Año 7 Nº 48 Septiembre-Octubre de 2023

Revista SEGURIDAD .Online
& DEFENSA
LA PRINCIPAL PLATAFORMA DE INFORMACIÓN DE SEGURIDAD EN LATINOAMÉRICA

REALIDAD VIRTUAL
Su influencia en la capacitación en seguridad

REPORTAJE ESPECIAL
Las nuevas tendencias que se exhiben en SeguridadEXPO

SeguridadExpo 2023
Anticipándonos al futuro

SEGURIDADEXPO
by Fisa | CHILE

07 - 09 de Noviembre 2023
Metropolitan Santiago
Santiago - Chile

STAND 320

Ven a conocer nuestras novedades

digifort

ZKTeco

SOLUCIONES AVANZADAS DE SEGURIDAD

GESTIÓN DE VIDEO Y CONTROL DE ACCESO: 100% INTEGRADO

www.digifort.com www.zkteco.cl

EDITORIAL

Nº48 Septiembre - Octubre de 2023

En la víspera de una nueva edición de Seguridad Expo, es importante referirnos a la creciente relevancia de la incorporación tecnológica en materia de seguridad, la cual ya no solo se limita a soluciones para el área del monitoreo sino que además se amplía hacia áreas como la seguridad pública, ya sea mediante la incorporación de dispositivos de retención remota, sistemas de capacitación basados en el uso de realidad virtual, llegando incluso a avanzados software para predecir delitos e incivilidades.

Como sociedad debemos avanzar decididamente en la incorporación de este tipo de soluciones las que en definitiva permiten ampliar el acceso de mayores segmentos de la comunidad a mejores niveles de seguridad.

Resulta de gran importancia reiterar el llamado para que las nuevas políticas en materia de seguridad privada incorporen las nuevas tecnologías como una forma efectiva de proyectar a esta importante actividad hacia mayores estándares de eficiencia, servicio y accontability.

Robert Gutter Boim
Director

CONTENIDO

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

AÑO 7 N° 48 Edición Septiembre Octubre 2023

Revista Seguridad Online es una edición de Producciones Gótica Ltda.

Revista Seguridad Online
Director: Robert Gutter Boim
Dirección Creativa: Gótica Ltda
Ventas de Publicidad: +56 9 98246696
revistaseguridadonline@gmail.com ventas@revistaseguridad.cl

Rodrigo Lobo

Gerente General Adjunto FISA

Seguridad Expo se ha consolidado y anuncia una próxima versión para 2024

Seguridad Expo sin duda es una muestra consolidada y un referente en materia de seguridad. A días del comienzo de una nueva versión, Revista Seguridad conversó con Rodrigo Lobo, Gerente general adjunto de FISA, entidad que organiza este importante evento.

¿Cuáles son las principales novedades que se presentarán en esta nueva edición de seguridad Expo 2023?

Las principales novedades que tenemos en la feria hoy día van relacionadas a la tecnología en toda su gama. Es un rango amplio, pero en el fondo va desde el uso y la aplicación de tecnología del equipamiento más básico -como botas, chalecos, cascos, lentes-, hasta aplicaciones biométricas, uso de cámaras, drones y sobre todo la administración de la información, entendiendo que la información es la imagen o los datos de telemetría que se generan. Yo creo que la principal novedad hoy es la tecnología y su integración en distintas dimensiones.

El organizar un evento en materia de seguridad implica un enorme desafío y a la vez una gran responsabilidad en consideración al nivel de relevancia del tema a nivel país ¿Cómo asume Fisa en su calidad de organizador esta responsabilidad?

La tomamos con mucha humildad y con un gran desafío que abordamos estableciendo relaciones con todas las instituciones que están involucradas con la seguridad a nivel país. Hablamos de instituciones gubernamentales, fuerzas armadas, orden y seguridad, asociaciones gremiales y proveedores. Todos estos actores son claves en una industria que crece a pasos agigantados, sobre todo considerando el actual contexto político y social que vive la región. Y, efectivamente, tenemos la convicción de que somos capaces de convocar en un solo espacio a los principales actores de la industria.

Sin duda cada día la tecnología asume un rol más relevante en materia de seguridad. ¿Qué nos puede comentar en relación a la muestra tecnológica de esta edición?

La tecnología sin duda es lo más importante, pero más que la tecnología yo volvería a insistir en que las prestaciones de cada producto año a año se superan. Los drones cada vez van a volar más alto y por más tiempo, las cámaras van a tener una mejor nitidez, y las cámaras corporales cada día son más pequeñas e inviolables, lo que hace que no puedas sacarle información ni romperlas. Pero un tema central es cómo todo eso mediante data science, se reúne desde una matriz y se administra; eso es hoy día un tremendo salto. El plan piloto que implantó la Municipalidad de Ñuñoa donde a partir del uso de tablets están conectados a su señal, y permiten tener una integración de la información y control móvil en tiempo real, es un gran ejemplo práctico y de uso en terreno. Yo creo que la integración a través del uso de tecnología de primer nivel y el cruce de ésta, configuran un tema relevante.

Debido a la relevancia del tema seguridad, ¿se prevé que a futuro esta muestra llegue a tener un carácter anual?

Sí, el próximo año se vuelve a realizar Seguridad Expo. Estamos consolidando esta feria y gracias a la gran recepción de todos los actores, sin duda nos hemos transformado en el principal punto de encuentro a nivel país.

Probablemente la mayor innovación en materia de seguridad pública de la última década la constituye el desarrollo del sistema de retención remota Bola Wrap, actualmente en uso por Carabineros de Chile y el cual fue exhibido por primera vez en Chile en la pasada edición de Seguridad Expo 2021. ¿Contaremos este año con la presencia de dicha empresa y con demostraciones en vivo?

Absolutamente, es un expositor de nosotros, y en Seguridad Expo estamos muy contentos de tener esta empresa líder en las armas no letales. Esperamos que puedan hacer demostraciones de su producto y lograr cerrar muchos acuerdos comerciales, con las diferentes instituciones que puedan utilizarlas.

¿Existe una estimación con respecto a la cantidad de empresas que participarán de esta edición de Seguridad Expo?

Vamos a tener más de 80 empresas presentes en la feria participando in situ, pero lo que es importante destacar es que cada empresa que participa representa a un número desde dos, hasta siete u ocho marcas. Esa particularidad multiplica de manera exponencial la cantidad de marcas de empresas que están participando en la feria.

¿Contaremos en esta oportunidad con demostraciones de equipamiento en seguridad?

Por supuesto, tendremos presentaciones de drones y demostraciones de armas no letales. Y si bien el nuevo layout ferial que tenemos en Seguridad Expo, está pensado para su desarrollo en nuestro de centro de convención Metropolitan Santiago, que será la sede del encuentro, la zona de demostración es un aspecto ya tradicional que convoca a muchas personas.

GTS

Referente en capacitación mediante realidad virtual se presenta en Chile.

Traer a chile las últimas tecnologías en materia de seguridad es parte del compromiso de Revista Seguridad. Ya en la edición 2022 de Seguridad Expo presentamos al mercado chileno el sistema de retención remota Bola Wrap, el cual ya ha sido incorporado por Carabineros de Chile. Para esta versión 2023 y gracias a las gestiones de la empresa nipona Nichiei International , presentaremos en Seguridad Expo a los principales exponentes en materia de capacitación mediante realidad virtual, entre los cuales se encuentra GTS (Gun Tactical Simulation), cuyos productos detalllamos en la presente crónica.

¿Qué nos puede comentar sobre la evolución de los sistemas de formación policial basados en la simulación básica y cuándo se empiezan a implantar los sistemas basados en la realidad virtual?

Los sistemas de simulación de realidad virtual para uso militar se han desarrollado y probado durante más de 15 años. En dicho momento, eran muy caros y de mala calidad, pero la realidad virtual ha esperimentado un gran avance en áreas en las cuales el movimiento humano, las habilidades manuales y motoras, y la inmersión, son esenciales.

Los avances tecnológicos han hecho posible que la tecnología esté disponible, no sólo para los militares de gran presupuesto, sino también para la policía. En eso estamos trabajando.

Los oficiales de policía pueden encontrarse con situaciones que son peligrosas, que ponen en peligro la vida, y necesitan emplear sus habilidades de toma de decisiones rápidas y buenas, habilidades tácticas y tomar acciones legítimas regulares, tal vez con el uso de equipos de aplicación como teaser, envoltura o pistola.
Fuimos los primeros en adoptarlo, y nuestro simulador incorpora 4 años de investigación académica y más de 7 años de experiencia en el desarrollo de simulaciones de realidad virtual.

La tecnología, incluyendo el software y el hardware, determina para qué herramientas de simulación se pueden utilizar. Las capacidades tecnológicas deben determinar exactamente qué se puede utilizar para la formación.

Ampliamos estos límites en la medida de lo posible con nuestras soluciones. El sistema está listo para ser utilizado en el mundo real, con gran utilidad y eficiencia, pero requiere algún tipo de integración con la organización que lo aplica.

¿Hasta qué punto el software u operador puede hacer una evaluación objetiva respecto al nivel de desempeño de la persona que se está formando o evaluando, y hasta qué punto la tecnología actual nos permite acceder a informes fiables y realmente predictivos?

Consideramos que la medición de datos es tan importante como la simulación realista. Debido a que GTS es una solución basada en software y microelectrónica, medimos y almacenamos cada gesto, lo que permite una evaluación integral.

Una funcionalidad básica es la reproducción de una sesión de entrenamiento, donde el instructor puede pausar, rebobinar, ralentizar los eventos en el espacio 3D, observados desde cualquier ángulo.

Esto es muy importante para la revisión posterior a la acción, ya que en una situación compleja la tarea puede ser analizada junto con el equipo después de la ejecución.

Todo a partir de los datos recopilados es evaluado digitalmente y procesado por el sistema de puntuación, que crea automáticamente puntuaciones y eventos de error basados en reglas personalizables. Es complejo, pero el punto es que al final creamos una sola puntuación y un registro para el instructor sobre los errores de los alumnos.

Este registro ayuda a los comentarios del instructor, y puede profundizar más en los detalles si lo desea. Adicionalmente decenas de parámetros y

reglas son la base de la evaluación automática, y creamos parámetros tácticos objetivamente medibles, como el tiempo de maniobra de fuego, el tiempo de reacción completa, etc. En la simulación de realidad virtual, se aplican las mismas normas de seguridad que en la realidad, por lo que también se comprueban automáticamente.

¿Qué tipos de armas se pueden incorporar para este tipo de prácticas?

Cualquier arma puede ser utilizada en una simulación, pero hay un proceso de desarrollo. Necesitas una réplica del arma, con controles que funcionen, por ejemplo, un airsoft o un arma desactivada. Luego tenemos que instalar la electrónica y, en base a nuestra experiencia, podemos producir en masa la llamada arma instrumentada.

Además, cualquier dispositivo electrónico con controles o equipos personales puede ser simulado con réplicas apropiadas, como una radio, una porra, un teaser. Ahora disponemos de armas instrumentadas Glock 17, M4 y CZ805 en funcionamiento.

¿Las sesiones de entrenamiento son individuales o pueden ser sesiones grupales?

Nuestro sistema es versátil. Desde el entrenamiento de un solo hombre, hasta los equipos de diez hombres, puede entrenar y probar. Los instructores pueden configurar varias sesiones de capacitación o examen para individuos o equipos, que se enfocan en una sola habilidad o una habilidad compleja que emplea práctica / prueba.

¿Qué nos puedes contar sobre el avance en la calidad de los gráficos que se observan actualmente en este tipo de simuladores, teniendo en cuenta que en el caso de otras áreas como la simulación aérea y los juegos, ya se alcanzan niveles de realismo impresionantes?

Los gráficos están en constante evolución. Es increíble lo que hemos logrado hoy en 3D. Yo diría: fotorrealista.

En comparación con los gráficos 3D en una pantalla plana (monitor), la realidad virtual es computacionalmente exigente, porque debe calcular casi la misma imagen dos veces para ambos ojos, 90 veces por segundo. No significa que los gráficos de la realidad virtual sean la mitad de buenos que en el monitor, pero hay una ligera disminución en la calidad. Está muy sobrecompensado por la visión espacial 3D y la inmersión, por lo que no decepcionará a nadie, todos nuestros usuarios dijeron que es una experiencia "wow".

Nuestro objetivo es mantenernos a la vanguardia, por lo que hemos diseñado el sistema para poder integrar las nuevas tecnologías a medida que surgen.

El nivel de realismo es clave en nuestro caso, al igual que la simulación aérea puede ser muy cercana a la vida real. En los simuladores de vuelo, la plataforma móvil puede ser un problema, mientras que en nuestra simulación táctica el tamaño del área utilizable. Podemosagregar fácilmente los nuevos elementos de hardware, por lo que a medida que obtenemos un casco de realidad virtual inalámbrico y liviano con resolución de ojos reales y campo de visión humano real, precisión

de color y nitidez, podemos comenzar a temer que podamos causar a alguien trastorno de estrés postraumático.

¿En qué consiste el sistema y equipamiento del sistema GTS y qué lo diferencia de otros sistemas?

El sistema GTS es de doble uso (militar y policial). Antes de empezar a desarrollarlo, realizamos mucha investigación y análisis científico. Colaboramos continuamente con entrenadores de tiro, entrenadores tácticos, veteranos de combate militar, expertos policiales, organizaciones antiterroristas y unidades de intervención.

También tenemos más contratos firmados y completados con la Universidad de la Administración Pública, que es el principal centro de formación de oficiales en Hungría.

Basándonos en la amplia experiencia que hemos comprendido que el formador y el aprendiz son igualmente importantes. Puedo enumerar extensamente las soluciones diferenciadoras que hemos implementado en base a nuestra investigación, pero sería demasiado largo.

El diablo está en los detalles, pero la conclusión es que hemos construido un sistema de capacitación y exámen adaptable y centrado en el estudiante que es eficiente y facilita el trabajo de los instructores. Además de esto, también queremos ayudar a los comandantes, con datos estadísticos de alta calidad.

Dado que somos dueños de todo el desarrollo, podemos adaptar el proceso de capacitación, las condiciones, las ubicaciones y el sistema de puntuación a las necesidades del cliente para que se ajusten al plan de capacitación. La implementación básica de GTS se puede separar en cuatro módulos:

-"Equipo personal ": estas son las cosas que se pueden usar y usar, como auriculares de realidad virtual, armas y herramientas instrumentadas, dispositivo de medición de pulso y chaleco háptico para detectar lesiones. Algunos de estos pueden ser opcionales, pero para los operadores de primer nivel, la ATF y los agentes especiales, la medición adicional y la inmersión podrían ser importantes.

-"Estación de simulación GTS": esta es la unidad de procesamiento principal para los aprendices, la simulación se ejecuta en este conjunto de dispositivos. Por lo general, es una computadora que se conecta al "Equipo personal" de forma inalámbrica. Para más usuarios, debe agregar más de estos dos conjuntos principales.

-"GTS Instructor Workstation - IWS": esta es la parte central del sistema. Solo se necesita uno incluso para las operaciones del equipo. Cubre los dispositivos de comunicación y presentación, como la televisión de pantalla grande, pero la parte más importante es la interfaz del instructor. Aquí pueden coordinar y medir la capacitación y hacer la revisión posterior a la acción.

-"Módulo Central de Datos y Comandante": aquí encontrará toda la información de entrenamiento y examen recopilada y analizada. Se trata de una solución de software opcional, distribuida e interconectada a la web que permite la formación adaptativa centrada en el estudiante para los alumnos y ofrece muchas opciones para los comandantes.

¿Cuáles son las principales áreas de clientes que demandan este tipo de formación y sistemas de formación?

El sistema fue diseñado para múltiples áreas desde el principio. En la investigación, definimos las partes comunes del entrenamiento táctico, principalmente en torno al desarrollo de habilidades relacionadas con las armas de fuego. Después de eso, construimos un enfoque en el que podemos separar el plan de entrenamiento y las características de las organizaciones armadas de, por ejemplo, Aduanas, Policía, Fuerzas Antiterroristas y Militares.

La mayoría de las experiencias son compartidas, pero el entorno legal, el entorno físico, las armas utilizadas y el protocolo pueden ser diferentes.

Tenemos una gran experiencia en el campo militar y antiterrorista, pero el sistema también es muy útil para practicar y enseñar tareas policiales cotidianas y de alto riesgo.

Chile enfrenta grandes dificultades para cumplir con niveles de entrenamiento adecuados (largas distancias de viaje, pocas prácticas, etc.) en qué medida la solución tecnológica GTS puede contribuir a resolver esta delicada situación.

En muchos países nos enfrentamos a las mismas dificultades, y podemos enviar la solución perfecta.

El sistema GTS permite a las organizaciones locales o nacionales mejorar y controlar sus capacidades de manera muy efectiva. Además de los muchos beneficios, las sinergias hacen de GTS un gran salto para sus usuarios, la organización puede decidir sobre la dirección de escalado.

para explicar en detalle este punto digamos que el escenario más simple, GTS puede preparar a los miembros del servicio para su entrenamiento de mantenimiento de nivel con fuego real para ahorrar tiempo y dinero para alcanzar los niveles adecuados. Estamos hablando anualmente de unos diez mil dólares de ahorro para cien personas. Este ahorro es solo para la práctica básica obligatoria de tiro, y proviene del tiempo y los gastos de viaje, la munición desperdiciada para la práctica y la seguridad del campo de tiro.

Todos sabemos que los conocimientos adquiridos en un campo de tiro "estéril" no son suficientes. Las situaciones inciertas, peligrosas, el miedo a tomar las medidas adecuadas, el estrés puede dar lugar a un estado mental en el que se pueden perder algunas habilidades cognitivas y manuales.

Podemos poner a los alumnos en una simulación inmersiva y realista en la que deben utilizar sus conocimientos combinados y demostrar su tolerancia al estrés. Bajo el fuego enemigo simulado, los aprendices tenían una frecuencia cardíaca elevada, los menos entrenados tenían regresión cognitiva, peor conciencia situacional e incluso perdieron algunas habilidades importantes que se habían practicado muchas veces antes, como cambiar rápidamente de revista. Después de que pudieron practicar en el simulador y aprendieron a manejar estos efectos, la mejora del rendimiento fue medible, pudieron controlar más y más aspectos de una situación compleja.

El entrenador, basándose en los datos recopilados previamente, puede configurar y modificar la complejidad de la situación para mejorar las habilidades cambiando el entorno, añadiendo distracciones, más sospechosos o civiles o su comportamiento aleatorio.

Los alumnos tienen una idea de una situación que pueden encontrar en la vida real y pueden aprender a manejarla gradualmente. Este conjunto de habilidades integradas no se puede probar exhaustivamente en sesiones de práctica, pero podemos configurar tareas que no se pueden practicar de ninguna otra forma.

Por último, nos gustaría que nos hablara de la trayectoria, de GTS y de los principales hitos y retos para el futuro.

Estamos trabajando junto con el ejército húngaro y el departamento de aplicación de la ley de la Universidad de Servicio Público de Budapest para mejorar el sistema e integrar sus solicitudes. Las características principales están hechas, vamos con la mejora continua, por lo que estamos trabajando en la última integración de hardware y más tipos de armas.

Los nuevos auriculares tendrán lentes más claras para la simulación, por lo que los clientes obtendrán gráficos más agradables y, además, incluiremos retroceso en las armas instrumentadas. El "Módulo Central de Datos y Comandante" está en desarrollo, vendrán muchas funciones, planeamos incluir más capacidades de IA pronto.

Mayores informaciones:

Csongor Hubay, director ejecutivo
de Infinit Simulation Ltd.
+36309676753
csongor.hubay@infinitsimulation.com

Llega a Chile
El primer simulador aéreo reconfigurable

Con una trayectoria cercana a los 21 años,RAZBAM Simulators constituye uno de los principales referentes a nivel mundial en el área de los simuladores aéreos, gracias a su capacidad de desarrollar avanzadas soluciones que integran las últimas tecnologías, entre las cuales destaca la creciente presencia de la Realidad Virtual. A lo anterior se suma su capacidad de desarrollar un producto cuya calidad grafica sorprende incluso a los mejores profesionales, logrando un nivel de realismo e inmersión nunca antes visto. Revista Seguridad & Defensa tuvo la oportunidad de conversar con el creador de esta empresa Ronald Zambrano, quien ya confirmo la presencia de uno de sus sistemas de simulación aérea para la próxima edición de Seguridad Expo 2023.

