina en la década de 1990. Comprando la mercancía en el lugar de origen en Colombia y organizando el transporte de vuelta a Europa, los italianos pudieron recaudar ellos mismos la mayor parte de los enormes beneficios..

Otras mafias europeas empezaron pronto a imitar este modelo, que se utiliza cada vez más en la actualidad, sin embargo, es engañoso pensar sólo en mafias nacionales en el panorama delictivo actual, hoy en día, el tráfico de cocaína lo llevan a cabo diversos grupos delictivos, compuestos por muchas nacionalidades diferentes. Ya no existen estructuras criminales como el cártel de Medellín, que controlaba la producción de cocaína en Colombia y vendía su droga en las calles de Miami y Nueva York. Las redes delictivas dependen ahora de la subcontratación de gran parte del trabajo a diversos especialistas en transporte, asesinos a sueldo, centros de corrupción y blanqueo de dinero, agentes jurídicos como abogados, contables y banqueros.

El transporte de contenedores y el juego del escondite con la cocaína

El carguero MSC Gayane atracó en el puerto de Filadelfia el 17 de junio de 2019. En lugar de dirigirse a su destino previsto -los Países Bajos- fue abordado por agentes federales que utilizaron rayos X, perros rastreadores y prismáticos para examinar los miles de contenedores de los barcos.

En siete de ellos encontraron un total de 20 toneladas de cocaína. Fue una de las mayores incautaciones de la historia de EE.UU., pero la historia del MSC Gayane dice mucho más sobre el destino del barco, Europa, a través de los Estados Unidos. Ello demuestra que el tráfico de contenedores ha alcanzado tales proporciones que los traficantes se sienten seguros enviando cargamentos multimillonarios de cocaína a Europa, además, muestra el constante desarrollo delictivo de lo que hoy es la forma más importante de tráfico con Europa.

El método "drop off" y el uso de las "rutas frías"

La Fiscalía de EE.UU. cree que los narcotraficantes que estaban detrás del envío de MSC Gayane utilizaron un método que las autoridades denominan "drop off", que consiste en que el remitente deja el paquete en uno de los puntos de conveniencia y el destinatario lo recoge en otros puntos de conveniencia. Los atestados judiciales mostraron que dos de los seis tripulantes detenidos confesaron haber aceptado 50.000 euros para subir rocas de cocaína a bordo desde 14 embarcaciones más pequeñas que se acercaron al carguero desde la costa peruana durante la noche.

Los agentes antinarcóticos peruanos creen que la operación fue un ejemplo de otra táctica del narcotráfico, el uso de "rutas frías", puertos con vínculos poco conocidos con el narcotráfico que ofrecen una seguridad mínima y hacen saltar pocas alarmas. Los investigadores creen que al menos una parte de la cocaína se cargó en Chile, un país que rara vez se menciona en relación con el tráfico transatlántico de cocaína, en cualquier caso, el cargamento del MSC Gayane fue producto del constante juego del escondite entre los narcotraficantes y las fuerzas del orden, en el que los traficantes buscan constantemente nuevos métodos y rutas para adelantarse a las autoridades.

El cambio a los contenedores: una respuesta a las medidas de seguridad

Durante el auge de la cocaína en la década de 1980, los cárteles colombianos preferían utilizar avionetas para llegar a Estados Unidos, sobrevolando el Caribe.

En los primeros tiempos del comercio transatlántico de cocaína, los traficantes enviaban pequeñas cantidades de cocaína a Europa a través de correos aéreos comerciales o mulas.

Los grandes cargamentos de cocaína solían dejarse en buques nodriza, normalmente pesqueros, que eran recibidos en alta mar por lanchas rápidas que llevaban la droga a tierra -una técnica perfeccionada por los contrabandistas de cocaína gallegos (los denominados "narco-gallegos")-. En los últimos diez años, el transporte marítimo en contenedores se ha convertido en la forma más habitual de tráfico de drogas hacia Europa.

Cada año se embarcan 750 millones de contenedores en todo el mundo, pero menos del 2% de ellos son inspeccionados, esto brinda a los traficantes la oportunidad perfecta para llegar a los mercados mundiales. El reto consiste en camuflar los grandes cargamentos de cocaína para minimizar el riesgo de incautación y maximizar al mismo tiempo los beneficios. El transporte de cocaína en contenedores ya fue introducido por la mafia italiana en la década de 1990.

