

AL-GHURABÁ

REVISTA DE CONTRA-NARRATIVA PARA LA PREVENCIÓN DE LA RADICALIZACIÓN VIOLENTA DE ETIOLOGÍA YIHADISTA
FREE COUNTER-NARRATIVE MAGAZINE FOR 'THE PREVENTION' OF VIOLENT EXTREMISM OF JIHADISM ETIOLOGY

by
CISEG

ARMAS IMPROPIAS

Y su uso en atentados terroristas

MANUALES DEL TERROR

La propaganda que arma a los fanáticos y desata el caos global

LA CRIMINALÍSTICA

Ante artefactos explosivos en México

AL-GHURABÁ

NÚMERO 89 / FEBRERO 2025 / ISSN 2565-2222

Producción y edición

CISEG

Creadores

David Garriga

Marc Fornós

Equipo Redacción

David Garriga

Ariadna Trespaderne

Bahae Eddine Boumnina

José C. Prado

Alejandro Cassaglia

Diseño y Maquetación

Ariadna Trespaderne

CISEG

info@intelciseg.com

Web

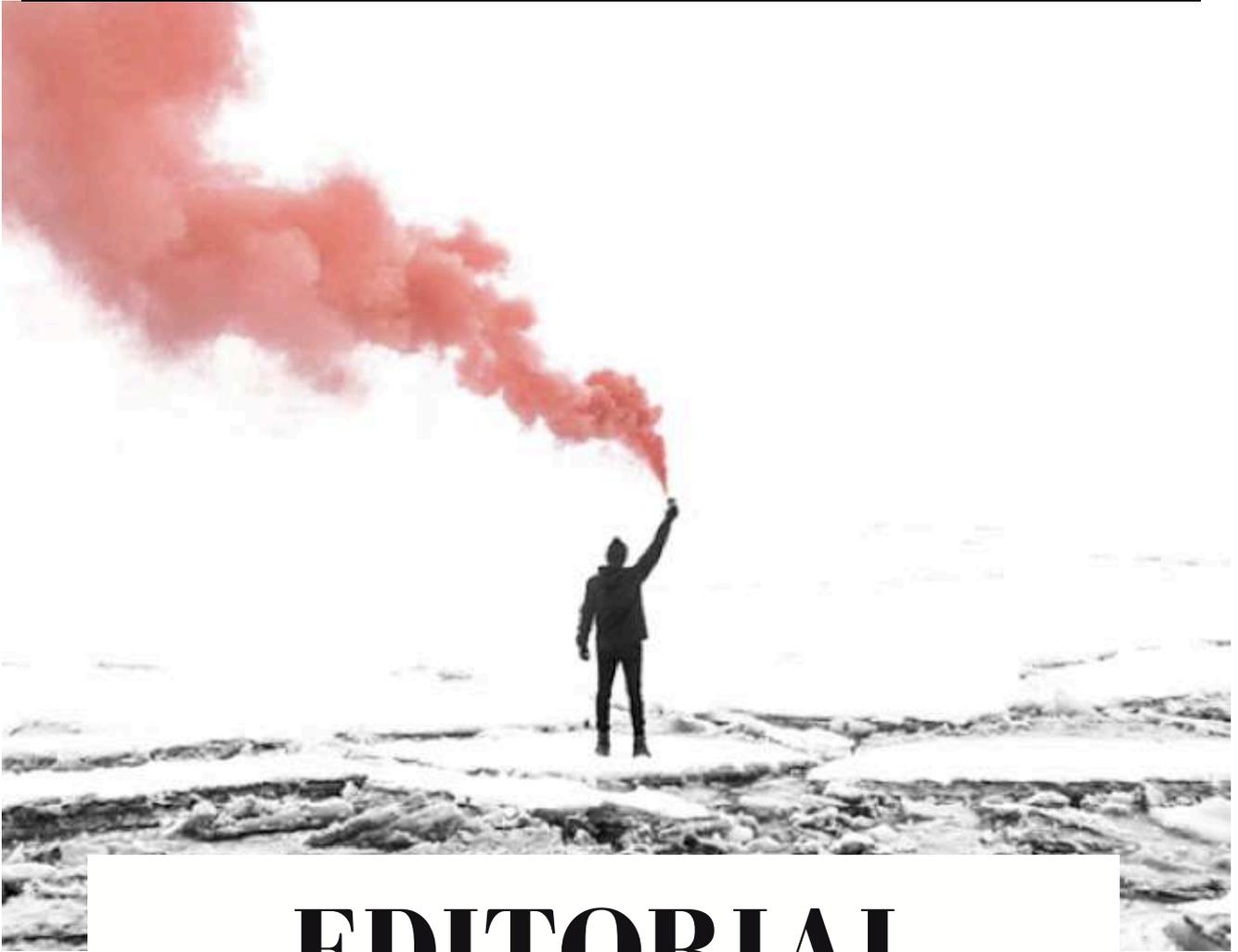
www.alghuraba.org

Envío de artículos

alghuraba@intelciseg.com

La revista Al-Ghurabá de CISEG no se hace responsable de las opiniones que se emitan en esta publicación, puesto que son de carácter individual y desarrolladas exclusivamente por los autores/as. No necesariamente reflejan la posición de la presente editorial.





EDITORIAL

La revista Al-Ghurabá de CISEG, es una herramienta de narrativas alternativas para prevenir la radicalización violenta de etiología yihadista y nace en agosto de 2017 como un proyecto de la Comunidad de Inteligencia y Seguridad Global. Al-Ghurabá es gratuita, online y mensual y persigue implicar a la sociedad civil en este sector y ofrecer herramientas de prevención y de contra-narrativa para prevenir la radicalización violenta en el seno de las comunidades a través de publicaciones accesibles realizadas por analistas.

Esta problemática nace en las comunidades, entre las personas y cualquiera puede hallarse en una situación de cercanía con un perfil radicalizado o un agente radicalizador. En consecuencia, brindar herramientas a la sociedad civil permite que sean personas empoderadas, informadas y formadas. Por otro lado, también sirve para difundir contra-narrativa frente a esta radicalización destinada a los grupos más vulnerables a ser radicalizados. El objetivo es crear contenido que analice la situación actual y consiga erosionar y deslegitimar los discursos que facilitan estas organizaciones terroristas.



SUMARIO

INTELIGENCIA Gumercindo ´Ávila Cuautle	07
SEGURIDAD Diego C. Zorzoli	13
TINTA IMPRESCINDIBLE Carmelo J. Aguilera	18
CONTRA-NARRATIVA Jorge Gómez	20
TERRORISMO Francisco Javier Moreno Oliver	27
ENTREVISTA Gustavo Merani	37
CRIMINOLOGÍA Francisco Javier Ramos	44
TRIBUNA DE OPINIÓN David Garriga	48
AGENDA	51
AMENAÇA GLOBAL PODCAST	57

Un libro de

Víctimas de la yihad negra de Dáesh

Contranarrativa para luchar
por la convivencia y la paz

**Ilham Majure
David Garriga**



Ilham Majure y David Garriga



INTELIGENCIA

WWW.ALGHURABA.ORG

EL CRIMINALISTA

ANTE ARTEFACTOS EXPLOSIVOS EN MÉXICO

Gumercindo Ávila Cuautle.

Criminólogo y criminalista. Oficial B operaciones. Instructor formaciones prevención frente artefactos explosivos.



Introducción

La criminalística ante artefactos explosivos en México es una disciplina que se enfoca en la investigación y análisis de los artefactos explosivos y sus efectos en la escena del crimen. El fundamento legal mexicano para la criminalística y los artefactos explosivos caseros se refleja en el siguiente marco legal.

Marco legal

La investigación y persecución de los delitos relacionados con artefactos explosivos caseros en México se rigen por las siguientes leyes y reglamentos:

- 1. Código Penal Federal (CPF):** Establece los delitos y las penas relacionadas con la fabricación, posesión y uso de artefactos explosivos caseros (CPF, Art. 83-85).
- 2. Ley Federal de Armas de Fuego y Explosivos (LFAFE):** Regula la fabricación, comercio, posesión y uso de armas de fuego y explosivos, incluyendo los artefactos explosivos caseros (LFAFE, Art. 10-15).



3. **Código Nacional de Procedimientos Penales (CNPP):** Establece las reglas y procedimientos para la investigación y persecución de los delitos, incluyendo los relacionados con artefactos explosivos caseros (CNPP, Art. 211-214).

A continuación, se presentan algunos aspectos clave de la criminalística ante artefactos explosivos en México:

Aspectos clave de la criminalística ante artefactos explosivos en México

1. **_Análisis de la escena del crimen_:** La criminalística ante artefactos explosivos en México comienza con el análisis de la escena del crimen, donde se busca identificar y documentar todos los indicios relacionados con el artefacto explosivo (García, 2019, p. 123).

2. **_Identificación del artefacto explosivo_:** La identificación del artefacto explosivo es crucial para determinar la causa y el origen del explosivo (Ruiz, 2020, p. 145).

