Año 7 Nº 49 Noviembre- Diciembre de 2023

Revista SEGURIDAD .Online & DEFENSA

LA PRINCIPAL PLATAFORMA DE INFORMACIÓN DE SEGURIDAD EN LATINOAMÉRICA

MIGRACIÓN IRREGULAR
Un nuevo desafío para la politica de seguridad del siglo XXI

CONTROL DE ACCESO
Su importancia en los juegos panamericanos de Chile 2023

Tendencias de Ciberseguridad para hisponoamérica en 2024

REDSEG

RED LATINOAMERICANA DE EMPRESAS Y PROFESIONALES EN SEGURIDAD TECNOLÓGICA

REGÍSTRESE, ES GRATIS.

www.redseg.org

SOLICITE SU MEMBRESÍA OFICIAL

planes.redseg.org

PATROCINANTES OFICIALES

Revista SEGURIDAD

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

GRUPO RAM´S
Seguridad Integral

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

EDITORIAL

Nº49 Noviembre - Diciembre 2023

Hora de balances

Estamos finalizando el año 2023 con cifras históricas en materia de percepción de inseguridad, a lo que se suma un preocupante incremento en las cifras de homicidios.

Si nos enfocamos en el año 2024, podemos concluir que las esperanzas y las expectativas están cifradas en la posibilidad de que las actuales autoridades implementen medidas efectivas, para lograr mayores niveles de disuasión para quienes cometen delitos. La temática de la seguridad debe ser considerada como una urgencia social, dejando de lado cualquier consideración de tipo política.

Somos testigos de décadas de intentos por entender y abordar la Genesis de este problema, sin embargo, como ciudadanos, seguimos incrementando nuestra sensación de inseguridad, asumiendo por primera vez la difícil decisión de cambiar nuestros hábitos y horarios de desplazamiento por temor a ser víctimas de la delincuencia.

Este próximo año 2024 veremos cómo se materializa la nueva institucionalidad en materia de seguridad privada, la cual esperamos resulte efectiva, dinámica y menos burocrática; asimismo deberemos analizar aspectos tan relevantes como son las atribuciones del personal de seguridad privada, quienes sin contar con elementos de retención adecuados no pueden incrementar de forma segura su nivel de cooperación con la autoridad, para lo anterior debemos abrirnos a la incorporación de sistemas de retención remota, ya disponibles en nuestro país.

Finalmente quiero compartir mis deseos de paz, prosperidad y seguridad para todos y cada uno de los habitantes de nuestro querido Chile.

Robert Gutter Boim
Director

CONTENIDO

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

AÑO 7 N° 49 Edición Noviembre-Diciembre 2023

Revista Seguridad & Defensa es una edición de
Producciones Gótica Ltda.

Revista Seguridad & Defensa
Director: Robert Gutter Boim
Dirección Creativa: Gótica Ltda
Foto portada: Image by freepik.com
Ventas de Publicidad: +56 9 98246696
revistaseguridadonline@gmail.com - ventas@revistaseguridad.cl

Tendencias de ciberseguridad para hispanoamérica en 2024

Foto de Mikhail Nilov: .pexels.com

Distintos actores y especialistas analizan ad portas del cierre del año, las tendencias en ciberseguridad que tendrán impacto en el escenario regional en 2024, sin lugar a dudas, un año que será desafiante para la seguridad informática.

Hispanoamérica durante 2023 se ha convertido en un paisaje vertiginoso en cuanto a seguridad informática se refiere, en una región donde los ciberdelitos crecieron en un 40% donde, hubo una subida en casos de fraude de línea, usurpación de identidad y secuestro de datos.

A nivel global, el cambiante panorama del cibercrimen y el comportamiento de los ciberdelincuentes se grafica con datos duros como el malware, que ascendió un 2% en total, con aumentos del malware de IoT (+87%) y el cryptojacking (+43%). Los sectores de la educación (+157%), las finanzas (+86%) y el comercio minorista (+50%), los más afectados por el malware. En Ucrania se han registrado niveles récord de malware (25,6 millones) y ransomware (7,1 millones). Con 33.000 millones de cuentas serán violadas este año. El 80 % de los delitos cibernéticos denunciados generalmente se atribuyen a ataques de phishing en el sector de la tecnología. Con un 16%, fue la segunda razón más común de filtraciones de datos y la más costosa, con un promedio de US$4,91 millones de dólares en costos de filtraciones. En resumen, el costo global total en pérdidas por ciberataques en 2023 fue de 8 billones de dólares, dos billones más de lo que causó en 2022.

Ergo, el próximo será un año tremendamente desafiante. Así como la tecnología avanza, también lo hacen las amenazas cibernéticas, lo que exigirá respuestas estratégicas para proteger la integridad de datos y sistemas y, así es como el panorama que se nos presenta se puede esbozar de la siguiente manera:

Impacto de las IA en la ciberseguridad

Con el avance de ChatGPT y otras aplicaciones que incorporan tecnologías de IA generativa, se abre una ventana de oportunidad para fortalecer la ciberseguridad. Otro aspecto positivo es que la implementación de modelos de lenguaje avanzados podrían potenciar elocuentemente la capacidad de la ciberseguridad: la IA permitiría mejorar la detección de amenazas, mediante sistemas que aprendan patrones de comportamiento y logren identificar anomalías de forma más precisa.

Sin embargo, la inteligencia artificial (IA) no es sólo una herramienta para la defensa de la ciberseguridad, sino también un arma potencial en manos de los ciberdelincuentes para desatar ataques basados en ingeniería social aún más sofisticados a los ya conocidos hasta hoy. Con los algoritmos de IA generativa se ha demostrado lo sencillo que puede ser generar correos electrónicos, mensajes o llamadas automatizadas que imiten de manera convincente a usuarios legítimos, por lo que se podría esperar para 2024 un incremento en este tipo de ataques aprovechando algoritmos de aprendizaje automático para eludir las medidas de seguridad tradicionales, identificar vulnerabilidades y lanzar ataques más selectivos y adaptables.

Crecimiento de los ataques a la cadena de suministros en Hispanoamérica

Los ataques a la cadena de suministro han sufrido un crecimiento exponencial en los últimos años y representan una amenaza en crecimiento también para Hispanoamérica. Este perfeccionamiento en la estrategia de los atacantes podría permitirles dirigirse de manera más específica a eslabones críticos de la cadena de suministros, interrumpiendo operaciones vitales en países de la región si no se implementan medidas de protección adecuadas.

Implementar medidas preventivas se tornan muy necesarias y se vuelven imperativas a lo largo de toda la cadena de suministro en la región, des-

Foto: pexels.com

de las grandes corporaciones hasta los proveedores más pequeños. La adopción de prácticas y tecnologías de seguridad sólidas en cada etapa se vuelve esencial para fortalecer la resiliencia frente a posibles ataques.

Asimismo, las compañías deberán verificar la seguridad de sus proveedores de servicios tecnológicos, especialmente en aquellas asociadas con infraestructuras críticas en Hispanoamérica. Concentrarse en consolidar la confianza en toda la cadena de suministro, reconocer la interdependencia entre cada eslabón y proteger la integridad del sistema en su conjunto.

Dicho enfoque se convierte en un elemento clave para salvaguardar la continuidad y seguridad de las operaciones en la región frente a las complejidades y riesgos asociados con los ataques a la cadena de suministro.

Evolución de los Troyanos bancarios en Hispanoamérica

Las mutaciones vistas durante 2023 en la forma de propagarse, y el diseño de los troyanos bancarios nos hacen pensar que este tipo de amenazas seguirán vigentes y evolucionarán aún más en 2024. Se espera una mayor sofisticación en técnicas de evasión, como el uso de técnicas de camuflaje y la exploración de vulnerabilidades específicas de la región.

Bajo este prisma, la ciberseguridad enfrenta la tarea crucial no solamente de verse obligada a reaccionar, sino también a prevenir. La capacitación continua de los usuarios se vuelve esencial para fortalecer la primera línea de defensa, contra los troyanos bancarios.

Fomentar la conciencia sobre prácticas seguras en línea y la identificación de posibles riesgos son elementos fundamentales para empoderar a los usuarios y reducir la efectividad de los ataques.

Amenaza Deepfake

La tecnología Deepfake amplifica aún más el daño potencial causado por los ataques de phishing impulsados por IA. Con las falsificaciones profundas, los atacantes pueden crear contenidos de audio y vídeo realistas que suplantan la identidad de personas u organizaciones. Esta técnica de manipulación puede engañar incluso a los individuos más vigilantes, erosionando la confianza y facilitando el éxito de los intentos de phishing.

Cibercrimen en aplicaciones de mensajería: de la oscuridad a la superficie

Para el nuevo año que pronto inicia, se espera que la monitorización de actividades sospechosas se intensifique en aplicaciones de mensajería como Telegram y plataformas similares, ya que el cibercrimen ha ampliado su alcance desde la dark web hasta aplicaciones de mensajería de uso generalizado. Esta expansión subraya la necesidad de ajustar las estrategias de seguridad para abordar el dinámico panorama del cibercrimen.

El principal reto radicará en encontrar un enfoque que logre armonizar la seguridad digital con la preservación de la li-

bertad individual y la protección de los datos. La búsqueda de este equilibrio se convierte en un elemento central para las estrategias de ciberseguridad, donde se busca garantizar la protección contra amenazas cibernéticas emergentes sin comprometer la privacidad y libertad de los usuarios.

Seguridad de confianza cero

La Seguridad de Confianza Cero es un enfoque estratégico que no confía automáticamente en nada dentro o fuera de la red de una organización. En su lugar, exige la verificación de cada persona y dispositivo que intente acceder a los recursos de la red, independientemente de si se encuentran dentro o fuera del perímetro de la red.

Con el aumento del trabajo a distancia, los servicios basados en la nube y las ciberamenazas, las medidas de seguridad tradicionales centradas en proteger el perímetro de la red ya no son suficientes. Es probable que las empresas adopten un enfoque de confianza cero para proteger sus redes, aplicaciones y datos, minimizando el riesgo de acceso no autorizado.

El Malware como Commodity y su uso en campañas de espionaje en la región

En los últimos meses, se ha observado un aumento significativo de campañas maliciosas que emplean commodity malware en la región, principalmente el uso de amenazas tipo RAT (Troyanos de Acceso Remoto) y el troyano bancario Qakbot (Qbot), otra de las amenazas que es un sustractor de información, que se propaga por la descarga de archivos de tipo Excel para robar contraseñas, los número de usuario y las tarjetas, ambos con el objetivo de obtener información valiosa y generar beneficios económicos.

En este contexto, las estrategias de seguridad se ven desafiadas a ir más allá de simplemente contar con tecnologías para identificar amenazas conocidas.

Se requiere una capacidad extendida para ampliar la visibilidad sobre comportamientos sospechosos que puedan indicar posibles intrusiones en un sistema. La adaptabilidad y la capacidad de aprendizaje de los equipos de seguridad emergen como elementos cruciales para mantenerse a la par de la continua evolución de los cibercriminales.

Conclusión

Mientras navegamos por las complejidades del panorama digital en 2024, la clave de la resiliencia de la ciberseguridad reside en mantenerse informado y proactivo. La preparación y la defensa proactiva son clave para contrarrestar estas amenazas emergentes.


Image by Gerd Altmann on Pixabay.com

Igualmente, estas proyecciones destacan la necesidad de una ciberseguridad dinámica y adaptable. La colaboración entre diversos actores, la implementación de tecnologías de seguridad y la concienciación continua serán esenciales para hacer frente a los desafíos emergentes en el panorama de la seguridad informática en 2024.

Así y todo, el objetivo para el 2024 debe tender a crear una seguridad de extremo a extremo para proteger toda la cadena de valor de las compañías, y luchar por alcanzar la excelencia en la ciberseguridad.

Autor: Javier Vargas Guarategúa
CEO & Founder de Vulcano Cybre Threat Hunters

TOME LA ACCIÓN SIN UTILIZAR LA FUERZA

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

BOLA WRAP 150

REMOTE RESTRAINT

TOP SECURITY

NICHIEI INTERNATIONAL INCORPORATED

www.bolawrap.cl • info@top-sec.org

Las razones de la masacre que sorprendió a Israel el 7/10

Ser prisionero del sistema y estar cegado por el aura de que los sistemas tecnológicos del ejército israelí, derrotarán la determinación de las amenazas.

Cual razón está en primer lugar, y porque estuvimos muy dormidos en la frontera, aquí hay una visión más de seguridad filosófica pensando en las razones y soluciones que no funcionaron, y cómo se puede mejorar para la próxima vez.

Suposiciones erróneas Los jefes del ejército israelí, SHabbak, Mossad y su círculo de asociados estaban ocupados con las cosas equivocadas, no estaban ocupados con el corazón de sus acciones, creían en la debilidad interna de Hamás y seguían el pensamiento de que la organización terrorista es interesado en la paz y el dinero.

Además, el ejército eliminó de sus filas a bastantes oficiales talentosos que se destacaban en el campo de batalla debido a desacuerdos sobre sus opiniones políticas.

La falta de experiencia y participación y la arrogancia de los nuevos comandantes, llamémoslo así, fue culpa nuestra.

Hubo incapacidad para aprender de los errores del pasado, ignorando por completo las condiciones sobre el terreno, eligiendo sistemas que no se adaptan al terreno, falta de planificación y mala gestión.

¿Primero sabemos que NO se realizó ningún verdadero análisis en términos de validez si Hamas, pueden ganarnos y paralizarnos en un ataque grande como el que fue, también nadie realizó un análisis bajo la óptica de los atacantes, ¿Casi nadie pensaba diferente de los altos oficiales del ejército, e incluso si pensaban lo contrario, fueron descartados desde el nivel de ideas y durante todo el camino con la afirmación de que el Norte y Hezbolá son más que el país?

La pregunta obvia es: ¿quiénes se preparan con anticipación para una situación de emergencia, siempre evitan sufrir víctimas?

Hay un atacante oculto que camina entre nosotros y está precisamente del lado de nuestros defensores.

Este enemigo que es del peor tipo, que nos ataca en todos los niveles de mando, este enemigo es "el fenómeno de la normalización, ¿estará bien, o estoy seguro de que pase lo que pase, ¿quién se atreverá a atacarme y más y más?" Es más, este es el fenómeno generalizado y por supuesto invisible... en cualquier momento un acontecimiento podría causar daños catastróficos e irreversibles.

Un enemigo invisible que existe dentro de nosotros, es un adversario que ataca a través de la emoción y que le allana el camino para encontrar un resquicio que le permita alcanzar su objetivo.

Entendieron bien, estoy hablando de un oponente que trabaja en el lado defensivo y en ocasiones es incontrolable y provoca que se realicen acciones destructivas.

Tanto el defensor como el atacante, ambos seres humanos de carne y hueso, tienen sentimientos relacionados con lo que han pasado en sus vidas y actúan en consecuencia.

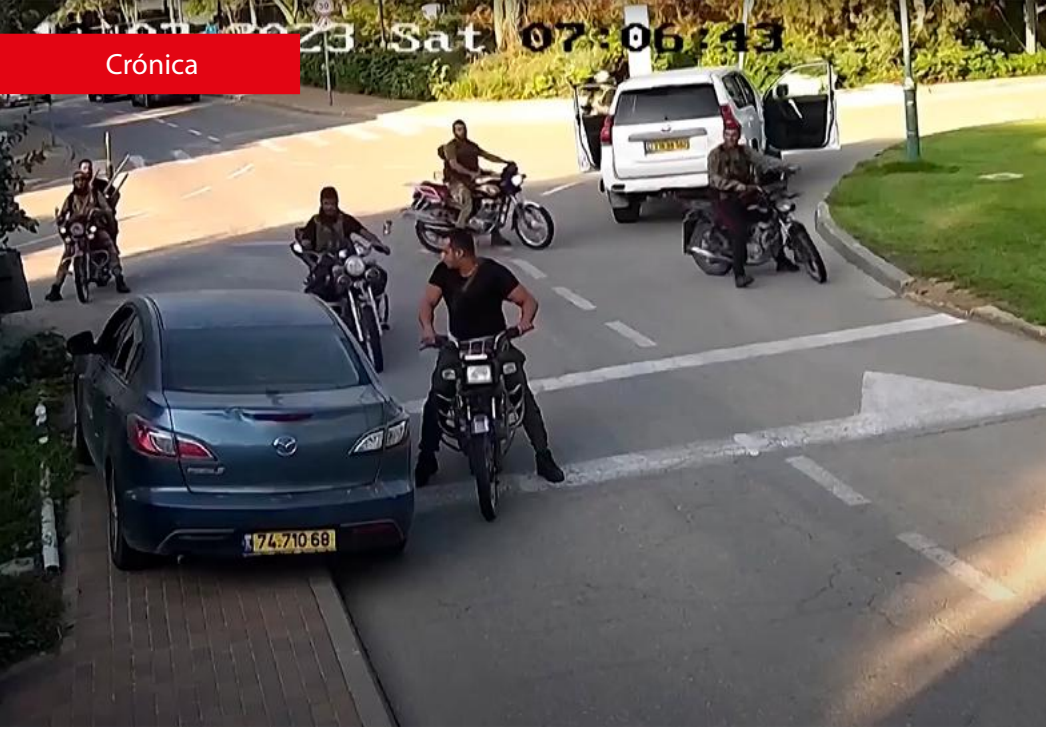
Ambos reaccionan a los fenómenos que suceden a su alrededor. Entonces, ¿quién es realmente el adversario oculto?

El atacante oculto está implantado en nuestra naturaleza como humanos y aparece de manera diferente sin diferenciar entre la organización responsable, los puestos directivos y el nivel real de operación.

El enemigo oculto es nuestra incapacidad para resistir la tentación de realizar una acción innecesaria en el momento equivocado.

El enemigo oculto es a veces nuestro impulso de actuar en contra de las reglas mientras ocultamos la verdad.

El enemigo oculto es nuestra actitud poco seria hacia nosotros mismos y hacia el trabajo que hemos elegido realizar.



El enemigo oculto es nuestra capacidad de "quedarnos estancados" en un lugar en el que claramente no encajamos con nuestro carácter.

El enemigo oculto es nuestra terquedad que provoca falta de escucha y fijación.

El oponente oculto es colocar a una persona en una posición por razones que no son puramente profesionales.

El enemigo oculto es rodearnos de directivos que piensan exactamente como nosotros (Yes man).

El enemigo oculto es nuestro deseo de desempeñar un papel sin tomar decisiones.

El enemigo oculto es nuestro deseo de pasar el tiempo ignorando por completo el terreno.

Después de la introducción, Solo sabíamos que estaban entrenando, conocíamos sus sistemas de entrenamiento, las bases y métodos de entrenamiento y la teoría de la lucha.

¿Cómo no funcionó nuestra preparación para emergencias y por qué no respondimos tras tantas horas después del evento?

Durante años, los jefes de las instituciones de defensa y del ejército no escucharon las duras críticas, ni siquiera desde dentro del ejército, adormecieron durante años todo el sistema, el sistema de ataque, no el sistema de defensa, que destacó durante el período con la postura de hierro contra los misiles, pero obviamente esta no es la respuesta, la respuesta era entender dónde nos pondrá a prueba el atacante, y cuáles son nuestras ideas, no sólo para detenerlo más tarde, sino para alcanzarlo mucho antes de cualquier ataque.

El hecho de que en algunos casos, aunque hayamos sido formados de antemano para afrontar situaciones de emergencia, existe, por supuesto, la posibilidad, por ejemplo, de que no podamos evitar un robo, pero esto no indica que vale la pena renunciar a la preparación previa.

La preparación para la respuesta a emergencias es necesaria en todos los niveles, desde el nivel del ciudadano individual hasta el nivel de una organización pública o privada, por la razón más clara y simple de que tomar acciones preventivas o frustrantes, puede prevenir completamente el daño o minimizar su alcance del daño.

La preparación temprana es muy importante, es la base de todo, porque cuando nos encontramos con situaciones de emergencia no tenemos tiempo para aprender y experimentar, y en respuesta debemos actuar instintivamente ante lo que sucede ante nuestros ojos.

Para que sepamos actuar según el instinto, debemos prepararnos y entrenarnos con antelación para diversos escenarios de emergencia que nos pueden suceder por diversos motivos.

Las emergencias pueden comenzar repentinamente, sin previo aviso, lo que significa que debemos estar preparados en cualquier momento dado y cuanto más hagamos en la fase de prevención, es decir, en la fase de preparación temprana y entendiendo la amenaza y encontrando la respuesta, es decir, la solución, mayores serán las posibilidades de que salgamos exitosamente de la situación de emergencia.

Podemos distinguir y aprender del comportamiento de los empleados de uno de los bancos más grandes de Estados Unidos, durante los dos ataques del 11 de septiembre de 2001 que los salvaron de uno de los mayores acontecimientos de emergencia. Las oficinas del banco estaban ubicadas en la torre sur. Los responsables de seguridad del banco se aseguraron de formar a todos los empleados sobre cómo evacuar la torre en caso de emergencia.

La torre norte fue atacada primero y la torre sur poco después. Los empleados del banco evacuaron escaleras abajo, cuando se dieron cuenta de que la torre norte estaba dañada.

Actuaron automáticamente de acuerdo con lo que recordaban de los simulacros de evacuación que les dieron los agentes de seguridad y no esperaron a que alguien viniera y les dijera que evacuaran.

El recuerdo les enseñó a clasificar el evento como una emergencia y los envió corriendo escaleras abajo y fuera de la torre, antes de que el segundo avión impactara la torre sur.

Surge la pregunta de qué debemos hacer para

prepararnos para situaciones de emergencia dentro de las fronteras del país:

En mi enfoque, todo comienza con escribir una teoría que funcione ordenadamente, creyendo que el adversario es capaz, pensando como el adversario, contrarrestando cualquier idea del adversario en capas de defensa que formarán, por ejemplo, la base de una atacar, y sobre todo creer que el adversario puede, a raíz de esto debemos redactar procedimientos para cada acción que se realice.

Hay que definir las amenazas relevantes: estos son los escenarios que podrían causarnos daño.

Debemos clasificar las amenazas según el nivel de daño para poder orientar mejor nuestros recursos. Se deben establecer e implementar contramedidas para todas las amenazas relevantes.

Incluyendo a quienes viven cerca de áreas de fricción, a nivel personal y familiar, es necesario asegurarse de que todos los miembros de la familia conozcan las definiciones y acciones requeridas en caso de una emergencia.