Las incautaciones en Europa

Las cifras de incautaciones muestran un aumento espectacular de los contenedores en la primera década del milenio. Las incautaciones de cocaína en Europa aumentaron rápidamente: de 32 toneladas en 1998 a 121 toneladas en el 2006, los niveles de pureza y los precios en la calle en Europa se mantuvieron estables o aumentaron, el flujo de cocaína era ininterrumpido y los traficantes habían mejorado a la hora de eludir el control de las autoridades, mientras que la proporción de incautaciones realizadas por vía marítima en el 2006 había aumentado hasta el 75% en el 2012 y 2013. El cambio a los contenedores podría ser

Image by Alexander Bobrov from Pixabay

una respuesta a las medidas de seguridad o simplemente porque los narcotraficantes eran cada vez más conscientes de los peligros.

Encontrar droga en contenedores es como buscar una aguja en un pajar, las redes delictivas han explotado esta vulnerabilidad y es probable que sigan haciéndolo. A medida que Europa fue adquiriendo importancia en el mercado mundial, los contenedores se convirtieron en una ventaja, se produjo una reestructuración de la industria de la cocaína y se hizo más internacional

Intermediación en puertos y puntos de partida

Cuando las autoridades empezaron a reconocer la amenaza que suponía el tráfico de contenedores, prestaron mayor atención a las líneas marítimas más utilizadas para transportar cocaína, y desde qué países provenían.

Los puntos calientes tradicionales, como los puertos colombianos de Turbo, Santa Marta, Buenaventura y Cartagena y puerto del Callao en Perú, ofrecen proximidad a las zonas de producción, líneas marítimas activas hacia Europa y redes e infraestructuras delictivas sofisticadas y de larga tradición, sin embargo, los envíos procedentes de estos puertos son ahora rutinariamente marcados en rojo por las autoridades europeas y sometidos a protocolos de seguridad reforzados para escapar del creciente riesgo de persecución, los traficantes han emigrado a otros puertos de la región, como Ecuador, Costa Rica, Panamá, la República Dominicana, Paraguay y, sobre todo, Brasil.

Las conexiones directas de Brasil con las zonas de producción de Colombia, Perú y Bolivia, los numerosos puertos de contenedores de la costa atlántica y el rápido desarrollo de la delincuencia organizada hacen de Brasil un destino tentador para los narcotraficantes que buscan nuevas rutas hacia Europa. El puerto de Santos se convirtió en un punto caliente, al que siguieron otros como Paranaguá e Itajaí. Según las aduanas brasileñas, las incautaciones pasaron de 4,5 toneladas a 66 toneladas en 2019, este éxodo continúa en la actualidad, con indicios de que los traficantes están recurriendo a puertos con historiales comerciales relativamente limpios, que están mal preparados para frenar el flujo de cocaína, como Argentina, Uruguay y Chile.

Otra opción son los desvíos a través de África Occidental, que experimentaron un auge en la primera década del nuevo milenio a medida que los beneficios de la cocaína alimentaban la corrupción y desestabilizaban profundamente a los gobiernos locales. Aunque esta ruta ha sido intervenida en repetidas ocasiones a lo largo de los años, una serie de incautaciones en 2019 sugiere que los informes sobre su declive pueden ser exagerados y que sigue siendo una buena opción para los traficantes transatlánticos de cocaína.

Un modus operandi en constante cambio

El mismo patrón puede observarse en el modus operandi de los narcotraficantes: A medida que las autoridades introducían nuevas medidas de seguridad, los narcotraficantes respondían cambiando y mejorando sus métodos.

Los primeros partidarios del tráfico de contenedores se inclinaron por una estrategia que las autoridades denominan "dentro de la carga", en la que la cocaína se camufla en exportaciones cotidianas, esta técnica exige que los traficantes operen con empresas tapadera, que ellos mismos crean o compran para que actúen como propietarios de empresas que llevan mucho tiempo exportando droga.

Luego ocultan la cocaína en sus exportaciones aparentemente legales, en la mayoría de los casos, los ladrillos de cocaína se introducen simplemente en cajas de carga, pero en otros, los traficantes han utilizado desde piñas huecas hasta barriles de sustancias químicas peligrosas, e incluso han alterado químicamente la cocaína para disfrazarla de productos como alimentos para animales o fertilizantes.

Lucha por los contenedores y el contenedor inteligente

El tráfico de contenedores, es ahora una prioridad para las autoridades de ambos lados del Atlántico en la lucha contra la droga. Tanto en el sector público como en el privado, algunos recurren a contenedores inteligentes que recogen y transmiten datos sobre la ubicación del contenedor, las fluctuaciones de temperatura y otros signos de manipulación, o a equipos aduaneros electrónicos que transmiten información en tiempo real sobre el movimiento del contenedor. Los contenedores inteligentes son desproporcionadamente caros y complicados de construir o instalar, además, pueden perder su señal en el mar, lo que da a los narcotraficantes la oportunidad de manipular los contenedores.