3. **_Análisis de los restos explosivos_:** El análisis de los restos explosivos puede proporcionar información valiosa sobre la composición y la potencia del explosivo (Hernández, 2018, p. 187).

4. **_Reconstrucción de la escena del crimen_:** La reconstrucción de la escena del crimen puede ayudar a determinar la secuencia de eventos que ocurrieron durante la explosión (García, 2019, p. 127).

Técnicas y herramientas utilizadas en la criminalística ante artefactos explosivos en México

1. **_Análisis químico_:** El análisis químico se utiliza para identificar la composición del explosivo y determinar su potencia (Ruiz, 2020, p. 147).

2. **_Análisis de partículas_:** El análisis de partículas se utiliza para identificar los restos explosivos y determinar su origen (Hernández, 2018, p. 190).

3. **_Reconstrucción 3D_:** La reconstrucción 3D se utiliza para recrear la escena del crimen y determinar la secuencia de eventos que ocurrieron durante la explosión (García, 2019, p. 129).

Importancia de la criminalística ante artefactos explosivos en México

1. **_Investigación de delitos_:** La criminalística ante artefactos explosivos en México es fundamental para investigar delitos relacionados con explosivos y determinar la causa y el origen del explosivo (Ruiz, 2020, p. 149).

2. **_Prevención de delitos_:** La criminalística ante artefactos explosivos en México también puede ayudar a prevenir delitos relacionados con explosivos al identificar y analizar los patrones y tendencias de los delitos (Hernández, 2018, p. 192).

3. **_Seguridad pública_:** La criminalística ante artefactos explosivos en México es crucial para garantizar la seguridad pública al identificar y analizar los riesgos y amenazas relacionados con explosivos (García, 2019, p. 131).

Operador criminalístico policial ante artefactos explosivos

El operador criminalístico policial ante artefactos explosivos es un profesional especializado en la investigación y análisis de los artefactos explosivos y sus efectos en la escena del crimen. A continuación, se presentan algunas de las responsabilidades y habilidades clave del operador criminalístico policial ante artefactos explosivos:

Responsabilidades del operador criminalístico policial ante artefactos explosivos

1. **_Análisis de la escena del crimen_:** El operador criminalístico policial ante artefactos explosivos es responsable de analizar la escena del crimen para identificar y documentar todos los indicios relacionados con el artefacto explosivo.
2. **_Identificación del artefacto explosivo_:** El operador criminalístico policial ante artefactos explosivos es responsable de identificar el artefacto explosivo y determinar su tipo y composición.
3. **_Análisis de los restos explosivos_:** El operador criminalístico policial ante artefactos explosivos es responsable de analizar los restos explosivos para determinar la causa y el origen del explosivo.
4. **_Reconstrucción de la escena del crimen_:** El operador criminalístico policial ante artefactos explosivos es responsable de reconstruir la escena del crimen para determinar la secuencia de eventos que ocurrieron durante la explosión.

Habilidades clave del operador criminalístico policial ante artefactos explosivos

1. **_Conocimientos en criminalística_:** El operador criminalístico policial ante artefactos explosivos debe tener conocimientos en criminalística y en la investigación de delitos.
2. **_Conocimientos en explosivos_:** El operador criminalístico policial ante artefactos explosivos debe tener conocimientos en explosivos y en la identificación de artefactos explosivos.
3. **_Habilidades analíticas_:** El operador criminalístico policial ante artefactos explosivos debe tener habilidades analíticas para analizar los datos y los indicios recopilados en la escena del crimen.
4. **_Habilidades de comunicación_:** El operador criminalístico policial ante artefactos explosivos debe tener habilidades de comunicación para presentar los resultados de la investigación a los superiores y a los tribunales.





CONCLUSIONES

1. Uso de artefactos explosivos improvisados: La mayoría de los ataques con artefactos explosivos en México se realizan con dispositivos improvisados, utilizando materiales como el ácido nítrico y el clorato de potasio (Espinosa, 2020, p. 12).
2. Motivaciones criminales: Los ataques con artefactos explosivos en México suelen estar motivados por conflictos entre grupos delictivos, extorsión y chantaje (García, 2019, p. 25).
3. Impacto en la sociedad: Los ataques con artefactos explosivos han generado un clima de miedo y inseguridad en la sociedad mexicana, además de causar pérdidas humanas y materiales significativas (Hernández, 2018, p. 32).
4. Necesidad de cooperación internacional: Es fundamental fortalecer la cooperación internacional para combatir el tráfico de materiales peligrosos y la fabricación de artefactos explosivos (López, 2020, p. 22).
5. Importancia de la inteligencia y el análisis: Es crucial mejorar la inteligencia y el análisis para identificar y prevenir los ataques con artefactos explosivos (Martínez, 2019, P. 25)

REFERENCIAS

Código Nacional de Procedimientos Penales. (2020). Artículos 211-214. México: Gobierno de México.

Espinosa, R. (2020). El uso de artefactos explosivos en México. Universidad Nacional Autónoma de México. Fundamento legal mexicano la criminalística y artefactos explosivos caseros en México

García, J. (2019). La criminalística ante artefactos explosivos en México. *Revista de Ciencias Forenses*, 10(2), 123-131.

García, J. (2019). La violencia en México: un análisis de los ataques con artefactos explosivos. Instituto Nacional de Estudios sobre la Violencia.

Hernández, R. (2018). Análisis de los restos explosivos en la investigación de delitos. *Revista de Ciencias Forenses*, 9(1), 187-192.

Hernández, A. (2018). El impacto de los ataques con artefactos explosivos en la sociedad mexicana. Universidad Autónoma de Ciudad Juárez.

López, M. (2020). La cooperación internacional para combatir el tráfico de materiales peligrosos. Instituto Nacional de Estudios sobre la Seguridad.

Martínez, E. (2019). La inteligencia y el análisis en la prevención de ataques con artefactos explosivos. Universidad Nacional Autónoma de México.

Enviado desde mi iPhone

Ruiz, M. (2020). La identificación del artefacto explosivo en la investigación de delitos. *Revista de Ciencias Forenses*, 11(1), 145-149.



COMING SOON...





SEGURIDAD

WWW.ALGHURABA.ORG

HOSPITALES PÚBLICOS

PREVENCIÓN Y SEGURIDAD

Diego C. Zorzoli.

Licenciado en Tecnología Aplicada a la Seguridad (UTN).



Introducción

Los hospitales públicos son centros asistenciales cuya actividad, dependiendo de las características y funciones de cada institución, está dedicada al diagnóstico, tratamiento y cuidado de las personas con alguna problemática relacionada con la salud.

Las instituciones de salud cumplen un propósito de suma importancia en el contexto social porque se dedican a brindar cuidado, asistencia y contención a un vasto sector de la sociedad que por diversas cuestiones (imposibilidad de contar con obra social, no contar con servicio de salud proveniente del sector privado, problemas económicos, elección voluntaria, entre otros) decide asistir a un centro sanitario.

Otra cuestión importante a tener en cuenta es la concienciación de todo el equipo de trabajo, sobre el servicio que se brinda, ya que este debe ser serio, profesional y sumamente responsable debido a que el entorno está conformado por personas en estado de necesidad que en muchos casos se debaten entre la vida y la muerte, con todo lo que ello conlleva.

El propósito del presente artículo, es realizar una mirada sintética (por cuestiones lógicas vinculadas a la edición del mismo) desde la perspectiva de la actividad de seguridad sobre este tipo de infraestructuras críticas tan sensibles e importantes,

haciendo especial hincapié en la importancia de las tareas de prevención y la importancia de la proactividad por parte de los responsables de la seguridad en las instituciones.

La Prevención y Seguridad en hospitales públicos. Consideraciones generales.

La Resolución N° 1523/2019 define a las infraestructuras críticas como “aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.”, siendo los principales criterios de identificación el impacto en la vida humana, en la economía, medio ambiente, público, social, etc., identificando a sectores como: energía, transporte, nuclear, finanzas, salud, entre otros.

Es por esto, que es menester llevar adelante una adecuada "gestión de la seguridad", que provoca una mejor calidad de la asistencia sanitaria y genera al mismo tiempo mejores condiciones de trabajo al garantizar la seguridad de las personas (empleados, pacientes y visitantes que se encuentren de manera transitoria o permanente en el nosocomio) y la conservación del patrimonio y la imagen del centro hospitalario.

Teniendo en cuenta lo expresado en el párrafo anterior, esa gestión de la seguridad debería comenzar con un análisis y evaluación de riesgos, diseño e implementación de un programa integral de prevención y seguridad, auditorías periódicas que permitan las correcciones necesarias en tiempo y forma y la capacitación constante de los miembros de los diferentes equipos, teniendo como premisas fundamentales la prevención y la proactividad en las acciones.