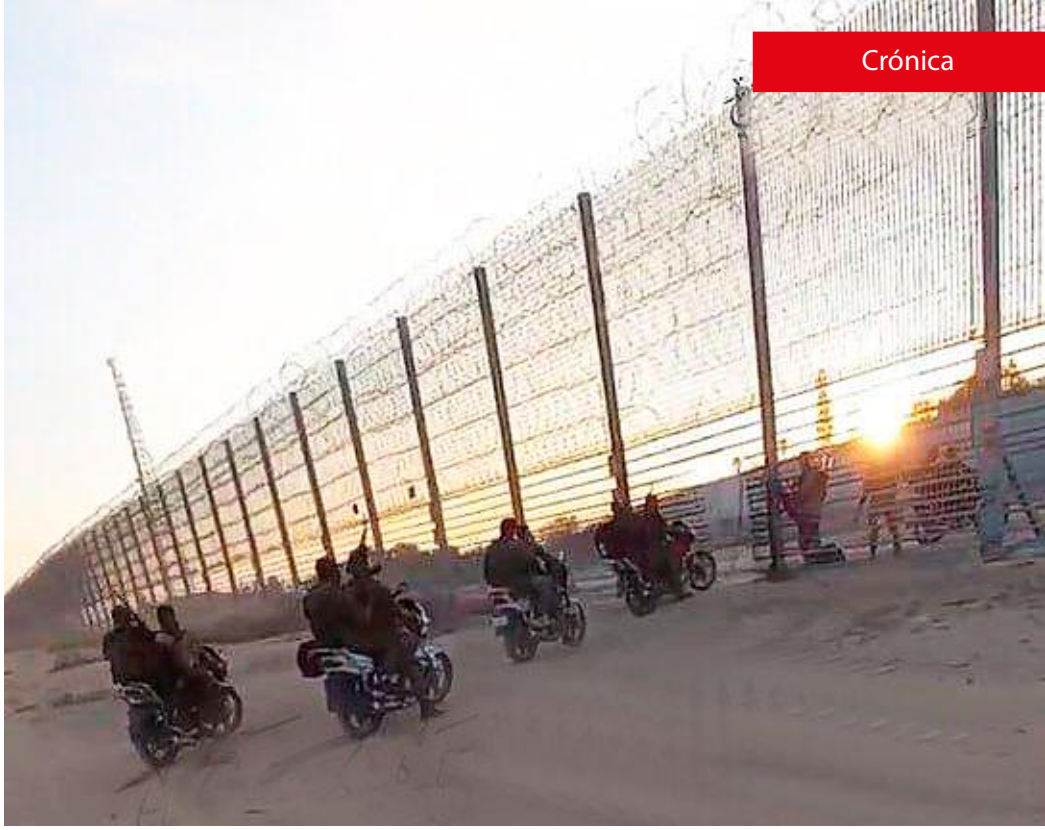
Se deben realizar ejercicios de preparación en los que realizaremos las acciones necesarias para emergencias: cuantos más ejercicios realicemos, más preparados estaremos.

Debe existir un control de calidad para la preparación para emergencias: control interno y control externo.

Recuerde, el desprecio y la confianza en el "no me pasará a mí, puede llevarnos nuevamente a una situación grave e irreversible; en cambio, una preparación temprana y minuciosa puede ayudarnos a prevenirla y frustrarla.

Escribo y pienso estratégicamente de manera diferente, a simplemente aumentar el número de soldados en la frontera.

La base de pensamiento tendrá que cambiar para estar en un estado de constante ataque y disuasión, ya no hay ningún pensamiento de defensa y el ejército no debería llamarse Fuerzas de Defensa de Israel, sino fuerza de ataque de Israel; piensen como atacantes, no como atacantes. de-



fensores!!!

El cambio mental debe ser inmediato.

Es apropiado construir un sistema de auditoría externa para el ejército por parte de contratistas externos y preferiblemente de diferentes ejércitos que mantienen alianzas militares con nosotros, ellos pueden probar nuestra preparación de una manera diferente, nos desafiarán y descubrirán las brechas que tenemos.

Deben establecerse nuevas reglas para prepararse para la guerra, reglas que dependerán más del soldado en el campo, y menos de la tecnología como factor primario, sino sólo como factor secundario y auxiliar.

Palabras claves:

1. Focus
2. Preparación
3. Determinación
4. Consistencia
5. Luchando por la victoria en cualquier situación.

Guy Sadeh- Profesional con 22 años de experiencia en el campo de la seguridad física y en el ejército israelí, Jefe de operaciones en diversas unidades de seguridad del estado de Israel. Consultor de Seguridad, especialista en protección -visible y encubierta, análisis de seguridad, seguridad escolar. Planear y ejecutar ¨Maccabiah Games¨ en México 2019. Miembro en la operación de la seguridad operativa - Juegos Pan Americanos Perú 2019.

ZKTeco sigue potenciando Armatura en Latinoamérica

Durante el mes de noviembre se realizó un webinar abierto, previa inscripción, a todo público sobre Armatura, en el cual se enfocó en la explicación de las credenciales móviles, funcionamiento, y cómo estos se pueden aplicar a distintos tipos de proyectos.

Armatura es la nueva línea de alta comercializada por ZKTeco, diseñada en USA y manufacturada en Tailandia, es un ecosistema completo que abarca una amplia gama de necesidades:

Control de Acceso: A nivel de plataforma gestiona quién accede a tus instalaciones y cuándo, junto con integrar herramientas de gestión para diferentes escenarios de riesgo. Mientras que, a nivel de hardware, el mismo incorpora diversos protocolos industriales y de redundancia como así también de la seguridad de la información.

Tiempo y Asistencia: Optimiza la gestión del tiempo laboral de tus empleados.

Gestión de Vídeo: Vigila y protege tus espacios con integración de vídeo mediante la integración de plataforma de VMS de clase mundial.

Automatización de Edificios: Integra y controla sistemas para una eficiencia óptima mediante protocolos Modbus, Modbus y KNX.

Alarma contra Incendios: Responde con rapidez y seguridad ante emergencias mediante integraciones de terceros para la centralización de la información y la gestión de emergencias.

Intrusión y Defensa: Protege tus activos con sistemas de seguridad avanzados.

Durante el encuentro virtual, Diego Fajardo, Product Manager de Armatura ZKTeco - Colombia se refirió a las funciones y beneficios de las credenciales móviles y el uso de los celulares, incluso de los modelos antiguos.

Esta explicación fue de suma importancia dado que la facilidad de uso y la comodidad de la experiencia del usuario son más importantes que nunca, los dispositivos Armatura aceptan dispositivos móviles como teléfonos inteligentes y dispositivos inteligentes para actuar como lectores habilitados para credenciales BT (Bluetooth) para acceder a áreas seguras específicas, oficinas y otras instalaciones empresariales. Permite a las empresas disponer de una autenticación de identidad completa en los puntos de acceso y reduce el consumo de material para las tarjetas RFID físicas.

También se especificó los pilares que dan más ventaja en relación al uso de la credencial móvil Armatura:

1.- Prevención de la perdida de la tarjeta
2.- Comodidad
3.- Mayor nivel de seguridad

La solución de control de acceso de Armatura funciona con BLE (Bluetooth Low Energy) y con nuestra aplicación Armatura ID instalada en los dispositivos móviles, permite a los usuarios abrir puertas con sus smartphones y dispositivos inteligentes.

La solución de credenciales móviles ofrece a los usuarios experiencias de desbloqueo móvil de cualquier dispositivo de seguridad y control de acceso con un dispositivo inteligente werable, Android y iOS en cualquier local como oficinas y otros lugares donde se instala una cerradura de puerta electrónica o cerradura electrónica.

Cabe precisar que las soluciones Armatura son ideales para cualquier situación que evite que el personal o los pacientes toquen las superficies de las manillas de las puertas. Esta solución ha sido ampliamente utilizada en muchos escenarios prácticos, incluyendo: hospitales, escuelas, fábricas, centros comerciales, transporte público, bancos, pequeñas y grandes empresas, y más.

Para quienes deseen revisar este contenido pueden hacerlo en el siguiente link: https://www.youtube.com/watch?v=g7RTPqZVyuE

ARMATURA

MADE IN THAILAND

DESIGNED & ENGINEERED IN THE USA
ARMATURA

RS485

AES-256

AHSC-1000

IP-Based Core Controller

- Core controller and integration hubs
- Scalable, Supports up to 32pcs AHDU-1460 and 258 readers
- Onboard Webserver
- Threat Levels and Port Failover

AHDU-1460

IP-Based Biometric Door Unit Controller

- Four Door Unit (supports 4 door and 8 readers)
- Scalable, Supports up to 24pcs AHEB expansion boards
- 4-States Supervised and Programmable Inputs

OmniAC20

Contactless Biometric Standalone Terminal

- Multi-Biometric technology: Palm and face recognition
- IP66 water & dustproof protection rating
- Slim design & form factor for a modern aesthetic design
- Supports 125 kHz and 13.56 MHz frequency RFID
- Supports Dynamic QR Code

OmniAC30

Contactless Biometric Standalone Terminal

- Multi-Biometric technology: Palm and face recognition
- IP66 water & dustproof protection rating
- Supports 125 kHz and 13.56 MHz frequency RFID
- Supports multiple mount types (Single gang/ European/ Asian box)
- Supports Dynamic QR Code

QR Code

Dynamic QR Code
Encrypted with AES256 and TOTP

Mobile Credential

Encrypted with RSA4096
(initial Communication) & AES256

RFID

Encrypted with DES/3K3DES/AES

OSDP
AES-128

OSDP
AES-128

EP30

Fingerprint

All Weather Outdoor Multi-tech Fingerprint Reader

- OSDP Biometric Reader
- Multi-tech RFID & Mobile credential
- IP65 Water & Dustproof Protection Level
- Advanced Fingerprint Scanning Technology

EP20CKQ-DF

QR Code, RFID & Keypad

All Weather Outdoor Multi-tech Smart Reader

- Up to IK07 & IP68 Protection Level
- Physical keypad
- Supports 100+ card types and dual RFID frequencies
- Supports Mobile Credentials (Bluetooth & NFC & QR code)
- Supports Asian/ European/ Single-gang box

Bluetooth NFC OSDP IP66 IK07

Lorem ipsum

EP10C

RFID

All Weather Outdoor Multi-tech Smart Reader

- K10 & IP68 Protection Level
- Supports 100+ card types and dual RFID frequencies
- Supports Mobile Credentials (Bluetooth & NFC)
- Mullion Mount Design
- Supports Asian/ European/ Single-gang box back-box spacing

Bluetooth NFC OSDP IP66 IK10

Mobile Credential | Facial Recognition | Palm Recognition | Multi-tech RFID

WRAP REALITY

- **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**

El Lacrim Central de la PDI fortalece su posicionamiento latinoamericano en Congreso Internacional de Ciencias Forenses.

Centrado en el intercambio de técnicas, metodologías de análisis e interpretaciones, que se han transformado en innovaciones, tanto por los medios empleados como por sus resultados y su nivel probatorio, fueron los objetivos abordados en el Congreso Internacional de Ciencias Forenses, que organizó entre el 14 y 15 de diciembre la Jefatura Nacional de Criminalística junto a su Laboratorio de Criminalística Central.

Las jornadas que se realizaron en modalidad presencial y telemática, contó entre ambos días con más de 500 conexiones virtuales, además del lleno total del auditorio del Lacrim Central.

Las actividades se organizaron en dos módulos. El primero de ellos titulado "Desafíos analíticos en la investigación de delitos asociados al uso de armas de fuego", y que agrupó ponencias relacionadas con problemáticas forenses emergentes en relación a la investigación de delitos violentos cometidos con este tipo de armamento.

El segundo módulo, denominado "Nuevas estrategias forenses aplicadas a la investigación criminal", convocó a expositores en áreas de análisis de la escena del crimen, innovaciones en metodologías emergentes para el análisis de huellas genéticas, estrategias de inteligencia artificial aplicadas al análisis forense.

Durante el congreso que se desarrolló en el contexto de actividades vinculadas a un proyecto de cooperación regional liderado por la PDI, a través de la Sección Microanálisis del Lacrim Central, participaron autoridades y expositores del Organismo Internacional de Energía Atómica, junto con asistentes de Honduras, México, Paraguay, Perú y República Dominicana.

Al respecto, el Jefe Nacional de Criminalística, prefecto inspector Mauro Mercado Andaur señaló "en el marco que orgullosamente ostenta la PDI en la investigación de delitos violentos, complejos y aquellos derivados del crimen organizado, que ha sido plasmado en el Plan Estratégico de Desarrollo Policial 2023 – 2028, asumimos el compromiso de promover el fortalecimiento de las investigaciones criminales profesionales, mediante la promoción del conocimiento y la cooperación regional a través de este evento de tan alto nivel científico y convocatoria".

En la clausura del congreso internacional, el jefe del Laboratorio de Criminalística Central, subprefecto Richard Biernay Arriagada, además de agradecer el apoyo de la Oficina de Investigación, desarrollo e innovación forense, por la organización del evento internacional, manifestó que "se aproximan grandes cambios para la realidad forense institucional, acordes a los nuevos desafíos y al compromiso con el país".

Publirreportaje

La importancia del control de acceso en los juegos panamericanos de Chile 2023

Los Juegos Panamericanos de 2023 en Chile es uno de los eventos deportivos de magnitudes históricas en nuestro país, reuniendo a atletas de toda América en una celebración de talento y competencia. Sin embargo, detrás de la grandiosidad de este evento, la seguridad y el control de acceso emergieron como aspectos críticos y que garantizaron el éxito y la integridad del espectáculo realizado entre octubre y noviembre de este año.

El control de acceso se posicionó como un pilar fundamental para salvaguardar tanto a los atletas como a los espectadores que asistieron al encuentro deportivo y de carácter familiar.

En un contexto donde la seguridad es prioritaria, implementar sistemas avanzados de control de acceso se convierte en una necesidad ineludible. Estos mecanismos no solo aseguran que solo personas autorizadas ingresen a las instalaciones, sino que también permiten una rápida respuesta ante cualquier eventualidad.

En esa línea, desde la empresa Rocktech, referentes en proyectos de seguridad electrónica e ingeniería, destacando en el mercado por el desarrollo de soluciones 360° adaptadas a las necesidades y problemáticas de cada rubro cubriendo toda la cadena de valor, y que fueron en este magno encuentro implementando distintas medidas en el control de acceso, comentan: "La experiencia fue enriquecedora e incomparable, ya que este es un evento de clase mundial, donde más allá de lo que fue entregar tecnología para la seguridad del mismo, todo era distinto a otros proyectos que hemos implementado, las interacciones, el tipo de personas, lo entretenido que fue ser parte de esto. Mientras nosotros hacíamos entrega de los equipos, nos topábamos con los deportistas, vimos de primera fuente el respeto desde Santiago 2023 con los deportistas y viceversa. Pudimos interactuar con algunos de ellos, lo que hizo que el trabajo fuera mucho más ameno.

El desplegado en Chile no fue algo muy distinto a nuestro trabajo habitual, ya que nosotros integramos soluciones siempre en las distintas regiones del país, tenemos la capacidad para hacer distintos recintos de manera simultánea", expresó Camila Lucero, jefa de Marketing de la empresa.

Camila Lucero, jefa de Marketing, Rocktech

Camila Lucero, además precisó sobre la importancia del uso de equipos que estuvieron a la altura que exigía un evento deportivo de esta envergadura: "El trabajo de las paletas consistía en controlar los accesos de los recintos deportivos con las paletas detectoras de metal, esto entregó mucha más comodidad y control a los guardias encargados, ya que es un equipo muy amigable de usar, de fácil interfaz y liviano. La recepción fue positiva, ya que todos encontraban interesante el control de acceso, de hecho, la gente esperaba y hasta tomaban registro de cómo estaba implementada la seguridad para entrar, muchas veces comparada con la que tienen los aeropuertos. La alianza junto a ZKTeco fue vital en esta instancia, ya que Rocktech realiza la ingeniería de los proyectos, sin embargo, la tecnología que utilizamos debe cumplir estándares de calidad altos, sobre todo para eventos masivos, donde es muy difícil guardar la seguridad de todos. Para evento de calidad mundial, necesitamos equipos de calidad mundial como son los productos de ZKTeco", puntualizó.

La identificación precisa y la autenticación de cada individuo son esenciales para evitar posibles amenazas y garantizar un ambiente seguro y

protegido. Tecnologías como lectores de tarjetas, sistemas biométricos y análisis de imágenes desempeñarán un papel crucial en la verificación de la identidad de los participantes, personal autorizado y espectadores.

Además de la seguridad, el control de acceso contribuye a la gestión eficiente del evento. Con la capacidad de regular el flujo de personas en áreas específicas, se pueden evitar aglomeraciones, facilitando así la movilidad y la comodidad de los asistentes. Esto no solo mejora la experiencia del público, sino que también facilita la ejecución fluida de las competiciones.

"El control de acceso no solo es una medida de seguridad esencial, sino también un componente crucial para la eficiencia operativa y la calidad de la experiencia en los Juegos Panamericanos de Chile 2023. Con un enfoque riguroso en esta área, Chile está preparado para recibir a atletas y espectadores de toda América en un evento que quedará marcado en la historia del deporte continental. Además, marca un precedente para futuros desafíos en donde la colaboración entre gobierno y privados, mediante profesionales especializados y empresas de primer nivel es esencial cuando se trabajan conjuntamente en implementaciones que no solo deben responder a estándares de los más altos niveles, sino que con plazos acotados con muy poca holgura.

Si bien como en cada proceso existieron pormenores de controversia y de conocimiento público, estos dejan una enseñanza y refuerza nuestra convicción de que, aunque existan los diferentes sistemas y tecnologías, si estas no son conocidas por las personas idóneas y tomadores de decisiones simplemente se dejan de lado y los problemas quedan para los usuarios finales. Como fue el caso de la gestión residencial de la Villa Panamericana, un recinto con 1.355 departamentos que se pudo haber mejor gestionado mediante sistemas Hoteleros y Cerraduras Inteligentes", agrega Gustavo Maluenda, CEO de ZKTeco Chile.

Gustavo Maluenda, CEO de ZKTeco Chile

El impacto del control de acceso en eventos multitudinarios y los desafíos

Respecto a esta experiencia y el rubro, conversamos con el experto Alvar Orellana McBride, CEO de Griffin Risk, referente en seguridad laboral, asesor internacional en materias como seguridad corporativa, ciberseguridad electrónica en ASIS International, profundizó sobre los desafíos en esta área.

Alvar Orellana McBride, CEO de Griffin Risk

"Recientemente fuimos testigos de uno de los mayores eventos deportivos de la historia de Chile, en la que más de 1.3 millones de espectadores, junto a casi 11 mil voluntarios, más de 1.200 profesionales de comunicaciones y sobre 5 mil Carabineros y otros actores sumaron a los cerca de 7.000 atletas y equipos técnicos que dieron vida a los Juegos Panamericanos y Parapanamericanos Santiago 2023 en 22 locaciones a lo largo de nuestro país.

El desafío logístico no estuvo exento de problemas y chascarros, pero eso lo dejaremos para otros análisis y solo nos enfocaremos en lo concerniente a los incidentes de seguridad y oportunidades de eficiencias que se pueden lograr por medio de

la implementación de tecnología de seguridad. Además, consideraremos cómo éstas nos pueden ayudar en futuros desafíos tales como el Mundial Sub20 en menos de dos años más en el 2025 y no solamente de esa talla, sino también eventos masivos tanto deportivos como de otro tipo de espectáculos. En Santiago 2023 se pudo demostrar que es factible realizar eventos masivos sin tener que lamentar incidentes graves de seguridad, y eso es destacable.

¿Qué podemos sacar en limpio?

Que para cumplir este objetivo fue necesaria una convergencia en cuanto a seguridad pública y privada, como asimismo la incorporación de tecnología que permitiese dar soporte a las necesidades de protección de los diferentes centros deportivos. El resultado fue auspicioso, no se presentaron delitos graves ni se ha podido obtener información que permita conocer de hechos relevantes de seguridad que afectasen a atletas ni espectadores; solo fue noticia el robo de equipamiento de televisión por parte de criminales antes de que fuese custodiado el recinto por Carabineros de Chile y que fueron recuperados en corto tiempo por parte de la misma policía.

Dentro de los recintos deportivos no se ha informado que se hubiesen presentado incidentes de seguridad, solo inconvenientes en el funcionamiento de los servicios de guardias por temas administrativos, que de igual manera fueron resueltos. Esto plantea desafíos que está por verse si son corregidos por la nueva Ley de Seguridad Privada, próxima a ser publicada.

El equipamiento de seguridad principalmente estuvo compuesto por arcos y paletas detectoras de metales y máquinas de RX instalados en los puntos de acceso público; además, controles estrictos que impedían el paso de personas no autorizadas por el resto de los puntos de tránsito. Dentro de las medidas se mantuvo la prohibición de ingreso de personas que estuviesen vetado su acceso a eventos deportivos por delitos relativos a violencia en los estadios.

Los procesos de control fueron fluidos y permitieron procesar un alto número de asistentes a los múltiples eventos que se llevaban a cabo en recintos como, por ejemplo, el Estadio Nacional.

Por información recabada de distintos medios, se pudo evidenciar delitos que afectaron a turistas, asistentes y atletas, pero fuera del ámbito de las actividades deportivas, sin tener que lamentar situaciones graves.

Por otro lado, en cuanto a problemas de gestión en infraestructura donde la tecnología de seguridad podría haber hecho la vida bastante más fácil de los organizadores, fue el importante problema que significó resolver la identificación de las 1.355 llaves correspondientes a los departamentos usados por los atletas en la Villa Panamericana. La utilización de las diversas opciones de cerraduras electrónicas que existen disponibles en el mercado habría evitado varios dolores de cabeza y facilitado la operación y gestión de accesos a las delegaciones.

La experiencia vivida en estos últimos juegos, abre un desafío importante para los eventos masivos, y este no es otro que realmente ¡se pueden efectuar estas actividades sin incidentes! Para ello se requirió de voluntad política, una efectiva administración de los recursos, convergencia pública y privada, también el uso de tecnología para que en conjunto se adoptasen las medidas necesarias que resultó en que los asistentes estuviesen seguros.

Hace aún más notable este resultado, que se haya realizado un evento de estas características en medio de una crisis de seguridad en el país, lo que nos puede ayudar a concluir que sí es posible adoptar medidas que permitan que eventos históricamente violentos, se puedan efectuar ya en un ambiente que habilite el volver a recibir

familias, por ejemplo, en el fútbol. Los medios están al alcance, corresponde ahora a la autoridad ejecutar medidas concretas para erradicar los comportamientos no deseados en los eventos masivos e implementar las herramientas, entre ellas las tecnológicas que faciliten el control de los asistentes, asegurando con ello que no ingresen personas que tengan prohibición de acceso, detectando criminales que tengan ordenes de aprehensión pendientes y sean sacados de circulación. Para ello la biometría juega un papel fundamental, ya que le entregará a la autoridad información en tiempo real sobre infractores que sean detectados y puedan actuar con eficiencia.

No hay que dejar de lado en esta ecuación, a la relación que mencionamos hace unos momentos entre la parte pública y privada, ambos tienen misiones y capacidades diferentes, pero se necesitan mutuamente para proveer de un espacio que asegure la continuidad operacional de los eventos, por qué deben trabajar en apoyo mutuo es debido a que la deber de proveer seguridad a los ciudadanos es y será del Estado, como asimismo responsabilidad del privado adoptar las medidas necesarias para asegurar a quienes interactúan como por ejemplo, los eventos masivos.