¿Qué nos puede comentar en relación al desarrollo de la realidad virtual, en especial durante esta última década?

Creo que la aparición del Oculus Rift en el 2012 que comprobó la vialidad comercial de equipos de realidad virtual a nivel consumidor, provocó una verdadera explosión de productos relacionados que se mantienen en constante desarrollo y la oferta no cubre la demanda actual ya que día a día se suman más usuarios de estos equipos, y en la actualidad es ya una herramienta standard usada en desarrollos médicos, arquitectónicos y de entrenamiento a nivel civil y militar que ha generado que se desarrollen equipos específicamente para estos fines los cuales por su elevado costo no están al alcance del consumidor general pero dichas tecnologías una vez superadas pasan a la siguiente iteración, pasan directa e indirectamente al mercado del consumo general a un público cada vez más ávido de la experiencia y que crece exponencialmente con el tiempo. La realidad virtual, desde mi punto de vista, ha venido para quedarse y es algo muy excitante.

¿En la actualidad cuáles son las principales áreas de aplicación de la realidad virtual?

Quizás el área más conocida es la del entretenimiento, video juegos, experiencias virtuales y hasta marketing, pero en donde este tipo de tecnología brilla como el sol, es en el área de entrenamiento en ramas especificas en donde su uso alivia costos de operación de una manera significativa, hablamos de entrenamiento militar, rescate, aviación y uso de maquinaria pesada.

Últimamente también está muy difundida en el área de la medicina en el entrenamiento de estudiantes de medicina en cirugías, en un ambiente totalmente controlado.

Una aplicación incipiente es el uso en el desarrollo de vehículos, maquinarias y todo lo relacionado con la nanotecnología en donde es más fácil visualizar un prototipo antes de llegar a su elaboración.

Recientemente he podido ser testigo de su uso para el estudio del comportamiento humano en casos severos de stress mientras opera algún tipo de maquinaria, creo que el límite lo pone nuestra inventiva.

¿Que nos puede mencionar en relación al nivel de inversión que involucra una solución basada en realidad virtual? ¿resulta rentable para quien la incorpora a sus procesos?

El punto principal aquí seria cuanto es el presupuesto asignado para este tipo de soluciones, pero mientras un sistema de simulación "tradicional" (domo, plataforma, replica de cabina y computadoras) puede fácilmente superar los 5 millones de dólares, un sistema de realidad mixta que involucra una réplica de cabina más un equipo MR y una computadora no llega al millón de dólares y tiene absolutamente la misma funcionalidad y dependiendo del software, hasta superior.

No olvidemos que mientras más partes posea, ya sean proyectores, domos, o brazos hidráulicos, el costo de mantenimiento será exponencialmente superior, algo que no existe dentro de un equipo de realidad mixta ya que no existen partes móviles (en concepto, pero el cliente puede añadirlas) y todo funciona a través de una computadora con partes fácilmente encontradas en el mercado y con un costo de reemplazo MUY inferior.

La diferencia de costos de operación e inversión son drásticamente inferiores, en donde aun teniendo un buen presupuesto de inversión se pueden incorporar mas sistemas de entrenamiento en contraste con un sistema "tradicional".

En el ámbito de la capacitación ¿Qué comparativos existen con respecto a los niveles de aprendizaje y de retención de nuevos conocimientos al comparar entre un sistema de aprendizaje tradicional y uno basado en realidad virtual?

Dependiendo mucho del tipo de inversión que se realice y el software de simulación que se use, no existe una verdadera diferencia en este sentido.

Herramientas como la realidad mixta pueden suplir a un costo más bajo lo que sería un simulador con domo y brazos hidráulicos ya que posee exactamente la misma funcionalidad.

Los equipos de realidad virtual suman una nueva capacidad: La simulación táctica de combate, en donde el alumno que ya sabe volar el equipo en el cual está entrenando, aprende a usarlo en sus funciones específicas en distintos escenarios, ya sea combate aéreo, interdicción o rescate, en donde los sentidos están totalmente inmersos en la simulación que se le presenta en frente y ensayar lo que aprendió académicamente antes de pasar al equipo real, llevando consigo conocimientos previos antes del ensayo en el quipo verdadero a un costo muy inferior de operación.

Algo que además añaden estas tecnologías es el sentido de "caja de arena" (sandbox) en donde los usuarios verdaderamente tienen como límite su inventiva e imaginación en como explotar las bondades que todo esto brinda.

¿Cómo visualiza la incorporación de soluciones en materia de capacitación mediante realidad virtual a nivel Latino Americano considerando la necesidad de incrementar las capacidades del recurso humano local?

Pienso que el mercado latinoamericano está muy necesitado o de este tipo de soluciones ya que costo de poner este tipo de sistemas en funcionamiento, sumado a su versatilidad y bajo costo operativo, es exactamente lo que buscan las Fuerzas Armadas de la región que viven con presupuestos muy estrictos en donde a veces no cubre temas tan importantes como el constante entrenamiento.

Adicionalmente este tipo de plataforma proporciona a los usuarios control total de dichos sistemas al ser todos basados en soluciones desktop es decir las piezas y partes de repuestos o aquellas que cubren su vida útil, se encuentran en el mercado comercial sin ningún problema, es más, facilita el uso a través del tiempo ya que pueden renovar su hardware de acuerdo a los tiempos y así tener un sistema al día sin pensar en una obsolescencia en el corto plazo. Todo eso se traduce en una inversión que se paga a sí misma durante su tiempo de vida útil.

Al referirnos al nivel de inmersión ¿podemos pensar que en un futuro próximo accederemos a la incorporación de sensaciones realistas como el tacto?

Actualmente se está trabajando en ese tema, ya existen trajes hapticos que permiten la sensación de calor, frio o simular golpes y durante la IT2EC realizada en Rotterdam en Abril de este año tuve la oportunidad de probar personalmente un prototipo de equipo haptico que incluía estas características; lo novedoso es que era totalmente autónomo, luego en Septiembre estuve en el Tokio Game Show en donde pude observar dicha tecnología a nivel consumidor aunque aún no a disponibilidad al público, es una tecnología incipiente que está avanzando muy rápido y estoy convencido que en un par de años serán tan normales como los equipos de realidad virtual.

Lo importante para que estas tecnologías crezcan y maduren es que exista una demanda, la cual en la actualidad está al alza ya que el ahorro en costos de operación es muy grande y la inmersión es total y los sentidos son totalmente engañados logrando una simulación completa, la cereza en el pastel es que se cimienten en el mercado del consumidor normal/gamer que haría que esta tecnología se siga expandiendo.

¿Cómo describe el nivel de desarrollo y de incorporación de la realidad virtual en el área de la defensa y de la seguridad?

Uno de los desafíos más grandes que enfrentan en la actualidad las instituciones de seguridad y

defensa nacionales son los altos costos de entrenamiento lo cual está directamente ligado al nivel tecnológico de los equipos actuales, las horas de vuelo han incrementado su costo al ser los aviones más modernos, munición, traslados y un largo etc.

Por medio de estas tecnologías se puede mantener un elevado nivel de entrenamiento/aprendizaje usando el concepto circular de entrenamiento-planificación-ensayo-ejecución-AAR (after action review)-entrenamiento en donde solo la parte de ejecución comprendería el mover los activos reales y la mayor parte de la preparación se hace en un ambiente simulado en donde predomina la realidad virtual y mixta.

Pero hay que ser muy claros también, absolutamente nada puede reemplazar el vuelo real o la ejecución en el terreno de maniobras de entrenamiento, pero al ser estos ejercicios en los cuales se aprende por repetición, la simulación usando realidad virtual y mixta son claves para mantener al personal capacitado la mayor cantidad de tiempo posible a un costo bajo de operación.

¿Qué nos puede comentar con respecto a la trayectoria de Razbam y de su posicionamiento en el ámbito de la realidad virtual?

RAZBAM Simulations, LLC es una compañía que empezó operaciones en el año 2002 creando contenido para simuladores de tipo comercial como la serie de simuladores creados por Microsoft: Flight Simulator en sus versiones FS8, FS9 , FSX y Prepar3D por Lockheed Martin.

En el año 2014 cambiamos de plataforma principal a DCS (Digital Combat Simulator) de la compañía Eagle Dynamics la cual por sus características particulares su potencial como herramienta de instrucción profesional son enormes.

A finales del añ0 2015 publicamos nuestro 1er producto para dicha plataforma en la forma del Mirage 2000C RDI. La calidad del producto hizo que fuéramos contactados por un oficial muy visionario de la Armée de l'air et de l'espace que buscaba una solución de entrenamiento para sus RDI que estaban al final de su vida operativa, corría el año 2017 y en el transcurso de 5 años no solo se convirtió en la solución perfecta (que permitió extender la vida operativa de los aparatos hasta el año 2022, cuando estaban programados al retiro en el 2019) sino que se experimentó con éxito en el uso de la realidad virtual y ha sido la prueba irrefutable de que el concepto paso del ensayo a la práctica, tanto que desde el 2022 a la fecha muchas fuerzas aéreas actualmente están incorporando esta tecnología en sus silabus de entrenamiento y creando otros para explotar al máximo esta capacidad.

El simulador reconfigurable permite en una misma plataforma simular cazas y entrenadores de ala fija, y rotatoria ampliando las capacidades de entrenamiento sin incurrir en un hardware específico para cada aeronave.

RAZBAM participó activamente por 5 años de manera muy cercana con la Armée de l'air et de l'espace lo que permitió conectarnos con empresas de tecnología de punta con productos específicamente diseñados para ser usados como herramientas de entrenamiento, como es el caso de los headsets Xtal 3 de Vrgineers.

¿En qué consiste el simulador que Razbam presentará en Chile y cuáles son sus principales características y particularidades?

El simulador que vamos a presentar es manufacturado por la empresa Vrgineers, y es uno dentro de una serie de soluciones VR que posee la empresa y gira alrededor de su producto estrella que es el Xtal 3, su nombre es Portable Trainer, que como su nombre indica es totalmente portable ya que toda su estructura es abatible dentro de una carcasa con ruedas y se convierte en una especie de baúl de mucha resistencia tanto así que puede ser desplegado a un área pertinente por medio de paracaídas sobre un pallet.

Su construcción es metálica de alta resistencia de grado militar y es fácilmente configurable para simulación de equipos de ala fija como ala rotatoria, siendo posible hacerlo en cuestión de minutos, es totalmente autónomo y no es dependiente de ningún software de simulación en particular lo que significa que es una herramienta altamente versátil.

Su sistema VR es el Xtal3 que es un headset de realidad virtual de alto rendimiento y amplio FOV (Field of View) o campo de visión periférica de 180 grados de manera horizontal y 120 grados de manera vertical, con una resolución de 3840×2160 por ojo en un par de pantallas de LCD de 4k cada una.

Es un headset diseñado desde sus inicios para ser usado en simuladores de vuelos y es la punta de lanza en esta tecnología en la actualidad.

Como software de simulación presentaremos Mission Combat System (MCS) producido por la empresa Suiza EDMS el cual es en la actualidad el software de simulación mas capaz del mercado. RAZBAM SImulations, LLC tiene licencia de desarrollo en dicho software así que mostraremos algunos de nuestros productos como lo es el F-15E Strike Eagle y productos del catálogo de EDMS como lo es el F-16 B52 en uso en la actualidad por la FACH.

¿Qué nos puede mencionar en relación a la capacidad de su empresa para desarrollar soluciones customizadas para el área de la defensa y de la seguridad?

RAZBAM Simulations, LLC es una empresa desarrolladora de contenido para simuladores de vuelo, eso implica que tenemos el conocimiento y la capacidad para crear de acuerdo a las necesidades del cliente lo que sea necesario, llegando a un grado muy grande de réplica del producto real lo que lo convierte en una herramienta de entrenamiento muy completa.

Bajo nuestro lema de que "todo hardware es tan bueno como el software que lo corre" tenemos la visión de proveer exactamente lo que el cliente necesita de manera explícita, con resultados ya comprobados y clientes muy satisfechos. Siempre abiertos a nuevos retos, tenemos el compromiso de cubrir totalmente las expectativas de nuestros clientes al nivel que ellos esperan.

Dentro de eso, tenemos la capacidad de trabajar en todas las plataformas de simulación actualmente existentes, aunque de acuerdo a las necesidades de cliente siempre sugerimos la plataforma óptima para cubrir sus necesidades.

Seguridad y la Conjetura de Poincaré

La Conjetura de Poincaré es un problema de topología que se refiere a la clasificación de las variedades tridimensionales. Una variedad es un espacio que localmente se parece a un espacio euclídeo de cierta dimensión. Por ejemplo, la superficie de una esfera es una variedad bidimensional, porque cada punto tiene un entorno que se parece a un plano. Una variedad tridimensional es un espacio que localmente se parece al espacio tridimensional ordinario.

La conjetura se planteó en el año 1904 por el matemático francés Henri Poincaré. Se trata de una pregunta sobre la forma de los objetos tridimensionales que no se pueden ver directamente, como, por ejemplo, el universo. La Conjetura de Poincaré afirma que si un objeto tridimensional es cerrado (no tiene agujeros ni bordes) y simplemente conexo (cualquier curva cerrada se puede encoger hasta un punto sin salir del objeto), entonces ese objeto tiene la misma forma que una esfera tridimensional, llamada 3-esfera. Esta conjetura fue uno de los problemas más difíciles y famosos de la matemática, hasta que fue resuelta en el año 2006 por el matemático ruso Grigori Perelmán, quien usó una técnica llamada flujo de Ricci para transformar cualquier objeto tridimensional en una 3-esfera.

La Conjetura de Poincaré tiene una relación con la seguridad, ya que se puede usar para estudiar la criptografía, que es el arte de cifrar y descifrar mensajes secretos. La criptografía se basa en la teoría de números, que es una rama de la matemática que estudia las propiedades de los números enteros y sus generalizaciones. La teoría de números usa conceptos de la topología, que es la rama de la matemática que estudia las propiedades de los objetos geométricos que no cambian cuando se deforman de manera continua, como estirarlos o encogerlos. La conjetura es uno de los resultados más importantes de la topología, ya que clasifica los objetos tridimensionales según su forma.

Un ejemplo de cómo se puede usar la Conjetura de Poincaré para la criptografía es el siguiente: supongamos que queremos enviar un mensaje secreto a otra persona usando un código basado en números primos, que son aquellos números enteros mayores que 1 que solo se pueden dividir por sí mismos y por 1. Para ello, elegimos dos números primos grandes, p y q, y los multiplicamos para obtener un número compuesto n = p x q. Luego, usamos una función matemática llamada función phi de Euler, que cuenta cuántos números enteros menores que n son coprimos con n, es decir, no tienen ningún divisor común con n. La función phi de Euler tiene la propiedad de que si n = p x q, entonces phi(n) = (p-1) x (q-1). Esto significa que, si conocemos p y q, podemos calcular fácilmente phi(n), pero si solo conocemos n, es muy difícil encontrar p y q, a menos que usemos un método muy sofisticado llamado factorización. La factorización consiste en encontrar los factores primos de un número compuesto, y es un problema muy difícil de resolver cuando los números son muy grandes.

Ahora, para enviar el mensaje secreto, lo convertimos en un número m usando un alfabeto numérico, por ejemplo, asignando a cada letra un número del 1 al 26. Luego, elegimos otro número e que sea coprimo con phi(n), es decir, no tenga ningún divisor común con phi(n). Usamos el algoritmo de Euclides extendido para encontrar otro número d tal que e x d sea congruente con 1 módulo phi(n), es decir, que al dividir e x d entre phi(n), el resto sea 1. Estos números e y d son las claves del código: e es la clave pública, que se puede compartir con cualquiera, y d es la clave privada, que se debe guardar en secreto.

Para cifrar el mensaje m, usamos la clave pública e y calculamos c = m^e módulo n, es decir, elevamos m a la potencia e y dividimos el resultado entre n, quedándonos con el resto c. Este número c es el mensaje cifrado, que se puede enviar sin riesgo de ser interceptado. Para descifrar el mensaje c, usamos la clave privada d y calculamos m = c^d módulo n, es decir, elevamos c a la potencia d y dividimos el resultado entre n, quedándonos con el resto m. Este número m es el mensaje original, que se puede convertir en letras usando el alfabe-

to numérico.

Este método de cifrado se llama RSA, por las iniciales de sus creadores, Ronald Rivest, Adi Shamir y Leonard Adleman, quienes lo inventaron en 1977.

El RSA se basa en la dificultad de la factorización, y por eso es muy seguro, ya que nadie puede descifrar el mensaje sin conocer la clave privada d, que depende de los números primos p y q. Sin embargo, la seguridad del RSA podría verse comprometida si se encontrara un método más rápido y eficiente para factorizar números grandes.

Aquí es donde entra en juego la Conjetura de Poincaré, ya que algunos matemáticos han propuesto usar la topología para encontrar algoritmos de factorización basados en la forma de los objetos tridimensionales.

Por ejemplo, se podría usar una técnica llamada cirugía, que consiste en cortar y pegar pedazos de objetos tridimensionales para obtener otros objetos diferentes. La Conjetura de Poincaré garantiza que si hacemos una cirugía en una 3-esfera, el resultado será otra 3-esfera o un objeto homeomorfo a ella. Esto podría usarse para encontrar los factores primos de un número n, si se pudiera representar n como una 3-esfera y sus factores como otras 3-esferas más pequeñas.

Este es solo un ejemplo hipotético de cómo la Conjetura de Poincaré podría tener aplicaciones en la criptografía y la seguridad. Sin embargo, todavía no se ha encontrado un método práctico y eficaz para usar la topología para factorizar números grandes. Por lo tanto, sigue siendo un resultado teórico muy interesante y profundo, pero no tiene una utilidad inmediata para la seguridad. No obstante, esto no significa que no pueda tenerla en el futuro, ya que la matemática es una ciencia que avanza constantemente y descubre nuevas conexiones entre sus diferentes ramas.

Su importancia radica en que permite entender mejor la estructura del espacio y sus propiedades. En el ámbito de la gestión de la seguridad, podría ser útil preliminarmente, para analizar los riesgos y las vulnerabilidades de los sistemas complejos, así como para diseñar soluciones eficientes y robustas.

La conjetura de Poincaré nos invita a pensar en la seguridad desde una perspectiva global y holística, considerando todos los factores y variables que pueden influir en el resultado final.

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

Emilio García Perulles

Director General de Internacional del grupo EULEN

Buscamos fortalecer la estrategia de expansión de nuestra compañía

Con casi 28 años de experiencia en el sector y más de 13 años dentro del Grupo EULEN, Emilio García Perulles asumió en junio de 2023 el nuevo cargo de Director General de Internacional. Con motivo de su llegada al puesto, Emilio visitó Chile como parte de una gira por los mercados latinoamericanos más importantes en los que tiene presencia la compañía, lo anterior con el objetivo de abrir paso a su gestión en la región sudamericana y trasladar el conocimiento en seguridad privada y Facility Services que la compañía tiene consolidado en España y diversos países, adaptándolo a la diversidad de situaciones socioeconómicas del país.

La incorporación tecnológica es una realidad y siendo la seguridad uno de los rubros que mayores cambios ha presentado en esta materia ¿Cómo asume el Grupo EULEN el desafío de incorporar estos cambios sin que necesariamente esto implique reemplazar recurso humano por tecnología?

Durante los últimos años, Grupo EULEN ha realizado importantes inversiones en tecnología, precisamente porque entiende, e incluso lidera, el proceso de integración que viven hoy las habilidades humanas con los desarrollos tecnológicos en la industria de la seguridad. Esta convergencia, o como le llamaos nosotros; seguridad integrada, ha traído consigo un cambio importante en cuanto a las posibilidades que nos entrega la tecnología para disminuir la ocurrencia de errores y amplificar las capacidades humanas.