A la hora de diseñar el Plan Integral de Prevención y Seguridad, sería conveniente tener en cuenta el concepto de seguridad integral, es decir, que se contemple el abanico de actividades y disciplinas involucradas en el centro hospitalario, entre las que podemos mencionar: procedimientos médicos, peligros biológicos, seguridad e higiene laboral, protección contra incendios, seguridad en instalaciones auxiliares, protección en depósitos de farmacia, seguridad en las instalaciones de gases medicinales, seguridad en





las instalaciones radiológicas, plan de evacuación en caso de incendio, plan de contingencia, relación con los departamentos de compras y almacenes, modificaciones arquitectónicas, protección contra robo e intrusión.

Prevención en zonas críticas del hospital

De las diferentes áreas que podemos encontrar en un centro de salud: Dirección Administrativa, Departamento de Finanzas, Servicio Social, Comunicaciones, Departamento de Sueldos, Departamento de Recursos Humanos, Sector de Rayos, Áreas de cuidados críticos, Área de neonatología, Departamento de Sistemas, Departamento de Suministros, Sector de Compras, Servicio de Limpieza, Seguridad, Admisión, Guardias de Emergencias, etc. estas últimas suelen presentar los mayores niveles de conflictividad dado que la idiosincrasia del sector está caracterizada por el arribo de personas con padecimientos de salud, lo que dependiendo del grado de afectación, puede generar irritabilidad, impaciencia, alteración, etc.. que de no ser tratados con la seriedad correspondiente, pueden derivar en actos de violencia.

Es aquí, donde se deberán aplicar las técnicas adecuadas de negociación y resolución de conflictos ya que pacientes y familiares se encuentran en un estado de excitación que puede escalar de no dotar adecuadamente al personal de los conocimientos necesarios a la hora de controlar estas situaciones.

Teniendo en cuenta que cada situación conflictiva presenta características particulares, las técnicas de negociación deberían contemplar un trato adecuado y eficiente con el paciente o familiares de estos, respetuoso, amable y cordial, evitando ser frío y descortés mostrando en todo momento interés por colaborar en resolver los problemas, manifestando un enfoque solucionador en nuestras actitudes. Evitar discusiones con el paciente/familiar o allegado que ocasionen un clima de tensión. Conceder inicialmente al entrevistado un desahogo emocional. Transformar cualquier queja o reclamo como un reto o una oportunidad. Mantener siempre la calma, permanecer enfocado generando tranquilidad. Evitar transformar los problemas primarios en situaciones más complejas, caóticas y conflictivas.

Programa Integral de Seguridad Hospitalaria

A la hora de llevar adelante una gestión seria en el ámbito de la seguridad hospitalaria, el primer paso, luego del análisis de riesgos a los que está expuesta la organización y la evaluación de la situación interna, debería ser diseñar un Programa Integral de Seguridad Hospitalaria, que será presentado a la Alta Dirección con el objetivo de lograr la homologación y el apoyo necesario para su implementación. Este Programa tendría que ser totalmente dinámico y adecuado a las características físicas, sociales, organizativas y funcionales de los diferentes centros de salud.

Este Programa deberá contemplar las acciones necesarias en lo que a seguridad del paciente se refiere, garantizando las medidas preventivas necesarias para la protección del Equipo de Salud (personal médico, enfermeros, técnicos, administrativos, seguridad, mantenimiento, camilleros y todos aquellos que presten servicio en el ámbito del centro de salud) como así también los bienes muebles e inmuebles.

En cuanto a la acción preventiva en materia de delitos en centros de salud: Delitos contra la vida, Delitos contra la integridad personal. Delitos contra el honor. Delitos contra la integridad sexual. Delitos contra la libertad individual. Delitos contra la seguridad pública. Delitos contra la propiedad. Delitos contra el orden público, la función del personal de seguridad



debería estar orientada al diseño de medidas preventivas enfocadas en la disuasión y detección temprana y en el caso de que estos ocurran, comunicar de forma rápida y efectiva la situación a las fuerzas públicas de seguridad para que estos realicen las actividades correspondientes, asentando las novedades en los Libros de Novedades correspondientes.

A modo de resumen, podemos mencionar que una correcta implementación del mencionado Programa, debería cumplir con algunas acciones previas:

- Obtener el compromiso de quienes tienen a su cargo la toma de decisiones y la conducción estratégica de la Institución.
- Realizar un Análisis de Riesgos con el objetivo de identificar los riesgos potenciales y las consecuencias que éstos puedan producir, determinar que puede ser dañado y como, realizar las evaluaciones correspondientes, registrar los hallazgos y tomar las medidas necesarias de manera tal que se lleven adelante las acciones de gestión del riesgo de manera profesional y teniendo presente los costos y beneficios de los programas a implementar.
- Hacer una valoración de las necesidades de toda la institución.
- Identificar las prioridades e instituir medidas preventivas.
- Desarrollar políticas y procedimientos de seguridad en forma escrita.
- Realizar auditorías periódicas con el fin de mantenerlo actualizado y de ser necesario, realizar las correcciones necesarias en tiempo y forma.

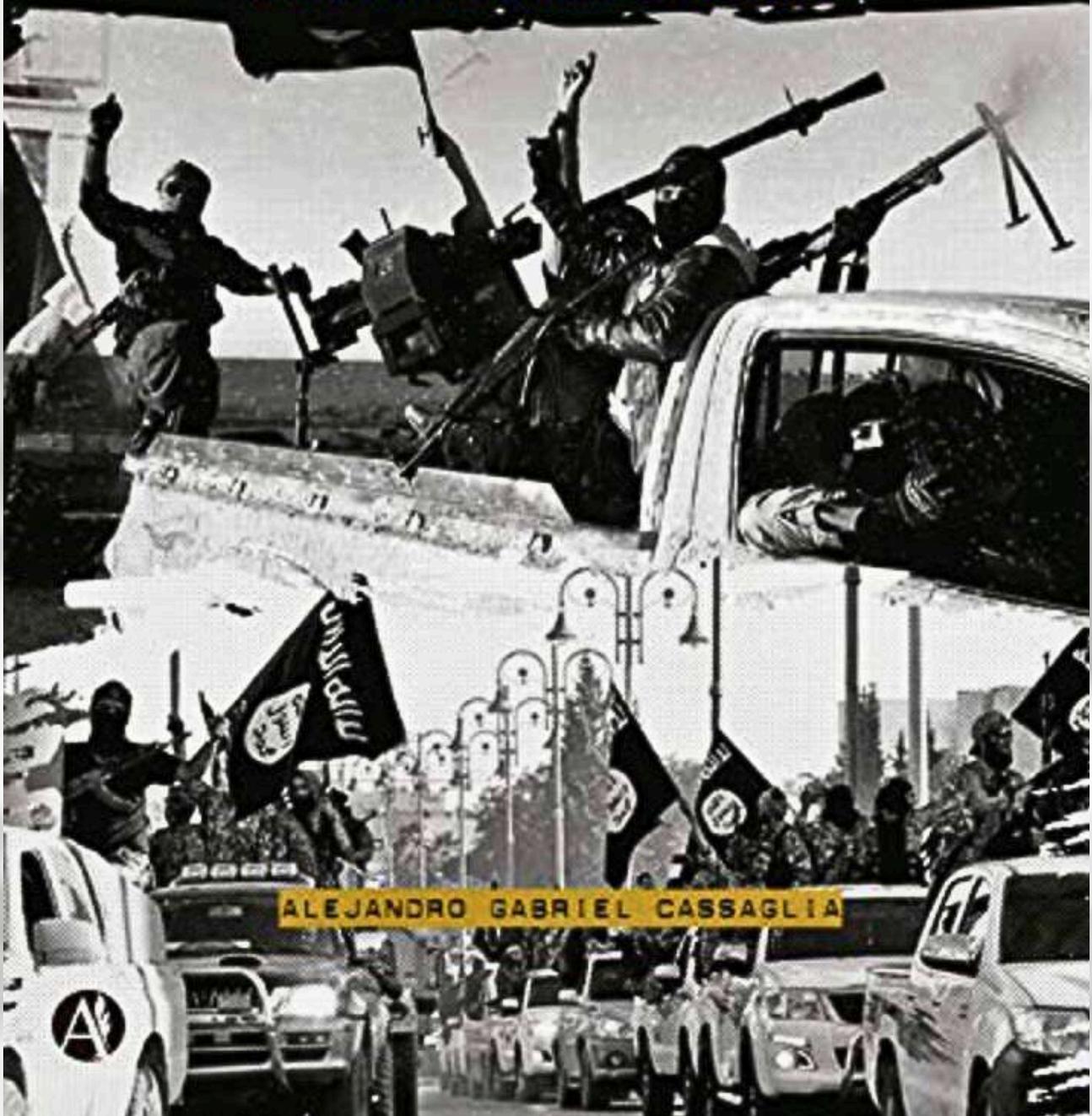
Conclusiones

A modo de conclusión, es necesario tener presente la importancia que las infraestructuras críticas (en este caso los hospitales), representan a nivel social, por lo que será de suma importancia trabajar en la formación integral de quienes desempeñan tareas en esta clase de objetivos, incluyendo a todos los miembros del Equipo de Salud (médicos, enfermeros, técnicos, auxiliares, etc.), haciendo especial hincapié en que el paciente es el núcleo de atención y que un buen obrar contribuirá de la mejor manera a que el tránsito por la institución, sea acompañado de una labor profesional, empática y de respeto por los derechos, por parte del Equipo de Salud, hacia quienes asisten a recibir atención de manera transitoria o permanente.