Esto hace que la cooperación mutua sea vital para la generación de espacios seguros y cada uno dentro de su misión y funciones trabaje para que los anillos que les corresponde resguardar funcionen adecuadamente.

La nueva Ley de Seguridad Privada y el Reglamento que regule esta industria deberían dar marcos claros para su interacción, y a la vista del texto en proceso constitucional, es imperativo seguir iterando el cuerpo legal para realizar los ajustes necesarios. Se hace necesario exigir al privado que trabaje con programas de gestión de riesgos que identifiquen adecuadamente las amenazas a las que está expuesto y las vulnerabilidades que posee, de modo que se establezca una estrategia de mitigación adecuada al riesgo a enfrentar.

Dentro de las estrategias de mitigación podemos considerar en vez de llenar de guardias, normalmente mal entrenados y con inadecuado equipamiento, invertir en equipos reducidos, con entrenamiento especializado, equipo de protección y para proceder frente a hechos delictuales con equipos de similares características a las de Carabineros.

Algunos ejemplo son Bolawrap, bastones retráctiles, esposas, gas pimienta entre tantas otras herramientas. También equipar a los centros de eventos con la tecnología que permita identificar adecuadamente a los asistentes, detectar elementos prohibidos antes de su ingreso, instalar sistema de cámaras que facilite la detección temprana de situaciones que pongan en riesgo a los asistentes e identifique quienes estén detrás de acciones delictuales de modo que puedan ser perseguidos y reciban una consecuencia disuasiva.

Los Centros de Operaciones de Seguridad "SOC" (por sus siglas en inglés, Security Operation Center), son claves en la gestión de operaciones y respuesta ante incidentes, ayudan a asegurar la continuidad de las operaciones y la coordinación entre los actores que deban actuar frente a amenazas que afecten a los asistentes y eventos.

Queda ver si la autoridad toma esta experiencia como un estándar y toma la iniciativa e impulsa las medidas necesarias para continuar abriendo los eventos a todo público en espacios que den la tranquilidad y contribuyan al disfrute de sus asistentes. Esto es bueno para los negocios, es bueno para vivir en armonía ciudadana.

Doce indicadores de seguridad ciudadana en América Latina

La seguridad ciudadana es un tema de gran relevancia para el desarrollo y la convivencia en América Latina, donde año tras año, se registran altos niveles de violencia, delincuencia e inseguridad. Estos fenómenos afectan la calidad de vida, el desarrollo económico y la cohesión social de los países de la región. A continuación, se presentan doce de los indicadores más importantes sobre esta materia, basados en datos del año 2022 e incluyendo fuentes de instituciones públicas y privadas.

Tasa de homicidios: mide el número de muertes violentas intencionales por cada 100 mil habitantes. Según el Observatorio de Violencia de la Organización de Estados Americanos (OEA), el promedio regional fue de 18,7 en 2022, con una reducción del 5% respecto al año anterior. Sin embargo, persisten grandes disparidades entre los países, siendo los más afectados Venezuela (56,3), El Salvador (46,9) y Honduras (38,9).

Tasa de robos: mide el número de delitos contra la propiedad por cada 100 mil habitantes. Según el Banco Interamericano de Desarrollo (BID), el promedio regional fue de 1.234 en 2022, con un aumento del 3% respecto al año anterior. Los países con mayor incidencia fueron Argentina (2.567), Chile (2.354) y Brasil (1.948).

Tasa de secuestros: mide el número de casos de privación ilegal de la libertad por cada 100 mil habitantes. Según la Comisión Interamericana de Derechos Humanos (CIDH), el promedio regional fue de 0,8 en 2022, con una disminución del 10% respecto al año anterior. Los países con mayor prevalencia fueron México (2,4), Colombia (1,6) y Guatemala (1,2).

Tasa de violencia doméstica: mide el número de denuncias por agresiones físicas o psicológicas dentro del ámbito familiar por cada 100 mil habitantes. Según la Comisión Económica para América Latina y el Caribe (CEPAL), el promedio regional fue de 154 en 2022, con un incremento del 8% respecto al año anterior. Los países con mayor registro fueron Bolivia (312), Perú (278) y República Dominicana (256).

Tasa de violencia sexual: mide el número de denuncias por abusos o agresiones sexuales por cada 100 mil habitantes. Según la Organización Panamericana de la Salud (OPS), el promedio regional fue de 36 en 2022, con una reducción del 4% respecto al año anterior. Los países con mayor incidencia fueron Nicaragua (72), Costa Rica (58) y Ecuador (54).

Tasa de extorsión: mide el número de casos de amenazas o coacciones para obtener beneficios económicos o materiales por cada 100 mil habitantes. Según el Programa de las Naciones Unidas para el Desarrollo (PNUD), el promedio regional fue de 12 en 2022, con una disminución del 6% respecto al año anterior. Los países con mayor prevalencia fueron El Salvador (34), Honduras (28) y Guatemala (22).

Tasa de corrupción: mide el grado percibido de corrupción en el sector público por parte de los ciudadanos y los expertos. Según la organización Transparencia Internacional, el promedio regional fue de 35 puntos sobre 100 en 2022, con una mejora del 2% respecto al año anterior. Los países con menor puntuación fueron Venezuela (15), Nicaragua (22) y Haití (23).

Tasa de impunidad: mide el porcentaje de delitos que no son investigados, ni sancionados por las autoridades competentes. Según el Índice Global de Impunidad elaborado por la Universidad de las Américas Puebla, el promedio regional fue de 66% en 2022, con un empeoramiento del 1% respecto al año anterior. Los países con mayor índice fueron México (99%), Honduras (96%) y Venezuela (94%).

Tasa de confianza en la policía: mide el grado de satisfacción y credibilidad que tienen los ciudadanos en las fuerzas policiales como garantes del orden público y la seguridad ciudadana. Según la encuesta Latinobarómetro, el promedio regional fue de 44% en 2022, con una mejora del 3% respecto al año anterior. Los países con mayor confianza fueron Uruguay (74%), Chile (67%) y Costa Rica (66%).

Tasa de confianza en la justicia: mide el grado de satisfacción y credibilidad que tienen los ciudadanos en el sistema judicial como garante del estado de derecho, y la protección de los derechos humanos. Según la encuesta Latinobarómetro, el promedio regional fue de 34% en 2022, con una mejora del 2% respecto al año anterior. Los países con mayor confianza fueron Uruguay (60%), Chile (49%) y Costa Rica (48%).

Tasa de participación ciudadana: mide el grado de involucramiento y compromiso de los ciudada-

nos en las actividades cívicas, políticas y sociales que contribuyen a la convivencia pacífica y democrática. Según el Índice de Desarrollo Democrático elaborado por la Fundación Konrad Adenauer, el promedio regional fue de 0,54 puntos sobre 1 en 2022, con una mejora del 1% respecto al año anterior. Los países con mayor puntuación fueron Uruguay (0,77), Chile (0,69) y Costa Rica (0,68).

Tasa de percepción de seguridad: mide el grado de tranquilidad y confianza que tienen los ciudadanos en su entorno inmediato y en su capacidad de protegerse de posibles amenazas o riesgos. Según la encuesta Latinobarómetro, el promedio regional fue de 52% en 2022, con una mejora del 4% respecto al año anterior. Los países con mayor percepción fueron Uruguay (84%), Chile (76%) y Costa Rica (75%).

Estos indicadores nos permiten tener una visión integral y comparativa de la situación de la seguridad ciudadana en América Latina, así como identificar los principales desafíos y oportunidades para mejorarla. A continuación, presentamos algunas recomendaciones derivadas del análisis:

• Fortalecer las capacidades institucionales y operativas de las fuerzas policiales y del sistema judicial, mediante la profesionalización, la capacitación, la dotación de recursos, la rendición de cuentas y el control social.

• Promover la prevención social del delito, mediante el diseño e implementación de políticas públicas integrales que atiendan las causas estructurales y coyunturales de la violencia, tales como la pobreza, la desigualdad, la exclusión, la falta de oportunidades, la educación, la salud, la cultura y el deporte.

• Fomentar la participación ciudadana y la corresponsabilidad en la seguridad ciudadana, por medio del fortalecimiento de los espacios de diálogo, coordinación y cooperación entre los actores públicos, privados y sociales involucrados en esta materia, así como el desarrollo de mecanismos de información, consulta y veeduría por parte de la ciudadanía.

• Impulsar la cooperación regional e internacional en materia de seguridad ciudadana, considerando el intercambio de experiencias exitosas, el apoyo técnico y financiero, el fortalecimiento de los organismos multilaterales y el cumplimiento de los compromisos asumidos en los diversos foros y acuerdos sobre esta temática.

Los indicadores de seguridad ciudadana son herramientas que permiten medir y evaluar el nivel de violencia, delincuencia y victimización en una sociedad. Se basan en fuentes oficiales, como registros policiales, judiciales y administrativos, así como en fuentes alternativas, como encuestas de victimización, percepción y opinión pública. Los indicadores tienen una gran importancia para el diseño, implementación y seguimiento de políticas públicas orientadas a prevenir y reducir los fenómenos delictivos y sus consecuencias sociales. Asimismo, contribuyen a la rendición de cuentas, la transparencia y la participación ciudadana en materia de seguridad. Por lo tanto, conocer y analizar los indicadores de seguridad ciudadana es fundamental para mejorar la calidad de vida de las personas y fortalecer el estado de derecho en una sociedad democrática.

Autor: Alfredo Yuncoza.
Presidente del Consejo Consultivo Latino. IFPO

ESEM 2023
Encuentro de Seguridad Empresarial Proyectando a la seguridad en Chile

Recientemente se realizó la segunda versión del Encuentro de Seguridad Empresarial, ESEM, instancia que se ha convertido en un referente y en un punto de inflexión respecto del enfoque con el cual se ha abordado tradicionalmente la seguridad, en especial a nivel empresarial. Conversamos con Alvar Orellana McBride, uno de los precursores de esta iniciativa, quien nos da a conocer los principales alcances de este importante evento.

¿Qué nos puede comentar en relación a este encuentro denominado ESEM?

Se trata del segundo encuentro de seguridad empresarial y nace en el alero del Hub de líderes de seguridad empresarial, entidad creada y destinada a generar un punto de conexión entre usuarios finales, es decir, líderes que cumplen la función de seguridad en distintas empresas.

¿Cumplió este encuentro con las expectativas proyectadas?

Por supuesto. Es importante mencionar que el objetivo de este evento es generar puntos de encuentro con soluciones innovadoras invitamos a empresas proveedoras a presentar servicios específicos e innovadores a quienes son tomadores de decisión o tienen responsabilidad en influir en las decisiones de adquisición de productos y servicios.

En esta oportunidad incorporamos un panel de autoridades, entre los cuales destacó la presencia de Daniela Cañas de la Subsecretaría de Prevención del Delito, Carabineros de chile representado por el Prefecto de OS10 , Crl. Miguel Calderón y Daniel Johnson de Paz Ciudadana quienes nos relataron sus experiencias con respecto al trabajo que realizan en materia de prevención del delito, además de abordar aspectos relativos a la nueva ley de seguridad privada, desafíos y oportunidades.

Adicionalmente se realizaron diversas presentaciones, en las cuales proveedores expusieron respecto de sus productos y de soluciones que pueden hacer más eficiente la función de seguridad dentro de las empresas.

¿Existen proyecciones a futuro por parte de este hub de líderes de seguridad considerando el preocupante momento que vive chile en esta materia?

Existe consenso respecto de aquellas cosas que en las que podríamos trabajar, eventualmente en el Hub de líderes de seguridad donde he tenido el honor y el privilegio de asumir la presidencia de la agrupación. Nos encontramos en un proceso para convertirnos en una asociación gremial; la idea es que podamos constituirnos en un actor relevante dentro de la industria de la seguridad, para que demos soporte a otras industrias y también al gobierno con respecto de cómo enfrentar este problema.

En una entrevista reciente a otro medio, me tocó abordar el problema con el cual estamos lidiando relativo a la percepción de inseguridad y que manera resolvemos esta realidad; la respuesta es sencilla y contundente: mediante una adecuada gestión de riesgos y mitigaciones de seguridad más tecnología, es decir, diversas acciones, pero en conjunto con la autoridad.

Es un trabajo en conjunto con la autoridad y con las distintas industrias. En este hub de líderes de seguridad queremos generar esa interacción.

Tal como mencionaba, en otras oportunidades en esta materia la seguridad es la reina y la percepción es el rey; eso indica que no importando lo que se haga en materias de seguridad, si la percepción no es buena los resultados tampoco serán buenos.

Debemos desterrar conceptos simplistas o explicaciones basadas en argumentos de tipo político, ya que en definitiva no aportan en pro de soluciones efectivas y permanentes. Debemos ser capaces de conocer la manera en que estos problemas o estas inquietudes llegan a solucionarse.

¿Cree usted que la autoridad percibe que en materia de seguridad existe una contraparte ya debidamente validada con la cual poder avanzar en el desarrollo de políticas de mayor efectividad?

Por un lado, tenemos los requerimientos de la comunidad, las inquietudes reflejadas en las encuestas y por otro lado los profesionales que aportan conocimiento y soluciones específicas. Podríamos pensar que en este caso esta agrupación es el inicio de la generación de un interlocutor válido.

El Hub de líderes de seguridad agrupa a más de 320 profesionales quienes, a su vez, se desempeñan en más de 60 tipos de industrias y quienes tenemos la disposición de aportar en pro de mayores niveles de seguridad.

Pretendemos constituirnos como un organismo técnico, que se relaciona con tanto con la parte pública como con la parte privada, pues no podemos olvidar que la actual institucionalidad en materia de seguridad pública y privada suele renovarse cada cuatro años. Cabe mencionar en este punto la importancia de replicar experiencias, como la de la industria de la seguridad de Estados Unidos, en la cual la industria se nutre de la experiencia de los casos de éxito, generando desde esa base mayor conocimiento lo que es aprovechado por la autoridad y empresas

¿Se tienen planificados nuevos encuentros de ESEM?

Efectivamente, para el calendario de actividades 2024, estamos considerando dos encuentros, el primero durante el mes de Abril y el segundo en Agosto del mismo año.

El segundo Encuentro de Seguridad Empresarial ESEM 2023, contó con una masiva presencia de proferionales y empresas quienes compartieron experiencias además de exponer los últimos avances y soluciones para el área de la seguridad.

La Pericia Documental, en el nuevo escenario digital

¿Será tiempo de una metamorfosis?

Hoy, damos la bienvenida a un nuevo año. Para los lectores de Revista Seguridad Online aprovecho de saludarles y desearles un próspero 2024 lleno de oportunidades y éxitos. El tiempo -a nuestros ojos- pasa cada vez más rápido. Nuestros hijos crecen, nos volvemos más desconfiados, más cautos, más lentos. Todo está cambiando de manera rauda con el paso del tiempo.

De igual forma, y atendiendo la temática que nos convoca para estas columnas o publicaciones, podemos afirmar que la delincuencia, la inteligencia criminal y el desarrollo de nuevos delitos también avanza, frente a nuestros ojos, de una manera extremadamente acelerada.

Hemos sido testigo con los años, de los cientos de intentos que las autoridades de turno hacen por lograr dar frente a los fenómenos criminales modernos.

Sabíamos que la apertura de fronteras en Europa y América era un avance en materias de integración social, empleo y oportunidades, pero el descontrol migratorio que vemos hoy, particularmente en España y Estados Unidos, nos habla del lado oscuro del fenómeno.

Por su parte, la criptomoneda, celebrada en otrora como una respuesta inteligente y robusta a la seguridad monetaria, hoy muestra que también es volátil, no se encuentra del todo regulado, y es igual de insegura que la moneda tradicional. La firma digital en documentos, fue considerada un avance en materias de sostenibilidad medioambiental por la reducción de papel, ejemplo de eficiencia por abaratar costos en insumos, tiempos y traslados. Sin embargo, hoy se presenta como un nicho más para la delincuencia organizada, que a través de nuevas tecnologías, diseñan, producen y emiten documentación digital falsa; o peor aún, en algunos casos ideológicamente falsa pero emitidas en documentos originales.

Frente a este último ejemplo me quiero detener, y presentar esta nueva columna de opinión. Pues es mi deseo compartir con el lector mi particular inquietud, y que tiene relación con la investigación y análisis forense que se realiza en materias de falsificación o adulteración de documentos.

El antes, el hoy y el futuro de la Pericia Documental, conforme al nuevo escenario digital. Para ello haremos una breve alusión al sentido y alcance de la documentología, como la conocemos hasta hoy, para luego dejar abierta una puerta para cuestionamientos sobre el hacia donde debemos ir con su aplicación digital.

Para quienes nos adentramos -recientemente- en el estudio pericial de esta disciplina, podemos definir documentología como una ciencia auxiliar que integra la Criminalística. Se orienta hacia el estudio de cualquier documento, pudiendo ser este un diploma, una carta, u otro escrito que ilustra acerca de algún hecho particular. Surge aquí la noción de pericia documental, que no es más que un conjunto de investigaciones tendientes a esclarecer las posibles falsificaciones y adulteraciones, y a revalidar los documentos manuscritos o mecanografiados. De la documentología surge la pericia caligráfica y la dactilográfica.

Con respecto a la denominación "documentología", existen muchas designaciones para referirse a esta disciplina.

La documentología ha sido siempre una especialidad que, según variados autores o escuelas carece de un pasado como otras ciencias. Esto debido a que a pesar de que el hombre siempre se valió de distintos medios para cambiar o adulterar los documentos, las modalidades para llegar a descubrir los engaños no se encuentran registradas o documentadas.

Una característica que hace especial a esta disciplina, en relación con otras disciplinas hermanas auxiliares de la criminalística, es que a pesar de contar hoy con elementos tecnológicos y con va-

riados adelantos en ciencia aplicada, siempre existen y existirán dudas a la hora de dilucidar con certeza los interrogantes que se presentan en el análisis de todo documento. Así, el análisis sobre documentos puede establecer su autenticidad o falsedad (ya sea por medio de borrados, lavados, correcciones, agregados o modificaciones).

En el estado del arte, muchos autores indican que en los peritajes documentales se analizan las falsificaciones de las firmas, ya sea por imitación o calco, las falsificaciones sobre documentos de identidad, papel moneda, sellos, estampillas o documentos valorados.

Para el trabajo de análisis y las respectivas conclusiones del perito, la documentología se vale de la ampliación del elemento dubitado (por medio de lupas o microscopio) de la fotografía, a través de la cual se demuestran las conclusiones periciales. También se pueden utilizar reactivos químicos o demás herramientas tecnológicas disponibles.

Al leer el párrafo anterior se puede comprender que los procedimientos propios del peritaje documental señalado por diferentes autores consideran en su regla general un soporte de papel impreso. Aquí surge una gran interrogante, ¿qué hay de las falsificaciones en formatos digitales? ¿Se analizan bajo los procedimientos y equipamientos actuales?

Al respecto, resulta importante referirse al contenido, sentido y alcance de la Ley 21.459 del 20 de junio de 2022 del Ministerio de Justicia y Derechos Humanos, que establece normas sobre delitos informáticos, y deroga la Ley 19.223; que actualiza la legislación chilena en materia de delitos informáticos, y que de una manera ejecutiva -en sólo 21 artículos- aborda materias como los delitos informáticos, la interceptación ilícita, la falsificación informática, el fraude informático, los datos informáticos; entre otros temas propios de la documentología, pero en un escenario digital.

Imprescindible entonces resulta considerar el desarrollo de un proceso kafkiano, que implique elevar a un siguiente nivel de abstracción el conocido peritaje documental, que al igual que la obra Metamorfosis de 1915, permita a la documentología, como ciencia auxiliar dentro de la criminalística moderna, no ajustarse simplemente al formato preestablecido por la sociedad, sino que dar un salto de fe al actual y futuro escenario de la criminalidad organizada, las plataformas digitales, la inteligencia artificial, y por que no decirlo al mismísimo metaverso. Creo que es hora de enfrentar los desafíos de la documentología, con nuevos conocimientos, nuevas competencias y nuevas herramientas.

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

Capitulo 233 de ASIS International

Proyectando un año 2024 con importantes metas y desafíos

Fundada en 1955 , ASIS International es la comunidad global de profesionales de la seguridad,cuyos miembros representan prácticamente todas las industrias de los sectores público y privado, y organizaciones de todos los tamaños. Sus 34.000 miembos y 340 capítulos alrededor del mundo, hacen de ASIS International, un referente en el mundo de la seguridad. En nuestro país esta organización es representada por el capítulo 233 el cual recientemente realizó una renovación de directiva. Conversamos con Marcelo Serey, nuevo presidente del capítulo 233, quien compartió con Revista Seguridad sus principales propuestas y objetivos.

Para quienes no pertenecen específicamente al sector de la seguridad privada ¿Nos podría resumir el historial, antecedentes y relevancia de Asis a nivel mundial?

ASIS International es una organización global dedicada a apoyar a profesionalizar el rubro de la seguridad. Fue fundada en 1955 y tiene su sede en Alexandria, Virginia, Estados Unidos. Originalmente conocida como la "American Society for Industrial Security" (Sociedad Americana para la Seguridad Industrial), la organización cambió su nombre a ASIS International en 2002, para reflejar mejor su alcance global y su enfoque en la seguridad en diversos contextos.

ASIS International desempeña un papel clave en la promoción de las mejores prácticas y estándares en el campo de la seguridad a nivel mundial. La organización cuenta con más de 34.000 miembros en más de 150 países, en muchos de los cuales existen Capítulos que ofrece programas educativos, recursos y eventos para profesionales de la seguridad.

¿Cuáles son los principales objetivos que usted se plantea al asumir la presidencia del capítulo 233 de Asis?

Nuestro capítulo para este año 2024 tiene grandes desafíos, tanto en lo organizacional como para el crecimiento profesional de nuestros miembros.

Nuestras actividades este 2024 estarán dirigidas a potenciar nuestro capitulo como referente en la profesionalización de quienes desarrollamos actividades entorno a la seguridad estratégica organizacional, y seguridad privada en nuestro país. Para ello, buscamos incorporar nuevas socias y socios, y hacerlos participes de nuestros cuatro pilares que nos hemos planteado para nuestro crecimiento.

Queremos incorporar a profesionales de seguridad y ciberseguridad que quieran participar activamente de dos importantísimos proyectos NEXTGEN (nueva generación) que busca incorporar a talento joven y WIS (women in security) que busca incorporar a mujeres profesionales.

A través de estas agrupaciones, cuyas iniciativas serán lideradas por Ignacio Santibañez e Isabel Hinojosa, nuestros miembros podrán acceder a webinars de capacitación y actualización de contenidos con importantes expositores vinculados a ASIS Internacional, accederán a reuniones presenciales y a foros nacionales e internacionales, como también la oportunidad de asistir a congresos internacionales, como el que se llevará a cabo de manera presencial en Ciudad de Panamá para WIS este 2024.