Por eso, hoy la labor que cumplen nuestros técnicos especialistas en seguridad instalados en nuestro CCSI (Centro de Control de Seguridad Integral) ya no comprende la mera observación de cámaras o imágenes que pueden llevar a errores o ineficacia, sino que monitoreamos alertas de seguridad que generan nuestros softwares con inteligencia artificial, las cuales son gestionadas por técnicos especialistas y preparados para interpretarlas, atenderlas y derivarlas de la forma más rápida posible a las unidades policiales.

Ahí radica una de las mayores virtudes del recurso humano respecto a la gestión de seguridad y que nunca podrá ser reemplazada, ya que como la tecnología hoy nos permite automatizar funciones repetitivas y delegar en ella tareas que antes realizaban personas, es esta misma inédita disponibilidad de tiempo con la que hoy cuentan los trabajadores la que nos ofrece la oportunidad de que nuestros equipo puedan enfocarse en tareas más complejas o de supervisión del trabajo que realiza la tecnología o la IA, y que muchas veces requieren del criterio humano.

De hecho, uno de los pilares de la Responsabilidad Social Corporativa del Grupo EULEN apunta precisamente a nuestra apuesta por el recurso humano, y por supuesto a su diversidad, objetivo que como compañía abordamos en las cuatro principales líneas en las que estamos trabajando en esa dirección: género, generacional, funcional y cultura. De hecho, hoy un 3,2% de nuestros trabajadores tiene alguna discapacidad, mientras que un 55,3% de nuestro personal a nivel global son mujeres.

Las distintas legislaciones en materia de seguridad privada difieren de un país a otro. En el caso de chile se acaba de proponer una nueva norma ¿Cómo podemos avanzar hacia estándares de capacitación que vayan más allá de los mínimos requeridos y que permitan realmente proyectar al personal que se desempeña en este importante sector?

Primero cabe destacar el enorme aporte que hacen las más de 150 mil personas que actualmente ejercen labores de seguridad privada en Chile,

porque son la cara visible y la primera barrera con la que cuentan las compañías y sus trabajadores para resguardar su seguridad. Por esto en Grupo EULEN siempre valoramos toda norma o nueva legislación de seguridad privada que profesionalice el sector, que aumente los requisitos y los resguardos de los operadores de seguridad privada.

En este sentido, para nosotros es una muy buena noticia la reciente aprobación del proyecto de ley de seguridad privada, ya que también lo vemos como un paso fundamental para enfrentar la crisis de seguridad que vive el país, que busca fortalecer el rol de los privados en la prevención del delito. En este sentido, es un orgullo para Grupo EULEN el poder poner a disposición del país nuestras herramientas y tecnología de seguridad cada vez que la autoridad lo requiera, porque entendemos que cualquier medida que ayude a enfrentar la delincuencia en el país -y en todo el continente- es sin duda un aporte a nuestro objetivo de ofrecer una mayor seguridad a la población.

¿Cuál es el análisis que usted puede realizar sobre la situación y potencial del mercado chileno considerando nuestra actual situación país en materia de seguridad?

En general, a nivel internacional nuestro negocio en la mayoría de los países en los que estamos presentes ha experimentado un crecimiento sostenido en 2023, a pesar de las variaciones en cada país que generan los desafíos económicos globales, el aumento de tipos de interés, precios de energía y salarios debido al incremento del IPC, entre otros.

Específicamente en la región nuestra compañía cuenta con un plan estratégico con metas y objetivos planteados para conseguir un crecimiento sostenido y significativo.

Chile no ha sido la excepción, donde hemos estado en línea con las previsiones establecidas, y aunque la posición de mercado es más difícil de medir ahora por la mezcla de guardias con tecnología de seguridad, sumado a la diversidad de marcas y soluciones con las que se puede trabajar, nosotros estimamos que en la actualidad somos la segunda o tercera mayor empresa de seguridad que opera en el país, con opciones de ampliar nuestra presencia gracias a la reciente adjudicación de importantes proyectos en distintas industrias y en especial en minería, donde estamos penetrando fuertemente con nuestro servicio de guardias y seguridad electrónica.

Hoy contamos con más de 300 clientes a nivel nacional, de los cuales 150 son empresas a las que les ofrecemos específicamente el servicio de seguridad integrada, y en 2022 tuvimos ventas por sobre los $39 mil millones de pesos, de los cuales nuestro negocio de seguridad representó un 55% del total de Grupo EULEN Chile.

Respecto a si la actual situación del país en materia de seguridad influye y potencia nuestra visión del mercado chileno y perspectivas de crecimiento local, es un hecho que las compañías, viéndose afectadas por diversos tipos de delitos, los que por cierto son cada vez más sofisticados, buscan en las empresas de servicio de seguridad privada un resguardo no solo de sus instalaciones, sino que principalmente de sus trabajadores, quienes hoy se pueden ver expuestos a actos de mucha violencia.

En este contexto, el crecimiento del negocio en el país ha avanzado de manera natural, a pesar de que nuestro mayor deseo es que la situación se normalice y podamos contar todos con un entorno seguro y en el que las personas y negocios pueden desarrollarse de manera normal.

Dicho esto, con nuestro servicio de seguridad estimamos crecer en ventas en un 5% para 2023, y entre un 7% y 9% para 2024 y 2025. nuestro foco está en crecer en soluciones integrales de seguridad, las que, por ser proyectos más eficientes, no traen inicialmente un alto crecimiento en facturación.

¿Qué nos puede comentar sobre los proyectos de inversión tecnológica en materia de seguridad para el mercado chileno?

Uno de los objetivos de mi visita a Chile es fortalecer la estrategia de expansión de nuestra compañía, porque tenemos la intención de diversificar y especializar nuestros servicios, siempre apuntando a la incorporación de nuevas tecnologías que potencien nuestro negocio de seguridad. Incluso en la región estamos abiertos a la adquisición de compañías que ofrezcan servicios que aún no tienen presencia en este u otro país, y que puedan aportar valor y ampliar nuestra huella en diferentes áreas del mercado local.

En línea con este objetivo, hoy la compañía ya está completamente instalada en Chile después de haber invertido 3 mil millones de pesos en tec-

nología en los últimos años en proyectos y soluciones implementadas en diversos clientes.

Esa experiencia y contar con un centro de control moderno y multimarca (el CCSI, ubicado en la comuna de Macúl) nos permite una posición privilegiada para ofrecer soluciones con seguridad electrónica "a la medida" del cliente. Esto también nos abre la posibilidad de ofrecer soluciones especializadas en lugares remotos, incluso donde no hay electricidad y con tecnología en base a energía solar o eólica, o utilizando comunicación satelital, por ejemplo. Las soluciones tecnológicas hoy no tienen límite.

Mas allá de las legislaciones locales ¿Cree usted que el personal de seguridad privada debiera contar con mejores niveles de equipamiento no letal para cumplir de mejor manera su rol de respaldo a la seguridad pública? (¿por ejemplo, incorporación de sistemas de retención remota como el Bola Wrap u otros?

En Grupo EULEN creemos que toda industria necesita investigación, formación, desarrollo y profesionalización de nuestro personal, porque esa es la fórmula para que podamos mejorar nuestra oferta de valor. Con esta premisa, cuando pensamos en la formación de nuestros guardias, compartimos el diagnóstico de que este aspecto necesita mejorar en Chile y estandarizarse el servicio, de manera que las empresas requieran de certificaciones y exista un acabado registro de las compañías que operan en el rubro.

Por otra parte, también hemos ido entendiendo lo importante que es para nuestra operación la capacitación constante de ingenieros y técnicos que desarrollan soluciones con tecnologías que van evolucionando día a día, lo que también se extiende a quienes cumplen el rol de guardia de seguridad. Es sumamente importante que ellos puedan contar con el mejor y más moderno equipamiento que existe en la actualidad para el rubro, ya que ellos muchas veces pueden ver expuesta su propia vida en un delito. A evitar esta situación apunta precisamente las herramientas tecnológicas con las que cuenta Grupo EULEN en seguridad, ya que hoy permiten, por ejemplo, hacer alertas por medio de voceo para ahuyentar a delincuentes sorprendidos en actos delictivos, sin necesidad de exponer físicamente al trabajador.

En esta línea cada país en el que Grupo EULEN está presente, la compañía les ofrece a sus trabajadores la posibilidad de, primero, terminar sus estudios, y segundo, capacitarse permanentemente en habilidades y nuevas tecnologías que requiera su trabajo en particular.

¿En qué medida la experiencia de prestar servicios en 12 países permite al Grupo EULEN potenciar sus procedimientos y traspasar conocimientos a los distintos mercados?

En nuestros más de 60 años de experiencia en el mercado y hoy abarcando 13 diversos países, lo que incluso nos ha llevado a contar en la actualidad con una plana de trabajadores de más de 75 mil personas de 97 nacionalidades distintas, sin duda que son antecedentes que nos han permitido ir comparando y mejorando nuestros distintos procedimientos de manera transversal en todas nuestras operaciones, tanto en España como en el resto del mundo en los que el Grupo EULEN está presente.

Otro de los temas más importantes que Grupo EULEN busca desarrollar en América Latina y precisamente buscamos replicar de nuestros logros alcanzados en otros países, tiene que ver con la implementación de proyectos en temas medioambientales, porque vemos el potencial de crecimiento en esta área debido al transversal aumento de compromisos de reducción de emisiones y sostenibilidad que adquieren los distintos países.

En cuanto a Chile y su nivel de "conocimientos" en el marco de la industria, estamos bastante desarrollados, y más que comparaciones con países vecinos, nos comparamos con nosotros mismos hace tres años atrás, y vemos que hemos sabido aprovechar la pandemia para avanzar y ponernos al día en soluciones modernas y valiosas para nuestros clientes.

¿Existen planes para avanzar en Chile en la implementación de soluciones tecnológicas en seguridad para segmentos como el residencial considerando el alto nivel de conectividad existente en nuestro país?

No específicamente en el mercado residencial, pero que Chile tenga un excelente nivel de conectividad, efectivamente ha colaborado a que las empresas puedan acceder a nuestros servicios de seguridad y que cuentan con tecnología de primer nivel, incluso en los lugares más remotos. Y aunque en otros países los usuarios se han atrevido un poco más en probar tecnologías vanguardistas, ese mismo hecho nos permite tener altas expectativas de crecimiento en Chile, especialmente en cuanto a la implementación de nuevas tecnologías en seguridad.

Por nuestra parte, la compañía cuenta con un departamento de I+D+i (Investigación, Desarrollo e innovación) que tiene vida propia dentro de la empresa y plena libertad para ir innovando, por ejemplo, en soluciones tecnológicas de seguridad. Este año también implementamos el sistema "Esfera tecnológica", por el que ya más de 200 de nuestros trabajadores, distribuidos en distintas partes del mundo, nos han propuesto más de 50 proyectos de innovación para nuestro negocio, que ya los estamos aplicando a nuestros propios servicios.

Hoy canalizamos las motivaciones, logros e ideas innovadoras de nuestros trabajadores por medio de esta esfera tecnológica.

TOME LA ACCIÓN SIN UTILIZAR LA FUERZA

1000 agencias policiales y 60 países son nuestra mejor carta de presentación

Visítenos en el Stand 618

SEGURIDADEXPO by Fisa | CHILE

BOLA WRAP 150

REMOTE RESTRAINT

TOP SECURITY

NICHIEI INTERNATIONAL INCORPORATED

www.bolawrap.cl • info@top-sec.org

BE1
Comienza su apertura hacia el mercado Chileno

En el marco de un viaje regional, la presidenta de BE1 Defense Technologies & Solutions, Ilil Podliszewski visitó nuestro país, territorio en el cual es representada por la empresa Intercon. Revista Seguridad compartió con la alta ejecutiva y con su contraparte chilena representada por Patricio Cañete, gerente general de Intercon..

¿En términos generales qué nos puede comentar con respecto a la trayectoria y experiencia de BE1 en el área de la seguridad y la defensa?

BE1 DEFENSE TECHNOLGIES & SOLUTIONS, es una empresa que hoy por hoy ha evolucionado en estos 16 años en la rama de la Defensa Nacional, Seguridad Nacional Emergencias y más, proveyendo con su metodología y soluciones tecnológicas capacidades de prevención a los diferentes clientes con los que BE1 trabaja en todo el mundo y en especial América Latina. Asimismo, somos una compañía que realiza grandes inversiones en desarrollo y análisis de nuevas tecnologías mejorando continuamente en nuestra calidad de equipos y manteniéndonos a la vanguardia tecnológica de las necesidades reales.

Cabe mencionar que somos desarrolladores de tecnologías para Guerra Electrónica, UAV y metodología de ciberseguridad.

¿Qué perfil de profesionales componen esta empresa?

Primeramente, cada uno de los expertos y profesionales de las diferentes Directivas de BE1, vienen de la carrera Militar, ya que siendo una compañía israelí enfocada en la Defensa y Seguridad Nacional es indispensable esa experiencia y conocimiento para poder responder de la mejor manera ante las necesidades reales de los diferentes países que se tienen operación. Asimismo, contamos con una gran diversidad de profesionales que colaboran grandemente en los desarrollos tecnológicos de las diferentes soluciones con las que cuenta el portafolio de BE1.

¿A qué obedece el enfoque comercial de BE1 hacia el mercado latinoamericano?

Obedece principalmente a la necesidad de evolucionar como empresa ya que para BE1, es un reto enorme hacer esta incursión en el mercado latinoamericano, debido a la peculiaridad con la que esta enfrenta sus diferentes amenazas como el terrorismo, las narcoactividades y la inseguridad en general.

Por otro lado, es importante mencionar que las limitaciones tecnológicas impuestas de manera directa o indirecta por gobiernos o producto de la corrupción no dejan tratar de raíz las causas reales de los problemas y es ahí donde identificamos la necesidad de ayudar a toda Latinoamérica.

¿Qué nos puede mencionar con respecto al creciente nivel de influencia de la tecnología y su rol en el área de la seguridad?

Si bien es cierto la tecnología va evolucionando a pasos agigantados no solo en la vida cotidiana, sino que también en la salud, economías, Defensa y Seguridad Nacional, producto de esto es de vital importancia estar a la vanguardia de los cambios tecnológicos para evitar quedarnos desactualizados y no ser competitivos en el mercado. Ahora bien, es importante destacar que la tecnología facilita grandemente el trabajo para las instituciones que combaten directamente la criminalidad y el terrorismo, pero al mismo tiempo se convierte en una desventaja debido a la complejidad de la tecnología y a las posibles vulnerabilidades en ciberseguridad.

Existe en Chile una propuesta orientada a la creación de una policía fronteriza ¿Qué soluciones nos ofrece BE1 en esta materia considerando la extensa frontera norte de nuestro país lo cual se ha traducido en una inmigración descontrolada y en el ingreso del crimen organizado?

Los temas fronterizos han venido siendo uno de los más grandes problemas en común que tiene toda Latinoamérica y Chile no es la excepción, pero con respecto a ese punto en específico no podemos comentar mucho al respecto por los

convenios de confidencialidad firmados, pero si podemos decir que chile está avanzando grandemente en muchas areas paralelamente con la intención de combatir directamente todos los problemas que actualmente los afectan como la inseguridad, las operaciones de carteles del narcotráfico, tráfico de drogas, migración, pescas ilegales entre otras más.

¿Qué propuestas de solución existen para abordar las crecientes necesidades en materia de seguridad considerando las restricciones en materia de uso gradual y racional de la fuerza?

Tenemos diferentes soluciones tecnológicas desde equipo de protección de la Fuerza que obviamente busca salvaguardar la integridad física de los elementos que brindan seguridad hasta soluciones más complejas de video analítica que identifican comportamientos, armas, tipos de armamentos, frecuencias, identificación facial y más, ahora bien, es importante entender correctamente el termino de proporcionalidad o uso gradual y racional de la fuerza, porque hay muchos gobiernos que se ven sometidos por las instituciones de los derechos humanos que defienden fervientemente este término de manera incorrecta exigiendo a sus elementos de seguridad la correcta aplicación de la proporcionalidad de la fuerza el cual busca únicamente salvaguardar la vida humana, pero tal principio se ve violentado cuando un delincuente decide utilizar un arma blanca, una pistola o inclusive un bate de baseball, donde tiene como objetivo asesinar a una persona, ahora bien cuál es la misión de un "policía o soldado" esta es brindar a grandes rasgos seguridad y estabilidad a una sociedad, ante tal eventualidad no es incorrecto que dicho elemento utilice su arma de equipo para defenderse o defender a un tercero con el objeto de neutralizarlo totalmente o parcialmente, ya que el fin que se busca es salvaguardar la vida humana de un inocente, los derechos humanos deben entender que estos criminales que atentan directamente con la vida son el verdadero enemigo y elementos de seguridad.

¿Considerando el largo historial de chile en materia de desastres naturales (terremotos, erupciones maremotos etc.) disponen ustedes de soluciones enfocadas a esta área?

Efectivamente tenemos muchas soluciones tecnológicas y equipamiento para el sector de emergencia, protección civil, bomberos y búsqueda/rescate, nosotros como BE1 tenemos un lema que dice "PREVENIR Y NO REACCIONAR" traducido para nuestro mundo es que, tomamos todas las medidas necesarias para evitar cualquier amenaza posible y eso lo logramos atreves de la tecnología y las diferentes metodologías.

¿Qué nos puede comentar con relación a la trayectoria y casos de éxito de BE1 en centro américa?

Actualmente nos encontramos en los primeros pasos en Centro América, pero estamos muy contentos con los resultados y aceptación que tienen nuestras tecnologías, es importante recalcar que el Director Regional para América Latina y España, ha jugado un papel muy importante en el desarrollo de la región con el profesionalismo, mentalidad y conocimientos, se están proporcionando muchas soluciones a diferentes países, desde nuestra cede principal para la región de América Latina en El Salvador, volviéndose centro logístico, técnico y desarrollo de estrategias para la Defensa Nacional, a las cuales no podemos entrar en detalles pero solo basta con poder ver algunos canales nacionales y ahí se podrán ver nuestras tecnologías en operación.

El futuro profesional de la seguridad debe ser capaz de dominar las nuevas tecnologías, pues de lo contrario simplemente se convertirá en un espectador del cambio y no en un parte de él.

¿Qué soluciones nos ofrece BE1 para el área de la capacitación?

Como parte de las bases que fundaron esta compañía, puedo decir que la metodología es un factor fundamental para el entendimiento y operación de las tecnologías que se desarrollan, nuestras metodologías están desde la parte de la Defensa Nacional, hasta las de emergencias, tenemos un amplio catálogo de capacitaciones que son de gran ayuda para los operativos cotidianas de seguridad, protección VIP, infiltraciones entre otras.

Ilil Podliszewski presidenta de BE1 Defense Technologies & Solutions, junto a su representante para chile Patricio Cañete, gerente general de Intercon.

Considerando que nuestro país se encuentra en un proceso de modernización de su legislación en materia de seguridad privada ¿Qué aporte puede brindar BE1 para esta área?

BE1, como parte de nuestras capacidades y experiencia en otras latitudes del mundo, podemos trabajar de la mano en el desarrollo, creación e implementación de planes estratégicos que tengan como finalidad el mejoramiento de la Seguridad Nacional; Asimismo, los desarrollos de los planes estratégicos de Nación son elaborados en conjunto con las instituciones de estado para una mejor aplicación de estos.

¿Qué nos puede comentar con respecto al inicio de las actividades de BE1 en Chile?

Chile es un país con mucha demanda en temas de Seguridad Nacional y nosotros estamos muy conscientes de las grandes necesidades que posee este lindo país, recientemente hemos visitado a chile y sostuvimos reuniones con diferentes Ministerios para ponernos a la disposición y así poder contribuir en la solución que necesita todos los chilenos.

Sin duda uno de los mayores objetivos de la tecnología es incrementar nuestra capacidad de prevención y anticipación tanto en materia de seguridad pública como en el área de la defensa nacional ¿Cuál es el nivel de actualización y vigencia que BE1 puede ofrecer en materia de tecnología, seguridad electrónica, asesoría y capacitación?