Se pueden encontrar soluciones más fundamentadas en la cooperación multinacional y en iniciativas como el "Programa de Control de Contenedores", una iniciativa conjunta de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDC) y la Organización Mundial de Aduanas. El programa ha aumentado la capacidad de seguridad y ha creado redes de cooperación internacional tanto en puertos latinoamericanos como europeos, y ha contribuido directamente a un aumento de las incautaciones y de las operaciones que han llevado ante la justicia a importantes

narcotraficantes. Sin embargo, a pesar de estos esfuerzos, es poco probable que las autoridades lleguen a interceptar el tráfico de contenedores. Es imposible controlar ni siquiera una fracción de los cientos o millones de contenedores que se transportan por todo el mundo.

La guerra por los puertos

La importancia de los contenedores ha cambiado la naturaleza del narcotráfico en América Latina, ha transformado las ciudades portuarias, donde antes había poca delincuencia organizada, en asentamientos delictivos apetecibles, lo que ha provocado luchas por el dominio y el fortalecimiento de los sindicatos delictivos locales.

El tráfico de cocaína a través de los puertos ha convertido a bandas callejeras como las panameñas "Calor Calor" y "Bagdad" en importantes actores criminales, y las ya poderosas bandas carcelarias de Brasil han evolucionado hasta convertirse en importantes narcotraficantes cuyos líderes negocian acuerdos transfronterizos.

En el puerto del Callao en Perú, la campaña de "Barrio King" para establecer el monopolio del tráfico de drogas a través del puerto no sólo dio lugar a la violencia entre bandas, sino también a un brutal exterminio de los vendedores que se resistieron a su control.

Autor: Javier Gamero Kinosita

SSeguridad y ZKTeco
firmaron un importante acuerdo de cooperación mutua

Confianza y profesionalismo son dos conceptos que caracterizan a SSeguridad, empresa con más de 25 años de experiencia en soluciones de seguridad privada y seguridad tecnológica y que cuenta con un equipo multidisciplinario de profesionales que, por medio de un trabajo conjunto, tienen como misión entregar a sus clientes un servicio de alta calidad y competitividad dentro de las exigencias del mercado, destacando el monitoreo de instalaciones a distancia, la caseta de seguridad inteligente, guardias con amplia experiencia, los servicios de Hogar Seguro y cualquier alternativa que involucre soluciones creativas y tecnológicas.

Durante estos días se concretó uno de los acuerdos de cooperación más esperados ya que SSeguridad unió fuerzas con ZKTeco para dar paso a un importante escalón en las alianzas estratégicas que la filial chilena del gigante asiático en materia de seguridad viene haciendo hace un tiempo.

Carlo Seves, Gerente Comercial y Marketing de SSeguridad, Gustavo Maluenda, CEO ZKTeco Chile, Juan Marchini Barthelmess, Gerente General Corporativo y Francisco Venegas Gerente de Tecnología y Ciberseguridad de SSeguridad

"Acá las partes acuerdan promover el crecimiento y desarrollo conjunto. Agradecemos a ZKTeco Chile por esta nueva muestra de confianza en nuestro trabajo. De nuestra parte seguiremos entregando, una vez más, la mejor calidad y profesionalismo en nuestro trabajo. Este nuevo acuerdo viene con nuevas funciones y desafíos, las que pronto daremos a conocer" cuentan desde SSeguridad.

Mientras que Gustavo Maluenda, CEO de ZKTeco Chile, cuenta que "esta alianza refuerza lo que es nuestra labor hacia el mercado y lograr la profesionalización del mismo, el foco de nuestra empresa es potenciarnos con quienes quieren dar soluciones reales al tema de la seguridad en nuestro país.

Nosotros hemos estado a la vanguardia de las soluciones biométricas y hemos incorporado estas a sistemas de; control de acceso, video vigilancia CCTV, sistemas de control de asistencia, sistemas IoT y de ciudades seguras, todo dentro del contexto de seguridad electrónica, pero siempre queremos potenciarnos con quienes llevan décadas en nuestro país".