Un eje fundamental de nuestras actividades, es nuestro compromiso por capacitar a nuestros socios para que puedan acceder a las Certificaciones Profesionales que ASIS Internacional tiene a su disposición. APP, PCI, PSP y CPP, son certificaciones que permiten validar el conocimiento de los profesionales en las áreas de la investigación, seguridad física y ESRM Enterprise Security Risk Managenet.

Para los socios activos del Capítulo, vamos a retomar nuestras reuniones presenciales y webinars online, donde nuestro objetivo será el análisis de la actualidad nacional e internacional, como asimismo, actualizar conocimiento para nuestros afiliados. Asimismo, nos hemos planteado como desafío llevar a cabo tres congresos con expositores de renombre, que sin duda acaparara la atención del público y prensa especializada.

Finalmente, queremos reforzar nuestros procesos de comunicación interna y externa, para que nuestros usuarios puedan acceder y tomar conocimien

to de lo que significa ASIS Internacional, cuáles son nuestras actividades nacionales e internacionales, que beneficios aporta al profesional de la seguridad privada nuestras certificaciones como especialistas y ciertamente poder entregar información de primera línea entorno a los estándares de seguridad que ASIS Internacional crea para la gestión de riesgos empresariales.

Chile atraviesa por una delicada crisis en materia de seguridad ¿de qué manera entidades como Asis pueden aportar en generar los cambios que el sector de la seguridad privada en chile requiere?

Existen varias asociaciones a nivel mundial entorno a profesionales de la seguridad estratégica organizacional, pero ASIS Internacional es el referente mundial.

La industria de la seguridad Privada en Chile debe cambiar y todos los vinculados al rubro coincidimos en este diagnóstico; pero para ello, todos los actores involucrados en este ecosistema, deben estar dispuestos al cambio. El nutrirse de nuevas metodologías de trabajo, actualizar normativas, incorporar nuevas tecnologías, necesidades de especialización etc., provocan una incertidumbre, porque siempre tenemos temor a lo desconocido, pero debemos tener la capacidad de adaptarnos a las nuevas exigencias y realidad que en materia de seguridad nos demandan los usuarios, y por cierto la industria.

En este contexto, ASIS International a través de su capítulo chileno, busca la especialización de sus afiliados con los más altos estándares para la industria de la seguridad, para formar profesionales que estén acorde a las expectativas que hoy exige el mercado.

Los riesgos y amenazas que pueden afectar las operaciones en una organización se deben abordar de manera holística en 360°, y para ello el profesional de la seguridad moderno, debe estar al corriente de no tan sólo gestionar la realidad criminal, sino que debe estar al tanto de la gestión de amenazas cibernéticas, protección de la información, gestión de desastres, protección ejecutiva, violencia y abusos en el trabajo etc., un sin número de fenómenos que pueden afectar a las personas, infraestructura, información, imagen corporativa o su entorno.

Desde el punto de vista profesional ¿cuáles son las principales ventajas que para un profesional chileno implica incorporarse a una entidad como ASIS International?

ASIS International ofrece un conjunto de cuatro certificaciones especializadas para profesionales de la seguridad, adaptadas a diferentes niveles de experiencia y responsabilidad. La certificación APP está diseñada para personas que ingresan recientemente al campo de la seguridad principalmente jóvenes, brindándoles un respaldo reconocido a medida que comienzan sus carreras. Para aquellos especializados en seguridad física, la certificación PSP se centra en validar y elevar las habilidades en esta área específica.

Los investigadores en seguridad pueden obtener la certificación PCI, que destaca su competencia en las técnicas de investigación aplicadas al ámbito de la seguridad. Finalmente, la certificación CPP representa la "dorada" certificación dirigida a Gerentes o Directores de Seguridad, reconociendo un nivel avanzado de experiencia y liderazgo en la gestión integral de la seguridad.

La asociación se centra en diversas áreas de seguridad, como la seguridad corporativa, la gestión de riesgos, la ciberseguridad, la protección de activos y la prevención de pérdidas. Sus conferencias anuales y otros eventos proporcionan oportunidades para el intercambio de conocimientos y la creación de redes entre profesionales de la seguridad de todo el mundo.

Los requerimientos que se solicitan en Chile los profesionales de seguridad privada distan enormemente los niveles de capacitación y exigencia que existen en el extranjero, ¿De qué manera ASIS International a través de su capítulo chileno puede aportar en pro de mayores niveles de capacitación?

ASIS International es referente mundial entorno a la creación de estándares de seguridad para las organizacionales, y nuestros socios podrán acceder a nuestros programas de capacitación a través de plataformas virtuales. Nuestro desafío es que cada uno de nuestros socios acceda a estos programas de certificación para que sirvan como agentes multiplicadores de las buenas prácticas y metodologías que debieran imperar en la industria de la seguridad.

¿Cómo califica usted el actual momento por el cual atraviesa ASIS International, considerando los múltiples eventos y encuentros que debieron suspenderse a raíz de la reciente pandemia?

La pandemia representó una gran oportunidad para que ASIS llevara a cabo una significativa digitalización de su contenido, transformando diversas actividades que históricamente se realizaban de manera presencial hacia un entorno virtual. En la actualidad, la organización lleva a cabo al menos un webinar semanal, con iniciativas respaldadas tanto por las comunidades globales como por cada uno de los más de 250 capítulos distribuidos en todo el mundo.

Con el levantamiento de las restricciones de movilidad a partir del año 2022, ASIS retomó la realización de sus grandes eventos a nivel mundial. El año pasado marcó el debut del primer congreso de Latinoamérica y el Caribe, celebrado en Cancún, México. El 2023 se destacó por ser un año lleno de actividades, incluyendo la participación en el renombrado GSX en Dallas, Estados Unidos, el segundo congreso de la región LATAM en Lima, y el Foro de las Mujeres de Seguridad celebrado en Río de Janeiro. Este retorno a eventos presenciales fortaleció la conexión entre profesionales de la seguridad y reafirmó la importancia de estos encuentros para el intercambio de conocimientos y experiencias en el ámbito de la seguridad a nivel global.

El 2024 se también se realizarán congresos en Europa y Asia. Además, se llevará a cabo el evento anual en USA, el GSX en Orlando, que corresponde al evento de la seguridad más grande e importante del mundo. En Latam, tendremos el evento de WIS en Panamá, agosto y luego el 3er. Congreso Latinoamericano en Costa Rica, Noviembre.

Como presidente del capítulo chileno de ASIS International, ¿considera la posibilidad de generar alianzas orientadas a consolidar un referente único en materia de seguridad privada en chile?

Para nuestro Capitulo y sus respectivos miembros asociados, sería un privilegio crear alianzas estratégicas que nos ayuden a generar un cambio en la industria de la seguridad nacional.

Nosotros ponemos a disposición de organismos especializados de gobierno, municipalidades y sector privado, nuestras experiencias y conocimiento para contribuir a generar una asociatividad entorno a la cultura de seguridad, donde la seguridad sea considerada una inversión como parte de las operaciones cotidianas de las organizaciones y no un gasto innecesario de recursos.

La seguridad constituye un tema de gran dinamismo ¿Cómo ha enfrentado ASIS International el actual escenario en el cual temas como la ciberseguridad y el crimen organizado se posicionan entre las principales amenazas para la comunidad?

La seguridad privada en Chile necesita rápidamente adaptarse a una realidad delictiva que al correr de los años mutó. Hoy el crimen organizado transnacional no es una amenaza emergente sino que representa una amenaza latente para nuestra realidad, en cuyo nuevo escenario, sabemos que la oferta pública de seguridad resulta insuficiente para enfrentar amenazas que no conocíamos y que en muchos casos no se estaba preparado para enfrentar.

Los adversarios son cada vez más violentos, en algunos casos muy especializados y con un alto poder técnico, tecnológico y organizacional, que les han permitido posicionarse rápidamente en nuestro territorio.

Por lo mismo, en este contexto urge modernizar el ecosistema de la seguridad, con un nuevo marco legal que signifique una modernidad tanto en lo procedimental, como en lo técnico para poder enfrentar tales amenazas.

Los delincuentes en el transcurso de los años se especializaron en su core de negocios y accedieron a nuevos nichos de mercados, secuestros, extorciones, sicariato, defraudaciones, robos con fuerza, asaltos, trata de blancas, ciberataques, vandalismo, etc. La seguridad privada sigue trabajando con un marco legal que data de los años 80' y donde los estándares para la actividad son bastante bajos, tanto para quienes desean emprender como prestadores de servicios en esta industria, como para quienes desarrollan actividades tácticas y/o operativas. En su contexto político y social, esta normativa cumplió su objetivo para la época, pero no para nuestros tiempos.

ASIS, puede contribuir a cambiar la industria de la seguridad en nuestro país de la mano del conocimiento y especialización, no hay otra fórmula. Nuestra fortaleza radica en que al ser una organización internacional y especializada, estamos al tanto gracias a nuestros socios, de la realidad de muchos países y cómo han enfrentado sus fenómenos criminales o gestión de desastres en sus respectivos países de la mano de las metodologías que entrega ASIS.

Marcelo Serey, presidente del Capítulo 233 Santiago - Chile de ASIS International

Con el levantamiento de las restricciones de movilidad a partir del año 2022, ASIS retomó la realización de sus grandes eventos a nivel mundial.

Conflictos de la Ciberguerra

Image by aleksandarlittlewolf on Freepik

Hace años que se considera el ciberespacio como un espacio más en el que puede desarrollarse el conflicto bélico más allá de los tradicionales tierra, mar y aire. Hay que tener en cuenta que Rusia es una de las potencias mundiales en ciberseguridad.

La situación de las guerras ha cambiado, o al menos, como la conocemos, cuando Rusia invadió Ucrania, arrancó una segunda y menos visible batalla en el ciberespacio, ellos buscaron o crearon una red voluntaria de hackeo con un grupo de Telegram de casi 200.000 usuarios, con esto lograron para secuestrar estaciones de radio rusas y transmitir el sonido de sirenas antiaéreas falsas que alertan a ciudadanos para que busquen refugio.

Muchos expertos predijeron que los hackers jugarían su papel en el conflicto de Ucrania, pero la escala está sorprendiendo. Ejércitos de hackers emergen en ambos bandos, por ejemplo, la pandilla de hackers rusos Killnet, con un grupo de Telegram de casi 100.000 suscriptores, trabaja directamente con los cibermilitares rusos.

Killnet ha llevado a cabo ataques perturbadores, aunque temporales, en sitios web de hospitales tanto en Ucrania como en países aliados, aunque no existe una Convención de Ginebra para la guerra cibernética, el Comité Internacional de la Cruz Roja argumenta que algunos códigos existentes podrían aplicarse. Atacar hospitales, por ejemplo, sería violar esos códigos.

Si países de la OTAN son atacados, esto también podría provocar una respuesta colectiva si se causan daños graves, el fin de semana de Pascua, el canal de Telegram de Killnet fue utilizado para crear un equipo llamado KillNATO Pshychos (Mata a los psicópatas de la OTAN). En pocas horas tenía cientos de miembros y lanzó una ola de ataques que desconectaron temporalmente sitios web de la OTAN. El grupo también publicó una lista de correos electrónicos de trabajadores de la OTAN e incitó a la gente a acosarles.

Sin embargo, los hacktivistas ucranianos no solo atacan la maquinaria de guerra rusa. Los hackeos están organizados para causar todos los problemas posibles al pueblo ruso. La ciberguerra en Ucrania es asistida por cibermilitares occidentales y compañías privadas de ciberseguridad, financiadas con millones de dólares donados por sus aliados.

Según la información publicada por UATV con referencia al Servicio de Seguridad de Ucrania, Rusia lleva a cabo una media de más de diez ciberataques diarios al país ucranio. De hecho, desde principios de año, la cifra de este tipo de ataques se ha disparado y se ha multiplicado incluso por tres con motivo de la guerra que se está librando en el norte de Europa.

Un detalle significativo, pues es lo que diferencia a las guerras modernas de las guerras del pasado. Básicamente, se trata de privar a la otra parte de obtener recursos. Además, es un acierto atacar los centros de datos. Un estudio de Venafi, una firma estadounidense especializada en protección cibernética, reveló a fines de agosto que el 77 por ciento de las organizaciones del planeta modificaron sus estrategias de ciberseguridad, como "respuesta directa al conflicto entre Rusia y Ucrania".

En los últimos meses se ha observado un creciente número de ataques dirigidos a altos cargos del gobierno de Ucrania y de su ejército, así como de diferentes países miembros de la OTAN. Este tipo de ataques suelen intentar recabar información sensible sobre movimientos de tropas, estrategia militar, aprovisionamiento de bienes de primera necesidad y armamento, etc.

El primero fue el ataque a Viasat una hora antes de que comenzara la invasión. Se trata de una compañía estadounidense en la que confiaba el

ejército ucraniano para disponer de enlaces de comunicación vía satélite.

El ejército ruso empleó un malware denominado AcidRain para inutilizar completamente millas de terminales de comunicaciones de la red KA-SAT, tanto routers como módems. Este ataque afectó también a otras infraestructuras europeas, por ejemplo, a turbinas de generación de energía eólica.

La guerra entre Rusia y Ucrania ocasionó una serie de ataques cibernéticos que afecta los servicios básicos de ambos países.

La ciberseguridad y el conflicto entre Rusia y Ucrania tienen una relación estrecha porque, en un mundo cada vez más digitalizado, en el cual los procesos sociales y económicos dependen de tecnologías informáticas el planeta es testigo de enfrentamientos de tipo convencional, invasiones y tensiones diplomáticas en la frontera entre Rusia y Ucrania. Simultáneamente, se dan altercados cibernéticos entre sistemas de inteligencia y ciberactivistas (estos últimos congenian con una u otra nación).

Por ejemplo: Ataques a sistemas de entidades: el 13 de enero de 2022, un malware destructivo atacó los equipos tecnológicos de entidades sin ánimo de lucro y empresas tecnológicas de Ucrania, y dejó inutilizables los datos que contenían.

Hacking a estaciones de radio: una estación rusa fue intervenida el 17 de enero de 2022 por un grupo cibernético, que inhabilitó la transmisión y publicó imágenes en sus señales.

Daños a sitios web gubernamentales: setenta sitios web del gobierno ucraniano fueron atacados el 14 de enero de 2022; seis de ellos quedaron fuera de servicio y sin posibilidad de recuperación.

Secuestro de información de sistemas ferroviarios: durante el trayecto del 24 de enero de 2022, en las vías de tren bielorrusas, un grupo de personas capturó la información del sistema ferroviario, lo que inhabilitó el transporte de tanques y maquinaria militar de origen ruso.

Israel - Palestina

En la reciente guerra no parece que Israel vaya a necesitar mucha ayuda para mantener lo que ya es una clara superioridad cibernética. Si se han convertido en una de las grandes potencias militares, gran parte de culpa la tiene la inversión en desarrollo tecnológico del país, algo que no solo incluye armamento, sino también herramientas de reconocimiento facial, las vallas inteligentes o el software de espionaje.

En el conflicto actual entre Israel y Hamás, se han visto a grupos hacktivistas intentar muchas de las mismas técnicas que se utilizaron con éxito contra Rusia. Sin embargo, ahora parecen ser menos eficaces.

El factor principal que diferencia estas tácticas de guerra cibernética es el tiempo entre conflictos.

En los 19 meses transcurridos desde que los hacktivistas declararon la ciberguerra contra Rusia, los expertos en ciberseguridad y los servicios de inteligencia de todo el mundo han tenido tiempo para analizar, prepararse y tratar de aislarse aprendiendo de las fallas de las ciberdefensas de Rusia. Después de todo, es un hecho que la guerra cibernética desempeñará un papel importante en cualquier conflicto actual y futuro.

El ciberespacio actúa ahora como un segundo frente sin reglas de enfrentamiento definidas. Los hacktivistas y los grupos afiliados al gobierno pueden elegir un bando y lanzar numerosos ataques en función de sus

Image by DCStudio on Freepik

habilidades específicas, inclinando la balanza del conflicto aparentemente con sólo unos pocos clics.

Entre los atacantes se encuentran grupos extranjeros: hackers rusos propalestinos y hackers indios proisraelíes, pero no hemos visto ataques de borrado de datos como los que sufrió Ucrania, aunque Irán está en condiciones de proporcionar tales herramientas. Es cierto que el nivel de ciberdefensa de Israel es muy alto, aún más que en Ucrania.

Por otro lado, grupos indios han atacado sitios web palestinos. Esto es una consecuencia de los lazos diplomáticos entre India e Israel.

En el pasado, Hamás ha sido acusada de distribuir versiones maliciosas de la aplicación Red Alert, que la población de Israel para emplear notificaciones sobre bombardeos, y saber cuándo tiene que dirigirse a un refugio.

Estos últimos días el grupo AnonGhost parece haber atacado de nuevo a este sistema para provocar caos y confusión, pero todavía se deben analizar los detalles de este ataque y no se sabe qué tipo de vulnerabilidad, si de la aplicación o de la plataforma, se ha explotado. Los impactos producidos han sido falsos mensajes de alerta y spam.

En lo que se refiere a los ciberataques en el sentido contrario, no parece que Israel o su esfera de influencia los vayan a considerar esenciales en esta guerra, en la que se ha anunciado un cerco total a Gaza que bloqueará su suministro de combustible, electricidad. y comunicaciones y que va a implicar un apagón total.

El grado de destrucción física que están sufriendo las pocas infraestructuras tecnológicas que funcionan allí hace completamente innecesaria la utilización de ciberataques.
En cuanto al resto de la población, de momento no se ha observado un incremento en los ataques a infraestructuras críticas en otros países. Pero sí se está advirtiendo de la posibilidad de que en los próximos días internet, y en concreto las redes sociales, se vea inundado de vídeos muy duros, con torturas o ejecuciones en tiempo real.

Es especialmente importante saber esto, sobre todo, para proteger a los menores y a otras personas sensibles a estos contenidos que pueden afectar a su futuro desarrollo o a su salud mental. No es algo a lo que se hayan enfrentado en muchas ocasiones en el pasado y deben estar preparados.

En el contexto del conflicto Israel-Hamas, el ciberespacio se ha convertido en un terreno fértil para la lucha encubierta, ya que se subraya la necesidad urgente de una mayor seguridad cibernética y cooperación internacional para abordar las amenazas cibernéticas en el contexto de conflictos políticos.

En última instancia, la escalada de ataques cibernéticos en el conflicto Israel-Palestina destaca la necesidad apremiante de un enfoque global y colaborativo para abordar los retos de seguridad cibernética en el mundo actual. La colaboración entre países, agencias de seguridad y sectores público y privado se vuelve esencial para identificar, rastrear y neutralizar las operaciones de estos grupos extremistas en línea.

En resumen, la incorporación de Libyan Ghosts Hackers a la lista de actores cibernéticos en el conflicto Israel-Palestina subraya la necesidad apremiante de una acción global coordinada para abordar las amenazas cibernéticas en evolución, proteger las infraestructuras críticas y garantizar la seguridad de las personas en línea.

Financiamiento por Criptomonedas

Una vez pasada la fiebre, las criptomonedas han vuelto a aparecer en Gaza, donde nadie las esperaba. Estas monedas digitales han sido la forma de evitar las restricciones de financiación de Hamás, la Yihad Islámica Palestina (YIP) y Hezbolá, que habrían recibido cantidades equivalentes a decenas de millones de dólares en los últimos meses a través de esta vía, según datos del Gobierno de Israel y firmas de la industria cripto, recogidos por The Wall Street Journal. Entre ellos, YIP habría sido quien habría recibido una suma mayor, con una cifra que ronda los 93 millones de dólares.

Algunas de las cuentas ya estarían siendo cerradas por Tel Aviv, aunque la sospecha es que solo podrán hacerlo con un pequeño porcentaje de ellas, ante la dificultad de seguir el rastro de las cadenas de bloques en las que circulan estas divisas.

Latinoamérica cuarto de juego para los hackers

Los hackers utilizan la región latinoamericana para entrenar a sus recursos antes de enviar un ataque destructivo contra una infraestructura mucho más madura, Latinoamérica es un cuarto de juegos para los ciberatacantes; hackers internacionales vulneran los sistemas informáticos de instituciones y empresas como parte de su proceso de entrenamiento, para incluirlos en operaciones más complejas.

Ante la eventualidad de que la guerra de Ucrania y la crisis de Taiwán escalen, expertos en ciberseguridad latinoamericanos consideran que el Canal de Panamá, que es esencial para el comercio mundial, está en un "gravísimo riesgo", como en otras infraestructuras de pasos navales bloqueados por Rusia en medio de su guerra contra Ucrania.
Al igual que en el conflicto rusoucraniano, el número de ciberataques ha aumentado. Pero no podemos hablar de ciber guerra: son principalmente ataques de denegación de servicio, una congestión intencional sin gravedad que hace que un sitio web sea inaccesible durante algunas horas.

Conclusiones

No hay duda de que se está produciendo una guerra cibernética en línea junto con la actual guerra física. Por ahora, el impacto de estos ataques cibernéticos parece ser mínimo y solo causan interrupciones menores. A medida que más grupos y actores se unan a la lucha, las amenazas a la seguridad cibernética no harán más que aumentar. Agregaremos actualizaciones a este artículo a medida que se produzcan ataques cibernéticos importantes.

Fuentes:
www.google.com
www.defensa.com
www.alainet.org
www.theconversation.com

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

La IA, la ciberseguridad y la nube serán las tendencias tecnológicas que marcarán el 2024

Se acerca fin de año y el momento de hacer las compras navideñas, Tivit detalla los pasos seguros para adquirir regalos con tranquilidad.

El e-Commerce sigue creciendo después del impulso de la pandemia y Argentina no es ajena a esta realidad. Sin embargo, este panorama de conveniencia y accesibilidad conlleva también un aumento significativo en los riesgos de ciberdelitos. Según las cifras recientes se registran 90.000 millones de ataques de ransomware en América Latina; 2.1 millones de sitios de phishing en 2022; y un costo para las organizaciones de USD$6 billones al año. También se reporta un 88% de ataques que se gestan a través de la filtración de datos y el promedio de pago es de USD 228.000.

Ante esto el aumento de transacciones electrónicas ha aumentado. De hecho la Cámara de Comercio de Santiago indicó que la edición de Black Friday 2022 alcanzó 8,4 millones de transacciones, por cerca de US$ 300 millones, ratificando la relevancia de este evento en el país.

Pero como pasa en todos los ámbitos de la vida, hay que mirar las dos caras de la misma moneda. A medida que avanza el comercio online, crece el ciberdelito. Así como las empresas se preparan en ciberseguridad, los ciberdelincuentes también lo hacen innovando y encontrando nuevas formas de ataque, sobre todo, a través del ransomware, ataques que utilicen deepfake y el phishing geodirigido.

Según un informe realizado por FortiGuard Labs. Chile recibió 14 mil millones de intentos de ciberataques en 2022, un crecimiento de 50% frente a 2021.