Nuestras soluciones tecnológicas están siempre a la vanguardia e innovando constantemente, debido a que son políticas de nuestra compañía ya que necesitamos mantenernos como número uno, en el mercado de la Defensa y Seguridad Nacional, es importante entender que en todas nuestras soluciones tanto en asesorías, capacitaciones y equipamiento; nuestros expertos están actualizándose constantemente para dar las mejores soluciones a las diferentes necesidades de la región; por otro lado, nuestra misión es "PREVENIR Y NO REACCIONAR", lo que conlleva a tomar todas las medidas necesarias para contrarrestar amenazas de todo tipo y eso solo se logra anticipándose a los diferentes movimientos de la delincuencia tal cual lo dicta la estrategia militar o como lo indica el ajedrez.

Mayores informaciones:

Be1 Defense Technologies & Solutions LTD
office@alpacos.com / www.alpacos.com

Be1 Defense El Salvador (Sede Latam)
info@alpacos.com / www.alpacos.com

WRAP REALITY

Visítenos en Stand 618

SEGURIDADEXPO by Fisa | CHILE

- **Inmersión completa**. Experimenta una amenaza de 360 grados. Sectores que traen el estrés del mundo real en el espacio virtual desde todas las direcciones.
- **Contenido fresco y de calidad.** Incorporamos una biblioteca de más de 38 módulos de formación con las pertinentes escenarios del mundo real y en tiempo real diseñados por expertos en formación policial.
- **Conjuntos de habilidades superiores**. Oficial de perfeccionamiento y avance. Capacitación en uso de la fuerza, reducción de tensiones y conflictos.resolución, proceso y procedimiento, y más.
- **Tecnología innovadora**. Disfrute del acceso práctico una tecnología de vanguardia que es compacta, fácil de transportar y rápido de configurar.
- **Control total**. Repetir y revisar cada entrenamiento. sesión -incluyendo colocación del tiro, trayectoria, y precisión con Reality Rewind.
- **Fácil de implementar.** Dominar el funcionamiento básico en menos de una hora y aprovecha la instalación profesional en el sitio y sesiones de formación de formadores.

EQUIPE A SU INSTITUCIÓN CON WRAP REALITY

Para mayores informaciones y cotizaciones contactenios a: **info@top-sec.org**

Image by DCStudio on Freepik

Agencia Seguridad Chile

La única agencia de Marketing Digital especializada en empresas de seguridad en Chile

Conformada por un equipo multidisciplinario con más de 20 años de experiencia atendiendo clientes de la industria de seguridad, esta agencia se especiliza en proporcionar una respuesta integral a los requerimientos de las empresas del área de la seguridad mediante la utilización de herramientas de vanguardia, análisis de mercado y tácticas innovadoras, asegurando que cada empresa de seguridad alcance y supere sus objetivos online, manteniendo los estándares más altos de disciplina, compromiso y profesionalismo. Para conocer mayores antecedentes con respecto a esta importante iniciativa conversamos con Werner Ossandón Tengelin, director de negocios e innovación en Agencia Seguridad Chile.

¿Cómo sure la idea de ofrecer servicios de apoyo a emprendedores en el área de la seguridad?

La idea de ofrecer servicios de apoyo a emprendedores en el área de la seguridad surgió de mi propia experiencia como emprendedor. En mi trayectoria, tuve que contratar los servicios de varias empresas de marketing y publicidad digital, pero ninguna de ellas tenía el conocimiento especializado en seguridad que necesitaba. Tuve que enseñarles los conceptos de seguridad, productos y servicios específicos, y la relevancia de estos en el mercado.

Pasé por más de 13 empresas antes de encontrar un equipo con la disposición de aprender y el profesionalismo necesario para comprender la industria de la seguridad. Fue en esta última empresa, en la que trabajamos juntos durante 3 años, donde logramos que Biat Defense y otros emprendimientos de seguridad tuvieran el impacto que realmente debían tener.

A raíz de este exitoso trabajo y el impacto positivo que logramos con el equipo de marketing y publicidad digital, identificamos una estrategia, técnicas y tácticas específicas para la industria de seguridad. Decidimos que era hora de crear una agencia de marketing y publicidad digital especializada en seguridad para compartir nuestro conocimiento con todos los emprendedores del sector de seguridad. Queríamos evitar que pasaran por la misma frustración de probar con múltiples empresas y gastar su dinero sin obtener los resultados deseados.

Si yo enfrenté ese problema, me di cuenta de que otros emprendedores en el sector de seguridad también lo estaban experimentando. Fue entonces cuando vimos la oportunidad de brindar servicios especializados que ayudaran a estas empresas a destacar y comunicar sus servicios de manera efectiva.

¿Cuál es la relevancia de mantener un adecuado posicionamiento en línea para difundir y proyectar un producto o servicio en el área de la seguridad?

En la actualidad, es esencial contar con una presencia digital sólida para destacar en el mercado. De hecho, podría compararse con la antigua tarjeta de presentación, ya que, si tu negocio no está en línea, prácticamente no existe en el mundo digital en el que vivimos.

El primer paso para establecer esta presencia digital es contar con un sitio web que muestre tus servicios o productos. Ayudamos a los emprendedores a dar este primer paso, pero es importante entender que no es suficiente. El mercado es altamente competitivo y agresivo, y las formas en que los clientes buscan información y servicios cambian constantemente. Por lo tanto, tanto tu sitio web como tus redes sociales deben adaptarse para seguir siendo relevantes y mantenerse en los primeros resultados de búsqueda.
En el contexto del área de la seguridad, el posicionamiento en línea cobra una importancia aún mayor. Este sector se basa en la confianza y la credibilidad. Un buen posicionamiento te permite comunicar de manera efectiva los valores de seguridad, resaltar la experiencia y el profesionalismo de tu empresa, y convencer a los clientes de que pueden confiar en tu empresa.

No se trata solo de estar en línea, sino de estar en línea de manera efectiva y adaptarse constantemente a las necesidades cambiantes del mercado y las preferencias de los clientes. Un adecuado posicionamiento en línea te ayudará a proyectar una imagen sólida y a destacar en un mercado competitivo y agresivo como el de la seguridad.

¿El hecho de ser una empresa líder exime de la necesidad de afianzar la presencia en las redes?

No, ser una empresa líder y encontrase a la vanguardia e innovación no exime de la necesidad de fortalecer la presencia en las redes. La competencia en el sector de la seguridad es intensa y está en constante evolución.

Aunque ser líder es un logro destacado, la presen-

cia en línea es esencial para atraer nuevos clientes y fortalecer relaciones con los actuales. Las redes sociales ofrecen una plataforma valiosa para interactuar con la audiencia y mantenerse al tanto de las tendencias en tiempo real.

Ignorar esta necesidad podría abrir la puerta a que competidores ocupen el espacio en línea, incluso como líder de la industria.

¿Qué nos dice la experiencia comparada sobre la relevancia de invertir en asesoría en materia de posicionamiento, especialmente en un sector altamente competitivo como el de la seguridad?

La experiencia comparada demuestra que la inversión en asesoría en posicionamiento es crítica en un sector altamente competitivo como el de la seguridad. Las empresas que han priorizado el marketing y la comunicación en línea han logrado atraer a más clientes, retener a su nicho de mercado y destacar en un mercado saturado.

Si bien ofrecemos asesoramiento a nuestros clientes, preferimos llamarlo "acompañamiento".

Estamos totalmente comprometidos con sus objetivos y resultados, y nuestra labor va más allá de simplemente proporcionar consejos.

Trabajamos codo a codo con nuestros clientes para garantizar que alcancen sus metas de la manera más efectiva y exitosa posible. Nuestro enfoque es más que una simple consultoría; es un compromiso continuo para lograr el éxito conjunto.

¿En qué medida un trabajo profesional en materia de posicionamiento permite conservar y mantener a su nicho de mercado o segmento objetivo?

Un trabajo profesional en materia de posicionamiento desempeña un papel fundamental en la conservación y el mantenimiento del nicho de mercado o segmento objetivo de una empresa.

En el caso de nuestra agencia, como pioneros y la única especializada en atender la industria de la seguridad, nuestro enfoque es singular. Nos hemos comprometido exclusivamente con esta industria, lo que significa que no atendemos a empresas de otros sectores, como alimentos, automóviles, bebidas, etc.

Esta elección se basa en nuestro profundo conocimiento, experiencia y entendimiento de lo que busca nuestro cliente que está dedicado a la seguridad, lo que nos permite ofrecer un servicio altamente especializado.

El trabajo profesional de posicionamiento nos permite asegurar que nuestro negocio sea fácilmente visible para las empresas de seguridad, lo que fortalece nuestra relación con el nicho de mercado. Además, nos ayuda a ser recordados y reconocidos como la principal opción en marketing y publicidad para esta industria. Esto contribuye a la fidelización de clientes, ya que las empresas de seguridad confían en nuestra experiencia y compromiso. Al mantener una presencia en línea sólida y relevante en el ámbito de la seguridad, contribuimos al crecimiento sostenible de las empresas de este mercado, al tiempo que consolidamos nuestra posición como líderes en el mercado.

¿Dónde pueden los emprendedores y profesionales del área de la seguridad acceder a mayor información con respecto a este nuevo servicio?

Los emprendedores y profesionales del área de la seguridad pueden acceder a mayor información sobre nuestro servicio a través de nuestro sitio web en línea, donde encontrarán detalles sobre los servicios ofrecidos, ejemplos de proyectos anteriores y formas de contacto para obtener asesoramiento personalizado. Además, pueden mantenerse al tanto de las últimas tendencias y consejos a través de nuestras redes sociales y blog en línea.

Los invitamos a visitarnos en nuestro Sitio web https://agenciaseguridad.cl/ para explorar cómo podemos ayudar a fortalecer tu presencia en línea y lograr tu éxito en el sector de la seguridad. No duden en contactarnos, estamos aquí para acompañarlos en su camino hacia el crecimiento y la excelencia en marketing y publicidad digital.

Werner Ossandón Tengelin, director de negocios e innovación en Agencia Seguridad Chile.

Image by freepik.com

“Universalidad del concepto de Compasion: Más allá de la práctica profesional en las instituciones de salud”.

Foto de Kindel Mediapexels.com

La compasión es una virtud humana que ha sido valorada y cultivada a lo largo de la historia de la humanidad, entre ellas, en la práctica asistencial de salud ya sea pública y/o privada. Se basa en el compromiso genuino y empático, la solidaridad y la comprensión de las necesidades físicas, emocionales y sociales de los pacientes y las comunidades a quienes proporcionamos un servicio.

Desde una perspectiva holística y como persona, que valora la responsabilidad individual y la eficiencia en la prestación de servicios de salud, la compasión sigue siendo fundamental en la atención de salud, ya que implica varios aspectos importantes, entre ellos, la profunda conciencia del sufrimiento de uno mismo y del de otros seres vivientes, junto con el deseo y el esfuerzo de aliviarlo” (Gilbert, 2009), está enraizada en la capacidad biológica del cuidado (Gilbert, 2005), es decir, el reconocimiento del sufrimiento de un otro y actuar en consecuencia, brindando apoyo, cuidado, comprensión y la voluntad de asumir la responsabilidad de ayudar a otro, y su importancia trasciende la esfera individual para influir en aspectos más amplios de la sociedad.

Para comenzar, la compasión, es un concepto polisémico, se manifiesta en las acciones y/o gestos diarios de las personas. Estos gestos de compasión son esenciales para fortalecer los lazos comunitarios y crear un entorno más cohesionado.

En el ámbito de salud, aboga por la atención centrada en el paciente y la consideración de todas las dimensiones de la salud. Es un marco que no solo beneficia a los pacientes y las comunidades, sino que también puede mejorar la calidad de la atención, fortaleciendo la relación profesional de salud-paciente, reduciendo el estrés y la ansiedad y, en última instancia, contribuye a mejores resultados y/o adherencia de salud a largo plazo.

Este enfoque reconoce que la salud no se limita a la ausencia de enfermedades, sino que también se relaciona con el bienestar físico, emocional y social de los pacientes y se beneficia de la colaboración interdisciplinaria y se extiende más allá de la relación profesional de salud-paciente, aplicándose al trabajo en equipo, ya que pueden combinar sus conocimientos y habilidades para brindar una atención más personalizada y efectiva. Esto es especialmente valioso tanto para su aplicabilidad en la vida cotidiana, instituciones de salud y pacientes con alguna condición de salud compleja o crónicas donde se requiere un enfoque más integral para garantizar una atención de calidad y excelencia.

Algunas consideraciones para la práctica de la compasión en salud y en la cotidianidad:

1.**Cultivar habilidades de Comunicación** “promoviendo la empatía” y la resolución de conflictos

No solamente los profesionales de la salud deben ser formados en la empatía para comprender las preocupaciones y necesidades de los pacientes y las personas en general, es también una labor de los padres o cuidadores, ámbito educativo, laboral, entre otros. Esto incluye escuchar activamente, validar las experiencias de los pacientes y las personas, independientemente de sus creencias y su cultural, mostrando interés genuino por su bienestar.

Singer y Klimecki (2014) y otros investigadores han ido mostrando que neurobiológicamente la empatía y la compasión activan zonas cerebrales diferentes, la empatía activa áreas asociadas al dolor, mientras que la compasión activa áreas asociadas al alivio del dolor.

La pregunta que entonces surge es, ¿Qué compartimos como humanidad?, ante lo cual, se reconoce que, a su vez, compartimos algunas de las siguientes condiciones, tales como: a) Somos seres emergentes y sensibles, expuestos al dolor,

la enfermedad y la muerte, deseamos estar libres de sufrimiento; b) Las experiencias, son importantes sobre todo los momentos de encuentro y conexión, ya que somos seres relacionales, no vivimos aislados; y c) Compartimos una sensibilidad común, somos vulnerables desde lo biológico, por lo tanto, necesitamos del cuidado de otros y de nosotros mismos. Nuestra condición de ser vulnerables puede llevarnos a protegernos y separarnos de los demás, sin embargo, ser conscientes de nuestra vulnerabilidad tiene la capacidad de conectarnos con los demás, es decir, la compasión se basa más bien en la experiencia de humanidad compartida, en que todos estamos expuestos al sufrimiento y anhelamos aliviarlo.

Un ejemplo relevante, es la respuesta a la Pandemia de COVID-19 (Sars-CoV2). La compasión se ha manifestado en la dedicación incansable de los trabajadores y profesionales de la salud, en cuanto a la comprensión de las necesidades de los pacientes y en la promoción de prácticas saludables para la sociedad. Esta compasión y vocación de servicio no solo salvo vidas, sino que también fortaleció la seguridad nacional al contener la propagación de este virus.

Por lo anterior expuesto, la compasión no debería limitarse únicamente al ámbito de las atenciones médicas. La fractura del orden, la seguridad, la ética y la probidad, además del debilitamiento de la democracia en Chile ha generado un ambiente de polarización en todos los aspectos de vida de las personas, particularmente en la interacción con autoridades como Carabineros de Chile y otras instituciones que cumplen con su deber. Por lo tanto, promover el respeto mutuo y el sentido de pertenencia es fundamental para construir un futuro en unidad, seguro y en paz para toda la población chilena.

2.**Ámbito de la salud**, importancia de la personalización de la atención: Cada paciente es único, y la medicina integral se basa en adaptar la atención a las necesidades individuales. Esto implica considerar las preferencias, valores y los determinantes sociales de la salud de cada paciente al desarrollar un plan de atención.
El cuidado es una experiencia ancestral fundamental que está intrínsecamente relacionada con la adaptación y las distintas etapas del ciclo vital del ser humano. Esta praxis se manifiesta principalmente a nivel interpersonal e implica a la persona que brinda el cuidado, en este caso, el equipo interdisciplinario de salud y a la persona que recibe el cuidado, es decir, el paciente.
Tanto en el ámbito de la atención médica y sus especialidades como en nuestra cotidianidad, el primer acto de compasión implica reconocer a la otra persona y aceptar su humanidad. En muchas ocasiones, el simple acto de prestar atención y reconocer la humanidad del otro puede aliviar significativamente el sufrimiento.

Figura 1: Flujo interactivo de la Compasión, diseño de autor.

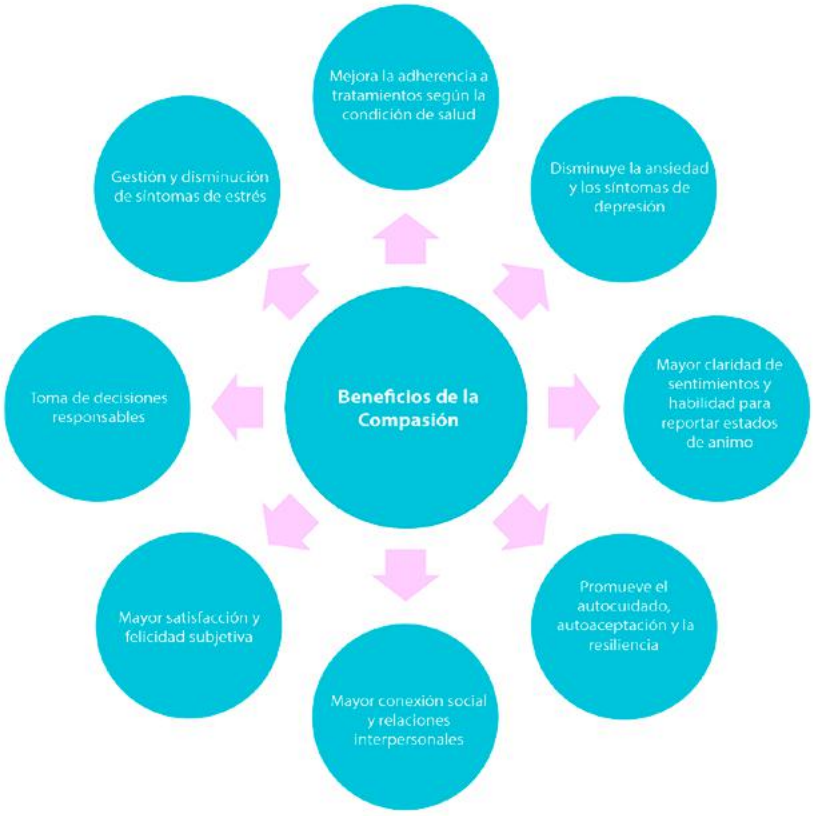


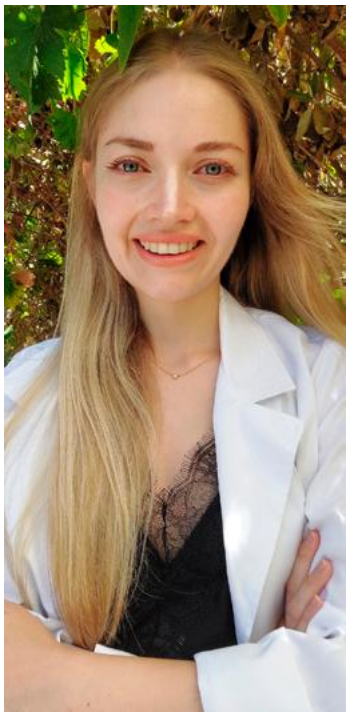
Figura 2: Algunos beneficios de la compasión en el ámbito de la salud mental tanto para los individuos que la practican como para aquellos que la reciben, lo que contribuye al bienestar psicológico (Neff et al., 2012).

A través de la reflexión y la experiencia, los profesionales de la salud que desarrollan y practican la compasión en un contexto clínico o en las experiencias personales, aportan a la salud, bienestar y a la calidad de vida tanto de las personas y las comunidades a las que sirven, es un recurso muy preciado para abordar los desafíos de la seguridad en el mundo actual.

3.**Colaboración interdisciplinaria**: La visión de salud de forma holística se beneficia de la colaboración entre profesionales de diferentes especialidades, tales como; medicas, ciencias sociales, educación, entre otras, ya que pueden enriquecer las soluciones, proporcionando una atención más completa y eficiente al abordar todos los aspectos de la salud del paciente.