TERRORISMO

'TERRORISMO YIHADISTA'

UNA AMENAZA EXTERNA

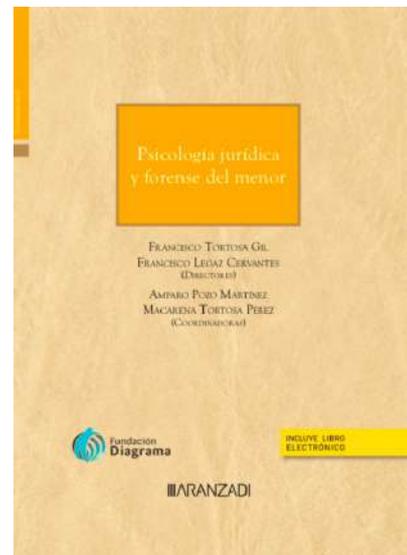


ALEJANDRO GABRIEL CASSAGLIA

CÓMPRALO EN AMAZON

[¡Haz clic aquí!](#)

TINTA IMPRESCINDIBLE



Título: Psicología Jurídica y Forense del Menor

Autor: Fc. Tortosa Gil y Fco. Legaz Cervantes

La intervención de la psicología jurídica y forense con menores ha evolucionado, siendo fundamental en procesos judiciales. La obra ofrece una visión amplia del papel de los/as psicólogos/as en este ámbito, detallando la evolución de la psicología aplicada a menores, sus áreas de actuación y la importancia de la ética profesional. Se profundiza en los principales ámbitos de intervención: protección de menores, ámbito familiar y conflictos sociales, abordando también la labor desde la victimología. En conjunto, la obra busca contribuir al estudio y análisis de la psicología jurídica y forense en la infancia y adolescencia.



CONTRA-NARRATIVA

WWW.ALGHURABA.ORG

MANUAL DEL TERROR

LA PROPAGANDA QUE ARMA A LOS FANÁTICOS Y DESATA EL CAOS GLOBAL

Jorge Gómez.

Analista en Seguridad.



Introducción

La propaganda como herramienta de terror: La propaganda es el núcleo operativo de los grupos terroristas. Su función no se limita a la difusión de mensajes, sino que busca:

- Reclutar adeptos: Ofrecen una visión distorsionada de justicia y heroísmo para atraer a jóvenes vulnerables.
- Legitimar la violencia: Justifican ataques brutales como parte de una lucha divina o ideológica.
- Inspirar miedo global: Promueven mensajes que desestabilizan a las sociedades objetivo y generan caos.

Un ejemplo de esta estrategia es la revista Inspire de Al-Qaeda, diseñada para inspirar y capacitar a individuos para llevar a cabo atentados de manera autónoma. Por su parte, Hamas y su brazo armado, Al-Qassam, utilizan la propaganda para justificar sus ataques terroristas contra Israel, mientras que ISIS destaca por su capacidad de descentralizar la violencia mediante manuales técnicos.



Revista Inspire: La estrategia de Al-Qaeda

La revista Inspire, producida por Al-Qaeda en la Península Arábiga (AQAP), es uno de los ejemplos más claros de cómo el terrorismo moderno se alimenta de la comunicación estratégica. En la edición número 14, se presentan tácticas y objetivos específicos, que incluyen:

- **Ataques de lobos solitarios:** Inspire promueve los ataques individuales como una forma de terrorismo descentralizado. Instrucciones como "Cómo fabricar una bomba en la cocina de tu madre" han servido como guías prácticas para actos de terror en Occidente. Esta estrategia busca:

- Maximizar el impacto psicológico: Los ataques aislados son impredecibles y generan una sensación constante de inseguridad.
- Reducir el riesgo organizativo: Al depender de individuos radicalizados, eliminan la necesidad de estructuras complejas que pueden ser infiltradas.

- **Objetivos estratégicos:** La revista identifica infraestructuras críticas, líderes políticos y eventos masivos como objetivos prioritarios. Al-Qaeda ve estos ataques como una forma de:

- Dañar las economías occidentales.
- Exacerbar las tensiones políticas y sociales.
- Amplificar su mensaje de odio y violencia.

- **Justificación ideológica:** Cada edición de Inspire refuerza la narrativa de que la violencia es una obligación religiosa y una respuesta legítima a las acciones de Occidente en el mundo islámico. La revista utiliza citas de textos religiosos y discursos de líderes de Al-Qaeda para legitimar sus mensajes.

Hamas y Al-Qassam: Terrorismo bajo el pretexto de resistencia

Hamas y su brazo armado, Al-Qassam, emplean propaganda para consolidar su apoyo local y justificar sus actos violentos. Un ejemplo de esto es el manual sobre inutilización de cámaras de vigilancia mediante láser. Este documento combina instrucciones técnicas con un mensaje ideológico que presenta estas tácticas como actos heroicos de resistencia contra la ocupación israelí.

- **Propaganda para la radicalización:** La propaganda de Hamas está diseñada para consolidar el apoyo de las comunidades palestinas y justificar sus actos violentos. Mensajes que glorifican a terroristas y llamados a la "liberación" de Palestina son ejemplos claros de su estrategia para perpetuar el conflicto.

- **Objetivos internacionales:** Aunque su foco principal es Israel, Hamas utiliza su propaganda para ganar simpatizantes en todo el mundo, presentándose falsamente como defensores de una causa humanitaria mientras llevan a cabo actos de terrorismo contra civiles.



ISIS: La descentralización del terrorismo

ISIS ha perfeccionado el uso de la propaganda digital para descentralizar sus operaciones. Un ejemplo es su manual sobre la fabricación de explosivos plásticos (C4), que detalla cómo fabricar armas potentes con materiales accesibles. Esto refleja su estrategia de:

- Empoderar a individuos: Permitir que cualquier persona, en cualquier lugar, pueda cometer actos de terror.
- Ampliar su alcance global: Utilizando internet como un medio para distribuir sus mensajes y radicalizar a simpatizantes.

Objetivos comunes de estos grupos terroristas

Los materiales analizados permiten identificar los siguientes objetivos:

1. Generar caos social: Dividir a las sociedades objetivo y exacerbar las tensiones internas.
2. Debilitar a los Estados: Atacar infraestructuras críticas y líderes clave para desestabilizar gobiernos.
3. Radicalizar y movilizar: Convertir a individuos descontentos en instrumentos de terror.
4. Prolongar el conflicto: Alimentar la narrativa de una lucha interminable para justificar su existencia.
6. Impacto global y amenazas emergentes

La propaganda terrorista ha transformado la naturaleza de los conflictos. Ejemplos como los atentados de París (2015) o Boston (2013) muestran cómo estos mensajes inspiran actos de violencia en todo el mundo. Además, las redes sociales y plataformas digitales han amplificado su alcance, complicando los esfuerzos para detener su difusión.

Estrategias para combatir la propaganda terrorista

Para enfrentar esta amenaza, es necesario un enfoque integral que combine:

- **Contrapropaganda efectiva:** Crear narrativas que desmientan las mentiras de los terroristas y destaquen las consecuencias reales de sus acciones.
- **Regulación tecnológica:** Trabajar con empresas digitales para eliminar contenido extremista.
- **Educación comunitaria:** Identificar señales de radicalización y ofrecer apoyo temprano.
- **Cooperación internacional:** Compartir inteligencia y coordinar esfuerzos entre países para neutralizar redes terroristas.

Conclusión

La necesidad de una respuesta contundente. La propaganda de grupos como Hamas, ISIS, Al-Qassam y Al-Qaeda no solo alimenta el odio, sino que perpetúa la violencia global. Documentos como la revista Inspire y los manuales de tácticas, demuestran la capacidad de estas organizaciones para adaptarse y evolucionar. Combatir esta amenaza requiere un enfoque decidido, que combine medidas de seguridad con iniciativas educativas y sociales para dismantelar sus redes de influencia. La seguridad global depende de nuestra capacidad para enfrentarlos con realismo y determinación.



Impacto de la FIMI en la Seguridad

La FIMI tiene un impacto profundo en diversas dimensiones de la seguridad:

1. Seguridad Nacional: La manipulación informativa puede debilitar la estabilidad política de un país al polarizar a la sociedad y erosionar la confianza en las instituciones democráticas. Un ejemplo notable es la interferencia en procesos electorales mediante campañas de desinformación en redes sociales, como se observó en las elecciones presidenciales de Estados Unidos en 2016 (Rid & Buchanan, 2015). Este tipo de estrategias también busca exacerbar tensiones étnicas, religiosas o culturales para fragmentar la cohesión social. Las consecuencias de estas acciones pueden ser devastadoras, resultando en disturbios civiles, inestabilidad política y debilitamiento del Estado de derecho.