La ciberseguridad ya no es solo una inversión necesaria para las empresas, es un requisito operacional básico. Según Mauricio Gálvez, Gerente de Ciberseguridad de TIVIT Cono Sur, "se trata de una herramienta ecléctica y holística que se ha transformado en la piedra angular". A continuación, Mauricio Gálvez, experto en esta materia en la compañía multinacional tecnológica TIVIT, entrega recomendaciones para prepararse para esta nueva fecha clave del comercio electrónico:

* La capacitación de los colaboradores en la mitigación de los riesgos es clave. Es necesario crear una conciencia institucional o cultura de protección que permita robustecer los mecanismos de seguridad. Es imperante trabajar para convertir a las personas en el eslabón más fuerte de la cadena.

* Comprender cuáles son los principales tipos de ciberataque y cuáles son los flancos más débiles dentro de la empresa. El phishing y ransomware son las modalidades más frecuentes de ataque, mientras que el correo electrónico es uno de los flancos de exposición más comunes. Para este año, se espera una evolución hacia el "phishing geodirigido", en el que los mensajes sean cada vez más elaborados, dirigidos a grupos poblacionales específicos y clickbaits más relevantes, con lenguajes característicos de distintas industrias o marcas, haciéndolos más difícil de detectar que el phishing tradicional.

Con respecto a los números, cifras recientes registran 90.000 millones de ataques de ransomware en América Latina; 2.1 millones de sitios de phishing en 2022; y un costo para las organizaciones de USD 6 billones al año. También se reporta un 88% de ataques que se gestan a través de la filtración de datos y el promedio de pago es de USD 228.000.

*Los Deepfakes o "falsedades profundas" son archivos de vídeo, imagen o voz manipulados mediante un software de inteligencia artificial (IA) de modo que parezcan originales, auténticos y reales. Estos archivos consiguen engañar fácilmente ya que se utilizan para inducir a error a las personas receptoras, por lo que representan una gran amenaza para la sociedad actual, pudiendo

facilitar la desinformación y que la ciudadanía pase a desconfiar de cualquier fuente de información.

* Una correcta implementación y uso de tecnologías para prevenir el fraude como lo son el blockchain, la inteligencia artificial y el software en la nube. Aunque no hay un camino para blindarse en un 100%, trabajar con las mejores herramientas y con profesionales capacitados puede reducir los impactos y probabilidades de un ciberataque.

Por su parte, los consumidores o usuarios también pueden prestar atención a diversos aspectos a la hora de concretar su compra.

* Conocer cuáles son los canales de información oficiales de las empresas, por qué medios se les solicitarán datos personales o claves, así como cuáles son las plataformas para realizar las transacciones.

* Al recibir correos, asegurarse de que la dirección del sitio web o e-mail remitente esté bien escrito y sea el dominio oficial. Si no es así, no hacer click ni descargar contenido.

* Al realizar transacciones fuera de casa, no utilizar las redes públicas sino los datos del celular.

* Más niveles de seguridad de acceso, utilizando un segundo factor de autenticación, basado en un código de única vez que llega, por lo general, vía SMS.

"La ciberdelincuencia no es solo un problema de política pública y de las grandes empresas, debe ser un asunto de preocupación para cada persona", concluye Mauricio Galvez, Gerente de Ciberseguridad TIVIT Cono Sur.

En los últimos años, en especial con el crecimiento de la economía digital, y las fechas especiales de este sector como es la navidad, se ha logrado avanzar en el camino por tener un entorno más seguro, pero aún queda mucho recorrido como país y en la región, para lograr alcanzar el desarrollo de Europa o Norteamérica. Trabajar en los 3 frentes —personas, procesos e infraestructura tecnológica— y buscar los mejores aliados para el camino, es clave para que las compañías puedan afrontar los nuevos desafíos en ciberseguridad.

Francisco López , Country Manager de TIVIT en Chile

Foto de Tara Winstead pexels.com/

La Migración Irregular: Un nuevo desafío para la política de integración y seguridad del siglo XXI

Conferencia magistral de Javier Gamero Kinosita en el seminario internacional "Gestión migratoria en la región: Avances y desafíos en integración y seguridad" organizado por la Superintendencia Nacional de Migraciones del Ministerio del Interior del Perú en la ciudad de Lima el 30 de noviembre y primero de diciembre de 2023.

Migración y globalización son procesos sociales hoy en día frecuentemente discutidos en los medios y la política. Si bien es cierto que el fenómeno migratorio es un fenómeno social que existe desde los albores de la humanidad, este se ha tornado en un fenómeno transnacional, complejo, multidimensional y policéntrico en la era global. La migración es una constante histórica en la raza humana, se puede apreciar grandes movimientos humanos en el planeta en aras de la libertad y supervivencia. Esto ha generado que las fronteras hayan sido tanto, zonas de interacción cultural como también zonas de rechazo, alcanzando hoy en día niveles dramáticos, vemos inmersos en los flujos migratorios de grupos humanos (menores de edad, mujeres, adultos mayores, personas con discapacidad) con destinos escurridizos y culturas y tradiciones distintas.

Esto ha dado lugar a leyes más restrictivas que fortalecen los controles de sus fronteras contra inmigrantes desarmados, un desborde de las capacidades de las autoridades fronterizas de los cuerpos de seguridad y policía, conllevando a una militarización del problema. En este sentido, el sociólogo austriaco investigador del fenómeno de la migración, Gerald Knaus y autor de la Iniciativa Europea de Estabilidad, se plantea la interrogante: ¿Qué tipo de fronteras necesitamos hoy?. El debate yace entre la empatía o compasión, el miedo, la fuga o el escape, la migración y el futuro del derecho de asilo está sobre el tapete.

La migración con resultado de los factores de estrés global del siglo XXI

Uno de los factores de estrés global del presente siglo es la demografía, al respecto se vaticina que al 2050 la población mundial crecerá 7 a 9 mil millones de habitantes y se prevé que al 2100 el número de habitantes se incrementará de 10 a 11 mil millones, ello tendrá una masiva repercusión en la vida sobre el planeta y en el uso de recursos lo que generará flujos migratorios.

Un segundo factor de estrés global es el cambio climático, estamos viviendo un proceso mundial de transición hacia la economía verde, que es equivalente o quizá más importante que la revolución industrial, pues se vaticina que en la economía verde yace el futuro de la humanidad, ello permitirá preservar los recursos naturales. Politólogos suizos advierten en la revista Polit Orbis del Gobierno Federal suizo que el siglo XXII será el "Siglo de los genocidios", en virtud de los gigantescos flujos migratorios que se originarán producto de las devastadoras consecuencias climáticas que darán lugar a zonas áridas y escasez de recursos, lo que originará un éxodo masivo en busca de alimentos, generándose conflictos sociales para subsistir.

Un tercer factor de estrés global es la geopolítica, como sabemos las relaciones de poder son volátiles, hay desplazamientos constantes de poder, siempre hay naciones que ascienden y descienden Estas dislocaciones y trastornos geopolíticos, han ocasionado por ejemplo, en el caso de la invasión militar de Rusia a Ucrania un éxodo masivo, inmigración irregular y peticiones de asilo y refugiados.

La migración como riesgo, amenaza y desafío global

El científico social alemán Ulrich Beck de la Universidad Ludwig Maximilien de Múnich, sostiene que vivimos en la sociedad de riesgo del siglo XXI, postulando que los riesgos son reflejos normales del progreso y desarrollo y que ya no es posible eliminarlos, solo reducirlos, tenemos que coexistir con ellos, es el precio que tiene que lagar la civilización por el triunfo, ya no existe puerto seguro, ya que estos riesgos son inherentes al nuevo orden mundial.

Dentro de los riesgos globales identificados te-

nemos el terrorismo internacional, las amenazas nucleares y peligros atómicos, el crimen organizado, las pandemias y la migración ilegal masiva.

Asimismo, los investigadores del Instituto de Estudios Internacionales para la seguridad Global (INISEG) de España, ha identificado las amenazas globales emergentes en los espacios comunes globales del siglo XXI identificando las armas de destrucción masiva, el crimen organizado, el terrorismo internacional, los conflictos armados, los conflictos militares, el espionaje, los ciberataques, y la masiva migración ilegal originada por los éxodos colectivos cuyas raíces yacen en la pobreza, el crecimiento demográfico, la guerra, la presión social y las devastadoras consecuencias del cambio climático. Dentro de los desafíos globales emergentes en los espacios comunes globales del siglo XXI tenemos el cambio climático, que dará lugar a una dependencia energética, crisis económica, desastres naturales, pandemias y flujos migratorios intensos.

Asimismo, los investigadores alemanes en política exterior y política de seguridad Andreas Rinke & Christian Schwägerl, identifican las inminentes guerras del futuro, entre ellas, la guerra helada producto del cambio climático, la guerra por las materias primas, la guerra por los tubérculos en las profundidades del Atlántico Norte, la guerra por las proteínas en el Mar del Norte, la guerra por la alimentación mundial, la guerra por el espacio interplanetario, la guerra por las nuevas tecnologías, la guerra por la tecnología de información, las pandemias (la maldición del conocimiento) y la guerra producto de la migración, en donde la "Gran Fortaleza", Europa está resistiendo el asedio constante de los invasores y bárbaros del Medio Oriente y el Norte de África.

SEGURIDAD URBANA Y MIGRACIÓN

La calidad de vida se da a través de la seguridad en el espacio público

La seguridad urbana implica espacios públicos seguros para todos, vivimos en una sociedad pluralista cada vez más diferenciada y la seguridad urbana abarca una variedad de tareas, entre ellas la prevención de la violencia, criminalidad, misantropía colectiva y protección de la población y la infraestructura crítica frente a los desastres naturales y otros peligros, pero también implica combatir la discriminación, así como las representaciones mediáticas de los conflictos en el espacio público.

El espacio público es un lugar de comunicación, encuentro, demostración política, actuación artística y cultural y diversos entretenimientos, que son indispensables para la vida urbana. Debemos tener en cuenta también que el espacio público del siglo XXI es un espacio virtual, en Internet puede haber impactos positivos como negativos.

El conferencista Javier Gamero Kinosita entrega su libro "Amenazas y desafíos a la política de seguridad del siglo XXI" al Superintendente Nacional de Migraciones del Perú Armando García Chunga

Miedo a la criminalidad extranjera y la reducción de la vida social

Hoy una gran parte de la población evita determinados lugares públicos o situaciones, especialmente las mujeres, existe un sentimiento de inseguridad, pues una de cada tres personas tiene la impresión, que la situación de seguridad ha empeorado, la personas con antecedentes migratorios tienen más temor que aquellos que no los tienen, la delincuencia callejera y de menor cuantía se ha incrementado ostensiblemente atribuyéndosela a los inmigrantes, dando lugar a restricciones a la libertad de movimiento y por ende una reducción de la vida social de determinados segmentos sociales (mujeres, niños, adultos mayores, personas con discapacidad).

Los investigadores alemanes Christian Kromberg y Anna Rau del Foro Europeo - Alemán para la Segu-

ridad Urbana, sostienen que la combinación del miedo abstracto a un ataque y la preocupación concreta de ser atacado en el centro de la ciudad o en la estación de tren aumenta la sensación de inseguridad, igualmente el incremento del desacato de las normas legales y disposiciones comunales, así como la falta de respeto e indisciplinas sociales genera problemas con las autoridades policiales. La protección de personas de color, personas con historia migratoria, inmigrantes, personas con discapacidad y diversos grupos religiosos y grupos de orientaciones sexuales distintas de la misoginia de grupo es de vital importancia para la cohesión social y la seguridad pública. Una sociedad abierta debe permitir a todos una vida libre y segura y un disfrute de los beneficios de la diversidad, para ello se requiere una comunicación sincera entre la policía, la administración y la ciudadanía.

Segregación étnica y social como factores de riesgo para el orden y la seguridad

El espacio público, el vecindario con sus plazas se han forjado a lo largo de la historia como un proceso social y comunicativo continuo.

Producto de la migración nuestra sociedad se ha tornado en comunidades pluriculturales conformadas por muchos grupos étnicos y sociales lo que conlleva a una convivencia heterogénea con su respectivo potencial de conflicto. Los investigadores alemanes Dorthe Flothmann y Christiane Howe de la Universidad de Ciencias Aplicadas de Policía y Administración Pública de Rin – Westfalia del Norte, afirman que es necesario contextualizar mejor las percepciones individuales de los ciudadanos y captarlas estructuralmente en 4 tipos de capital, el capital económico (dotación financiera) el capital cultural (conocimientos, activos y competencias culturales basados en los antecedentes familiares y la formación académica), el capital social (conjunto de recursos actuales y potenciales y red social de relaciones) y el capital simbólico (reputación, honores y reconocimientos, privilegios y posiciones).

Percepción de la heterogeneidad étnica y miedo a la delincuencia

El sentimiento de inseguridad general se ha incrementado en forma dramática, sin embargo, la percepción subjetiva de miedo a la criminalidad no corresponde a los datos estadísticos del desarrollo real y fáctico de la criminalidad, el miedo a la criminalidad se ve reflejado simplemente como "miedo al extranjero".

Eva Gross, investigadora de la Escuela Superior de la Academia de Policía de Hamburgo sostiene, que hoy existe un miedo social generalizado ante la criminalidad extranjera, lo que ha dado lugar en opinión del Dr. Karl Ludwig Kunz del Foro de Berna para las Ciencias Criminales de la Universidad de Berna a la creación de una nueva categoría de criminalidad, es la "criminalidad de extranjería", la cual puede ser hoy instrumentalizada políticamente.

Eva Gross agrega, que existe una relación entre el miedo social generalizado y el temor a la criminalidad extranjera, se percibe una correlación entre devaluación del extranjero, criminalidad y penalización. Las causas del temor generalizado se identifican en sentimientos de inseguridad relacionados con la delincuencia, el miedo a la criminalidad es fácilmente vinculado al miedo ante los "otros" peligrosos, vale decir, personas con antecedentes migratorios. El extranjero como prototipo del "otro", este miedo generalizado a los grupos extranjeros peligrosos a dado legar a respuestas punitivas, pues existe una relación miedo a la criminalidad – punibilidad, evidenciándose un resentimiento contra los extranjeros, el temor a la delincuencia y las ganas de castigo. Hoy el punitismo popular y la justicia consuetudinaria están a la orden del día.

LA INMIGRACIÓN DELICTIVA ("CRIMMIGRATION")

"Crimmigration" es un término genérico que surge en Estados Unidos haciendo referencia a la interrelación entre el control de la delincuencia y el control de la inmigración. Representa las distintas leyes y procesos jurídicos que los estados

emplean para ejercer el control sobre un sector de nuestra sociedad global, esta integración de las esferas de la inmigración y la delincuencia tiende a generar resultados más severos, limitando las protecciones procesales que segregan a los "no ciudadanos" e implica un trato diferenciado para los inmigrantes en situación irregular. Conlleva en determinadas sociedades a un sistema penal independiente (sistema de control de inmigración) y un proceso jurídico especializado (tribunales ad hoc y centros de detención en zonas seguras), dando lugar al uso de estas leyes, instituciones y prácticas, divorciadas del sistema de justicia penal (detención de menores edad en Europa).

Se trata de un entrelazamiento del derecho administrativo de inmigración y el derecho penal, es un reforzamiento mutuo, esta convergencia produce una panoplia instrumental de leyes orientada a la exclusión de los ciudadanos indeseables, ampliando el criterio de discrecionalidad de los funcionarios.

En la praxis, el derecho penal de extranjería contempla 4 mecanismos usuales: 1) los delitos de inmigración, que han proliferado, lo que antes eran infracciones administrativas hoy existe un delito penal, 2) la deportación de un "no ciudadano" como consecuencia de una condena penal (en el Reino Unido: todos los delincuentes no pertenecientes al Espacio Económico Europeo son condenados a 12 meses de prisión preventiva o más sufren una deportación automática al final de su condena, mientras que los pertenecientes a la EEE tendrán una deportación automática recién con 24 meses de detención), 3) la responsabilidad accesoria que aplica sanciones penales como civiles violándose el principio de proporcionalidad de la sanción y el principio de que nadie debe ser castigado dos veces por el mismo delito y 4) las exclusiones civiles, orientadas a crear un entorno hostil para los inmigrantes (los bancos no pueden abrir cuentas corrientes a inmigrantes sin permiso de residencia, no se puede conducir sin un estatus migratorio regular).

Vigilancia migratoria, Inteligencia y detenciones de inmigrantes ilegales

Hoy la policía de inmigración está facultada para efectuar registros, detenciones, confiscaciones y hacer uso razonable de la fuerza en caso necesario, se emplean barreras físicas, entre ellas, tecnologías defensivas como las vallas con alambre de cuchillas, y electricidad, el sistema transnacional de vigilancia y el control migratorio son cada vez más sofisticados e intrusivos

El control migratorio está cada vez más automatizado con el uso de sistemas informáticos y base de datos, biometría y sistemas fronterizos automatizados. Existen procesos de categorización: una lista negra, que conduce a la exclusión de delincuentes y terroristas. EURODAC ha elaborado una lista negra de la UE donde contempla severas sanciones a los transportistas, siendo poco probable que escuchen las explicaciones de los pasajeros, una lista gris que implica la elaboración de perfiles de riesgo a partir de la información anticipada sobre pasajeros, para ello realizan una emisión de alerta e intervención de las autoridades competentes y por último una lista verde: equivale a una inclusión facilitada. Los "deseables", que pueden pasar sin supervisión por las fronteras, tras un control e inspección preliminar inicial tenue. Las detenciones se realizan en zonas de seguridad, ya sea centros de expulsión de inmigrantes, centros de retención de corta duración en aeropuertos y puertos con una variabilidad significativa en el espacio físico. En suma, el sistema de control de la inmigración transnacional inmoviliza al sector supuestamente "indeseable" de nuestra sociedad global.

INMIGRACIÓN, DIVERSIDAD Y CONFLICTO CULTURAL

La identidad cultural

La identidad cultural es el resultado de una construcción social, participa igualmente de la complejidad de lo social (heterogeneidad de todo grupo social), la noción de identidad resulta fundamental para entender la situación intercultural en la que nos encontramos inmersos en el contexto de la globalización. Ella es una estructura dinámica. Hoy existe la tesis de la convergencia de la cultura global basada en que la globalización ha favorecido de alguna manera un modo de homogeneización y acercamiento cultural en el sentido de unificación de modos de vida, símbolos culturales y conductas.

Se habla de la Macdonalización del mundo, sin embargo, ello ha otorgado una renovada relevancia a las identidades étnicas y culturales, tanto en la configuración de los nuevos espacios nacionales, como en la emergencia de universos identitarios como referentes de la convivencia colectiva. El desvanecimiento de las diferencias culturales crea una política de nostalgia. El nuevo discurso de la identidad ofrece la promesa de formas de reconocimiento y de solidaridad que podría compensar la pérdida del antiguo y acogedor consuelo de la etnicidad.

El proceso identitario de los inmigrantes

La construcción de la identidad de los inmigrantes como tales o como miembros de identidades nacionales étnicas, culturales o religiosas es una dinámica más compleja que viene marcada por una serie de condicionantes íntimamente relacionados: los parámetros valorativos de las sociedades receptoras de la inmigración, vale decir el trato o el grado de aceptación que reciben los inmigrantes en la sociedad de acogida, la condición de sujetos fronterizos entre dos mundos, dos sociedades y la discordia entre las expectativas creadas por el inmigrante y la cruda realidad del proceso migratorio.

Se puede afirmar que el inmigrante está negociando constantemente su identidad, aunque en condiciones desfavorables (asimetrías notables y patente desigualdad entre el grupo hegemónico y la cultura minoritaria), la identidad del inmigrante es producto de todos los elementos que le han configurado su cultura, su idioma, sus tradiciones, el proceso migratorio, su integración en el país de acogida. El problema surge cuando la sociedad, tanto de origen como la de acogida, le exige que se defina y se posicione en un sentido o en otro generándose un conflicto cultural. Otro aspecto importante es el relativismo cultural que sostiene que la defensa, legitimación y justificación de las costumbres y tradiciones culturales de las minorías étnicas pueden dan lugar a prácticas contradictorias a la dignidad humana , verbigracia tenemos la mutilación genital.

Pluriculturalidad, multiculturalidad e interculturalismo

La pluriculturalidad es la situación en la que coexisten culturas diferentes en un mismo espacio geográfico, aunque sin una profunda interrelación equitativa. Es una coexistencia que implica una convivencia pacífica, aunque no exenta de conflictos, basada en el respeto mutuo o por lo menos, en una tolerancia entre ellas. El principal obstáculo en una sociedad pluricultural es el etnocentrismo de nuestra propia cultura pretendiendo imponer nuestros modelos culturales rechazando o despreciando lo que es diferente a nosotros. Es imprescindible contar con un discurso de tolerancia en donde prime el respeto y la aceptación de las ideas, creencias o costumbres de los demás aun cuando sean diferentes o contrarias a las propias, e incluso cuando las desaprobemos.

La multiculturalidad es la manifestación de la diversidad y del pluralismo cultural, reivindica el derecho a la diferencia y parte del reconocimiento de la diversidad cultural como un valor, un hecho positivo y enriquecedor. En un contexto espacial cohabitan en un mismo territorio cultural diversas naciones, en estos estados surgen conflictos de minorías nacionales o indígenas, en ellas existen también estados poli étnicos referida a la presencia de distintos grupos étnicos y religiosos. Por último tenemos el interculturalismo, que denota un paso más allá del multiculturalismo, se da en democracias sólidas que apuestan por la interconexión e influencias mutuas entre las culturas. .

LA MIGRACIÓN VENEZOLANA EN EL PERÚ: Realidades y perspectivas

Han inmigrado 7 millones de venezolanos, de los cuales 6 millones se han quedado en la región: es una migración de supervivencia que ha generado una crisis profunda en la región (Perú, Ecuador, Brasil, Colombia, Chile, Paraguay, Argentina, ningún país o población está preparado para acoger en un breve plazo tal volumen de migrantes.

El Perú es el primer país de acogida de venezolanos, de 1´618,000 millones de ciudadanos extranjeros el 71.2 % son ellos son venezolanos, vale decir 1´151,418 venezolanos, la mayoría de ellos cuentan con un permiso temporal de residencia (pasaporte es difícil de obtener), visas humanitarias y peticiones de asilo, ingresos irregulares..

La crisis existente en Venezuela

La crisis existente en Venezuela data desde el período 1999-2013 durante el gobierno de Hugo Chávez y Nicolás Maduro, Venezuela sufrió una crisis económica ocasionada por la caída del precio del crudo, el incremento del salario mínimo en un 1,705 % llegó a 353 $ para cubrir la canasta básica de alimentos, padeciendo el pueblo venezolano de una desprotección total y privación de los DDHH, inseguridad alimentaria, colapso del sistema de salud (25% no tiene acceso al agua, 65% no puede comprar artículos de higiene, ropa, calzado, 72% tiene un suministro irregular de gas), colapso del sistema educativo, corrupción, violencia y criminalidad y pérdida de capital humano y social

Situación actual del inmigrante venezolano

La situación actual del inmigrante es mus difícil, 73% del Perú está contra la migración venezolana por razones económicas, laborales y de criminalidad, ellos son objetos de explotación, discriminación y xenofobia. Se les denomina peyorativamente "venecos", "chamos", "cholos", "serranos". De las 730,000 denuncias policiales, solo el 1,8% involucra a los venezolanos.