Finalmente, la compasión es una virtud que no solo enriquece la vida cotidiana de las personas, sino que también desempeña un papel decisivo en la seguridad nacional. Practicar y construir la compasión en la sociedad promueve la cohesión social, la justicia y la prevención de conflictos y amenazas, entre otros. Al cultivar la compasión en nuestras vidas y en las comunidades, contribuimos a la construcción de un país más seguro y resiliente en su conjunto.

Por lo tanto, la compasión no debe ser subestimada, es un arte y parte de la ciencia, sobre todo en el campo de la salud, particularmente para garantizar que las personas, pacientes y las comunidades en general reciban la atención que necesitan de manera holística y humanizada.



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

La única agencia de marketing digital especializada en empresas de seguridad en chile

+56 9 9505 1017
contacto@agenciaseguridad.cl
www.agenciaseguridad.cl

Un número único de emergencias para Chile

Una verdadera urgencia país

El disponer de un número único de emergencia ha adquirido un rol fundamental en la seguridad y protección de las personas. Su implementción en nuestro país nos permite acceder a nuevas tecnologías que facilitan el trabajo y aseguran la respuesta eficaz y eficiente a volúmenes tan grandes como son las solicitudes a servicios de emergencia. Para abordar este interesante tema conversamos con ejecutivos de Motorola Solutions, líder a nivel mundial en la implementación de este tipo de soluciones.

¿Cuáles son las principales conclusiones del evento realizado recientemente en Chile durante el cual se abordó la necesidad implementar un número único de emergencias?

"Los expositores coincidieron en que Chile tiene todas las condiciones para avanzar hacia un número único de emergencias. La tecnología es el principal multiplicador de fuerzas, lo que permitiría a Chile proteger con mayor eficiencia y eficacia sus territorios, con soluciones colaborativas, conectadas e inteligentes que ayuden a sacar mejor partido a las fuerzas desplegadas en terreno ".

¿Qué nos puedes mencionar respecto de casos de éxito de otros países en los cuales Motorola Solutions ya ha implementado el sistema de número único de emergencia?

"La implementación de un número único en el mundo ofrece múltiples casos de éxito desde su creación, en febrero de 1968, en Estados Unidos.

En esa oportunidad, el presidente de la Cámara de Representantes de Alabama, Rankin Fite, realizó la primera llamada simbólica al 911. Hoy, es tal su valoración ciudadana que incluso existe en Alabama un festival dedicado al 911 y a las agencias de seguridad.

Ciudades como Los Ángeles, California; Miami, Florida; Bogotá, Colombia; Kingston, Jamaica; y centenas de otras utilizan nuestras soluciones para mejorar los servicios de atención de emergencias, acortando los tiempos de respuesta por parte de agencias de seguridad pública y emergencias. Incluso en Nueva York, luego de las lecciones que se extrajeron tras los atentados contra las Torres Gemelas, se implementó un número único capaz de integrar a todas las agencias de seguridad y protección civil".

¿Qué tipo de soluciones nos ofrece hoy la tecnología para disminuir los preocupantes índices de llamados inconducentes o "pitanzas" los cuales suelen atochar las actuales plataformas de emergencia?

"Tiene una utilidad muy importante en esta materia. En la práctica, NG911 es la tecnología de Motorola Solutions que determina y enruta las llamadas al centro de atención de emergencias, CAE (o PSAP, por sus siglas en inglés) apropiado y provee los mecanismos para registrar la localización de las llamadas malintencionadas o no procedentes, identificar al suscriptor de la línea utilizada para la llamada malintencionada e iniciar un manejo automático de la misma. Esto, en conjunto con los profesionales altamente calificados a cargo de dirigir cada caso a la agencia de seguridad correspondiente, simplifica los flujos de trabajo de misión crítica y el acortamiento de los tiempos de respuesta".

Más allá de tratarse de un medio de comunicación centralizado para emergencia, hablamos de una plataforma integrada de gestión de seguridad ¿Qué nos puede mencionar con respecto de la fortaleza de la solución que Motorola Solutions ofrece en esta materia?

"Una de las grandes fortalezas que ofrece Motorola Solutions es la posibilidad de implementar soluciones respaldadas por la Inteligencia Artificial (IA). Los avances en IA permitirán mejorar

Nueva generación de sistemas de seguridad

Sin cables. Sin problemas.

Aplicaciones sin costo para los instaladores y usuarios finales

ajax.systems

macOS Windows iOS Android

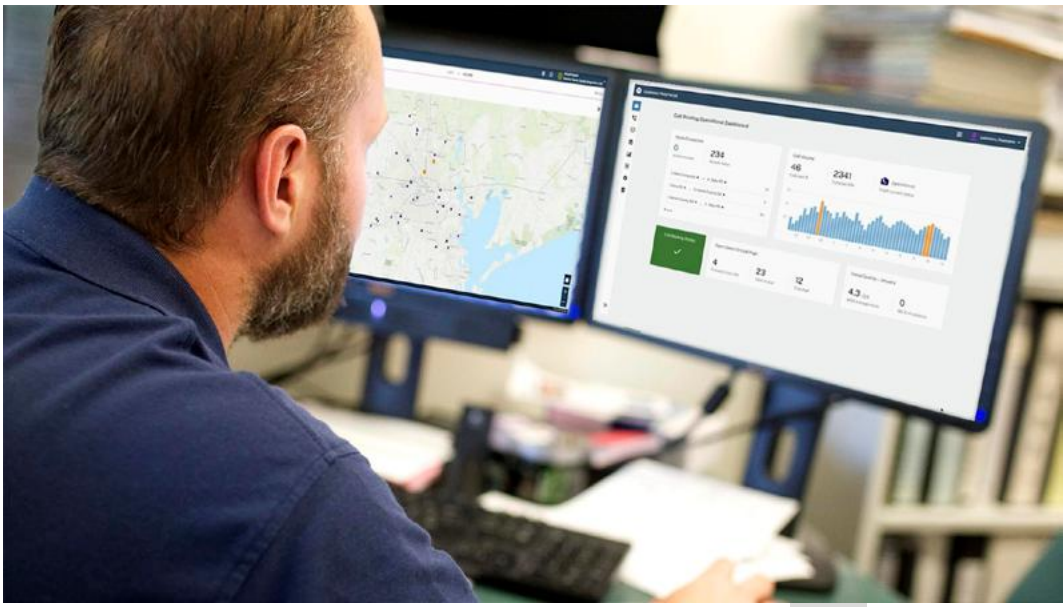
Mira el video aquí

significativamente la capacidad de respuesta y atención en situaciones críticas.

Gracias a algoritmos sofisticados, la IA tiene la capacidad de analizar rápidamente la información proporcionada por los usuarios y determinar los recursos óptimos para atender cada emergencia de acuerdo a su gravedad y en el menor tiempo posible. Esto posibilita la correcta asignación de los recursos necesarios de manera precisa y oportuna. Además, la inteligencia de la plataforma puede ofrecer instrucciones de primeros auxilios y medidas de seguridad básicas mientras se espera la llegada de los servicios de emergencia, brindando una valiosa ayuda adicional a las personas afectadas.

Otra ventaja es el uso de tecnologías de geolocalización, las cuales permiten rastrear y determinar la ubicación exacta del personal de emergencias y/o seguridad, incluso cuando este no puede proporcionar información precisa. Esta capacidad resulta especialmente importante en situaciones donde cada segundo cuenta, como en casos de secuestros, accidentes automovilísticos o eventos catastróficos. Gracias a esta tecnología, los servicios de emergencia pueden ser desplegados rápidamente y llegar al lugar correcto sin demora, aumentando así las posibilidades de salvar vidas".

¿De qué forma este tipo de plataformas basadas en número único pueden integrarse con las múltiples plataformas de comunicación las cuales no siempre permiten acceder a una llamada? (envíos de SMS, recepción de alertas masivas etc.



"La tecnología de Motorola Solutions permite a las personas que reciben las llamadas enviar y recibir no sólo llamadas de voz, sino mensajes de texto, así como imágenes, video y datos, hacia y desde las personas que llaman.

IP UserGroup® Latinoamérica

Foro Internacional de Tecnología en Seguridad

IP-in-Action LIVE SANTIAGO

EXPO SEGURIDAD & CONFERENCIAS

www.ipusergrouplatino.net

Forme parte del único Foro Tecnológico Internacional de la industria de la seguridad.

El centro para el aprendizaje y conocimiento de la seguridad física y en red.

Conéctese con la red de profesionales y grupo de compañías líderes de la industria de la seguridad.

SANTIAGO DICIEMBRE 06 2023

HOTEL PLAZA EL BOSQUE EBRO

8:30 a.m. a 5:00 p.m.

pr@ipusergrouplatino.com

PATROCINADORES

brivo · commend · EAGLE EYE NETWORKS · itecsa Your ID Solutions · Revista SEGURIDAD & DEFENSA .Online

InVid Tech Innovative Video Tecnology · MOBOTIX · SOUTHWEST MICROWAVE · VICON

INVITA

Ransomware avanzado

Estrategias básicas de defensa contra la nueva ola de ataques

Image by rawpixel.comon Freepik

En la era digital actual, el ransomware se ha convertido en una de las amenazas digitales más perniciosas y prevalentes. Este tipo de malware, que encripta los archivos del usuario y exige un rescate para su posterior recuperación, ha evolucionado de manera alarmante, adoptando tácticas cada vez más sofisticadas y destructivas. La presente columna busca explorar la evolución del ransomware, analizar sus impactos y proponer estrategias de defensa para contrarrestar esta creciente amenaza.

Desde sus inicios, el ransomware ha experimentado una transformación significativa. Los primeros ataques eran relativamente simples y se dirigían principalmente a personas. Hoy en día, los ciberdelincuentes han perfeccionado sus métodos, apuntando a organizaciones y entidades gubernamentales, causando daños multimillonarios.

Un ejemplo reciente fue el ataque al portal de Mercado Público, que dejó inutilizable la plataforma por poco más de 1 semana, lo que demuestra la capacidad de estos malwares para paralizar infraestructuras críticas.

El impacto del ransomware va más allá del costo del rescate. Las organizaciones afectadas enfrentan interrupciones operativas, pérdida de datos sensibles, daño reputacional y costos de recuperación significativos. Según Cybersecurity Ventures, se estimó que el daño global del ransomware alcanzó los 20 mil millones de dólares en 2021, subrayando la urgencia de abordar este problema.

Los ciberdelincuentes están utilizando tácticas, técnicas y procedimientos (TTPs) cada vez más sofisticados para llevar a cabo ataques de ransomware. Entre estos, se incluyen el uso de malware polimórfico, que puede cambiar su código para evitar la detección, y técnicas de evasión avanzadas que permiten al ransomware infiltrarse en redes sin ser detectado. Además, los atacantes están explotando vulnerabilidades de día cero, que son fallos de seguridad desconocidos para los desarrolladores del software afectado, permitiéndoles acceder a sistemas y datos críticos. También se ha observado un aumento en los ataques de "doble extorsión", donde los atacantes no solo cifran los datos, sino que también amenazan con publicarlos en línea si no se paga el rescate, que fue justamente lo que pasó en el ataque sufrido por IFX Networks (proveedor a cargo de la infraestructura tecnológica de Mercado Público), quienes vieron comprometidos más de 12 mil sitios de diversos países de América Latina, siendo amenazados en publicar la información en caso de no realizar el pago solicitado.

La continua innovación en TTPs por parte de los ciberdelincuentes pone de manifiesto la necesidad de una vigilancia constante y de estrategias de defensa que evolucionen al mismo ritmo que las amenazas. La inversión en inteligencia de amenazas y en tecnologías de detección y respuesta avanzadas es crucial para anticipar y contrarrestar estas tácticas emergentes.

Impacto del ransomware avanzado

El impacto del ransomware avanzado es devastador y multifacético. Más allá del pago del rescate, las organizaciones enfrentan pérdidas financieras significativas debido a la interrupción de las operaciones, los costos de recuperación y la pérdida de negocios.

La exposición de datos sensibles puede tener consecuencias legales y reputacionales a largo plazo, afectando la confianza de clientes y socios. Las estadísticas recientes revelan una tendencia alarmante: los ataques de ransomware están en aumento, y los montos de los rescates demandados están alcanzando cifras récord. La creciente sofisticación de estos ataques y su capacidad para eludir las defensas tradicionales subrayan la urgencia de abordar este problema de manera proactiva.

El alcance y la magnitud del impacto del ransomware avanzado requieren una reconsideración de cómo abordamos la ciberseguridad. La mitigación

del riesgo de ransomware no solo es una cuestión de seguridad de la información, sino también una cuestión estratégica y de gestión de riesgos empresariales que requiere la atención y el compromiso de los niveles más altos de la organización.

Estrategias de defensa

Para enfrentar el ransomware avanzado, las organizaciones deben adoptar estrategias de defensa integral. Esto incluye:

• **Implementación de soluciones de seguridad de endpoint avanzadas**: Implica instalar y configurar sistemas de seguridad especializados para proteger los dispositivos que se conectan a la red de una organización (endpoints), como computadoras y móviles, que son potenciales puntos de entrada para amenazas cibernéticas. Estas soluciones avanzadas incluyen Detección y Respuesta de Endpoint (EDR), protección contra malware avanzado, firewall de aplicación, control de aplicaciones, encriptación de datos, gestión de parches y Prevención de Pérdida de Datos (DLP). La implementación adecuada de estas tecnologías permite la identificación y respuesta rápidas a incidentes de seguridad, minimiza los riesgos de compromisos de seguridad, protege datos sensibles, y ayuda en el cumplimiento normativo, todo mientras se ajusta a las necesidades y políticas específicas de la organización. Además, la educación continua y la concienciación de los usuarios finales son cruciales para maximizar la efectividad de estas soluciones de seguridad.

• **Realización de evaluaciones de vulnerabilidades regulares**: Es un componente crucial de una estrategia de ciberseguridad robusta, consistiendo en el proceso sistemático de identificar, analizar y priorizar las vulnerabilidades presentes en los sistemas, aplicaciones y redes de una organización. Este proceso permite a las organizaciones descubrir fallos de seguridad y debilidades que podrían ser explotadas por actores maliciosos, proporcionando la oportunidad de remediar dichas vulnerabilidades antes de que puedan ser utilizadas para comprometer los sistemas. Al llevar a cabo evaluaciones de vulnerabilidades de manera regular, las organizaciones pueden mantenerse al tanto de los riesgos emergentes y adaptar sus controles y políticas de seguridad para mitigar eficazmente el riesgo de ataques cibernéticos y proteger sus activos críticos.

• **Adopción de un enfoque de seguridad en capas**: También conocido como defensa en profundidad, implica la implementación de múltiples estrategias y herramientas de seguridad en diferentes niveles y puntos de la infraestructura de TI para proteger los sistemas y datos de una organización. Este enfoque se basa en la premisa de que no existe una solución única que pueda abordar todas las amenazas y vulnerabilidades potenciales. Por lo tanto, se utilizan diversas capas de seguridad, como firewalls, antivirus, encriptación, controles de acceso y soluciones de seguridad de endpoint, trabajando de manera conjunta para proporcionar una protección robusta. Si una capa falla o es comprometida, las capas adicionales actúan como barreras de seguridad, mitigando el riesgo de exposición y compromiso de los sistemas y datos críticos de la organización.

• **Educación y la concienciación de los empleados**: Esto es fundamental, ya que los errores humanos suelen ser el eslabón más débil en la seguridad. Los programas de capacitación en ciberseguridad y las simulaciones de phishing pueden ayudar a los empleados a reconocer y responder adecuadamente a los intentos de ataque.

Además, las organizaciones deben desarrollar y mantener planes de respuesta a incidentes de ciberseguridad que incluyan procedimientos claros para la identificación, contención, erradicación, recuperación y lecciones aprendidas tras un incidente de ransomware.

A pesar de los avances en ciberseguridad, la lucha contra el ransomware sigue siendo un desafío monumental. Las soluciones actuales son insuficientes ante la rapidez con la que evolucionan estas amenazas. Es imperativo que las organizaciones, los proveedores de seguridad y los gobiernos colaboren para desarrollar estrategias de defensa innovadoras y proactivas. Los desafíos futuros incluirán la adaptación a nuevas variantes de ransomware y la anticipación a las tácticas de los atacantes.

El ransomware avanzado representa una amenaza creciente y evolutiva en el ciberespacio. La evolución de sus tácticas y técnicas requiere una respuesta igualmente evolutiva y multifacética. Es crucial que las organizaciones inviertan en educación, implementen medidas de seguridad proactivas y desarrollen estrategias de respuesta efectivas para mitigar los riesgos asociados con el ransomware. Solo mediante la innovación, la colaboración y la preparación podremos esperar contrarrestar eficazmente esta amenaza en constante cambio.

Image by kjpargeter on Freepik

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.

Cómo evitar ser víctima de la ingeniería social

Photo by cottonbro studio.pexels.com

La ingeniería social consiste en manipular a una persona para que esta realice aquello que el ingeniero social le propone. Aunque la seguridad 100% nunca está garantizada, tener conocimiento de las técnicas que utiliza el ciberdelincuente nos permitirá poder detectar antes cualquier evento sospechoso.

Phishing

Técnica de ciberdelincuencia que utiliza el engaño y el fraude para obtener información de una víctima. El ciberdelincuente utiliza un cebo fraudulento y espera a que algún usuario caiga en la trampa, para de esta manera poder obtener credenciales u otro tipo de información sensible. Se podría decir que el cibercriminal tira el cebo y espera a "pescar" (fishing en inglés) víctimas. (de ahí su nombre)

• Smishing: (SMS+ Phishing) Ataque de Phishing realizado a través de un SMS. Por lo general, el contenido del mensaje invita a pulsar en un link que lleva a una web maliciosa, en el que intentarán engañar con que la víctima introduzca información sensible o de que descargue una aplicación que en realidad es un malware. Estos SMS generalmente se hacen pasar por servicios habitualmente usados en la población, comúnmente bancos o servicios de delivery. Los usuarios ya tienen cierto nivel de concienciación con las estafas a través de email, pero no tanto con los SMS, es por eso que hay una falsa percepción de seguridad con la mensajería móvil y nos lleva a que este ataque sea más efectivo.

• Vishing: Ataque de Phishing realizado por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada, y, por ejemplo, haciéndose pasar por un servicio técnico, le pide a la víctima determinados requisitos para resolver la incidencia. Así pues, dependiendo de la estafa, intentará que la víctima revele información sensible, se instale alguna aplicación maliciosa, realice un pago, etc.

• Spear phishing: Ataque de Phishing concretamente dirigido a una víctima o conjunto de víctimas. El ataque busca los mismos propósitos que los casos citados previamente, con la variante de que están personalizados, lo cual los hace más complicados de detectar. El atacante emplea técnicas de OSINT para obtener toda la información disponible sobre la víctima, y de esta forma modelar y dirigir el ataque hacia esta. ¡Es por ello que es de vital importancia ser consciente de que información publicamos en internet sobre nosotros mismos!

• Whaling: Se trata de un ataque de Spear Phishing, dónde cuyo objetivo es un "peso pesado" de la organización. Los ciberatacantes consideran a los ejecutivos "High level" como "whales" de ahí el nombre del ataque.

Spam

Cualquier Email o mensaje recibido que no es deseado y/o solicitado. Su envío se produce de forma masiva a un gran número de direcciones. No siempre es malicioso, aunque constituye una pérdida de tiempo y un gasto de recursos innecesario. Muchas veces puede tener enlaces maliciosos o difundir información que no es verdadera.

• SPIM (Spam over Internet messaging): Spam realizado sobre mensajería instantánea, es decir, mensajes de Spam que se reciben por Whatsapp, Telegram, DM de Facebook, etc.… Suele ser más complicado de detectar que el spam "tradicional"

•Dumpster Diving: Acción de "bucear" en la basura de una organización para obtener información de documentos que iban a ser reciclados. Una buena práctica es destruirlos para evitar que el reciclaje de estos documentos sea con un uso indeseado. Hay un dicho popular que define bien esta técnica: "La basura de una persona es el tesoro de otra"

• Shoulder surfing: Acción de mirar los datos que un usuario introduce por teclado y muestra en pantalla. De una manera aparentemente "casual", el atacante puede obtener información sensible. Su nombre es muy descriptivo, ya que

hace referencia a mirar por encima del hombro (para conseguir información).