2. Seguridad Organizacional: Las empresas enfrentan riesgos significativos debido a ciberataques que pueden comprometer datos sensibles o paralizar sus operaciones. Además, las campañas de desinformación dirigidas a consumidores pueden dañar la reputación de una marca. Por ejemplo, el ataque de ransomware a la cadena de suministro de SolarWinds expuso a miles de organizaciones a vulnerabilidades críticas (Boyes, 2015). Estas vulnerabilidades no solo impactan financieramente a las empresas, sino que también pueden generar una pérdida relevante de confianza por parte de los clientes y socios comerciales.

3. Seguridad Social: La proliferación de contenido extremista en redes sociales puede incitar a la violencia, el odio y la discriminación. Grupos terroristas y extremistas utilizan estas plataformas para radicalizar a individuos y coordinar ataques. Un ejemplo claro es el uso de Telegram por parte de grupos neonazis para organizar protestas violentas (Conway et al., 2019). La propagación de este contenido también exacerba la polarización social, dificultando el diálogo y la resolución pacífica de conflictos.

Relación con Organizaciones Criminales y Terroristas

Las organizaciones criminales y terroristas han adoptado la FIMI como una estrategia central debido a su eficacia y bajo costo. Algunas de las principales formas en que estas organizaciones emplean la FIMI incluyen:

- **Reclutamiento y Radicalización** Grupos como Al-Qaeda y el Estado Islámico han perfeccionado el uso de redes sociales para difundir propaganda y reclutar combatientes. Mediante videos y publicaciones diseñadas para resonar con audiencias específicas, logran persuadir a individuos vulnerables para que se unan a su causa (Zelin, 2015). Este proceso de radicalización también utiliza discursos de victimismo y promesas de empoderamiento para captar seguidores en comunidades marginadas.
- **Financiación** La manipulación de información también se utiliza para recaudar fondos mediante estafas en línea o el uso de criptomonedas. Estas técnicas permiten a las organizaciones eludir los sistemas tradicionales de monitoreo financiero (Europol, 2020). Adicionalmente, las redes sociales sirven como plataformas para solicitar donaciones bajo pretextos falsos, obteniendo recursos de simpatizantes desinformados.
- **Coordinación de Actividades** Las plataformas en línea cifradas y las técnicas de ocultamiento de datos permiten a estas organizaciones planificar y ejecutar operaciones sin ser detectadas. Además, el uso de tecnologías emergentes, como la in-



-teligencia artificial, está mejorando sus capacidades de organización. Estas técnicas incluyen el uso de esteganografía para ocultar mensajes dentro de imágenes y videos, dificultando su detección por parte de las autoridades.

Respuesta y Estrategias de Mitigación

1. Desarrollo Tecnológico: El uso de herramientas basadas en inteligencia artificial para detectar desinformación es crucial. Estas herramientas analizan patrones lingüísticos y de distribución para identificar contenido falso. Asimismo, el uso de blockchain para verificar la autenticidad de los datos representa una línea prometedora en la lucha contra la manipulación informativa.

2. Fortalecimiento Legal: Actualizar las leyes para abordar el cibercrimen y la manipulación informativa es esencial. La colaboración entre países para armonizar estas leyes también es fundamental. Iniciativas como el Convenio de Budapest sobre Cibercrimen han sentado las bases para una cooperación internacional efectiva en este ámbito.

3. Educación y Conciencia Pública: Implementar programas de alfabetización mediática puede ayudar a las personas a discernir entre contenido veraz y manipulado, reduciendo el impacto de la FIMI. Estos programas deben enfocarse en fortalecer el pensamiento crítico y educar sobre el funcionamiento de los algoritmos de las redes sociales.

Conclusiones

La manipulación e interferencia de la información es una herramienta poderosa para las organizaciones criminales y terroristas. Su impacto se extiende desde la seguridad nacional hasta la cohesión social, poniendo en jaque a las democracias contemporáneas y a las economías globalizadas. Frente a esta amenaza, resulta imprescindible adoptar estrategias integrales que combinen tecnología, legislación, educación y cooperación internacional. Solo mediante esfuerzos coordinados se podrá mitigar el impacto de la FIMI y garantizar la resiliencia de nuestras sociedades ante futuras amenazas.

REFERENCIAS

- Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*.
- Cinelli, M., Quattrocioni, W., Galeazzi, A., et al. (2020). The COVID-19 Social Media Infodemic. *Scientific Reports*.
- Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.
- Conway, M., Scrivens, R., & Macnair, L. (2019). Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. *Studies in Conflict & Terrorism*.
- Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA)*.
- Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2020). The Rise of Social Bots. *Communications of the ACM*.
- Rid, T., & Buchanan, B. (2015). *Attributing Cyber Attacks*. *Journal of Strategic Studies*.
- Sunstein, C. R. (2009). *Going to Extremes: How Like Minds Unite and Divide*. Oxford University Press.
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*.
- Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe.
- Zelin, A. Y. (2015). *The State of the Global Jihad Online*. The Washington Institute for Near East Policy.



Master of Science in Nonverbal & Deceit Detection

Este máster es el original, el pionero en esta formación. Su objetivo es formar analistas de la conducta no verbal que sean capaces de interpretar el comportamiento humano basándose en la evidencia científica, y aplicarlo a su entorno profesional.

- ✓ 100 % Online con clases semanales en vivo.
- ✓ Metodología de estudio de caso.
- ✓ Profesorado internacional.



Programa en español o inglés. Tú eliges.

www.evidentiauniversity.com



TERRORISMO

WWW.ALGHURABA.ORG

ARMAS IMPROPIAS

Y SU USO EN ATENTADOS TERRORISTAS

Francisco Javier Moreno Oliver.

Doctor en Psicología. ORCID iD: <https://orcid.org/0000-0002-9306-2125>



Introducción

Se entiende por "arma impropia" a cualquier objeto o instrumento de uso cotidiano que, aunque no haya sido diseñado ni fabricado con fines de ataque o defensa, puede ser utilizado para incrementar la capacidad ofensiva de quien lo emplea, con el potencial de causar daño a personas o bienes (Zelasco, A.M., 2023). Aunque estas herramientas o elementos tienen un propósito original no violento, pueden ser adaptados circunstancialmente para funciones agresivas o de protección, según los escenarios en que se encuentren.

En el contexto del terrorismo, las armas impropias adquieren una relevancia especial debido a su amplia accesibilidad y la dificultad para detectarlas. Un ejemplo paradigmático de esta amenaza es el ataque terrorista del 11 de septiembre de 2001, el cual evidenció la capacidad destructiva de los objetos cotidianos convertidos en armas. En este caso, aviones comerciales fueron utilizados como instrumentos de destrucción masiva, lo que subraya cómo elementos originalmente destinados a fines pacíficos pueden transformarse en herramientas letales en manos de actores malintencionados.

El uso de armas impropias plantea serias complicaciones en cuanto a la percepción del crimen y la seguridad pública (Giordani, J. F., 2020).



La dificultad para identificar y prever el uso de estos objetos como armas genera debates legales sobre su regulación y definición. Además, altera significativamente la percepción de los riesgos asociados con el crimen, afectando de manera profunda a la sociedad y presentando desafíos complejos para los sistemas judiciales y de seguridad encargados de prevenir y sancionar estos delitos.

Aspectos jurídicos

En el ámbito del derecho penal, el principio de intervención mínima desempeña un papel fundamental en la interpretación y aplicación de la ley, particularmente en lo relacionado con la clasificación y tratamiento de las armas (Penna, C., 2012).

Este principio sostiene que no todas las armas prohibidas desde una perspectiva administrativa tienen necesariamente relevancia penal (Giordani, J. F., 2020).

Para que un objeto sea considerado un arma desde el punto de vista penal, es esencial que su uso o posesión represente un peligro real para el bien jurídico protegido por la norma. La jurisprudencia ha ido matizando esta interpretación, estableciendo que, para que un objeto sea calificado como arma en términos penales, debe estar destinado específicamente a la ofensa o defensa personal. En este sentido, se excluyen aquellos objetos de uso cotidiano, ya sean domésticos o profesionales, que, aunque potencialmente peligrosos, no tienen como finalidad principal causar daño (Penna, C., 2012; Zelasco, A.M., 2023).

Esta distinción se refleja en la diferenciación legal entre las armas propias, particularmente las de fuego, y las armas impropias. Las primeras, debido a su naturaleza y finalidad, están sujetas a consecuencias legales más estrictas y claramente definidas, mientras que el tratamiento de las armas impropias depende en mayor medida de la interpretación judicial y del contexto en el que se empleen (Giordani, J. F., 2020).