Los discursos políticos son inadecuados culpando a los venezolanos de todos los problemas estructurales del país. Los medios de comunicación los incrimina y satiriza con mensajes grotescos. La migración venezolana ha generado deterioro urbano, informalidad, falta de empleo, inseguridad ciudadana. El Ministerio del Interior creó en el seno de la Policía Nacional del Perú una Brigada Especial contra la Migración Delictuosa venezolana, hecho que generó una fuerte crítica internacional para el gobierno.

La inmigración venezolana como amenaza a la seguridad de fronteras

Los extranjeros inmigrantes irregulares venezolanos cruzan la frontera Ecuador-Perú ingresando por Tumbes utilizando puentes móviles no auto-

El conferencista Javier Gamero Kinosita entrega su libro "Amenazas y desafíos a la política de seguridad del siglo XXI " al ministro del Interior del Perú General de la Policía Nacional del Perú PNP (r) Víctor Manuel Torres Falcón, graduado en la Escuela de Carabineros de Chile del General Carlos Ibáñez del Campo.

rizados. Los delitos conexos son el tráfico ilícito de drogas e insumos químicos, la tala y comercio ilegal de madera, la minería ilegal, la trata de personas, contrabando y cultivo de sembríos ilegales de hoja de coca.

Los nexos venezolanos con el crimen organizado

Los nexos venezolanos con el crimen organizado son con el "Tren de Aragua", el "Comando Vermehlo" y los "Caballos de Acero"

El "Tren de Aragua": que tienen presencia en el Perú desde 2022, cuenta con múltiples facciones en el Perú, opera en Lima y tiene apéndices en Ecuador, Colombia y Chile. Su propósito es el control del territorio peruano y está involucrado en delitos de trata de personas para explotación sexual y laboral, extorsión, robo agravado, tráfico ilícito de drogas y sicariato.

El "Comando Vermhelo": cuya presencia fue detectada en el país (Ucayali), tiene presencia en Brasil, Paraguay, Bolivia, su objetivo: los penales para establecer alianzas con bandas, reclutamiento y financiamiento de actividades delictivas. Su propósito es tomar el control absoluto de zonas de producción de cocaína (Madre de Dios, Loreto, Puno). Los delitos que perpetran son el tráfico de armas, sicariato, robo a gran escala, extorsión.

Los "Caballos de Acero": son colectivos armados de Venezuela, las denominadas "motos socialistas", son una estrategia elaborada por Diosdado Cabello (2002) cuando era Gobernador del Estado de Miranda, son grupos de choque a bordo de motocicletas (motocicletas marca ROBBIRA y marca BERA) que comenten actos de represión contra ciudadanos de bien, están armados y ejercen una violencia extrema, comparables al "Tren de Aragua" por su peligrosidad y accionar, son sinónimo de peligro, horror y muerte, y perpetran amenazas, amedrentamientos e infunden miedo colectivo. Aparecen con rostro social, penetran en zonas populares, bajo la fachada de apoyo al pueblo, pretenden ejercer control económico y territorial ("microestados").

En el Perú operan como servicios delivery distribuyendo pizas y pastas y realizan labores de inteligencia, vigilancia, seguimiento y observación.

Han tenido una participación en la denominada "Tercera Toma de Lima". En Venezuela tienen el respaldo de alcaldes, diputados, ministros y funcionarios militares y policiales, su estrategia es la captación de jóvenes en pobreza, ofrecen dinero mensual, les proveen una motocicleta y armamento, entrenados en Cuba, obligándolos a someterse a otros líderes de la zona y obligándolos al participar en acciones de sicariato y extorsiones bajo amenazas de escarmiento, están encapuchados, llevan prendas de color oscuro, se movilizan en motos cuyos tanques de gasolina exhiben calcomanías con la palabra socialista y su fuente de financiamiento es el crimen organizado.

NUEVOS DESAFÍOS DE LA POLÍTICA DE DDHH EN OCCIDENTE RESPECTO A LA MIGRACIÓN

Es necesario tomar acciones en el plano político y diplomático: diálogos, visitas regulares de misiones diplomáticas, comunicados y pronunciamientos, condena de hechos violatorios a los DDHH (sentencias de apedreamiento en determinados países islámicos, mutilaciones genitales femeninas), conferencias de prensa, contactos bilaterales, sanciones políticas y económicas (prohibición de venta de armas…) e iniciativas diplomáticas. En el ámbito de política economica exterior se percibe un ambiente de tensión entre la política economía internacional y la política de derechos humanos, de igual forma es necesario promover la consolidación de la democracia en otras latitudes, la reconversión del derecho internacional en derecho nacional es imprescindible, hay que observar el principio jurídico internacional de que "el derecho internacional quiebre el derecho nacional". Los logros obtenidos en los diálogos diplomáticos son pocos.

Las políticas migratorias constituyen un aspecto crítico, colisionando con los DDHH (reducción severa de asignaciones alimentarias, deportaciones alcanza a hijos menores de edad de ilegales (desarraigo), en caso de matrimonios y concubinatos binacionales, muchos cónyuges o parejas se ven afectados en caso de fallecimiento de los nacionales, negándoseles de los documentos migratorios respectivos, aun cuando hay hijos de por medio. Las adopciones que realizan las parejas de esposos en muchos países industrializados conllevan a la venta ilegal de niños recién nacidos en muchos países de desarrollo. El tráfico de mujeres ha tomado cierta dimensión en Europa, muchas jóvenes de los países en desarrollo son destinadas a la prostitución y son víctimas de maltrato y abuso sexual, otro aspecto importante que debe de ser considerado es el turismo sexual.

RECOMENDACIONES

Dentro de las recomendaciones finales, los Gobiernos deben realizar un planeamiento de estrategia migratoria desde la perspectiva económica (Ravenstein) y sociológica (Znaniecki) de la migración, esto implica desmitificar los mitos populares que existen sobre la migración como lo plantea el investigador holandés Hein de Hass de la Universidad de Ámsterdam, asimismo deben efectuarse reformas legislativas en materia migratoria, diseñar un proyecto intercultural basado en el diálogo y el respeto entre la población receptora y la población migrante, propiciar el involucramiento del estado, el sector privado y la sociedad civil, los medios de comunicación deben informar sin sensacionalismo así como la promoción y facilitación de la regularización migratoria de extranjeros.

Igualmente, se debe combatir la migración ilegal, fortalecer los controles fronterizos y aeroportuarios (nuevas tecnologías), agilizar de la expedición de documentos, las fuerzas de seguridad deben realizar una coordinación interinstitucional para acciones de rescate humanitario, crear un centro de formación de agentes migratorios, el trabajo de integración de la policía es clave para la seguridad pública. La policía debe desarrollar habilidades y competencia transcultural y una competencia de la diversidad que le permita interactuar con otras culturas interactuar con otras culturas.

Hans - Jürgen Lange de la Academia de Policía de Münster en Alemania sostiene, que !sin seguridad no hay integración! y !sin integración no hay seguridad!

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

Carl-Gustaf
En constante evolución

Completando un legado de 75 años, la familia del cañón multifuncional sin retroceso Carl-Gustaf® se encuentra ahora en su cuarta generación y en servicio en más de 40 países

En 1948, el Ejército sueco comenzó a recibir una nueva arma dedicada a combatir los popularmente conocidos tanques de guerra, sustituyendo así una familia de cañones sin retroceso que se venía desarrollado y perfeccionado en el país desde 1942.

A pesar de mantener el mismo nombre, el nuevo modelo Carl-Gustaf® era completamente diferente de sus predecesores e incorporaba soluciones que eliminaban la obsolescencia y la falta de efectividad contra algunos tipos de blindaje.

El calibre elegido, y que se sigue utilizando hoy en día, es de 84 mm, con la salvedad de que el Carl-Gustaf® tiene un cañón estriado para estabilizar parte de la munición por rotación (otras se estabilizan mediante aletas) durante su trayectoria hacia el blanco, una medida que ha aportado mayor precisión.

La nueva generación se desarrolló gracias a las sugerencias y peticiones del ejército sueco, que había estado utilizando el cañón amplia e intensamente, incluso en la crisis del Congo en la década de 1960.

Manteniendo su robustez, en 1964 se lanzó el Carl-Gustaf® M2, cuyo peso se redujo en 1 kg tras algunas mejoras. A partir de esa versión, el cañón comenzó a exportarse a gran escala.

La gran transformación llegó en 1986 con el Carl-Gustaf® M3, que incorporó el cambio del cañón de acero forjado de las versiones anteriores por otro más fino que contenía las estrías, pero recubierto de fibra de carbono para mayor resistencia. Su longitud se redujo en 6 cm, con lo que llegó hasta los 1,07 m, mientras que los herrajes y otras piezas de acero se sustituyeron por componentes de plástico y aleación de aluminio.Como resultado, el arma es cuatro kilos más ligera en comparación con la M1.

También destaca su ergonomía, lo que hace que sea mucho más fácil de transportar y manipular.

"La M3 ha seguido el ritmo de los avances tecnológicos y la compatibilidad con otros accesorios además de la mira telescópica.

El Ejército Brasileño (EB) adoptó esta arma en 1995 para equipar varias de sus unidades de infantería ligera y aeromóvil, estas últimas transportadas por helicópteros. La confiabilidad, multifuncionalidad y portabilidad del equipo fueron algunos de los atributos que guiaron esta elección", explicó Dielson Albuquerque, Director de Ventas de Saab Brasil.

Según el ejecutivo de Saab, el Carl-Gustaf® es un equipo probado en combate, y la prueba de esta experiencia operativa por parte de los operadores significa que Saab mantiene este sistema en constante evolución.

"En 2014 se lanzó la versión M4, que se adapta aún mejor al contexto operativo del siglo XXI. Su peso final es de 7 kg y su longitud se ha reducido a algo menos de 1 metro.

Al ser más pequeño y ligero, reduce el desgaste de las tropas durante las operaciones. La nueva versión ha incorporado importantes mejoras en ergonomía, con más posiciones de ajuste en la empuñadura delantera y en el apoyahombros del arma mediante raíles "picatinny". En el tubo, que ahora está fabricado totalmente en titanio y recubierto de fibra de carbono más ligera, es posible acoplar una mira inteligente con visión térmica y otros accesorios que ayudan al francotirador militar a lograr una mayor precisión y rapidez de tiro", explicó.

En la actualidad, más del 43% de los clientes de todas las versiones de Carl-Gustaf® son miembros de la Organización del Tratado del Atlántico Norte (OTAN) o de la Comunidad Europea. Más de 15 países ya han optado por el Carl-Gustaf® M4.

"El M4 ha permitido a los operadores combatir todas las amenazas del campo de batalla actual, como hemos visto en los conflictos más recientes, incluidos los que aún están en curso. El arma es inteligente y realiza los cálculos balísticos automáticamente, mientras que su nueva munición HE 448 se comunica electrónicamente con el arma, aumentando la velocidad y la precisión de puntería.

En términos logísticos, cuenta con un contador de disparos y diagnósticos computarizados que agilizan las operaciones de mantenimiento, aumentando la disponibilidad para el operador. La capacidad del equipo técnico de Saab para interpretar las demandas y necesidades de los operadores, manteniendo el sistema en constante evolución, ha llevado a muchos usuarios de las versiones M2 y M3 a migrar a M4", concluyó Albuquerque.

Fuente: SAAB en Foco

Carl-Gustaf® M4
Peso: 7kg

Munición: multifuncional -antitanque; contra tropas refugiadas en edificios; contra vehículosligeros; antipersonal; para uso desde entornos confinados; iluminativa; de humo; y de entrenamiento.

Vida útil del cañón:más de 1.000 disparos.

Remuniciamento: pocos segundos.

Guarnición: dos soldados (francotirador y reamunicionador).

Alcance: 300 a más de 2.100 metros, dependiendo de la munición.

Bloqueo: doble, para aumentar la seguridad al transportar el Carl-Gustaf® ya cargado.

Curiosidades
El nombre del cañón sin retroceso de Saab hace referencia a la Carl-Gustaf stads gevärsfabrik (fábrica de rifles de la ciudad de Carl-Gustaf). La ciudad se construyó en torno a las forjas del maestro herrero Reinhold Rademacher tras la concesión del "privilegio de ciudad" por el rey Carlos X Gustavo en 1659. En 1879, se fusionó con la ciudad de Eskilstuna.

Los Cibercomportamientos de Riesgo en la Etapa Infanto-juvenil

Consideraciones fundamentales para los padres y/o cuidadores

Image by pch.vector on Freepik

La pandemia de COVID-19 generó un cambio significativo en la dinámica habitual. Esta transición virtual significó que muchas de las actividades que normalmente se realizaban de forma presencial, tales como: ámbito laboral, educativo o dinámicas familiares, entre otras se adaptaron al ámbito virtual debido a las restricciones del contexto pandemia por COVID-19.

La era digital ha transformado significativamente la forma en que los niños, niñas y adolescentes interactúan con el mundo. La accesibilidad casi ilimitada a la tecnología y las plataformas en línea ha generado oportunidades invaluables, pero también desafíos significativos en lo que respecta a los cibercomportamientos de riesgo.

Los padres y/o cuidadores tienen un rol primordial en guiar a sus hijos (as) a través de este escenario digital, proporcionando orientación, límites saludables y apoyo emocional, entre otras para enfrentar los desafíos inherentes. Esta situación ha resaltado la urgencia de iniciar discusiones sobre cuáles son los hábitos digitales más adecuados para proteger la integridad y la privacidad de los menores de edad cuando navegan en el entorno digital y como los padres abordan esta problemática.

La primera consideración para los padres y/o cuidadores es la supervisión y el acompañamiento responsable. Radica en comprender la naturaleza de estos cibercomportamientos de riesgo que podrían afectar su integridad y la de sus familias. Diferentes estudios, señalan que las interacciones en línea pueden exponer a los niños, niñas y adolescentes a peligros, tales como: el ciberacoso, el sexting, la sobre exposición a redes sociales o a contenido inapropiado, y la adicción a la tecnología, entre otros. En este sentido, se deben abordar desde una perspectiva integral, reconociendo aspectos técnicos, como psicosociales en el uso de Internet por parte de los niños, niñas y adolescentes. Un ejemplo de ello es el ciberacoso y la importancia del aprendizaje vicario (con evidencia científica), donde los niños, niñas y adolescentes observan y modelan el comportamiento de los padres y/o cuidadores.

La evidencia disponible plantea que cuando los padres tienen una relación saludable y constructiva, están proporcionando un modelo a seguir para los niños, niñas y adolescentes, ya que aprenden a manejar conflictos, y a comunicarse de forma efectiva, estableciendo relaciones basadas en el respeto y la empatía al observar estas interacciones positivas entre sus padres. Esto se relaciona con el ciberacoso porque la dinámica saludable entre los padres sirve como un factor de protección, tienden a tener un mejor ajuste emocional, académico y social.

Los niños, niñas y adolescentes que experimentan conflictos en el hogar pueden ser más vulnerables a involucrarse en situaciones de ciberacoso como forma de escape. Un entorno familiar positivo y de aprendizaje puede fortalecer la autoestima y la resiliencia de los niños, niñas y adolescentes disminuyendo así, la probabilidad de ser víctimas o perpetradores del ciberacoso.

En segundo lugar, los padres deben enfocarse en establecer una comunicación comprensiva y flexible con sus hijos; subrayando la importancia de construir un ambiente en el hogar donde los niños, niñas y adolescentes se sientan en un espacio seguro y de confianza para compartir sus experiencias en el entorno digital, incluyendo las positivas y las negativas. La confianza y el entendimiento mutuo son esenciales para que los padres y/o cuidadores puedan orientar sin generar resistencias por parte de los menores de edad. La

crianza positiva en la práctica parental durante situaciones de riesgo o de crisis juega un rol fundamental, ya que las experiencias adversas en la infancia, aquellas relacionadas como, por ejemplo: con la falta de apoyo emocional, ciberacoso, tipos de violencia, entre otros puede tener un impacto en la salud mental infantil a largo plazo, especialmente en los contextos de aumento de tensiones y demandas de nuestra sociedad chilena actual.

En tercer lugar y último, el apoyo de las instituciones educativas y de salud hacia los padres y/o cuidadores, es importante. A modo de ejemplo, la transición virtual significó que las instituciones educativas adoptaran rápidamente herramientas y plataformas digitales para impartir clases, realizar evaluaciones y mantener la continuidad del aprendizaje a distancia. Este cambio no solo implicó la utilización de tecnología, sino también adaptaciones en los métodos de enseñanza, la comunicación entre docentes y estudiantes sumado a la interacción con los profesionales de la salud, y la gestión de los recursos educativo, entre otros.

Desde esta óptica, la familia constituye social y jurídicamente el contexto natural y esencial de protección y seguridad para el desarrollo de niños, niñas y adolescentes, en donde deben estar actualizándose continuamente sobre las últimas tendencias y desafíos en la era digital. Esto significa que los riesgos también cambian con el tiempo.

Existe evidencia disponible sobre esta temática en torno a que los padres deben ser conscientes de las plataformas, horarios de uso, aplicaciones y tendencias emergentes que pueden impactar la seguridad y bienestar de los niños, niñas y adolescentes en el entorno digital y/o presencial y viceversa.

Finalmente, se subraya la importancia de la participación activa de los padres y/o cuidadores en la etapa infanto-juvenil frente al cibercomportamiento de riesgo; 1) Identificar y comprender situaciones de conflicto, acoso escolar y ciberacoso, entre otros. Destacando los cibercomportamientos de riesgo que se pueden desarrollar en la etapa infanto-juvenil, tanto en los contextos escolares y/o familiares, por ejemplo: el impacto en la salud física, psicoemocional y contexto social y educativo de las víctimas, entre otras; 2) Desarrollar competencias asociadas al modelo parental positivo en torno a la comunicación, la supervisión parental, la responsabilidad y establecimiento de límites, para la prevención de problemáticas como el acoso escolar y el ciberacoso, entre otros; y 3) Apoyo institucional de distintas disciplinas: Intervención familiar fortaleciendo las competencias parentales para influir en los cibercomportamientos de riesgo de la población infantojuvenil, además de proponer otras herramientas de intervención desde el aula en el ámbito educativo.

Surge la necesidad de establecer hábitos digitales saludables para proteger la integridad, física, mental y social de los niños, niñas y adolescentes, ya que la tecnología presenta desafíos complejos y la familia tiene un rol fundamental de protección y desarrollo de los niños, niñas y adolescentes, donde la constante actualización de los padres y/o cuidadores en torno a las tendencias digitales emergentes y la colaboración de varios sectores de la sociedad, mejorarían el bienestar, calidad de vida y la prevención del suicidio de niños, niñas y adolescentes.

Fig.1: Aspectos claves de la tecnología y diferentes estrategias para padres y/ cuidadores a

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

Teoría y práctica sobre Gestión de Riesgos

Image by master1305 on Freepik

La gestión de riesgos es un elemento esencial para cualquier empresa. Sin embargo, no todos los riesgos se abordan de la misma manera. Algunas medidas de control destinadas a mitigar o compartir riesgos son obligatorias debido a requisitos legales, mientras que otras se implementan en función de las necesidades individuales y circunstancias específicas de cada organización. En este artículo, nos centraremos específicamente en ejemplos de medidas de mitigación o compartición de riesgo que son obligatorias por exigencias legales. Desde seguros obligatorios, normativas de salud y seguridad en el trabajo, hasta regulaciones de privacidad de datos y leyes contra el lavado de dinero.

Si eres un profesional en gestión de riesgos, un empresario, o simplemente alguien interesado en entender mejor cómo las leyes ayudan a dar forma a las prácticas de gestión de riesgos, este artículo te proporcionará una visión clara y amplia de estas cuestiones complejas y cruciales.

Las leyes ayudan a dar forma a las prácticas de gestión de riesgos. Como es conocido por muchos, una vez analizados los riesgos y determinado su nivel, comparándolo con los criterios de riesgo establecidos en la etapa de contextualización (ISO 31000), tendremos una OPINIÓN.

Esta opinión nos ofrece un primer nivel de decisión, como: Actuar; Actuar y observar; Solo observar; e Ignorar. En los casos en los que se decida actuar, se necesita implementar un tratamiento basado en controles. En los casos donde se indique observar, será necesario definir una estrategia de monitoreo y control de los respectivos riesgos.

En la ISO 31000:2018, en su ítem 5.5.1 (Tratamiento de riesgo > Generalidades), se consideran las siguientes opciones de tratamiento de riesgos a continuación.

Destacando que estas opciones NO son necesariamente excluyentes. a) Evitar el riesgo decidiendo no iniciar o discontinuar la actividad que genera el riesgo; b) Tomar o aumentar el riesgo en busca de una oportunidad; c) Eliminar las fuentes de riesgo; d) Modificar la probabilidad; e) Modificar las consecuencias; f) Compartir los riesgos (por ejemplo, mediante contratos o compra de seguros); g) Retener el riesgo basándose en una decisión informada.

En general, podemos determinar que estas siete opciones de tratamiento indicadas por la ISO 31000 pueden incluirse en uno de los tres grupos siguientes: 1. Evitar; 2. Minimizar; 3. Aceptar, retener o asumir más riesgo.

Entre las opciones destinadas a evitar los riesgos, la norma indica: a. Evitar el riesgo al decidir no comenzar o continuar la actividad que genera el riesgo; y c. Eliminar la fuente de riesgo. Entre las opciones destinadas a minimizar los riesgos se consideran: d. Modificar la probabilidad; e. Modificar las consecuencias; y f. Compartir el riesgo.

Entre las opciones de aceptación y retención están: Aceptar o aumentar el riesgo en busca de una oportunidad y retener el riesgo basándose en una decisión informada.

Opciones: Evitar; Minimizar; o Aceptar, retener y asumir más riesgo. En las clases y cursos que impartimos, es común escuchar la siguiente pregunta: Profesor, ¿puede dar algunos ejemplos de controles, con el objetivo de mitigar o compartir riesgos, que sean obligatorios debido a requisitos legales? Bien, vamos allá, ¡vamos a acercar la teoría y la práctica!

El tratamiento de riesgos busca evitar que la incertidumbre afecte nuestros objetivos. Sin embargo, retener el riesgo, es decir, aceptar que intentaremos alcanzar un objetivo asumiendo la incertidumbre, también es una opción. Pensando

en ello, en esta reflexión, vamos a imaginar el siguiente escenario: Supongamos una situación ficticia en la cual identificamos un evento que podría ocurrir en la organización el próximo año con una probabilidad de 0,01 (es decir, si pudiéramos repetir la operación de la empresa cien años seguidos, en las mismas condiciones, sería de esperar que, en esos cien años, al menos una vez ocurriese dicho evento). Si ese evento se concretiza, tendríamos un desvío del 60% de nuestro objetivo respecto a nuestras expectativas.