Para evitar esto existen pantallas que se oscurecen o reflejan dependiendo del ángulo de visión, permitiendo que solo se vea correctamente desde el punto de vista del usuario del sistema. Además, es una buena práctica cerciorarnos de que no hay nadie alrededor cuando trabajamos con información confidencial.

• Pharming: Redirección maliciosa hacia una web falsa que simula ser igual a la legítima, y así, de esta manera robar datos a las víctimas. Su nombre viene de la mezcla de Phishing y Farming. Este ataque suele venir prevenido de otros ataques sobre DNS, de manera que cuando se busca por el nombre de dominio, DNS traduce este nombre de dominio a una IP maliciosa de la que el atacante es dueño.

• Tailgating: Consiste en seguir a una persona, para acceder con ella a una zona de acceso restringido. Esta técnica se basa en la generosidad de las personas, ya que por cortesía se suele aguantar de la puerta a quien viene detrás. En alguna situación, el atacante puede buscar complicidad con su objetivo ofreciéndole fuego en una zona de fumadores, después por reciprocidad el objetivo le aguanta la puerta al atacante y pasarán juntos. Para evitar estos accesos indeseados es interesante un sistema de tornos (como los que se emplean en gimnasios, estaciones de tren, de metro, etc.)

• Eliciting information: La elicitación sirve para obtener información de una víctima sin preguntarle directamente. Para conseguir esto, se basa en los principios de la ingeniería social, y en diferentes técnicas de comunicación.

Algunas de estas técnicas de comunicación son: escucha activa, Preguntas reflexivas o utilizar afirmaciones falsas (Para que el objetivo corrija con la información que interesa). De esta forma, en una conversación aparentemente casual, el atacante irá "tirando de la lengua" al objetivo y conseguirá información que le puede ayudar para futuros ataques.

• Prepending: Técnica que consiste en añadir el nombre de la víctima al principio con el fin de generar mayor "rapport" con esta. Entendemos, por rapport, el fenómeno psicológico con el que 2 personas se sienten en sintonía. Ejemplos de prepending serían esos correos que en la primera línea mencionan el nombre de la víctima, o post de redes sociales en los que aparece el nickname de la víctima al principio de todo. De esta manera el atacante gana una sensación de cercanía con la víctima, al dirigir el mensaje hacia esta.

• Identity Fraud: Una usurpación de identidad es

La ingeniería social consiste en manipular a una persona para que esta realice aquello que el ingeniero social le propone. Aunque la seguridad 100% nunca está garantizada, tener conocimiento de las técnicas que utiliza el ciberdelincuente nos permitirá poder detectar antes cualquier evento sospechoso.

Phishing

Técnica de ciberdelincuencia que utiliza el engaño y el fraude para obtener información de una víctima. El ciberdelincuente utiliza un cebo fraudulento y espera a que algún usuario caiga en la trampa, para de esta manera poder obtener credenciales u otro tipo de información sensible. Se podría decir que el cibercriminal tira el cebo y espera a "pescar" (fishing en inglés) víctimas. (de ahí su nombre)

• Smishing: (SMS+ Phishing) Ataque de Phishing realizado a través de un SMS. Por lo general, el contenido del mensaje invita a pulsar en un link que lleva a una web maliciosa, en el que intentarán engañar con que la víctima introduzca información sensible o de que descargue una aplicación que en realidad es un malware. Estos SMS generalmente se hacen pasar por servicios habitualmente usados en la población, comúnmente bancos o servicios de delivery. Los usuarios ya tienen cierto nivel de concienciación con las estafas a través de email, pero no tanto con los SMS, es por eso que hay una falsa percepción de seguridad con la mensajería móvil y nos lleva a que este ataque sea más efectivo.

• Vishing: Ataque de Phishing realizado por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada, y, por ejemplo, haciéndose pasar por un servicio técnico, le pide a la víctima determinados requisitos para resolver la incidencia. Así pues, dependiendo de la estafa, intentará que la víctima revele información sensible, se instale alguna aplicación maliciosa, realice un pago, etc.

• Spear phishing: Ataque de Phishing concretamente dirigido a una víctima o conjunto de víctimas. El ataque busca los mismos propósitos que los casos citados previamente, con la variante de que están personalizados, lo cual los hace más complicados de detectar. El atacante emplea técnicas de OSINT para obtener toda la información disponible sobre la víctima, y de esta forma modelar y dirigir el ataque hacia esta. ¡Es por ello que es de vital importancia ser consciente de que información publicamos en internet sobre nosotros mismos!

• Whaling: Se trata de un ataque de Spear Phish-

Image by freepik.com

ing, dónde cuyo objetivo es un "peso pesado" de la organización. Los ciberatacantes consideran a los ejecutivos "High level" como "whales" de ahí el nombre del ataque.

Spam

Cualquier Email o mensaje recibido que no es deseado y/o solicitado. Su envío se produce de forma masiva a un gran número de direcciones. No siempre es malicioso, aunque constituye una pérdida de tiempo y un gasto de recursos innecesario. Muchas veces puede tener enlaces maliciosos o difundir información que no es verdadera.

• SPIM (Spam over Internet messaging): Spam realizado sobre mensajería instantánea, es decir, mensajes de Spam que se reciben por Whatsapp, Telegram, DM de Facebook, etc.… Suele ser más complicado de detectar que el spam "tradicional"

•Dumpster Diving: Acción de "bucear" en la basura de una organización para obtener información de documentos que iban a ser reciclados. Una buena práctica es destruirlos para evitar que el reciclaje de estos documentos sea con un uso indeseado. Hay un dicho popular que define bien esta técnica: "La basura de una persona es el tesoro de otra"

• Shoulder surfing: Acción de mirar los datos que un usuario introduce por teclado y muestra en pantalla. De una manera aparentemente "casual", el atacante puede obtener información sensible. Su nombre es muy descriptivo, ya que hace referencia a mirar por encima del hombro (para conseguir información).

Para evitar esto existen pantallas que se oscurecen o reflejan dependiendo del ángulo de visión, permitiendo que solo se vea correctamente desde el punto de vista del usuario del sistema. Además, es una buena práctica cerciorarnos de que no hay nadie alrededor cuando trabajamos con información confidencial.

• Pharming: Redirección maliciosa hacia una web falsa que simula ser igual a la legítima, y así, de esta manera robar datos a las víctimas. Su nombre viene de la mezcla de Phishing y Farming. Este ataque suele venir prevenido de otros ataques sobre DNS, de manera que cuando se busca por el nombre de dominio, DNS traduce este nombre de dominio a una IP maliciosa de la que el atacante es dueño.

• Tailgating: Consiste en seguir a una persona, para acceder con ella a una zona de acceso restringido. Esta técnica se basa en la generosidad de las personas, ya que por cortesía se suele aguantar de la puerta a quien viene detrás. En alguna situación, el atacante puede buscar complicidad con su objetivo ofreciéndole fuego en una zona de fumadores, después por reciprocidad el objetivo le aguanta la puerta al atacante y pasarán juntos. Para evitar estos accesos indeseados es interesante un sistema de tornos (como los que se emplean en gimnasios, estaciones de tren, de metro, etc.)

• Eliciting information: La elicitación sirve para obtener información de una víctima sin preguntarle directamente. Para conseguir esto, se basa en los principios de la ingeniería social, y en diferentes técnicas de comunicación.

Algunas de estas técnicas de comunicación son: escucha activa, Preguntas reflexivas o utilizar afirmaciones falsas (Para que el objetivo corrija con la información que interesa). De esta forma, en una conversación aparentemente casual, el atacante irá "tirando de la lengua" al objetivo y conseguirá información que le puede ayudar para futuros ataques.

• Prepending: Técnica que consiste en añadir el nombre de la víctima al principio con el fin de generar mayor "rapport" con esta. Entendemos, por rapport, el fenómeno psicológico con el que 2 personas se sienten en sintonía. Ejemplos de prepending serían esos correos que en la primera línea mencionan el nombre de la víctima, o post de redes sociales en los que aparece el nickname de la víctima al principio de todo. De esta manera

el atacante gana una sensación de cercanía con la víctima, al dirigir el mensaje hacia esta.

• Identity Fraud: Una usurpación de identidad es apropiarse de la identidad de otra persona generalmente con la intención de poder acceder a recursos y tener beneficios en nombre de la otra persona. Otra intención maliciosa es la de robar la identidad de otra persona para realizar malas acciones y de esta forma manchar su reputación.

• Invoice Scams: La estafa de las facturas falsas se produce cuando el atacante envía una factura fraudulenta a su objetivo, de manera que este, si no la revisa atentamente puede llegar a pagar la cantidad que se pide en la factura. En muchas ocasiones, el mensaje con el que llega la factura, avisa de las consecuencias (cortes de servicio, etc.) que podría tener no pagar de inmediato la cantidad pedida. Los atacantes emplean a su favor el miedo y el principio de la urgencia.

• Credential Harvesting: Consiste en el uso de diferentes técnicas para recopilar contraseñas y posteriormente darles un uso. Una vez que los atacantes tienen contraseñas, tendrán los mismos privilegios en los sistemas de las víctimas que estas mismas, lo que puede llevar a incrementar el impacto del ataque. Estar concienciado contra el phishing y la verificación en 2 pasos (2FA) reducirá las posibilidades de que un ataque de credential harvesting se realice con éxito.

• Reconnaissance: Obtener información sobre un objetivo, para posteriormente realizar algún ataque. Los cibercriminales recopilarán toda la información disponible sobre el objetivo, para de este modo poder personalizar y dirigir el ataque. Esta técnica se puede emplear como antesala de muchas de las otras técnicas que estamos tratando en este presente artículo. ¡Una vez más, es muy importante ser consciente de que información propia estamos haciendo pública en la red!

• Hoax: Son engaños, bulos. Son peligrosos porque intentan manipular a la víctima para que haga alguna acción en su equipo que lo deje desprotegido o incluso inservible. Estos ataques se basan una vez más en el miedo. Por ejemplo, el atacante buscará atemorizar a la víctima diciéndole que tiene un virus que le dejará inservible el equipo y que la solución pasa por hacer cambios en la configuración o borrar determinados archivos.

Suelen estar constituidos por 3 partes reconocibles:

Gancho: Sirve para captar la atención de la víctima y que lea el mensaje.

Advertencia: Enumera los peligros que hay si la víctima no reacciona o hace algo de inmediato. Juega con el miedo

Petición: Pide una acción para resolver el problema, y a mayores darle difusión al mensaje (Así el bulo sigue circulando)

• Impersonation: Hacerse pasar por alguien o decir tener un oficio que no es verdad para obtener sus ventajas. Un ejemplo podría ser la de la llamada en donde el atacante asegura formar parte de un servicio técnico, e incita a realizar acciones que aparentemente pretenden facilitar la vida a la víctima, cuando la realidad es justamente lo opuesto.

• Watering hole attack: Realizar un ataque infectando un tercero que habitualmente es utilizado por el objetivo. Después de recopilar información el atacante sabe que los empleados de la organización objetivo suelen visitar un sitio web (de un tercero).

Posteriormente el atacante infectará la página de ese tercero en cuestión, de manera que cuando las víctimas accedan a esta queden infectadas. Su nombre viene por una técnica con la que muchos depredadores del mundo animal se hacen con sus presas. Esta técnica consiste en que el depredador espera próximo al abrevadero (water hole) para lanzarse sobre la víctima cuando ésta acuda a beber.

• Typo Squatting: También conocida como URL hijacking. Técnica que consiste en utilizar un nombre de dominio muy similar al del dominio legítimo, con el fin de poder suplantarlo. Estas sutiles variaciones suelen coincidir con errores tipográficos de los usuarios. Por ejemplo, en vez de ser revistaseguridad.cl el dominio con typo squatting podría ser revistaseguridad.çl ¿Se ve? De este modo, e imitando la apariencia del sitio, un usuario podría pensar que está en el sitio legítimo y compartir información sensible en caso de que hubiera algún formulario que así lo requiriera. En este mismo blog podemos encontrar un interesante artículo para profundizar en el Typo Squatting (link)

Conclusiones

Estas son algunas de las técnicas más empleadas para realizar ataques de ingeniería social, pero sería un error pensar que los atacantes sólo utilizarán estas. Se suele decir que el mal nunca descansa y eso es completamente cierto, porque de la combinación de las técnicas vistas nacen nuevas técnicas. Además, hay que tener en cuenta que cada vez aparecen nuevas tecnologías, y por supuesto la imaginación de los cibercriminales desarrolla nuevas estafas para adaptarlas a los nuevos tiempos. Así es, cada vez surgen más engaños relacionados a las tendencias más recientes de las redes sociales, ingeniería social con criptomonedas y ya se empieza a hablar de la ingeniería social en el metaverso.

Como siempre repetimos, la seguridad 100% no está garantizada, pero con concienciación y formación se puede luchar por un mundo más ciberseguro.

Si quiere conocer más sobre seguridad informática y seguridad de la información, le invito a ingresar al site www.zentinelglobal.com donde podrá participar en mi curso de ciberseguridad básica.

Fuentes:
Google
Derechodelared.com
Alberto Fonte

Adolfo M. Gelder
@adogel
t.me/seguridadintegral
04127241188
@ritmofinsemana

¿Estás preparado para ser el futuro CRO de tu organización?

Image by Drazen Zigic on Freepik

Nuevo mundo, nuevos riesgos. A principios de este siglo, la práctica de gestionar sistemáticamente los riesgos empezaba a arraigar en las organizaciones y en casi dos décadas se había extendido considerablemente. En 2020, sin embargo, los líderes de seguridad vieron cómo sus roles cambiaron significativamente ante la pandemia de Covid-19. Se vieron obligados a actualizar planes de emergencia, evaluar nuevos riesgos, crear y supervisar procedimientos relacionados con la salud, el malestar social y mucho más. Ampliar el teletrabajo a niveles impensables y hacer frente a riesgos que antes no existían o eran insignificantes se ha vuelto imperativo.

Paralelamente, las inmensas ventanas abiertas por la inteligencia artificial han redefinido el poder de los datos en funciones cruciales de las empresas. Las fuentes de riesgo que pueden afectar la resiliencia operativa ahora incluyen nuevos servicios de TI y la migración a la nube. Los modelos de análisis predictivo pueden estar sesgados o desviarse del enfoque original de la iniciativa, exponiendo a una organización a responsabilidad legal o riesgo reputacional. Si no se maneja adecuadamente, un modelo de este tipo puede dar lugar a errores costosos, sanciones regulatorias millonarias y reacciones negativas de los consumidores con un impacto directo en la cotización de la empresa en la bolsa de valores.

Pandemia mundial de COVID-19

Debido a la pandemia, cambios que habrían tardado años en implementarse se implementaron en meses o semanas, a menudo con una planificación deficiente y una gestión de riesgos casi nula.

La mayoría de las organizaciones contaban con algunas políticas de seguridad y estrategias de capacitación antes de la pandemia. Sin embargo, pocos han establecido políticas detalladas o capacitación para establecer un espacio de trabajo remoto (oficina en casa) o pensar en otros riesgos asociados con la rápida adquisición e implementación de nuevas herramientas.

Por todo esto, la exigencia a los líderes de prácticas de riesgo ha aumentado enormemente y está exigiendo habilidades y conocimientos sin precedentes por parte del CRO (Chief Risk Officer). Las circunstancias exigen perfiles proactivos, innovadores y anticipadores.

Es esencial que el líder de riesgos aporte prácticas innovadoras, pensamiento diferenciado y un nuevo conjunto de habilidades al puesto. Se trata de un CRO con una fuerte convicción de influir en la estrategia, aportar más agilidad con la seguridad y moldear el futuro a favor de los objetivos de la organización.

"El CRO necesita una fuerte convicción para influir en la estrategia, proporcionar mayor agilidad con la seguridad y moldear el futuro a favor de los objetivos de la organización"

Hay pocos profesionales de la seguridad que gestionen los riesgos de diferentes fuentes y, además, estudien las probabilidades y visualicen los riesgos positivos antes que los competidores.

La evolución del papel del gestor de riesgos de seguridad es tan significativa que muchas empresas están sustituyendo el término "área de seguridad" por "área de inteligencia, protección empresarial, riesgos y/o resiliencia". El perfil del líder de seguridad ya ha estado cambiando rápidamente en los últimos años, y el atributo clave pospandemia es la perspicacia para los negocios.
Perspicacia para los negocios

El problema es que las capacidades de gestión de riesgos van por detrás de las necesidades y los profesionales de riesgos a menudo operan en silos separados, fortaleciendo una infraestructura que ya no se adapta a la realidad. La mayoría de las empresas parecen hacer poco ante los riesgos no financieros generados y exacerbados por las transformaciones digitales. Factores subjetivos como habilidades, mentalidades y formas

de trabajar, así como factores concretos como tecnología, infraestructura y flujo de datos, están cambiando al mismo tiempo durante esta transformación.

También es notoria la falta de patrocinio y adherencia de los ejecutivos en la priorización de las actividades de identificación y gestión de riesgos.

La generación de ingresos a corto plazo tiene prioridad, incluso cuando la pandemia pone patas arriba viejas creencias. Por ejemplo, la mayoría de las organizaciones todavía gestionan el riesgo manualmente mediante hojas de cálculo. Incluso aquellos que aplican herramientas más avanzadas no lo hacen consistentemente basándose en una política de riesgos integrada y una estrategia de gestión de riesgos.

A medida que el futuro se vuelve cada vez más sombrío, las organizaciones necesitarán anticipar y gestionar una lista de riesgos en constante expansión. Para ser eficaz, el CRO del futuro debe ser capaz de comprender las competencias centrales de la organización, cómo crean y mantienen valor, y luego explorar el futuro para comprender qué factores tienen el potencial de alterar la creación de valor. Combinará habilidades técnicas para liderar la estructura de riesgos (hardskills) con habilidades relacionales (softskills). Para el CRO los medios son los controles y el fin es el mismo que el de la empresa (objetivos estratégicos).

El CRO necesita crear y mantener valor.

La crisis generada por el Covid-19 crea nuevos riesgos y, con ellos, nuevas necesidades al más alto nivel de la organización. Aquellos que estén perfectamente posicionados para identificar riesgos que representen amenazas y oportunidades, influyendo en la estrategia de la organización en todos los niveles ejecutivos, saldrán victoriosos.

Con el talento adecuado, este CRO puede delegar la toma de decisiones tácticas de gestión de riesgos a gerentes expertos, al tiempo que realinea su enfoque hacia una gestión de riesgos más estratégica, centrándose en la asignación de capital e inversiones que aumenta el valor de la empresa. El CRO que aplique este enfoque de gestión de riesgos tendrá un impacto muy positivo en la estrategia a largo plazo y se convertirá en un líder valioso a la hora de impulsar soluciones de sostenibilidad y gobernanza, así como fusiones y adquisiciones.

"La mayoría de las organizaciones todavía gestionan el riesgo manualmente mediante hojas de cálculo. Existen software como t-Risk capaces de automatizar este proceso"

Para ello, necesita conocer la gama de riesgos existentes y emergentes. Las habilidades esenciales de este líder son: capacidad para identificar señales de ruido aún muy débiles (riesgos embrionarios), identificar riesgos en evolución, proyectar su impacto potencial y responder rápidamente a las amenazas (o aprovechar las oportunidades); y tener el coraje y las habilidades de liderazgo para influir en la gestión empresarial en cursos alternativos, muchos de los cuales pueden implicar la interrupción de ciertas prácticas comerciales existentes. Al madurar su enfoque de diálogo dentro del C level, impulsando la estrategia basada en riesgos con un amplio conocimiento de la organización, el CRO también se posiciona como un futuro CEO. Desarrollando una visión empresarial, cultivando un espíritu emprendedor, influyendo en las personas, mejorando las habilidades de liderazgo y comunicación, puede estar en una posición única para liderar de manera segura la organización hacia el futuro.