En consecuencia, el tratamiento legal de las armas impropias tiende a ser más flexible y, por lo general, se traduce en sanciones menos graves.

Este enfoque subraya la importancia de un análisis contextual detallado en la determinación de la relevancia penal de un objeto que se utiliza como arma, reconociendo que la peligrosidad de un objeto no siempre radica en su naturaleza, sino en el modo y el propósito con que se emplea.

Tipos de armas impropias utilizadas en atentados terroristas

Como se ha señalado previamente, las armas impropias, que comprenden desde vehículos hasta productos químicos, evidencian como elementos inicialmente concebidos para fines pacíficos o civiles pueden ser reconvertidos y empleados con propósitos destructivos. En el contexto del terrorismo, estas armas adquieren una importancia singular debido a su alta accesibilidad, versatilidad y la dificultad inherente para ser detectadas.

A continuación, se expondrán algunos de los tipos de armas impropias que han sido utilizadas por grupos terroristas, destacando su impacto y el desafío que representan para la seguridad (CESEDEN, 2009; Valdés J.M., 2010; Quintana, Y., 2016; Agence France-Presse, 2017; De la Corte, L.; et al., 2022; MIOTI, 2023; Castresana, D., 2024; De la Calle, L.; et al., 2024; Euronews, 2024):



- **Vehículos:**

Los vehículos, especialmente los automóviles y camiones, se han utilizado como armas impropias en numerosos ataques terroristas. Esta táctica consiste en emplear dichos vehículos para arrollar multitudes, lo que genera un alto número de víctimas. A este tipo de táctica se le conoce como "vehículo ariete".

Los atentados con coches ariete, combinan simplicidad operativa con un alto impacto psicológico.

Casos emblemáticos incluyen el ataque de 2016 en Niza (Francia), que dejó 86 muertos y más de 400 heridos, el de Berlín (Alemania) en el mismo año, con 12 muertos y 56 heridos, y el de Barcelona (España) en 2017, con 13 muertos y más de 130 heridos, todos reivindicados por el ISIS. Más recientemente, el 20 de diciembre de 2024, en Magdeburgo (Alemania), se produjo otro ataque que dejó cinco muertos y más de 200 heridos, perpetrado por un inmigrante saudí.

Otra modalidad frecuente es el coche bomba, que se caracteriza por su capacidad para sorprender tanto a las autoridades como a la población. El vehículo, cargado con explosivos, puede pasar desapercibido hasta el momento mismo de la detonación, lo que aumenta su efectividad y amplifica el impacto psicológico del atentado. Esta capacidad de sigilo y planificación revela la sofisticación y el elevado riesgo asociados a este tipo de ataques.

Entre los atentados más trágicos con coche bomba, destaca el ataque en Beirut (Líbano) en 1983, donde dos camiones bomba dirigidos contra bases militares internacionales mataron a 307 personas, siendo uno de los primeros ataques de gran magnitud de la organización Yihad Islámica.

En Irak, el ataque en Karrada en 2016 se convirtió en uno de los más mortales, cobrando más de 340 vidas durante el Ramadán, y fue atribuido al Estado Islámico. De manera similar, el atentado en Bali (Indonesia) en 2002, con 202 muertos, fue llevado a cabo por el grupo terrorista Jemaah Islamiyah. En Mogadiscio (Somalia), un ataque en 2017 dejó más de 587 muertos, marcando un trágico récord, posiblemente a manos de Al Shabaab. La fácil accesibilidad a los vehículos convierte esta táctica en una herramienta particularmente eficaz para los grupos terroristas, quienes buscan no solo causar daño físico, sino también infundir temor y desestabilizar a la sociedad en su conjunto.

- **Aviones comerciales:**

El uso de aviones en atentados terroristas ha marcado un punto de inflexión en la historia contemporánea, no solo por la magnitud de la devastación que ocasionan, sino también por el simbolismo que impregnan en la percepción global de la seguridad. Los secuestros y ataques perpetrados con aeronaves comerciales han alterado profundamente la comprensión de la seguridad aérea, transformando estos medios de transporte en un nuevo vector de terror.

El atentado más emblemático y desgarrador fue, como hemos comentado, el del 11 de septiembre de 2001, en el que la organización terrorista Al Qaeda secuestró cuatro aviones comerciales. Dos de estos fueron estrellados contra las Torres Gemelas de Nueva York, otro impactó contra el Pentágono en Washington, y el cuarto se precipitó en un campo en Pensilvania, después de una valiente resistencia por parte de los pasajeros. Más de 3000 vidas fueron perdidas ese día, lo que no solo conmocionó al mundo, sino que redefinió las políticas de seguridad aérea a nivel global. Este ataque desencadenó la creación del

Departamento de Seguridad Nacional en Estados Unidos y la implementación de estrictas medidas de control en todos los aeropuertos internacionales, modificando para siempre las dinámicas de la aviación comercial.

Cada uno de estos atentados ha tenido un impacto devastador, no solo por las vidas humanas que se han perdido, sino también por el profundo cambio que ha provocado en nuestra concepción de la seguridad global. Sin embargo, el uso de aviones como herramientas de terror no se limitó al fatídico 11 de septiembre. En 1985, ocurrió otro atentado de gran impacto: la explosión del Vuelo 182 de Air India, que se desplomó sobre el océano Atlántico. La explosión fue provocada por una bomba colocada por un grupo separatista sij, como venganza por el asesinato de la primera ministra india Indira Gandhi. Este ataque cobró la vida de 329 personas.

Ese mismo año, otro ataque igualmente estremecedor tuvo lugar con el secuestro del Vuelo 847 de TWA, que viajaba de Atenas a Roma. Secuestrado por miembros del grupo terrorista Hezbolá, el avión fue desviado a Beirut (Líbano), donde los secuestradores mantuvieron a los pasajeros cautivos durante más de dos días. Durante ese tiempo, un pasajero estadounidense, Robert Stethem, fue ejecutado. Más tarde, en 1988, el Vuelo 103 de Pan American World Airways fue destruido en pleno vuelo sobre Lockerbie, Escocia, cuando una bomba colocada en su bodega de carga explotó. La tragedia resultó en la muerte de 259 personas a bordo y 11 más en tierra. Este ataque fue atribuido a agentes del gobierno libio, quienes supuestamente lo llevaron a cabo en respuesta a las sanciones internacionales impuestas a su país.

Más recientemente, en 2014, el Vuelo 17 de Malaysia Airlines fue derribado mientras sobrevolaba Ucrania, a manos de un misil lanzado desde una zona controlada por separatistas prorrusos. Aunque este ataque no utilizó el avión como arma directa, provocó la muerte de 298 personas y subrayó la creciente vulnerabilidad de la aviación civil en zonas de conflicto armado. La tragedia también puso de manifiesto la posibilidad de que aeronaves comerciales se convirtieran en blanco de misiles, lo que generó una nueva preocupación sobre la seguridad en el espacio aéreo.





- **Herramientas de uso doméstico:**

Diversos objetos de uso cotidiano, como cuchillos, hachas, sierras y otras herramientas, han sido utilizados por terroristas en ataques violentos. Estos elementos, aunque no están diseñados específicamente para causar daño masivo, pueden ser empleados para asesinatos individuales o ataques de menor escala.

Estos actos, a menudo perpetrados en lugares públicos como mercados, estaciones de tren o calles llenas de vida cotidiana, irrumpen en el día a día de personas comunes, transformando momentos ordinarios en tragedias inesperadas. Grupos como el Estado Islámico o Al Qaeda han utilizado habitualmente este tipo de táctica terrorista.

Los ejemplos de estos ataques abarcan todo el mundo. En Europa, escenas como las del Puente de Londres en 2017 o la iglesia de Niza (Francia) en 2020 muestran cómo el horror puede interrumpir momentos cotidianos y generar una oleada de miedo e incertidumbre.

En Asia, destaca el ataque en la estación de Kunming de 2014, un atentado terrorista ocurrido en la estación de trenes de Kunming, capital de la provincia de Yunnan, en el suroeste de China. El ataque fue perpetrado por un grupo de terroristas separatistas uigures que irrumpieron en la estación armados con cuchillos y machetes. Este asalto dejó 29 personas muertas y más de 140 heridas.

Por otro lado, no podemos dejar de mencionar la "Intifada de los cuchillos", que tuvo lugar entre 2015 y 2016 en Israel y los territorios palestinos ocupados. Este período estuvo marcado principalmente por ataques individuales con cuchillos y otros objetos punzantes, realizados por palestinos, en su mayoría jóvenes, que atacaban a israelíes en lugares públicos como estaciones de autobuses, mercados y calles.

- **Productos químicos:**

Los explosivos improvisados, conocidos como IEDs (por sus siglas en inglés, Improvised Explosive Devices), se han convertido en una de las armas más utilizadas en atentados terroristas. Estos artefactos, fabricados con materiales comunes como fertilizantes, productos químicos industriales y objetos de uso cotidiano, son fácilmente accesibles y pueden transformarse en explosivos poderosos. Esta facilidad de acceso y la capacidad de crear armas letales con recursos mínimos los han hecho especialmente atractivos para quienes buscan causar daño sin necesidad de grandes infraestructuras o presupuestos.