Con esta suposición, vamos a reflexionar: ¿Qué puede determinar si decidimos tratar el riesgo mediante compartición (ej.: seguro) o mitigación (ej.: disminución de frecuencia o impacto)? La determinación de tratar el riesgo a través de la compartición o mitigación puede estar condicionada por varios factores. Aquí hay algunas opciones que pueden influir en esta decisión:

1. Impacto en los objetivos: La magnitud del impacto del evento en los objetivos de la organización es fundamental para evaluar la opción de compartición o mitigación del riesgo. Si el desvío de la meta del 60% se considera inaceptable o pudiera tener graves consecuencias para la empresa, la mitigación del riesgo podría ser considerada.

2. Coste de la compartición: Compartir el riesgo implica contratar seguros u otras formas de compartición (transferencia) de parte de la responsabilidad a terceros. Si el costo de transferir el riesgo mediante primas de seguro u otros mecanismos es razonable y justificable en comparación con el impacto potencial del evento, la transferencia podría ser una opción viable.

3. Capacidad de mitigación: La empresa debe evaluar su capacidad para implementar medidas efectivas de mitigación y reducir la probabilidad o el impacto del evento. Si existen estrategias o acciones concretas que puedan implementarse para disminuir la probabilidad de ocurrencia o reducir el impacto del evento, la mitigación podría ser una opción preferible.

4. Apetito, tolerancia y capacidad de riesgo: El apetito, la tolerancia y la capacidad de riesgo de la empresa y su disposición a asumir cierto nivel de incertidumbre también influyen en la decisión. Si la empresa tiene un mayor apetito y tolerancia al riesgo y está dispuesta a aceptar el impacto potencial del evento (capacidad) sin significativa mitigación, podría optar por retener el riesgo en lugar de transferirlo o mitigarlo.

5. Evaluación de la probabilidad: La evaluación precisa de la probabilidad del evento es esencial para tomar una decisión informada. Si la probabilidad de ocurrencia es baja, como 0,01, la transferencia del riesgo podría no ser una opción viable, ya que podría ser difícil encontrar aseguradoras dispuestas a cubrir estos eventos improbables.

6. Disponibilidad de recursos: La disponibilidad de recursos financieros, tiempo y humanos puede influir en la decisión de cómo tratar el riesgo. Si cuenta con los recursos necesarios para implementar medidas de mitigación efectivas, podría ser preferible optar por esta opción, en lugar de la transferencia de riesgo.

7. Contexto y naturaleza del evento: La naturaleza y el contexto del propio evento pueden influir en la elección del enfoque de tratamiento del riesgo. Algunos eventos pueden ser más adecuados para la mitigación, mientras que otros pueden ser más propicios para la compartición. Por ejemplo, si el evento es altamente improbable, pero tiene un impacto catastrófico, podría ser más apropiado transferir el riesgo mediante un seguro, o instrumentos financieros adecuados.

Apetito, tolerancia y capacidad de riesgo. En última instancia, la determinación de cómo tratar el riesgo dependerá de un análisis exhaustivo que tenga en cuenta estos y otros factores, así como la evaluación de alternativas y la consideración de los recursos y capacidades disponibles para la empresa.

Image byFreepik

Es importante señalar que la elección entre compartir (transferir) el riesgo y mitigar el riesgo no es necesariamente mutuamente excluyente. En algunos casos, puede ser apropiado usar una combinación de ambas estrategias, dependiendo de la naturaleza del riesgo y de los recursos y capacidades disponibles.

Otra pregunta común que nos obliga a aterrizar la teoría en la práctica es la siguiente: Profesor, ¿es aceptable que la organización retenga el riesgo? En este caso, ¿bajo qué condiciones sería aceptable retener riesgos? ¡Vamos allá! La decisión de retener el riesgo es una opción válida en determinadas circunstancias y depende del apetito, tolerancia y capacidad de riesgo de la organización, así como de la habilidad para manejar las posibles consecuencias.

Asumir el riesgo implica aceptar que los objetivos se alcanzarán a pesar de la incertidumbre y de la posibilidad de que ocurra el evento no deseado. La decisión de retener el riesgo es una opción válida en determinadas circunstancias y depende del apetito, la tolerancia y la capacidad de riesgo de la organización.

Sin embargo, antes de optar por retener el riesgo, es necesario evaluar cuidadosamente las implicaciones, considerar algunos aspectos y condicionantes:

• Impacto económico: Es importante evaluar si el desvío del objetivo debido al evento adverso es económicamente aceptable para la organización. Si el desvío del 60% en las expectativas pudiera tener consecuencias graves o comprometer la viabilidad del negocio, tal vez sea más prudente considerar el tratamiento del riesgo.

• Capacidad de recuperación: Es necesario evaluar la capacidad de recuperación y adaptación de la organización en caso de que ocurra el evento adverso. Si la organización tiene la capacidad de adaptarse y recuperar rápidamente sus operaciones, la retención de riesgos podría ser una opción viable.

• Planificación de contingencia: Retener el riesgo no significa ignorarlo completamente. Es importante desarrollar planes de contingencia, continuidad del negocio y tener estrategias alternativas en caso de que se concrete el evento adverso.

• Análisis continuo del riesgo: Retener el riesgo implica estar preparado para evaluar y monitorear continuamente la evolución del riesgo. La organización debe estar dispuesta a ajustar sus estrategias y planes según los cambios en el entorno y la evolución del riesgo. Planificación de contingencias Otra cuestión que nos exige acercar teoría y práctica es la siguiente:

Profesor, ¿puede darnos ejemplos de medidas de mitigación o compartición (transferencia) de riesgos que sean obligatorios debido a requisitos legales? Ciertas medidas de mitigación o compartición de riesgo pueden ser exigidas por requisitos legales o regulaciones específicas. La mayoría de los ejemplos a continuación están presentes en la vida cotidiana de las personas comunes. Aquí hay algunos ejemplos:

1. **Seguro obligatorio**: En muchos países, es obligatorio que los propietarios de vehículos tengan un seguro de coche. También puede ser necesario que los propietarios tengan un seguro contra incendios o inundaciones, o que los empleadores tengan un seguro de accidentes de trabajo.

2. **Cumplimiento con los reglamentos de seguridad**: Las empresas deben seguir los reglamentos de salud y seguridad en el lugar de trabajo, como proporcionar equipos de protección individual a los empleados o seguir los reglamentos de seguridad contra incendios.

3. **Prácticas de higiene en la industria alimentaria**: Las empresas alimentarias deben seguir los reglamentos de seguridad alimentaria para reducir el riesgo de contaminación de alimentos y brotes de enfermedades transmitidas por alimentos.

4. **Licencias y autorizaciones**: Profesionales de ciertas industrias deben tener licencias para operar, como médicos, abogados y electricistas.

Foto de Jimmy Chanpexels.com

Foto de Phúc Hoàng: pexels.com

Esto garantiza que estén debidamente calificados y entrenados para reducir el riesgo de errores o negligencia.

5. **Cumplimiento con los reglamentos de privacidad de datos**: Las empresas que manejan datos personales deben cumplir las leyes de protección de datos, como el GDPR en la Unión Europea o LGPD en Brasil, para mitigar el riesgo de violación de datos personales y multas legales.

6. **Evaluaciones de impacto ambiental**: Antes de iniciar proyectos a gran escala, las empresas pueden estar obligadas a realizar evaluaciones de impacto ambiental para mitigar riesgos al medio ambiente.

7. **Cumplimiento con los reglamentos contra el lavado de dinero**: Las instituciones financieras deben cumplir con reglamentaciones para prevenir el lavado de dinero y el financiamiento del terrorismo, que incluyen la identificación del cliente y reportes de transacciones sospechosas, etc.

8. Plan de Emergencia y Evacuación: En muchos lugares, se exige por ley que las empresas tengan un plan de emergencia y evacuación en caso de incendio, terremoto u otras emergencias.

9. **Cumplimiento con los estándares de calidad**: En ciertas industrias, como farmacéutica o alimenticia, los estándares de calidad deben ser cumplidos para garantizar la seguridad del producto.

10. **Seguridad cibernética**: dependiendo del país y de la naturaleza del negocio, algunas empresas pueden estar obligadas a implementar medidas de seguridad cibernética para proteger datos e información digital contra amenazas y ataques cibernéticos, incluido el seguro cibernético.

11. **Gestión de riesgos financieros**: En el ámbito financiero, las instituciones pueden estar sujetas a regulaciones que exijan la implementación de medidas de mitigación de riesgos, como requisitos mínimos de capital, pruebas de estrés y políticas de gestión de riesgos.

Estas medidas buscan proteger la estabilidad financiera y evitar riesgos sistémicos. Plan de Emergencia y Evacuación Otra pregunta común en las clases es: Profesor, ¿por qué existen riesgos sujetos a estas obligaciones de tratamiento y otros riesgos no? Las obligaciones legales para abordar ciertos riesgos a menudo surgen del deseo de proteger la salud, la seguridad, los derechos y el bienestar de las personas y del medio ambiente. Estas obligaciones pueden surgir de experiencias pasadas en las que la ausencia de tales obligaciones condujo a consecuencias dañinas, como accidentes laborales, contaminación ambiental, invasión de privacidad, problemas de salud pública, etc. Aquí algunas posibles razones:

1. **Protección de intereses públicos**: Las obligaciones legales de tratamiento de riesgos se establecen a menudo para proteger intereses públicos, como la salud y seguridad de las personas, la protección del medio ambiente o la estabilidad financiera. Los riesgos con un impacto significativo en estos intereses suelen estar sujetos a regulación específica para asegurar su mitigación.

2. **Historial de incidentes o impactos previos**: En algunos casos, los riesgos que resultaron en incidentes graves en el pasado, o que demostraron tener un impacto significativo en la sociedad pueden llevar a la implementación de regulaciones obligatorias. Estas regulaciones buscan prevenir la repetición de incidentes y garantizar una adecuada gestión de los riesgos asociados.

3. **Asimetría de información**: En ciertas situaciones, los riesgos pueden estar regulados cuando hay asimetría de información entre las partes involucradas. Por ejemplo, en la protección de derechos del consumidor, las regulaciones pueden imponer obligaciones de divulgación y transparencia para asegurar que los consumidores estén

informados sobre los riesgos asociados a los productos o servicios que compran.

4. **Externalidades negativas**: Algunos riesgos pueden generar externalidades negativas, es decir, impactos adversos en terceros que no son considerados por quienes toman decisiones relacionadas con el riesgo. En estos casos, las regulaciones pueden implementarse para internalizar estas externalidades y responsabilizar a las partes interesadas relevantes por los riesgos que generan.

5. **Intereses comerciales y económicos**: Algunos riesgos pueden estar sujetos a regulación debido a intereses comerciales y económicos. Por ejemplo, las regulaciones financieras buscan salvaguardar la estabilidad del sistema financiero y proteger a los consumidores, mientras que las regulaciones comerciales pueden buscar garantizar una competencia justa y prevenir prácticas comerciales desleales.

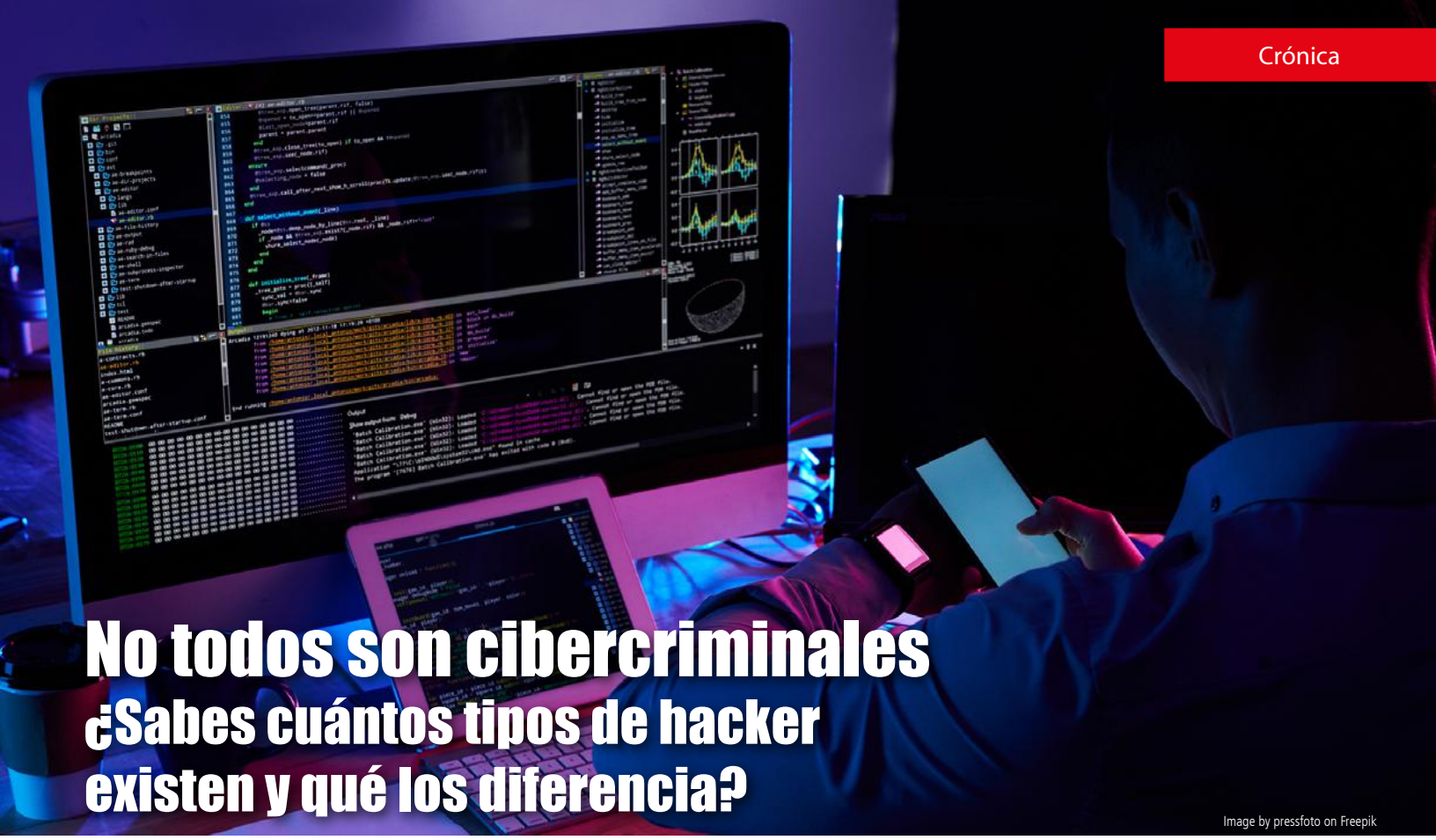
En conclusión, existen varias medidas de mitigación y compartición de riesgo que son obligatorias debido a requisitos legales. Estas incluyen seguros obligatorios, cumplimiento con reglamentos de seguridad, prácticas higiénicas en la industria alimentaria, obtención de licencias y permisos, cumplimiento con reglamentos de privacidad de datos, realización de evaluaciones de impacto ambiental, cumplimiento con regulaciones contra el lavado de dinero, implementación de planes de emergencia y evacuación, cumplimiento con estándares de calidad y la adopción de medidas de seguridad cibernética.

Estas obligaciones legales son a menudo el resultado de intentar proteger la salud, la seguridad, los derechos y el bienestar de las personas y del medio ambiente. Muchas de ellas buscan proteger al público, prevenir daños, proteger derechos individuales, promover la responsabilidad corporativa, ética y prevenir actividades ilegales.
Estas obligaciones a menudo provienen de lecciones aprendidas de incidentes anteriores donde la falta de regulación llevó a resultados dañinos.

Algunos riesgos se consideran parte inherente de determinadas actividades. Por otro lado, no todos los riesgos están sujetos a obligaciones legales de tratamiento. Esto puede deberse a que son difíciles de regular, se consideran parte inherente de ciertas actividades o porque las intervenciones legales pueden no ser el método más eficaz de gestionar estos riesgos.

En estos casos, la gestión de riesgos puede ser más informal o depender de los individuos u organizaciones involucradas. En resumen, las medidas legales de mitigación y compartición de riesgos buscan proporcionar un marco de seguridad y responsabilidad que proteja a las personas, organizaciones y al medio ambiente de posibles daños, aunque reconoce que no todos los riesgos pueden o deben ser gestionados mediante inter-

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 Ibros del área de la seguridad



No todos son cibercriminales

¿Sabes cuántos tipos de hacker existen y qué los diferencia?

Image by pressfoto on Freepik

Aunque es común que la palabra hacker se vincule (erróneamente) a la ciberdelincuencia, un hacker no es más que una persona con grandes habilidades en el manejo de sistemas informáticos, "que investiga fallos y desarrollan técnicas de mejora", según una de las acepciones de la Real Academia Española (RAE). Pero cuando en 2013 se había incorporado el término (jáquer) en el diccionario, la RAE solo lo definía como "pirata informático"; algo que reforzaba la asociación entre hacker y quienes hacen uso de sus habilidades con fines maliciosos. Finalmente, en 2018, después de fuertes debates en la comunidad, se incorporó esta nueva acepción que es más acorde a los tiempos que corren.

En el medio de estos dos conceptos, quedan quienes se mueven en una zona mixta, y sus actividades están entre la legalidad y la ilegalidad. Pero hay que comprender que, la mayoría de los hackers, usan sus habilidades de manera lícita y, de hecho, son contratados para evaluar y probar la seguridad de los sistemas digitales.

Desde ESET analizan cuál es la clasificación del universo hacker de acuerdo con sus motivaciones y sus niveles de experiencia, para comprender este panorama en constante evolución.

Hackers de sombrero blanco o éticos. Son profesionales altamente especializados cuya misión es proteger a las empresas y organizaciones de las amenazas digitales. Están autorizados a probar sistemas, identificando vulnerabilidades y fortaleciendo la seguridad de la información. Más aún, siguen estrictamente las normas y reglamentos. Su motivación es ayudar a las empresas a construir defensas sólidas, detectar brechas en la seguridad de la red y solucionarlas antes de que los ciberdelincuentes tengan la oportunidad de explotarlas, y así contribuir a un entorno digital más seguro y confiable.

Hackers de sombrero negro. Son expertos en informática, pero operan con malas intenciones. Piratean los sistemas con el fin de obtener acceso no autorizado para robar datos valiosos o comprometer la integridad de los sistemas. Su motivación y objetivos son claros: hackear las redes de las organizaciones en busca de datos financieros o información sensible, utilizar los recursos robados para su propio beneficio, venderlos en la deep web o causar un daño significativo a la empresa objetivo.

Hackers de sombrero gris. Ocupan una posición intermedia entre los hackers de sombrero blanco y negro. Operan sin autorización oficial, con motivaciones y ética que varían ampliamente. Sus objetivos no están claramente definidos y pueden abarcar una variedad de intereses. Con frecuencia explotan los sistemas en busca de vulnerabilidades, pero sin la intención explícita de dañar a terceros, lo que hace que este grupo sea diverso y ambiguo en sus acciones e intenciones.

Script Kiddies. Son hackers aficionados que carecen de conocimientos profundos en el campo de la ciberseguridad. Intentan entrar en sistemas, redes o sitios web utilizando scripts y herramientas desarrolladas por hackers más experimentados. Su objetivo principal es llamar la atención, recurriendo a ataques de denegación de servicio (DoS) para interrumpir los servicios en línea.

Hackers Green Hat. Son hackers de nivel básico que actúan como aprendices en la búsqueda de perfeccionar sus habilidades de hacking. A diferencia de aquellos más experimentados, se centran en aprender y adquirir conocimientos en el campo. A menudo tienen un gran interés en colaborar con hackers más experimentados, con el objetivo de absorber conocimientos y técnicas avanzadas. Aunque no son maliciosos por naturaleza, su inexperiencia y curiosidad pueden llevarlos a veces a explotar sistemas y redes sin autorización.

Hackers Red Hat. También conocidos como "Eagle Eye Hackers", su principal intención es combatir a los hackers de sombrero negro. Si bien comparten algunas similitudes con los hackers White Hat, ya que actúan en el lado de la ciberseguridad, tienden a adoptar tácticas más agresivas de sustitución de sistemas comprometidos y la adopción de medidas directas para combatir las amenazas digitales.

Hackers patrocinados por el Estado/nación. Se trata de individuos o grupos generalmente contratados o designados por los gobiernos para llevar a cabo operaciones cibernéticas en beneficio del Estado. Su objetivo principal es obtener información sensible de otros países para reforzar la seguridad y prepararse contra posibles amenazas, ya sean de naturaleza militar, política o económica. Operan en secreto y, con frecuencia, tienen

recursos sustanciales a su disposición, lo que les permite llevar a cabo campañas cibernéticas avanzadas.

Hacktivistas. Utilizan sus habilidades de hacking para promover causas políticas o sociales. Su objetivo es exponer información, generalmente relacionada con gobiernos o entidades poderosas, con el fin de llamar la atención sobre temas que consideran importantes. Sus acciones suelen tener motivaciones políticas o sociales, y pueden incluir la divulgación de documentos confidenciales, hackeos a sitios web o redes sociales, e incluso la interrupción de los servicios en línea en un intento de promover el cambio o aumentar la conciencia pública sobre ciertos temas. Pueden operar de forma anónima y, a menudo, utilizan seudónimos para protegerse de las represalias.

Insiders malintencionados o denunciantes. Son personas que trabajan dentro de las organizaciones y revelan deliberadamente información confidencial o realizan acciones dañinas contra la propia empresa. Sus motivaciones pueden variar, y sus acciones a menudo son impulsadas por razones personales como descontento con la organización para la que trabajan. Además, pueden actuar con el objetivo de exponer actividades ilegales o poco éticas de la organización, las cuales pueden incluir la filtración de información confidencial, el sabotaje de sistemas o, en casos extremos, la colaboración con autoridades externas para investigar actividades sospechosas.

La variedad y enfoques de hackers refleja la complejidad del panorama cibernético actual, donde la lucha entre el bien y el mal digital está en constante evolución. La ciberdelincuencia tiene el potencial de afectar la seguridad de una nación, la privacidad de las personas y la integridad de las organizaciones. Por ende, el conocimiento y la concienciación son centrales en la protección contra las amenazas, independientemente de la motivación que haya detrás de ellas.

Autor: Mario Micucci, Investigador de Seguridad informática de ESET Latinoamérica.

ZKTECO fue parte del encuentro de referentes en seguridad a nivel mundial organizado por el capítulo 233 de ASIS

El pasado 15 de diciembre, en las dependencias del Hotel Regal Pacific, se realizó el encuentro ASIS Chile Night, una innovadora dinámica de networking que contó con destacados profesionales del ámbito de la seguridad.

ASIS International fue fundada en 1955 y es una comunidad global de profesionales de la seguridad, sin fines de lucro y la más grande del mundo de profesionales de seguridad, en la cual cada uno de sus miembros tiene un papel preponderante en la protección de los activos de una organización, esto es, personas, bienes o propiedades y también la información.