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

Un caso Real:
El doble rasero de Google con la eliminación de los enlaces reputacionales

Image: Sacha Bosshard Unplash

Recientemente, Google ha habilitado una opción para que si usas Google Saved (el servicio de Google que te permite guardar como si de marcadores del navegador se tratase, páginas para consultar más adelante), y uno o varios de los contenidos que tenías guardados han sido marcados como infractores del Copyright, te desaparezcan.

La medida puede ser más o menos ética, pero era de esperar teniendo en cuenta que ahí, Google, lo que está haciendo es cumplir la ley internacional.

Igual que está obligada a desindexar contenido que infringe su política de uso en Google buscador, y la política de moderación de contenido de cada uno de los diferentes países, también tiene todo el sentido del mundo que censure dicho contenido en el resto de sus plataformas.

Ha empezado con Google Saved, que es un servicio hasta cierto punto minoritario, pero ya me estoy viendo lo que va a ocurrir cuando aplique el mismo rasero a Google Chrome, y que de la noche a la mañana, los marcadores que tengas en tu navegador que hayan sido previamente marcados como ilegales, desaparezcan.

Va a ser simpático cómo muchísimos usuarios van a levantar el grito en el cielo.

Avisado quedas.

Pues bien, a colación de esto, que recalco que puede parecerte mejor o peor, pero es lo que hay, te quería contar una experiencia que hemos tenido recientemente con un cliente de nuestro servicio de desindexado EliminamosContenido.

Un servicio que ofrecemos desde la consultora reputacional CyberBrainers, y que tiene como objetivo tramitar todas las peticiones de borrado y desindexación de contenido que puedan considerarse difamatorias o falsas, o que vulneren alguna regulación vigente, como puede ser el caso del contenido sexual expuesto sin consentimiento explícito de ambas partes, o el que atenta a los derechos intelectuales de una obra, marca o idea.

Petición de eliminación de contenido aceptada… pero con matices

Te pongo en antecedentes.

El cliente, dueño de una editorial de libros, nos escribía hace ya unas semanas a CyberBrainers para ver qué se podía hacer con tres páginas webs (seis enlaces en total), presumiblemente subidas por el mismo usuario (se ve que el contenido es prácticamente el mismo, y por la forma de escribir, ha sido la misma persona quien lo ha subido a las tres páginas) que habían publicado un artículo poniendo a parir a la editorial, tachándola por supuesto de un fraude.

Como hacemos siempre en estos casos, revisamos la defensa que nos hacía el cliente y el contenido en sí, y nos queda claro que el cliente tiene razón.

Esas tres páginas están publicando sistemáticamente el mismo contenido con diferentes editoriales, siempre tachándolas de fraude y, mientras tanto, ofreciéndose el dueño de las páginas para ayudar a los presuntos estafados con sus servicios de redacción, corrección y publicación.

Además, pide donaciones para seguir haciendo su campaña desacreditando a todas las presuntas editoriales, según su criterio, fraudulentas, y como nos constata el cliente, tras la publicación de la pieza se puso en contacto con ellos para exigir un pago de varios cientos de dólares para eliminar dicho contenido.

Es decir, una extorsión en toda regla: Publico un contenido reputacionalmente dañino contra tu empresa, lo posiciono en Internet, y alerto a los administradores de ese negocio de que si me pagan, lo eliminaré, y aquí tan amigos.

Obviamente, el dueño del negocio se negó, y de ahí que recurriera a nuestros servicios.

Al ver motivos claros para poder tramitarlo (en caso contrario no aceptamos los encargos; de ahí que tengamos una tasa de éxito prácticamente del 100%), nos pusimos a ello.

Petición de eliminación de contenido aceptada… pero con matices

Tras el análisis inicial, recopilamos la documentación oportuna para poder ejercer las labores de representación legal en nombre del cliente, y comenzamos los trámites para pedir la elimi-

nación de dichos enlaces del buscador.

Google tiene por ley que respondernos antes de los 30 días hábiles posteriores al envío de toda la documentación, pero en este caso lo hicieron a los pocos días, dándonos la razón y avisándonos de que, en las próximas horas, eliminarían dicho contenido de dos de los enlaces que habíamos pasado.

Les respondimos cordialmente, recordándoles que había cuatro enlaces más (dos entradas, y los dos enlaces del blog donde estaban publicadas dichas entradas).

Y aquí viene lo simpático.
Para los cuatro restantes, que recuerdo, tenían exactamente el mismo contenido que los dos anteriores, Google se niega a eliminarlos argumentando que estos contenidos no vulneran la política de uso de la plataforma.

Nos quedamos a cuadros.
¿Cómo no van a vulnerar si son exactamente iguales que los dos anteriores?

Pues muy sencillo.
La única diferencia es que los dos anteriores, que según la propia Google SÍ eran un claro caso de difamación, estaban alojados en una página gratuita de WordPress.

¿Los cuatro restantes? En dos páginas, también gratuitas, de Blogger.
Es decir, en la plataforma de CMS de la propia Google.

Google favorece a sus servicios por encima de los de la competencia, incluso con las tramitaciones de eliminación de contenido por motivos legales.

Obviamente, se trata de un abuso de posición dominante por parte del gigante de las búsquedas en Internet, que intenta con ello beneficiar a sus servicios frente a los de la competencia.

Les explicamos que esto es punitivo, y que de seguir en sus trece, les llevaremos a los tribunales, y estamos en el momento de escribir esta pieza aún en espera de la respuesta final por parte de Google.

Pero, hasta que llegue el momento, me sorprende ver cómo estas compañías son capaces de defender en la misma tramitación, con el mismo caso, que un mismo contenido es o no ilegal dependiendo dónde haya sido subido: a una plataforma de la competencia, o a la suya propia.

*Si es de la competencia, entonces es un delito y debe ser eliminado.

* Si es en la suya, ya no es delito.

Máxime a sabiendas que son casos que, llevados a juicio, van a perder, al haber registros de toda la comunicación que se hizo desde nuestros abogados a los agentes de Google encargados del caso. Y que no tienen otra forma de defenderlo que la obvia: el querer favorecer los enlaces a sus servicios frente a los de la competencia.
…
En fin, que en estas estamos.

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.

El policía moderno
Un agente social, estratégico y político

Imagen: freepik.com

Para efectos de esta columna, se sugiere conocer las definiciones que nos brinda el estado del arte sobre los conceptos esbozados en el titular de esta crónica.

Al respecto, la RAE, indica que "Agente" viene del latín "agens y entis" y lo define como "persona que tiene a su cargo una agencia para gestionar asuntos ajenos o prestar determinados servicios"; "Social" por su parte viene del latín "socialis" y lo define como "perteneciente o relativo a la sociedad"; "Estratégico", en cambio viene del latín "strategicus" y significa "poseedor del arte de la estrategia, de una importancia decisiva para el desarrollo de algo"; y finalmente "Político" oriundo del latín "Politicus" y que define como "perteneciente o relativo a la actividad política, que interviene en las cosas del gobierno y negocios del Estado".

Pues bien, el 16 de febrero del año 2022, fue publicada la Ley 21.427, del Ministerio del Interior y Seguridad Pública, que Moderniza la gestión institucional y fortalece la probidad y la transparencia en las Fuerzas de Orden y Seguridad Pública.

Tal como ya publicamos hace unas ediciones atrás en Revista Seguridad Online, dicha ley contenía algunas diferencias que debieron ser subsanadas, al duplicar por ejemplo el rol preventivo y de control del orden público de Carabineros de Chile, para con la Policía de Investigaciones de Chile, produciendo con ello una modificación esencial en la Ley Orgánica de la PDI, desconociendo su rol esencialmente investigativo y otras funciones específicas que cumple actualmente la organización policial, otorgando a ambas instituciones atributos específicos en temas de prevención.

Fue así como se tramitó, promulgó y publicó la Ley 21.552 que "modificó nuevamente el DL N°2.460, de 1979, que dicta la Ley Orgánica de Policía de Investigaciones de Chile, en lo referente a su labor investigativa especializada", indicando que la Policía de Investigaciones de Chile, como parte de la Administración del Estado, está al servicio de la comunidad y sus acciones se orientarán a la investigación especializada de todos los delitos, especialmente aquellos complejos y relacionados con el crimen organizado, contribuyendo a evitar la perpetración de hechos delictuosos y de actos atentatorios contra la estabilidad de los organismos del Estado. Además, deberá efectuar el control de ingreso y egreso de personas al territorio nacional, fiscalizar la permanencia de extranjeros en el mismo y desarrollar otras funciones que le encomienden las leyes".

En concordancia con lo anterior, la Ley 21.427 incorpora el artículo 5° bis, que señala que la Policía de Investigaciones de Chile deberá elaborar, de acuerdo a las directrices emanadas de la Subsecretaría del Interior, un Plan Estratégico de Desarrollo Policial, el cual contemplará un período de ejecución de a lo menos seis años, debiendo ser evaluado y actualizado cada tres años o conforme lo ameriten las circunstancias. Este Plan y sus modificaciones deberán aprobarse por el Ministerio del interior y Seguridad Pública.

Así es como recientemente, la PDI lanzó su nuevo Plan Estratégico de Desarrollo Policial 2023-2028, cuya visión renovada es "Posicionar a la PDI al año 2033 como el referente regional en la investigación criminal de delitos de alta complejidad y crimen organizado transnacional".

Para ello, su misión institucional "investigar los delitos", ha debido dar un salto cualitativo a fin de consolidar nuevos y más robustos procesos estratégicos, sin dejar de lado los aspectos valóricos, éticos y morales que definen al policía moderno, visión ciudadana que conforme a las últimas encuestas dejan de manifiesto el reconocimiento que la comunidad tiene por la Policía de Investigaciones de Chile, al ser reconocida como una de las instituciones más cercanas y confiable del país.

Imagen: Centro de prensa PDI

Su alta rentabilidad y legitimidad social, son parte fundamental de la estrategia elaborada para esta nueva versión, los que sumados a la transparencia al servicio de la verdad y su alta valoración del conocimiento para el aporte a las políticas públicas, asoman como la punta del iceberg en este Mapa Estratégico 2023 - 2028.

La nueva propuesta en cuanto a pilares estratégicos, considera impulsar la transformación digital en los procesos institucionales; optimizar la infraestructura, equipamiento y tecnología; fortalecer permanentemente el capital humano con enfoque de género; promover una mayor colaboración y cooperación intrainstitucional.

Todo el despliegue señalado no sería fecundo si no fuera de la mano de valores éticos y morales sólidos. Es así que la institución ha asumido como elemento fundamental "el establecimiento de la ética, la probidad, los derechos humanos y enfoque de género", pues con los años han comprendido que la transparencia, la responsabilidad, la integridad y la cercanía con la comunidad son definiciones esenciales en un país donde la relación entre autoridad y sociedad deben ser complementarias.

Los valores del policía moderno orientan el comportamiento de la institución y, por lo tanto, les proporciona el marco de referencia que delimita el espacio de acción posible, determina su identidad, lo que son, y de igual forma el cómo los ve la sociedad, actuando conforme a los conocimientos y competencias profesionales que la institución les ha brindado; con probidad, primando siempre los intereses institucionales por sobre los particulares; con vocación de servicio, sirviendo siempre al bienestar de la ciudadanía como bien superior; y con integridad, mantenido siempre un comportamiento honesto, respetuoso y transparente con los derechos humanos y enfoque de género.

He aquí la importancia del policía moderno como un agente social, estratégico y político, vinculado con la ciudadanía y con las instituciones de servicio público que trabajan al alero de la seguridad interior del Estado, y como agente político al ser un actor relevante en la definición de respuestas a fenómenos mundiales como la migración, la delincuencia organizada, el cuidado del medio ambiente, y la ciberseguridad; siendo una autoridad estratégica relevante para los objetivos del Estado y de los gobiernos, contribuyendo desde su área de competencias a la idealización y promoción de políticas públicas de la nación y, a través de ellas, ser sujetos activos en la toma de decisiones.

Richard Biernay Arriagada
Ingeniero Civil Industrial,
Universidad Mayor
Relacionador Público,
Universidad Santo Tomás
Magíster, Universidad de Tarapacá

Chile requiere de un pacto en materia de política criminal

Pacto es una palabra que resuena bastante por estos días, tanto en los círculos políticos, como en los medios de comunicación. Esta palabra, para unos, constituye una estrategia del gobierno para relanzar la fallida reforma tributaria, la que embebería al proyecto de ley de una idea que otorgue la sensación de acuerdo beneficioso para todos; para los otros, corresponde a un proyecto de ley que contibuirá a disminuir la brecha social, para cuya aprobación requiere el esfuerzo de todos, dejando de lado los intereses partidistas. En cualquier caso, la sola palabra, en el contexto político, implica abandonar los intereses particulares, realizar algunas concesiones y centrarse de manera profesional en el foco del problema.

La reforma procesal penal significó un gran acuerdo, o pacto, entre los diferentes sectores políticos.

Comenzó como una iniciativa de la sociedad civil, que a los pocos años contó con el patrocinio del gobierno de la época. Es justamente su génesis lo que constituyó una novedad para aquellos tiempos, en el diseño de políticas públicas, y sin duda, la causa del éxito en las etapas legislativas.

Así, mientras la Corporación de la Promoción Universitaria se dedicaba a influir entre los sectores de la centroizquierda, poniendo énfasis en las garantías del nuevo proceso, la Fundación Paz Ciudadana hacía lo suyo entre los sectores conservadores del espectro político, subrayando en los menores plazos de investigación que conllevaría el mismo. De esta forma, ambos sectores se embarcaron en la discusión parlamentaria, sobre un paquete de proyectos de ley, que involucraba varias reformas constitucionales, gestadas por organismos fuertemente técnicos, especializados, cuyo sustento jurídico se basaba en experiencias internacionales, principios procesales y penales reconocidos, y en evidencia científica recabada.

Los sectores que en ese momento hacían parte del espectro político nacional se comprometieron en un fin, y en base a tal, desarrollaron discusiones y realizaron concesiones, en el único sentido de obtener un nuevo sistema de justicia que brindara la tan anhelada paz social, máximo propósito de cualquier sistema de justicia en un país democrático. Sin que la palabra fuera aún tan utilizada como sinónimo de "acuerdo", lo que sucedió con la llegada de los Reality Shows, las fuerzas políticas chilenas realizaron un pacto y desarrollaron la más grande de las reformas en materia de políticas públicas, la que llegó a ser conocida como "La Reforma del Siglo".

Con el garantismo consagrado en nuestro sistema judicial, comienza en la población una demanda de resultados, fruto de una creciente sensación de impunidad, la que se expresa en la necesidad de una mayor disuasión penal, una mayor protección de las víctimas frente sujetos considerados como peligrosos, y demandas de castigos más duros para los delincuentes.

En el ambiente político, lo anterior se tradujo en una serie de reformas de corte penal (cuya discusión requeriría de mucho detalle, que excede los fines de esta columna) que intentaron expresar una "mano dura", reformas que se preocuparon más por transmitir la indignación que provocaba el delito en la población, o "dar señales", que por abordar sus causas estructurales. Es así como nuestro país cae en el populismo sancionador (populismo penal o populismo punitivo), el que se transforma en el modelo de gestión y revisión del acontecer criminal, donde se brinda poca cabida a la revisión de expertos, a cifras criminológicas, a las ciencias del comportamiento, a los límites del derecho penal. De esta manera, se diluye la política criminal concebida de manera formal.

La criminología, ciencia que tiene como objetivo determinar las causas y motivos que llevan a al ser humano a delinquir, con el fin de reducir la comisión de estos hechos, debería ser siempre la fuerza motriz, o sustrato, que impulse a la política criminal a realizar las reformas pertinentes, dentro de los límites que impone el derecho penal de una sociedad democrática. Sin embargo, aquel impulso que alimentó el desarrollo y la discusión de la reforma procesal penal, se ha perdido.

Cada gobierno de turno, o grupo parlamentario, ante la sola posibilidad de dar señales de preocupación frente a un determinado problema de seguridad, se ha embarcado en la confección de políticas criminales, muchas veces sin el sustento científico ni jurídico necesario y, por ende, sin los resultados prometidos.

Photo by Ekaterina Bolovtsova, pexels.com

El diseño de la política criminal se ha apartado de esta línea científico-jurídica, y en función de la alerta creada en razón del hecho criminal, otorga las "soluciones" que requiere la masa, aplica y/o legisla la medida, en algunos casos de forma irrespetuosa con los principios del derecho penal.

Hace unos meses, fuimos testigos del intento de erradicación de vendedores ambulantes en el Paseo Ahumada de Santiago y en el Barrio Meiggs; en los noticieros observamos como una columna de tanquetas, carros lanza-agua y un gran contingente de Carabineros, avanzaban lentamente por dichos lugares, levantando las precarias instalaciones comerciales. Las autoridades nacionales y locales evocaron grandilocuentes palabras, alabándose entre ellos el éxito de las estrategias que permitieron acabar con algunos nichos de delincuencia, entre otras externalidades, que trae consigo el comercio ejercido de forma ambulante y sin control. Al poco tiempo, todos fuimos testigos de cómo ambos sectores de Santiago nuevamente se encontraban colmados por los mismos excluidos del sistema laboral, acompañados, y en algunos casos sometidos, por los abusadores delictivos de tales escenarios.

Es un hecho que, en nuestro país, aproximadamente cada 18 meses ocurre un hecho criminal que transgrede la indemnidad sexual y acaba con la vida de un menor de edad, el que, por su crudeza, adquiere ribetes de alta connotación periodística y social.

Frente a estos escabrosos hechos, tan pronto comienza la cobertura noticiosa en los medios de comunicación, se inicia la tanda de declaraciones de parlamentarios, proponiendo tal o cual reforma penal, siempre prometiendo endurecer las sanciones, e incluso, para este tipo de crueles delitos, se declinan en apoyo al retorno de la pena de muerte. ¿Acaso se acaba de cometer un delito nunca visto en Chile, que obliga al legislador a repensar una derogada pena? La respuesta es no; lo que sucede es que existen pocos eventos que provoquen más redito político que el populismo punitivo.

Existiendo en la ciudadanía un fuerte desaliento por el atroz crimen, es el momento propicio para ofertones legislativos sobre una venganza patrocinada por el estado, que alivie, al menos en parte, el deseo generalizado en la población, que el imputado "pague" por lo que hizo. A estas alturas, poco importan los cientos de artículos científicos del ámbito criminológico y penal, que demuestran el nulo efecto disuasorio que tiene en los delincuentes este tipo de penas, frente a los delitos violentos y crueles, cometidos contra menores de edad; ciertamente, las promesas de "mano dura" calan más hondo la población que una propuesta político-criminal responsable, aunque la primera sea completamente ineficaz.

Con las debidas diferencias, pero en una tónica populista, es recurrente observar comportamientos similares cuando se publicita algún crimen violento, en donde existen adolescentes imputados, cuyas edades oscilan entre 14 y 17 años.

Desde el mundo político inmediatamente surgen declaraciones donde manifiestan la posibilidad de legislar sobre brindar un trato de adultos a los adolescentes que delinquen, en cuanto a responsabilidad penal. Esta acción no sólo socaba los siglos de reflexión en los que se ha desarrollado el derecho penal, sino que también aquellos fundamentos de la psicología del desarrollo, con sustento en la neurología del desarrollo, sin cuestionarse si los adolescentes responden a estándares adultos de culpabilidad criminal, o si los adolescentes poseen las capacidades necesarias para funcionar como imputados competentes en un proceso judicial de adultos, ni mucho menos, sobre cómo se ven afectados los delincuentes juveniles por sanciones punitivas de muy larga duración.

Sin duda, las acciones y opiniones derivadas de las luchas de poderes políticos en el desarrollo de la política criminal nacional, ha menguado la importancia en eficacia criminal y en materia de garantías, que la triada criminología-política criminal-derecho penal aporta, tanto al diagnóstico del problema delictivo, como a las soluciones, muchas de las cuales no han de ser necesariamente de corte penal, sino social. La interacción de estas ciencias entre sí reviste importancia porque ponen de relieve una relación de complemento necesaria en la lucha contra el crimen, si es que se requiere que las medidas sean eficaces contra el mismo.