El uso de bombas caseras ha sido particularmente común en zonas de conflicto como Irak y Afganistán, donde los IEDs se han empleado como una táctica recurrente tanto contra fuerzas militares como contra civiles. A lo largo de las últimas décadas, el uso de explosivos caseros ha sido una constante en varios atentados terroristas, destacándose la utilización del nitrato de amonio como uno de los componentes principales. En América Latina, uno de los ataques más devastadores ocurrió en Buenos Aires en 1994, cuando un atentado contra la Asociación Mutual Israelita Argentina (AMIA) utilizó 300 kilogramos de nitrato de amonio, resultando en 85 muertos y más de 300 heridos.

Otro caso igualmente significativo tuvo lugar en 1995 en Estados Unidos, cuando Timothy McVeigh llevó a cabo el atentado en Oklahoma City utilizando aproximadamente dos toneladas de nitrato de amonio mezcladas con combustible (ANFO) para fabri-



-car un explosivo que detonó frente a un edificio gubernamental. Este ataque causó la muerte de 168 personas y dejó más de 600 heridos, demostrando la tremenda capacidad destructiva de este compuesto y la facilidad con la que puede ser adquirido y utilizado con fines terroristas.

En Europa, el uso de explosivos caseros también ha sido frecuente en diversos atentados. En 2011, en Noruega, Anders Breivik utilizó nitrato de amonio extraído de fertilizantes para fabricar una bomba que explotó en el distrito gubernamental de Oslo, matando a 8 personas. Este atentado fue solo el inicio de una matanza aún más grande en la isla de Utøya, donde Breivik asesinó a 69 personas más.

Más recientemente, en 2016, los atentados en Bruselas evidenciaron nuevamente el uso de bombas caseras. Los atacantes utilizaron explosivos improvisados en el aeropuerto y estaciones de tren, dejando un saldo devastador de 35 muertos y más de 300 heridos.

En España, desde 1958 hasta 2018, el grupo terrorista Euskadi Ta Askatasuna (ETA) también utilizó en numerosas ocasiones explosivos improvisados, causando centenares de muertos y heridos a lo largo de su historia. El uso de productos químicos en estado gaseoso como armas en atentados terroristas también ha dejado su huella. En 1995, en el metro de Tokio (Japón), miembros del culto Aum Shinrikyo liberaron gas sarín, causando la muerte de 13 personas y dejando miles de heridos.

Otro caso notorio ocurrió en 2001, cuando se enviaron cartas con esporas de ántrax en Estados Unidos, generando pánico y movilizando recursos a pesar de no ser un ataque masivo. Ese mismo año, en Japón, se intentó un ataque con gas VX, un neurotóxico, aunque el plan no se llevó a cabo por completo.

- **Informática:**

Aunque no se trata de un objeto físico, los ciberataques pueden considerarse un tipo de arma impropia en la medida en que utilizan tecnologías comunes, como ordenadores y redes de comunicación, para causar daños masivos a infraestructuras críticas, sistemas financieros o servicios públicos. Los ataques de denegación de servicio (DDoS), el robo de datos sensibles o el sabotaje de infraestructuras se han convertido en formas de ataque utilizadas por grupos terroristas en el ciberespacio.

Los ciberataques recientes han demostrado el impacto disruptivo que pueden tener sobre infraestructuras críticas y la estabilidad global. En 2010, el malware Stuxnet fue uno de los primeros ejemplos claros de cómo los ciberataques pueden dañar físicamente infraestructuras clave, al sabotear instalaciones nucleares en Irán. En 2013, el hackeo a la presa de Nueva York mostró cómo las amenazas cibernéticas pueden afectar directamente sistemas de seguridad esenciales para la protección física de las personas.

El ataque a la red eléctrica de Ucrania en 2015 y 2016, ejecutado por hackers vinculados al grupo ruso Sandworm, dejó a 230.000 personas sin electricidad, exponiendo vulnerabilidades en los sistemas de energía de un país entero. En 2017, el ransomware Wannacry, atribuido al grupo Lazarus de Corea del Norte, afectó a dispositivos en 150 países, paralizando sectores clave como la salud y el transporte, y generando pánico global. Posteriormente, en 2021, el hackeo al oleoducto Colonial Pipeline en Estados Unidos, realizado por el grupo DarkSide, desató una crisis de seguridad nacional al generar una escasez de combustible en varias partes del país.



Desde principios de los años 2000, grupos como ISIS y Al-Qaeda han utilizado Internet para difundir propaganda, coordinar ataques y ampliar su alcance ideológico. Durante la pandemia de COVID-19, los ciberataques a hospitales empeoraron aún más la crisis sanitaria, subrayando la letalidad indirecta del ciberterrorismo. Estos eventos destacan el creciente peligro de las amenazas cibernéticas, que no solo afectan a la información, sino también a la seguridad y bienestar de las personas a nivel global.

Conclusiones

El uso de armas impropias en atentados terroristas pone de manifiesto la vulnerabilidad de la seguridad cuando objetos cotidianos se convierten en herramientas de destrucción. Estos ataques, que hacen uso de elementos comunes como cuchillos, vehículos o explosivos caseros, reflejan la capacidad de los grupos terroristas para adaptarse y aprovechar la facilidad de acceso a estos materiales. Por ello, enfrentarlos requiere respuestas integrales y efectivas.

En primer lugar, es esencial limitar el acceso a materiales peligrosos y combatir el tráfico ilegal de los mismos (Magaz, R., 2012). Medidas como las regulaciones que restringen los precursores de explosivos o los esfuerzos de cooperación internacional han demostrado ser valiosas en esta lucha (De la Corte, L.; et al., 2022). No obstante, estas iniciativas deben complementarse con el uso de tecnologías avanzadas capaces de detectar amenazas a tiempo, así como con programas de formación continua para que las fuerzas de seguridad puedan anticiparse a las tácticas en constante evolución de los terroristas.

Un aspecto igualmente crucial es cortar las fuentes de financiamiento de estas organizaciones. La aplicación de sanciones contundentes y la creación de leyes claras que penalicen sus actividades delictivas puede debilitar significativamente las operaciones y la capacidad de acción de los grupos terroristas (De la Calle, L.; et al., 2024).

Asimismo, la lucha contra las armas impropias no se limita a medidas técnicas o legales. También es necesario abordar la prevención de la radicalización y el extremismo violento. Fomentar sociedades más inclusivas, donde la educación y el diálogo intercultural jueguen un papel central, puede reducir las condiciones que facilitan el reclutamiento de personas vulnerables.

Enfrentar el uso de armas impropias en el terrorismo exige una respuesta conjunta, constante y adaptable.

Solo mediante un esfuerzo global coordinado, el fortalecimiento de las capacidades tecnológicas y legales, y la creación de sociedades más resilientes, será posible proteger vidas y garantizar un futuro más seguro para todos.

REFERENCIAS

Agence France-Presse (2017). Casos de vehículos lanzados contra la multitud en Europa y EEUU. Defensa y seguridad. <https://ednh.news/es/casos-de-vehiculos-lanzados-contr-la-multitud-en-europa-y-eeuu/>

Castresana, D. (2024). Cronología de los atentados del 11-S. <https://elpais.com/noticias/atentados-aereos/>

CESEDEN (2009). La seguridad frente a artefactos explosivos. Ministerio de Defensa.



De la Calle, L.; et al. (2024). La naturaleza del terrorismo: violencia política y clandestinidad. Catarata.

De la Corte, L.; et al. (2022). Terrorismo: causas, efectos y tendencias. Autoedición.

Euronews (2024). Ataque con cuchillos. <https://es.euronews.com/tag/ataque-con-cuchillos>

Giordani, J. F. (2020). ¿Puede incluirse a los perros dentro del concepto de arma impropia a los fines del agravante? Lecciones y Ensayos,104,107-137.

Magaz, R. (2012). Criminalidad y globalización. IUGM.

MIOTI (2023). ¿Cuáles han sido los mayores ciberataques de la historia? <https://miot.es/es/blog-cuales-han-sido-los-mayores-ciberataques-de-la-historia/>

Penna, C. (2012). Robo con armas y armas impropias. Editores del puerto.

Quintana, Y. (2016). Ciberguerra. Catarata.

Valdés J.M. (2010). Terrorismo y artefactos explosivos aspectos penales y criminológicos: estudio de la incidencia de este fenómeno entre los años 1993 y 2006 en el País Vasco. [Tesis Doctoral Universidad Nacional de Educación a Distancia (UNED)]

Zelasco, A.M. (2023). El concepto de “arma impropia” como artificio punitivo. Revista pensamiento penal, 482, 1-6.