ASIS se organiza a nivel global por medio de Capítulos (Chapters) que agrupan a los miembros representantes de un determinado país, con miras a hacer expansivos los beneficios de su pertenencia. En este orden de ideas, ASIS CHILE (Capítulo 233), se orienta a fomentar y aumentar la eficacia y la productividad de los profesionales de la seguridad, por medio del desarrollo de programas y certificaciones que amplían el espectro de conocimientos, experiencias y habilidades sobre los intereses generales de la seguridad.

Durante la jornada, estuvieron presentes Carlos Ramírez, CPP presidente capítulo 233 Chile para el año 2023, Marcelo Serey presidente capítulo 233 para el año 2024, Ignacio Santibáñez, APP vicepresidente Capítulo 233 Chile, entre otros directivos, quienes manifestaron su compromiso respecto al trabajo realizado en 2023.y las proyecciones en Chile durante este 2024.

"Quienes formamos parte del ASIS Internacional Chapter 233 Chile, estamos muy animados por la convocatoria que estuvo abierta a especialistas de la industria de seguridad, y les instamos a todos a desarrollarse profesionalmente por medio de las oportunidades que están disponibles en organización", declaró Alvar Orellana, Director Board LARC (Latam y El Caribe) de ASIS International .

"Como directiva, nos enfrentamos a diversos desafíos para el año 2024. Nos comprometimos a llevar a cabo actividades de difusión destinadas a destacar la relevancia de ASIS y sus beneficios para los profesionales de la seguridad en Chile. Nuestro objetivo principal es aumentar significativamente el número de socios del capítulo, estimando un crecimiento de entre un 25% y un 30% para el próximo año.

Nos centraremos especialmente en atraer a mujeres y jóvenes profesionales del ámbito de la seguridad, y para lograrlo, planeamos establecer alianzas estratégicas con universidades e institutos profesionales que actualmente ofrecen programas relacionados con la gestión de la seguridad privada, nuevas tecnologías y ciberseguridad.

Otra iniciativa clave será fortalecer nuestra colaboración con las policías y fuerzas armadas, destacando los beneficios de ser parte de asociaciones como ASIS International. Buscamos orientar y brindar apoyo a profesionales que, al egresar de estas instituciones, estén interesados en explorar oportunidades laborales en el sector privado.

Adicionalmente, estamos en proceso de planificación de los próximos webinars y seminarios presenciales que se llevarán a cabo a lo largo del año. Nuestra intención es contar con la participación de expertos y proporcionar espacios para que las empresas presenten las nuevas soluciones disponibles en el mercado. Queremos fomentar el intercambio de conocimientos y experiencias en beneficio de la comunidad de seguridad en Chile", expresó Ignacio Santibáñez, APP vicepresidente Capítulo 233 Chile.

En un aspecto de esta innovadora dinámica de networking, apreciamos de izq. a der. a Alvar Orellana McBride, CEO de Griffin Risk, Raúl Muñoz, gerente general de Infostrata Consultores y Gustavo Maluenda, CEO de ZKTeco Chile

Seguridad Ciudadana
Un gran desafío del siglo XXI

El día sábado 11 de noviembre de 2023 se llevó a cabo en el Cantón de Santa Ana en Costa Rica el II Congreso Internacional de Seguridad Ciudadana en Costa Rica, organizado por la Municipalidad de Santa Ana y la Red Internacional de Profesionales en Seguridad (RIPS) – Capítulo Costa Rica. Las palabras de inauguración del evento estuvieron a cargo del Alcalde de ese cantón, Licenciado Gerardo Oviedo Espinoza y el Presidente fundador de RIPS, Julio Corrales Bustos.

Los conferencistas participantes en el evento fueron Gerardo Brenes Montoya de Costa Rica quién presentó "Las estadísticas criminales de Costa Rica", el licenciado Luis Solano Alfaro con el tema "El tráfico y la trata en la niñez costarricense y las nuevas tendencias", la licenciada Fiorella Rojas Ballestero con el tema "Análisis de conductas vulnerables en Internet y su relación con la trata y tráfico de personas", la magister Karen Jiménez Morales con el tema "Importancia de la profesionalización de la labor policial", el ex Ministro de Seguridad Pública de Costa Rica Juan José Andrade Morales con el tema "El impacto de la toma de decisiones en la seguridad Costa Rica" y finalmente como conferencista internacional invitado, el jurista y criminólogo magister Javier Gamero Kinosita, actual coordinador de la International Police Association (IPA) - Sección Perú en Europa, con residencia en Suiza con el tema "Amenazas y desafíos a la política de seguridad del siglo XXI"

EXTRACTO DE LAS CONFERENCIAS DEL CONGRESO

El plan fastidio como medida de prevención en Costa Rica

El plan fastidio es un estrategia implementada en algunas comunidades en Costa Rica, en virtud del deterioro de las condiciones sociales y el incremento de la inseguridad ciudadana en las últimas décadas, para fortalecer la seguridad ciudadana y reducir la comisión de faltas y delitos.

Este proyecto se centra en identificar e intervenir ipso facto ante comportamientos incómodos o molestos, que aunque no constituyen delitos graves afectan la calidad de vida de las personas y generan un ambiente de inseguridad en la comunidad. Dichas actitudes o comportamientos se refieren a situaciones que no pueden ser ilegales en sí mismas, pero que provocan malestar, incomodidad o sensación de inseguridad en el espacio público, verbigracia tenemos, el consumo de alcohol en la vía pública, grafitis, mendicidad agresiva, ruidos excesivos, comportamiento incívicos, hasta actitudes que generen un ambiente hostil en espacios públicos.

El plan fastidio se basa en la idea que al abordar de inmediato y controlar estos comportamientos incómodos y disruptivos, se puede prevenir la escalada de delitos más graves y mejorar la percepción de inseguridad de la comunidad. En lugar de esperar que los problemas de seguridad se agraven, se interviene de manera temprana en estas actitudes molestas para evitar posibles consecuencias negativas.

Las acciones del plan fastidio involucran una combinación de medidas preventivas y de control. Se un giro en la política criminal contemporánea, virándose de una política criminal post crimen, que demanda una actitud represiva activa por parte de la policía una vez perpetrado el hecho delictivo hacia una política criminal pre crimen, que demanda una actitud preventiva pro activa por parte de las autoridades policiales, para que no se perpetre ese hecho delictivo.

Entre las estrategias utilizadas se encuentran la sensibilización y educación, vale decir campañas de concientización para sensibilizar a la población sobre la importancia de mantener conductas respetuosas en el espacio público, presencia policial y patrullaje a pie y motorizado sobre todo en áreas con altos índices de comportamientos molestos, pues un patrullaje activo ayuda a disuadir y controlar estas inconductas, coordinación con servicios sociales, programas para ayudar a personas en situación de vulnerabilidad o personas en riesgos de caer en conductas delictivas, aplicación de sanciones leves (advertencias, multas,

etc.), mejoramiento del entorno e infraestructura urbana.

En virtud del deterioro de las condiciones sociales en las últimas décadas en Costa Rica, dicho plan tiene como finalidad arremeter contra toda inconducta y la más pequeña indisciplina social generando un ambiente hostil, hostigando e importunando permanentemente al ciudadano proclive a estas conductas antisociales, que puedan generar malestar y desorden bajo los paradigmas de la teoría de la tolerancia cero.

Estadísticas criminales en Costa Rica

Costa Rica, se ha tornado en un país inseguro y está en vía de convertirse en uno de los países más inseguros en el mundo, en donde el homicidio calificado, el sicariato, la migración ilegal, la prostitución clandestina y el tráfico ilícito de drogas se han acentuado en lo que va del año 2023.

La incidencia de delitos se han cuadruplicado, reinando la impunidad e inmunidad en la región. En relación al delito de homicidio, en los últimos meses se ha virado del homicidio simple al homicidio calificado.

Hasta el mes de noviembre de este año se han perpetrado en Costa Rica 13,281, hurtos, 9,536 robos, 9,080 asaltos, 3,685 robos de vehículos, 2,696 tachas de vehículos y 752 homicidios, especulándose que hasta fines del 2023 se alcanzará una cifra de 900 homicidios y se vaticina que en el año 2024 se incrementarán a 1,500 homicidios.

El crimen organizado se encuentra logísticamente bien dotado en la región, con recursos financieros, yates, aviones, y helicópteros. Los sicarios son entrenados en México, muchos de ellos inmigrantes menores de edad procedentes de Nicaragua, México, Colombia y Venezuela.

Tráfico y trata de la niñez en la actualidad

El tráfico y la trata de niños es considerada la esclavitud moderna del siglo XXI que se perpetra en base a la coacción y el engaño, constituyendo un delito global que roba el sueño y las ilusiones a las personas. Se calcula que mundialmente 3,000 niños son víctimas de trata infantil siendo un negocio muy lucrativo para el crimen organizado, generando 32,000 millones de dólares por año. Las personas aquí son objetos de un negocio jugando un rol importante para el negocio el lugar de origen y de destino de la víctima. Esta modalidad delictiva tiene distintas etapas, como la captación, el tránsito o viaje, la explotación, la retención, escape o fuga y la reintegración. Las razones son sexuales (prostitución, pornografía y turismo) y comerciales (venta de órganos, mendicidad forzada, matrimonios forzados y trabajo forzado).

Causas de este fenómeno son la pobreza crítica, la desintegración familiar, la falta de educación, la crisis humanitaria, el desgaste de valores, las actividades lucrativas y la legislación ineficiente.

Este fenómeno no es exclusivo de ningún país, se puede dar en países en desarrollo e industrializados, comprendiendo todo los estratos sociales, valiéndose de soportes tecnológicos avanzados, siendo los proxenetas el primer eslabón de la cadena delictiva junto a los reclutadores que son a veces familiares mismos, transportistas, hoteleros, etc.

Los delitos conexos son secuestro, engaño, proxenetismo y rufianería, fraude, sobornos, migración ilegal, falsificación de documentos, amenazas y coacción o empleo de la fuerza, matrimonio forzado, embarazo o aborto forzado, matrimonio servil. Se dice que un caso detectado de tráfico de personas o trata infantil equivale a 9 casos no detectados.

Hoy las nuevas tecnologías nos han raptado

Las nuevas tecnologías no han raptado, con ellas nos despertamos, vemos como está el tráfico, saben dónde vivimos, dónde trabajamos, qué medio de transporte usamos, conocen el número de cuentas de tarjetas, qué leemos, qué comemos , pues entregamos todos los datos y toda nuestra vida, tendemos a publicar toda nuestra vida. Es más, se dice que existen más celulares que personas, en el caso de Costa Rica, pues hay 8 millones de celulares y solo cuenta con 6 millones de habitantes.

Hoy el Internet de las cosas constituye una red colectiva de dispositivos conectados y tecnologías que facilita la comunicación entre los dispositivos y la nube, así como entre los propios dispositivos. El internet de las cosas integra las "cosas" de uso

diario con internet. Este sistema funciona mediante la recopilación e intercambio de datos en tiempo real, verbigracia tenemos los edificios inteligentes, vehículos inteligentes, hogares conectados, etc. Tiene su origen en Rudolf Hez, quién en 1888 crea la interconexión inalámbrica.

Asimismo tenemos el wifi, que significa fidelidad sin cables o inalámbrica, es un sistema de conexión inalámbrica dentro de una determinada área entre dispositivos electrónicos y frecuentemente para acceso a internet, hoy ambas se han desarrollado vertiginosamente almacenando datos que nos conducen a una ingeniería social, en la que todos nosotros, dejamos una huella digital, los administradores de estos datos saben que productos ofrecer según los gustos por región o por país, hacemos los pagos en línea. En consecuencia es necesario contar con censores policiales (Smart pólice), que diseñen una estrategia de ciberseguridad orientada a la seguridad de datos y a la protección en línea.

Gestión de la profesionalización policial en Costa Rica

Hoy en día, el tipo de policía que se desea profesionalizar es el de una policía democrática, que tenga un acercamiento a la comunidad y orientada a la democracia, los derechos humanos, los intereses sociales y la rendición de cuentas.

Las cualidades de una policía democrática son la rendición de cuentas tanto a la ley, más no al gobierno, la protección de los derechos humanos y una rendición de cuentas y actuación policial abierta al público con el fin de generar la confianza de la población. Costa Rica ha profesionalizado la policía con carreras de nivel universitario para la obtención del bachillerato y la licenciatura en ciencias policiales, implementando un plan de estudios y actualización de la carrera policial.

Las ciencias policiales abarcan un conjunto de disciplinas científicas orientada a la protección ciudadana, el orden público, la seguridad humana, la prevención, la investigación del fenómeno criminal, las funciones de policía, la gestión operativa orientada a la solución de problemas, gestión estratégica, gestión y liderazgo, estrategias preventivas contra la criminalidad, la incorporación de las nuevas tecnologías, los derechos humanos, la psicología social, análisis criminal, la psicopatología social, la política criminal, la resolución de conflictos, el derecho procesal penal para las ciencias policiales, seguridad organizacional, la elaboración de informes técnicos, el diagnóstico de riesgos, la planificación y desarrollo de planes de mitificación de riesgos, la inteligencia policial, la criminalística y la criminología, entre otros.

Impacto de la toma de decisiones en la seguridad pública en Costa Rica

El Estado moderno debe de tener una visión social de la seguridad. Benjamín Franklin sostenía que "cualquier sociedad que renuncie a un poco de libertad para ganar un poco de seguridad, no merece tener ambas", asimismo el ex Secretario General de la ONU Ban Ki Moon el 2007 sostenía, que "sin desarrollo no tendremos seguridad" y "sin seguridad no tendremos desarrollo".

La seguridad está dada en función de la calidad de vida de los ciudadanos, el desarrollo social, el desarrollo económico y la percepción. Hoy se atisba en el interior de la sociedad elementos de deshumanización, la brecha de desigualdad se ha incrementado recientemente como consecuencia de la pandemia global del Covid - 19. Costa Rica ha invertido 700 millones de dólares en materia de seguridad, el Banco Interamericano de Desarrollo (BID) ha incrementado en un 74% el gasto en seguridad, sin embargo la seguridad no ha mejorado.

El Banco Mundial afirma que 45 países han elevado su PBI y de esta manera han logrado revertir las cifras de la criminalidad, vale decir que es necesario poner énfasis en el desarrollo humano, el desarrollo económico y el desarrollo social, otro aspecto importante según el Banco Mundial es el impacto de la ética y estética en la seguridad, algo que ha sido corroborado por la teoría de las ventanas rotas, asimismo una reducción del 10% de la pobreza conllevará a una reducción de criminalidad, en la medida que se invierta en educación y en programas sociales (abastecimien-

to de agua, construcción de veredas, instalación de alumbrado eléctrico, construcción de áreas deportivas, complejos culturales, generación de trabajo y oportunidades etc.) se logrará una disminución de la violencia. No hay una formula milagrosa, la articulación local es lo primordial para generar espacios seguros.

El mercado global de la seguridad privada ha alcanzado 240,000 millones de dólares anual, lo que equivale al PBI de más de 100 países, las ganancias del crimen organizado se calculan en 2 billones de dólares por año, lo que equivale al 3.6 % del consumo por año.

En Costa Rica se perdieron como consecuencia de la pandemia 287,000 puestos de trabajo, la pobreza se incrementó en un 0.3 % dejando a 650,000 hogares en pobreza extrema y el poder adquisitivo disminuyó en un 0.2 % y la informalidad alcanzó un 46 % . Las estadísticas criminales reflejan un 2.9 % de homicidios por día.

Situación de la seguridad ciudadana en América Latina

América Latina es la región más violenta del mundo, priman en la región una política de seguridad reactiva y una ausencia de inteligencia preventiva, se ha dejado de lado la prevención, se carece de una política criminal racional, coherente y moderna, producto de la fractura de los consensos políticos, que han dado lugar al surgimiento de políticos advenedizos y oportunistas que ofrezcan respuestas populistas con fines electorales, asimismo se identifican serias asimetrías producto del centralismo político y administrativo de los gobiernos lo cual conduce a asimetrías administrativas presupuestarias y asimetrías en el acceso del conocimiento y la profesionalización del personal policial.

Otro aspecto importante es la narcotización de la política criminal, las policías de la región se han focalizado en la lucha contra el tráfico ilícito de drogas, flagelo que indiscutiblemente azota a la región, dejándose de lado la lucha contra la micro criminalidad urbana. De igual manera existe una bipolaridad en la concepción de seguridad en América Latina, por un lado existe una demanda colectiva de una mano dura contra la delincuencia, mientras que por otro lado, persisten los altos índices de pobreza, que es la generadora de la violencia. No olvidemos que el núcleo duro de la pobreza es la criminalidad.

Péndulo entre lo policial y lo militar

De igual forma, los políticos confunden los roles entre policías y militares, esto se ha agravado en la denominada sociedad post 11 de setiembre y en la pandemia global del coronavirus.

Debe tenerse claro que una cosa es "defensa" y otra cosa es "seguridad", los policías no deben de tener enemigos a quién combatir, sino más bien a ciudadanos a quién proteger.

Asimismo, las medidas coercitivas deben de ser la última ratio, así lo exigen las democracias modernas. Hoy es necesario fortalecer una policía de proximidad ciudadana, recuperando el espacio público involucrando al ciudadano, activando así la participación comunitaria dentro del actual paradigma intersectorial para neutralizar la desconfianza social en la policía, para así legitimarla y posicionarla y generar alianzas públicas-privadas.

Reflexión final

La seguridad es un gran desafío del siglo XXI ya que es un elemento esencial del Estado de derecho moderno y condición sine qua non para la vigencia de los derechos humanos y la cultura de paz. En consecuencia, es necesario atender a las comunidades no solo por las cifras de la violencia, sino también, por los números de la demanda social, si bien es cierto que tenemos que ser duros contra los delincuentes, como sociedad y país tenemos que ser aún más duros contra las causas de la criminalidad. Las crisis de moralidad y la cultura de ilegalidad toca en todos los niveles y todos los sectores de la población afectando la moral pública sostenible de toda sociedad.

La política criminal contemporánea debe de armonizar o conjugar lo público y lo privado, el Estado y el mercado, la centralización y la descentralización, el realismo y el idealismo, el ser humano y la naturaleza, el hombre y la mujer, el corto plazo y el largo plazo, la prontitud y la estabilidad, el norte global y el sur global, el derecho y el poder, el derecho nacional y el derecho internacional, los principios y el pragmatismo y las políticas de derecha y las políticas de izquierda, solo así consolidaremos una seguridad pública sostenible en el siglo XXI en esta era de la post globalización, la post digitalización, la post crisis financiera y la post pandemia.

RED INTERNACIONAL DE PROFESIONALES EN SEGURIDAD

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

INTERSEC 16 al 18 de Enero, Dubái

A menos de 3 semanas de la próxima edición de Intersec, que se celebrará del 16 al 18 de enero de 2024 en el World Trade Center de Dubái, estamos encantados de compartir que el espacio para expositores está 100 % agotado, lo que hará de Intersec 2024 la edición más grande del mundo.

Como feria comercial líder en el mundo para las industrias de seguridad, protección y protección contra incendios, la próxima edición de Intersec unirá a más de 45.000 profesionales de la seguridad global y acelerará las conversaciones para explorar estrategias y fuentes de tecnologías para los desafíos que enfrentan los líderes y profesionales de la seguridad global que promueven el comercio bilateral. , comercio e innovación a través de las fronteras. Intersec alberga varios pabellones nacionales que reúnen a pymes, proveedores de tecnología y servicios de todo el mundo.

Gartner Identity & Access Management 4 - 5 de 2024 Marzo, Londres

En un mundo donde el perímetro de la red corporativa tradicional se ha vuelto obsoleto, la infraestructura de identidad se ha convertido en el nuevo campo de batalla para los malos actores.

Los modelos de gestión de identidades y accesos (IAM) que se basan en enfoques heredados para gestionar las identidades de usuarios y máquinas en listas cada vez mayores de aplicaciones y entornos se han vuelto complejos y mal equipados para adaptarse a las necesidades cambiantes de los negocios y los avances tecnológicos. Los líderes de seguridad deben evolucionar su IAM hacia un enfoque que priorice la identidad y que coloque los controles basados en la identidad en el centro de la arquitectura de protección de su organización para mejorar su postura de ciberseguridad y, al mismo tiempo, ofrecer transformación digital y valor comercial.

ASIS Europe 20 al 22 de Marzo 2024, Viena , Austria

El evento se centra en los riesgos de seguridad física y cibernética, y en el papel que desempeña la seguridad en el apoyo a los objetivos comerciales. Es la reunión crítica de la región para líderes de seguridad establecidos y aspirantes que trabajan en entornos multinacionales.

Conferencias magistrales inspiradoras que abordan la intersección de la innovación, la política socioeconómica, la sostenibilidad y la resiliencia, y cómo esto afecta el entorno empresarial en el que operan los profesionales de la seguridad.

Más de 50 sesiones educativas y talleres interactivos impartidos por profesionales de la seguridad corporativa en empresas globales y asesores líderes, cuidadosamente seleccionados para cubrir el diverso panorama de amenazas híbridas de hoy.

Disasters Expo Miami 6 al 7 de Marzo, Miami USA

Disasters Expo Miami dará la bienvenida a miles de especialistas y expertos de la industria de gestión de desastres y emergencias de todo el mundo, todo bajo un mismo techo, lo que garantizará que nuestros asistentes abandonen la feria con las herramientas y el conocimiento que necesitan para prosperar en la industria de gestión de desastres y emergencias.

Las ciudades de Estados Unidos siempre han sido vulnerables a los riesgos asociados con los desastres, siendo las principales amenazas potenciales los huracanes y las inundaciones, que han socavado el crecimiento económico a largo plazo.Es por eso que, en Disasters Expo USA, destacamos la necesidad de estrategias integrales de gestión de desastres, que incluyan evaluación de riesgos, preparación, respuesta de emergencia y esfuerzos de recuperación para crear ciudades resilientes.

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

Revista SEGURIDAD & DEFENSA

SEGURIDAD TV

PROPORCIONAMOS A SU EMPRESA EL MEJOR VALOR AGREGADO DEL MERCADO

Por un valor fijo mensual su empresa podrá incorporarse a todas nuestras plataformas: Revista,plataforma Web, audiovisual, banner y redes sociales.

BENEFICIOS DE NUESTRA PLATAFORMA:

1.- Aviso en página interior de 1 página por edición.
2.- Publireportaje de 2 planas.
3.- Incorporación ilimitada en nuestra plataforma web de sus informaciones y novedades,
4.- Banner permanente en www.revistaseguridad.cl
5.- Incorporación de sus vídeos Youtube en nuestra plataforma Seguridad TV.
6.- Entrevistas para Canal Seguridad TV
7.- Difusión de en nuestras Redes Sociales.

PROMO PACK

Por sólo

$250.000 neto Mensual

Plataforma Web

Revista Digital

Canal Seguridad Televisión

Su marca puede serparte de la principal plataforma de información de productos y servicios de seguridad de Chile

Contáctenos hoy a: info@revistaseguridad.cl o al +56 9 98246696