Este convenio fue suscrito por Gustavo Maluenda, CEO de ZKTeco Chile y Juan Marchini Barthelmess, Gerente General Corporativo de SSeguridad

SHOT FAIR BRASIL 2-5 de Agosto 2023, Joinville, Brasil

El evento, el más grande de América Latina, se ha convertido en una referencia en el segmento de tiro deportivo, con el éxito en el cierre de negocios que se convirtieron en millones de reales, como las ediciones de 2021 y 2022. SHOT FAIR BRASIL también se ha convertido en un espacio único para el lanzamiento de productos . , dando una visibilidad sin precedentes a los sectores implicados.

En 2023, la SHOT FAIR BRASIL tiene como misión mantener unida la familia del tiro deportivo, con integración entre minoristas, importadores, marcas, atletas, instructores y clubes de tiro.

En la tercera edición, el público encontrará una oferta más amplia de expositores, superando el número de ediciones anteriores, además de consolidar el intercambio de conocimientos, con charlas, talleres y jornadas. Una de las novedades para 2023 es el Simposio Comex con el intercambio de información sobre la importación de PCE – productos controlados por el Ejército.

SECURITY EXIBITION 30 Agosto - 1 Sept. 2023 Sidney Australia

Durante más de tres décadas, Security Exhibition & Conference ha sido el evento comercial más establecido y respetado para la industria de la seguridad en Australia, reuniendo a todo el espectro de fabricantes, distribuidores, profesionales de la seguridad y usuarios finales para conectarse y crear oportunidades rentables.

La Exposición y Conferencia de Seguridad se encuentra en el epicentro de la seguridad como los únicos tres días del año en los que la industria despeja su calendario para reunirse. Más de 8500 visitantes y expositores convergen para buscar, negociar, trabajar en red y aprender en el entorno comercial más cautivo rodeado por el mejor escaparate de soluciones y productos innovadores de la región.

DANISH SECURITY FAIR 30 - 31 AGOSTO 2023, Dinamarca

La gran feria comercial de Dinamarca, que presenta las últimas tecnologías en productos y sistemas electrónicos y mecánicos; asegurar y salvaguardar personas, edificios y áreas.

Danish Security Fair tiene como objetivo marcar una diferencia positiva para las partes interesadas de la industria de la seguridad; tanto expositores como visitantes. Los contactos de calidad y el comercio son una calle de doble sentido, el diálogo y la creación de redes profesionales son los cimientos sobre los que se construye el crecimiento común.

Danish Security Fair es el foro donde la industria y otras partes interesadas pueden conocer nuevos clientes y contactos. La feria se centra en los negocios y los resultados, creando valor para todas las partes interesadas de la industria de seguridad danesa. La feria es un foro donde expositores y visitantes pueden establecer relaciones personales en una industria cada vez más digital.

BLACK HAT 5 - 10 DE AGOSTO Mandalay Bay Las Vegas

Ahora en su vigésimo sexto año , Black Hat USA regresa al Centro de Convenciones Mandalay Bay en Las Vegas con un programa de 6 días.

El evento comenzará con cuatro días de Capacitaciones especializadas en ciberseguridad (del 5 al 10 de agosto), con cursos para todos los niveles. La conferencia principal de dos días (del 9 al 10 de agosto) contará con más de 100 sesiones informativas seleccionadas, docenas de demostraciones de herramientas de código abierto en el Arsenal, un sólido Business Hall, eventos sociales y de redes, y mucho más.

Este año, Black Hat está lanzando el programa 'Certified Pentester': un examen práctico de día completo que cubre temas de pentesting. Consulte los aspectos más destacados de la conferencia a continuación para obtener más detalles.

MÁXIMOS REFERENTES EN ARMAMENTO NO LETAL

BULL SERVICE

* Disuasión efectiva dentro del marco legal
* No afecto a ley de Armas

DEFENSA DEL HOGAR

POLICIAS

INDUSTRIA DE LA SEGURIDAD

BLINDAJE AUTOMOTRIZ CUSTOMIZADO

SATISFACCIÓN 100% GARANTIZADA

www.bullservice.cl
+56 9 4623 8380 / +56 9 9909 1958

@bullservicechile @bull.service

Sé parte de la Gran Feria de Seguridad Integral de Chile

7-8-9 NOV. 2023
Metropolitan Santiago

SEGURIDADEXPO
by Fisa | CHILE

EJES TEMÁTICOS:

- Seguridad Pública y Privada
- Cyberseguridad
- Control Fronterizo
- Macrozona Sur

¡Hablemos! Y asegura tu participación

info@seguridadexpo.cl *+56 9 4481 6922*

GL events

@seguridadexpo

www.seguridadexpo.cl

ORGANIZA Y PRODUCE

Fisa
GL events Group