El desarrollo de medidas eficaces contra la delincuencia obliga a los diferentes sectores políticos, a desarrollar un esfuerzo conjunto, a mantenerse alejados de beneficios inmediatos de aprobación ciudadana y de mezquinas contiendas electorales, comprometiéndose en el desarrollo de un verdadero pacto en materia de política criminal. En tal esfuerzo es necesario aventurarse a un debate en base a evidencia empírica y fundamentos penales, especialmente aportados por las instituciones, públicas o privadas, que son especializadas en la materia criminal.

Una vez que los representantes políticos comprendan la necesidad de abandonar los exclusivos intereses partidistas, se comprometan a un proyecto político criminal con fundamentos científicos, y permitan ser asesorados por las instituciones expertas en la materia, nuestro país realizará un proyecto de reformas, con aspectos sociales y penales comprometidos con la seguridad, del que pueda sentirse orgulloso, y pueda denominar esta vez, quizás, "La Reforma del Milenio".

Cristóbal Mejías Reyes.
Bioquímico,
Pontificia Universidad Católica de Chile.
Máster en Política Criminal,
Universidad de Salamanca de España.

Terrorismo Yihadista

Una nueva amenaza global y nuevo desafío en el siglo xxi

El lunes 18 de septiembre de 2023 el jurista y criminólogo peruano Javier Gamero Kinosita, miembro de IPA Perú y actual coordinador de IPA Perú en Europa, ofreció la conferencia magistral internacional inaugural titulada "Terrorismo yihadista: una nueva amenaza global y nuevo desafío en el siglo XXI" en el marco del seminario internacional "El terror yihadista y la lucha de Europa contra él" llevado a cabo en el Castillo de Gimborn, Centro de Formación Profesional de la International Police Association (IPA) en Colonia, Alemania, organizado por las Secciones IPA de Alemania y España del 18 al 22 de septiembre de 2023. Extracto de la conferencia de Javier Gamero Kinosita

El terrorismo internacional como riesgo, amenaza y desafío global del siglo XXI

El terrorismo internacional está catalogado hoy en día como uno de los riesgos, amenazas y desafíos globales emergentes en los espacios comunes globales de la presente centuria y es considerado como el más grande reto del estado de derecho moderno. Los expertos en materia de defensa y seguridad sostienen que el neo terrorismo es la nueva forma de violencia colectiva, donde la bestia humana del siglo XXI ruge "urbi et orbi", acuñando nuevos términos, tales como el "hiper terrorismo", "super terrorismo", "mega terrorismo" o "terrorismo global".

Dentro de los riesgos y amenazas globales emergentes tenemos las armas de destrucción masiva, las armas nucleares, el crimen organizado, los conflictos militares, los conflictos armados, el espionaje, las amenazas ciber, las pandemias y el terrorismo internacional.

El profesor alemán Ulrich Beck subraya que vivimos en la denominada sociedad de riesgo, enfatizando que los riesgos globales son consustanciales con el nuevo orden mundial, ellos son reflejos normales del progreso y del desarrollo y que ya no es posible eliminarlos sino a lo más minimizarlos, agregando que ya no hay más puerto seguro y viviremos en una seguridad permanente.

El profesor alemán Hierfried Münkler de la Universidad de Humboldt en Berlín, Alemania sostiene que el terrorismo es la guerra del siglo XXI, considerándolo un conflicto de baja intensidad, se trata de una guerra asimétrica, una guerra híbrida y una guerra civil molecular subrayando la desestatización de la guerra, la individualización de la guerra, la invisibilidad del combatiente y la abstracción del enemigo.

El terrorismo posmoderno se da en un entorno híbrido impregnado de complejidad e incertidumbre en donde se combinan acciones militares y no militares, acciones convencionales y no convencionales y acciones encubiertas y no encubiertas.

La guerra contra el terror difiere de las reglas del campo de batalla del Mayor General prusiano y teórico militar Carl von Clausenwitz. Hoy nos encontramos ante formas inesperadas de violencia, una des individualización de la guerra, una desterritorialización de los conflictos, la abstracción del enemigo y el terrorista yihadista se ha convertido en el epítome del combatiente asimétrico de nuestros días.

Hacia un concepto de terrorismo posmoderno

El vocablo terrorista es muy difícil de definir, se trata de un vocablo discutible y subjetivo, pero sea cual fuese el ropaje con que se presente, ya sea político, económico, cultural, religioso, histórico, etc., será dentro de la óptica de la sociedad post 11/09 siempre liberticida y devastador.

El profesor suizo Nicolás Queloz de la Universidad de Friburgo afirma que la palabra terrorismo es hoy en día utilizada, usada, prostituida y enarbolada para todos los fines políticos a tal punto que ha provocado un efecto de saturación, añadiendo que ya no echen más agua, que el cántaro está lleno.

El Pequeño Diccionario de Ética de Paris nos ofrece la mejor definición de terrorismo, conceptualizándolo como un conjunto de medios ide-

ológicos, logísticos y técnicos puestos en escena en un medio social determinado, con el fin de ejercer una retórica de muerte, en donde se conjuga, lo exquisito de Platón y unas técnicas del crimen cada día más sofisticadas. El terrorismo es el arte de hablar bien da la muerte.

Prehistoria del terrorismo yihadista

La evolución histórica del terrorismo yihadista se remonta a la "Secta de los Zelotes" que fue una organización política y religiosa que surge en el siglo I d.C. conformada por un grupo de judíos fanáticos y radicales de origen hebreo, que arremetían contra la represión de los romanos y en los integrantes de la "Secta de los Asesinos", se trataba de una misión religiosa y ambición política en el mundo islámico en Irán y Siria contra el poder extranjero. Surgen en Irán, eran considerados los Santos del Islam y estaban focalizados en extender su doctrina chiita en Europa y arremeter contra la islamofobia.

El Islam, religión política y dictadura clerical

El Islam es una religión muy completa y muy variada, se trata de un proyecto político, no se trata de una filosofía de vida como el budismo por ejemplo, anhelando el dominio planetario, es integrista y fundamentalista y usa el terrorismo para conquistar el poder, inspirados en nacionalismos separatistas, anhelos independentistas y fines geopolíticos.

El Islam pretende recuperar y reconquistar territorios históricos como es el caso de España. En Europa el Islam político está perpetrando una serie de mini atentados orientados a la conquista del poder. El Islam es una religión política regida por el Corán, la Sunna y la tradición, el Corán cuenta con 114 capítulos y cada capítulo está conformado por "Sures" (certezas) y cada "Sure" tiene entre 3 y 100 versos, asimismo el Islam es un concepto de lucha social y priorizan la religión ante la nacionalidad, ellos son primero musulmanes y luego nacionales y anhelan la toma del poder y la mantención del mismo. El Corán y la Sunna son portadores de la verdad divina y el derecho islámico (la Sharía) debe de proveer justicia, bienestar y felicidad.

Hacia un nuevo orden político para mundial o pseudo califato

Los terroristas yihadistas se mueven inspirados en un nuevo orden político para mundial denominado por los expertos "pseudo califato" que difiere mucho del califato islámico tradicional que exhibía un pasado inmaculado con un origen impecable en un periodo de sabiduría y virtud política durante los regímenes de Abu Bakr, Omar, Uzmán e Ali, el califato originario tenía sus cimientos en la política, la religión, la economía y la ideología, y carecía de conflictos, revueltas y amenazas, para ser gobernante se exigía ausencia de defectos somáticos, capacidad de comprensión, adecuada educación, buena oratoria, amor a la verdad, desprecio a los bienes terrenales, inclinación a la justica y fortaleza de ánimo a diferencia de este nuevo universo político-religioso del pseudo califato, atestado de cambios, rupturas, quiebres, interrupciones, desplazamientos de poder y traumatismos inspirados en una prédica de violencia y odio y dictámenes dogmáticos yihadistas que están

Mónica Salinas Hofer, miembro honoraria de IPA Perú, Rene Kaufmannn, director del Castillo de Gimborn, Centro de Formación de la International Police Association (IPA) y Javier Gamero Kinosita, miembro de IPA Perú y expositor

Conferencia en Gimborn

inspirados bajo las ideologías del wahabismo, yihadismo, panislamismo, anti secularismo, anti cristianismo, anti semitismo, anti catolicismo, anti ateísmo, anti laicismo y anti occidentalismo. Los yihadistas o soldados del califato combaten hoy como actuando frente a una cámara como un actor de reparto (lestética de la violencia).

El islamismo y la yihad

El islamismo es un proyecto político dictatorial que promueve el desarrollo en grado superlativo del Islam y su imposición a la sociedad. Es una ideología de liberación y justicia, y postula un concepto del Islam universal y concibe al Islam como un modo de vida global, una lucha contra los opresores para crear una sociedad más justa. El Islam debe regular las creencias, el derecho, la educación, la economía y la familia (matrimonio, divorcio, castidad y embarazo), abarcando todos los ámbitos de la vida humana.

La yihad es una obligación divina, es considerada como una guerra contra los infieles, ella esgrime que es preferible no combatir al enemigo, sin haberle exhortado antes a abrazar la religión de Dios, a menos que este haya iniciado las hostilidades. Existe la "gran yihad" o la "yihad mayor", que exhorta a todo musulmán a ser una mejor persona, fiel a los postulados del Islam y la "pequeña yihad" que implica un esfuerzo menor, es la "Guerra Santa" que combate a los no creyentes, apóstatas e impíos. Luchan contra la corrupción moral y la decadencia moral y anhelan el regreso a las primeras interpretaciones del Corán. Volver al esplendor del pasado (velos, vestiduras tradicionales) y de dominio absoluto.

El terrorismo salafista - yihadista

La yihad fue concebida para crear un Estado Islámico, en donde se instaure un califato que esté regido por la Sharía y la tradición. Es la expresión más violenta del Islam que pretende volver al Islam estricto o Islam auténtico, esta modalidad de terrorismo pretende imponer por la fuerza y la violencia el retorno a la pureza originaria del Islam.

Salafismo proviene del término "Salaf" que significa predecesores, se refiere a los primeros musulmanes propugnando el regreso a los orígenes y a la aplicación estricta de la Sharía.

El coronel del Ejército de Tierra de España ® Pedro Baños distingue el "salafismo pacífico" del "salafismo violento" que pretende imponer el retorno a los orígenes a través del terrorismo. El Islam intenta fundir religión y política, es contraria a los cambios, en este sentido es intransigente, no se puede cambiar lo prescrito en la Sunna, los hadices y en las tradiciones trasmitidas oralmente. Los salafistas conciben el pasado como modelo

El yihadismo postula el empleo de las armas no solo para la defensa del Islam sino que adquiere una concepción ofensiva al permitir la imposición por la fuerza. Esta postura más radical se debe a los postulados del filósofo egipcio Sayyin Qubt, que afirmó en sus últimos días que la guerra ofensiva es completamente legítima si su objetivo principal es defender los verdaderos derechos de los musulmanes y liberarlos de la opresión de Occidente.

Gilles Kepel, profesor francés del Instituto de Estudios Políticos de Paris sostiene que el politólogo carismático Qubt es el ideólogo de la propagación del Islam por medio del sable, propugnando una sociedad islámica libre de corrupción, de la tiranía y la dominación foránea. Qubt estaba convencido de la superioridad del Islam y que solo este podía salvar al mundo de todos los males de Occidente.

Una nación islámica tenía la obligación de aniquilar todos los regímenes de la faz de la tierra e imponer una lucha sin tregua contra todos los enemigos del Islam para así poder extenderse a toda la humanidad. Todo musulmán tiene un deber hacia Dios y de defender la religión con las armas. Todos los musulmanes deben de apoyar a los combatientes.

El wahabismo

Es una corriente política religiosa que se destaca por su rigorismo en la aplicación de la Sharía y está inspirada por fuertes valores sociales, es equiparada a un comunismo creyente que propugna

una sociedad sin naciones, sin clases sociales, sin razas. Los wahabitas interpretan directamente las palabras del profeta Mahoma. La teología wahabí es puritana y legalista en materias de fe y prácticas religiosas. Los seguidores del wahabismo ven su rol como los defensores del Islam, así como ven la necesidad de restaurar la pureza de un Islam contaminado por desviaciones, herejías e idolatría que van en contra de la tradición islámica.

Suicidas yihadistas

Se consideran una arma de guerra, altruistas que sirven a una causa infinitamente superior a su propia vida o la de otras personas. Sus objetivos son la espectacularidad, la expectación, la amplificación mediática, generar angustia máxima y demostración de una voluntad absoluta.

Los terroristas yihadistas actúan como reacción frente a la opresión de Occidente, sienten responder con sus actos a la humillación impuesta por Occidente, evitando de este modo la vergüenza y preservar el honor, protegiendo así al Islam frente al insulto, rechazando así los valores occidentales que amenazan la identidad musulmana y generan caos moral en la sociedad islámica.

Wolfgang Schmidbauer en su obra "Psicología del terror," distingue los rasgos constantes en terroristas yihadistas tales como la venganza, la grandiosidad, la fascinación de lo apocalíptico, la psicología de la explosión, el fanatismo, la purificación de la vida a través de la muerte, el misticismo del sangrado, la cobardía, bizarría y arrojo y la búsqueda desasosegada e interminables de los jóvenes. Esta modalidad de actuación tiene como inconveniente que es de uso único y genera pérdida de combatientes. Ellos cumplen con un deber religioso bajo la promesa del paraíso, ahora y en el más allá, donde tendrán la oportunidad de una vida mejor.

Promesas a las mujeres suicidas

A las mujeres les prometen un papel destacado en la nueva sociedad en donde serán las esposas de los combatientes, madres de la próxima generación y trabajo en la sanidad y la educación, asimismo que pertenecerán a un grupo con igualdad absoluta entre sus miembros y que vivirán en una sociedad sin discriminación, así mismo tendrán garantía de seguridad, honor y dignidad, incluso para las viudas y que vivirán bajo un sentido de hermandad en la poligamia, en donde hasta 4 hermanas compartirán en armonía un mismo hombre. Asimismo se les promete a las mujeres un romance apasionado, en donde los jóvenes verdaderos creyentes son bellos y fuertes, el matrimonio les proporcionará estatus y las viudas de los mártires serán respetadas.

Reflexiones finales

Debe comprenderse que la mera represión policial y judicial y el fanatismo dificultará los resultados, pues las ideas no se pueden encerrar, debemos comprender que estamos frente a una ideología no se puede disparar a una idea, sino que una idea debe de ser combatida con una idea mejor siendo necesario para ello respetar los derechos humanos y los principios democráticos del estado de derecho, que el Occidente secularizado predica "urbi et orbi", de lo contrario perdería credibilidad, sin credibilidad no habrá legitimidad y sin legitimidad no habrá éxito.

Es necesario evitar la radicalización y fomentar la desradicalización, esto se debe hacer con políticas sociales y medidas psicológicas. Franz de Liszt solía decir, que "la mejor política criminal es la política social", para ello hay que adelantarse a los hechos y superar el proselitismo terrorista con contra - narrativas y con portavoces válidos, usando adecuadamente los medios de comunicación para relajar la tensión, evitando declaraciones desafortunadas y el sensacionalismo y en la medida de lo posible, a través de ciertas acciones psicológicas ofrecer una sensación de victoria.

De igual forma es necesario comprender las causas raíz motivadores de la acción terrorista (nacionalismo, revolución, separatismo, insurgencia, opresión, sectarismo, invasión militar, económica y cultural, religión…). Finalmente, se debe diferenciar el Islam del islamismo, el yihadismo y el terrorismo y debemos de comprender la verdadera y compleja dimensión de este extenso proyecto político religioso, pues el Islam es "ideología y fe", "patria y nacionalidad", "religión y estado" y "libro y espada".

Expositores Javier Gamero Kinosita, miembor de IPA Perú & Pedro Baños coronel del Ejército de Tierra de España (r) director del Instituto Geoestratega de España

Autor: Javier Gamero Kinosita/ Coordinador de IPA Perú en Europa & Miembro del Comité Científico de INISEG en España

SeguridadExpo 7 al 9 de Noviembre, Santiago Chile

Del 07 al 09 de novimbre en la ciudad de Santiago se realizará Seguridad Expo 2023, la feria comercial líder integral de seguridad convergente en Chile para Latinoamérica.

SeguridadExpo se consolida como el punto de encuentro de la industria de la seguridad nacional e internacional reuniendo en un solo lugar la oferta y demanda de este importante sector. En Seguridad Expo, tendrá la oportunidad de establecer contactos y conectarse con miles de profesionales de seguridad y protección pública, aprender del dinámico programa del congreso "Summit Seguridad Futuro", además de explorar las últimas tecnologías en control de acceso, alarmas , monitoreo y videovigilancia, mientras descubre tendencias emergentes en drones y robótica, ciberseguridad e IoT conectado, seguridad laboral, vial, ciudades inteligentes y más.

Safety and Health at Work 27 al 30 Noviembre 2023, Sydney Australia

Esta conferencia internacional es su oportunidad de reunirse y conectarse con líderes mundiales en seguridad y prevención de daños de más de 120 países. Escuchará nuevas ideas sobre salud y seguridad en el trabajo, obtendrá información sobre las últimas investigaciones y descubrirá soluciones innovadoras para su lugar de trabajo mientras crea alianzas y asociaciones estratégicas para promover la salud y la seguridad en el trabajo.

Proporciona un foro para el intercambio de conocimientos, mejores prácticas y experiencias para promover el trabajo seguro y saludable para todos.

MILIPOL Paris 14 al 17 de Noviembre 2023, París Francia

El evento se organiza cada dos años bajo los auspicios del Ministerio del Interior francés en colaboración con varios organismos gubernamentales. Su primera edición se ha celebrado en 1984, una época en la que los sistemas de información estaban en pañales; ¡cuando la videovigilancia apenas comenzaba a surgir y cuando el RAID (fuerzas especiales de élite francesas) aún no se había creado (sólo un año después)!

Desde hace casi 40 años, Milipol Paris disfruta de un estatus mundial como el principal evento dedicado a la profesión de la seguridad. Proporciona el foro perfecto para presentar las últimas innovaciones tecnológicas en el área, satisfaciendo eficazmente las necesidades del sector en su conjunto y también abordando las amenazas y peligros actuales.

Cyber Security & Cluod EXPO 30 Noviembre al 1 Diciembre, Londres

Únase a nosotros en Olympia Londres, Reino Unido, del 30 de noviembre al 1 de diciembre de 2023 para escuchar a los principales expertos en ciberseguridad y descubrir estrategias clave para que sus esfuerzos digitales sean un éxito. Explore las tecnologías y enfoques críticos necesarios para mejorar la participación del cliente e impulsar la cultura digital de su organización.

Esta conferencia es parte de TechEx Events , que consta de otros 5 eventos compartidos que exploran AI y Big Data, IoT, Blockchain, Transformación digital y Edge Computing, para que pueda aprender una variedad de soluciones tecnológicas empresariales clave, todo en un solo lugar.

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

¡ÚLTIMOS ESPACIOS DISPONIBLES!

SEGURIDADEXPO

by Fisa | CHILE

7 - 9 NOV. 2023

METROPOLITAN

REGISTRA TU VISITA AQUÍ

MÁS INFO EN

VISITANTES@SEGURIDADEXPO.C

- Exhibición y Congreso Internacional de seguridad integral
- Seguridad pública, privada y ciberseguridad
- Control del fuego, emergencias y desastres
- Seguridad industrial, laboral y bioseguridad

Participa como expositor ¡Contáctanos!: info@seguridadexpo.cl +56 9 4481 6922

PATROCINAN

Carabineros de Chile · Bomberos Chile · FAMAE · CPSEG Chile · ACHM · DGAC Chile · alog chile · AGACECH · Centros Comerciales de Chile

GL events

@seguridadexpo

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

www.seguridadexpo.cl

ORGANIZA Y PRODUCE

Fisa GL events Group