DESCIFRANDO LA MENTE DEL YIHADISTA

ya disponible
EN AMAZON

Islam

Martirio

Injinas

Yihad

Daes
Al Ibtla

Tagut

Takfir

Al Hakim

BAHAE EDDINE BOUMNINA



ENTREVISTA

WWW.ALGHURABA.ORG



GUSTAVO MERANI

CPO CERTIFIED PROTECTION OFFICER IFPO



Gustavo Merani es CPO Certified Protection Officer IFPO.

Miembro del Comité Directivo de la Comunidad de Protección Ejecutiva de ASIS Internacional.

Miembro del Consejo Consultivo Latino de IFPO.



1-. ¿Qué papel juega la seguridad privada en la protección de espacios públicos y privados en la actualidad?

La seguridad privada está desempeñando actualmente un papel muy importante en la protección de espacios privados y públicos, complementando y colaborando en forma permanente con las fuerzas de seguridad. Desde un tiempo atrás se viene trabajando en esto que denominamos “integración” entre los distintos sectores relacionados con la seguridad en beneficio de los ciudadanos; la seguridad privada tiene su ámbito regulado por leyes, pero trabaja en colaboración con las autoridades en eventos deportivos, festivales, parques, aeropuertos, estaciones de transporte público, hospitales siendo un aliado estratégico reportando incidentes, colaborando en casos de emergencia y muchas veces aportando tecnología poniendo a disposición central de monitoreo.

2-. ¿Cuáles son los principales riesgos de seguridad que enfrenta un espacio concurrido, como un centro comercial o un estadio?

En principio debo manifestarte, que cada uno de esos espacios tiene riesgos distintos, amenazas distintas, vulnerabilidades distintas entre otros puntos por la zona geográfica que se encuentran ubicados, o el público que asiste teniendo en cuenta sexo, edad, nivel económico, nivel de estudios, necesidad de concurrencia, etc. También debemos tener en cuenta cuestiones geopolíticas, ya que desempeñan un papel muy importante en la configuración de las estrategias de prevención. Y además debemos comprometer a todos los actores, mientras haya más actores comprometidos con los objetivos, más fácil será la mitigación de los riesgos. Un buen modelo de seguridad debe comprometer a todos a un cambio hacia la cultura de la prevención. Los riesgos no deben ser ignorados.

Por eso es tan importante que el profesional encargado de la seguridad tenga actualizado su estudio de seguridad, el análisis de riesgo y un PESTEL que lo ayudará a gestionar los riesgos hasta llevarlo a un nivel aceptable, el profesional a cargo debe saber cuál es el nivel de riesgo aceptable para la gestión eficiente teniendo en cuenta los riesgos naturales, los tecnológicos y los sociales. El riesgo es administrable. Entre sus desafíos no solo están la prevención de incendios, atentados, disturbios, cortes de suministro o fenómenos naturales, sino también los hurtos, robos, vandalismo, aglomeraciones, amenazas de atentado.

3-. ¿Qué estrategias son esenciales para garantizar la seguridad de grandes eventos con gran afluencia de público?

La seguridad en eventos masivos es un desafío enorme. No solo si nos referimos a eventos como partidos de fútbol, rugby o básquet también tenemos recitales de importantes grupos de música o eventos de música electrónica por poner algunos ejemplos; no es lo mismo un partido de fútbol de eliminatorias para participar de un mundial entre Argentina y Brasil o Inglaterra Serbia como pasó en la Eurocopa 2024, o partidos de final de Libertadores con equipos de Brasil en el Estadio Monumental de Argentina, o final de Copa Sudamericana entre un equipo de Argentina y otro de Brasil en Paraguay.

Un dato que puede llamar la atención a profesionales de Europa: en la Ciudad de Buenos Aires hay 18 estadios de fútbol; es la Ciudad con más estadios de fútbol en el mundo. Para los organismos de seguridad pública es una gran tarea de coordinación entre la policía, los servicios de emergencias médicas, los bomberos, defensa civil y también la seguridad privada. En Buenos Aires ha habido sábados o domingos con una maratón de 15.000 corredores, una fiesta electrónica con artistas internacionales de primer nivel de 65.000 tickets vendidos y varios partidos de fútbol, todo el mismo día.



Podríamos empezar con un enfoque sociológico analizando al público como categoría de grupo humano, también podemos hacer un enfoque psicológico con los patrones de conducta o el espíritu colectivo, y además los aportes desde la psicología social estudiando las masas y la psicología de los públicos. Debemos tener en cuenta los troncales de ingreso y egreso, controles físicos y electrónicos, aforo de los estadios, protocolos de actuación específica para este tipo de eventos y por supuesto debe estar coordinado integrando a los sectores públicos y privados.

4-. ¿Cómo colabora la seguridad privada con las fuerzas y cuerpos de seguridad del Estado en situaciones de emergencia o crisis?

Es de suma importancia que las personas que se dedican a la seguridad privada, estén capacitadas para poder colaborar con la policía y los bomberos en casos de emergencias o atentados. También debemos mencionar, aunque no suene simpático, que los actores estatales de seguridad deben tener la capacidad de entender que la seguridad privada “colabora” y quiere participar y en muchos casos tienen un alto nivel de capacitación, por lo tanto, debería ser aceptada esa colaboración. Los agentes de seguridad privada pueden colaborar despejando accesos, ordenando el flujo de personas, hacer espacio para que puedan ingresar las ambulancias o los bomberos. Si las acciones están coordinadas y cada uno respeta su lugar, la seguridad privada puede ser de gran utilidad.

5-. ¿Qué características debe tener un plan de seguridad efectivo para prevenir y responder a incidentes de seguridad graves?

Primero deberíamos saber que sería un “incidente de seguridad grave” dentro de nuestra corporación para poder establecer una respuesta efectiva, para tener capacidad de respuesta. Pero debemos tener claro si ese incidente grave está relacionado a la seguridad física o a lo tecnológico, si es un incidente dentro de la cadena de procesos de la corporación, si es un incidente de violencia en el ámbito laboral; es decir son varios los frentes que se abren y para todos debemos tener capacidad de respuesta. ¿Tenemos claro en cuanto tiempo vuelve al normal funcionamiento nuestra corporación después de ese incidente? ¿Tenemos claro cuál es la pérdida? Por qué la pérdida no solo es económica, nuestra empresa también ve afectada su imagen, su reputación. ¿Cómo nos verá después de ese incidente la competencia? O ¿Cómo nos verán nuestros propios colaboradores? Debemos tener claros tipos de análisis de riesgo, análisis de costos y pérdidas, evaluación de criticidad y probabilidad, contramedidas apropiadas y por supuesto cuestiones legales.

Paralelo a eso nuestro estudio de seguridad física tiene muchas facetas, por ejemplo técnicas y tecnología de encuesta, construcción de planes y datos a ser recolectados, métodos de recolección y análisis de datos, nivel de vulnerabilidad y evaluación de sistemas existentes y habilidad de recuperación de desastres e interrupciones.

6-. ¿Cuáles son las principales competencias que deben desarrollar los escoltas privados para cumplir con su labor de manera eficiente?

La protección ejecutiva o protección de personas de alto valor debe ser la rama de la seguridad que más ha evolucionado en los últimos 20 años. Hoy no alcanza con pesar 120 kilos. No alcanza con ser 3.er dan de algún arte marcial; no tienes ni para presentarte en una entrevista de trabajo con eso. Para muchas personas, la protección ejecutiva sigue siendo concebida únicamente como acompañantes armados que siguen al protegido por todos lados sin estrategia, esperando reaccionar en el



último momento y creyendo que su capacidad de respuesta será efectiva. La improvisación y una dosis de soberbia que asume que se sabe lo que no se sabe, pueden producir malos resultados. Hoy se necesitan profesionales competentes que son los que reúnen aptitudes y actitudes para la acción, que se manifiestan a través de un desempeño personal, profesional y social efectivo en la solución de los problemas de su entorno inmediato y mediato pudiendo incluso resolver aquellos no predeterminados.

Nosotros entendemos como protección ejecutiva si el cliente o usuario final reúne riesgos, recursos e importancia crítica y si su equipo de protección tiene la capacidad de reducir los riesgos a un nivel aceptable. Nosotros no somos “seguridad”, gestionamos riesgos. La evolución de la industria de la Protección Ejecutiva ha sido enorme y ha dado lugar a la creación de especialidades que antes no existían. Protección corporativa, Protección a familias, Protección de celebridades, Protección basada en la fe, Protección gubernamental, y Operaciones de protección en entornos hostiles.

La PE es un sistema, un conjunto de medidas que tiene como objetivo reducir significativamente la exposición del VIP / PMI al riesgo, desactivar los ataques en su fase de preparación, solamente acudiendo a la reacción como último recurso evitando daños no intencionales y protegiendo la imagen tanto de la persona como de la corporación y también la información sensible que el protegido posee. Hay algo que debemos entender, el equipo de protección de una corporación es parte fundamental de lo que se denomina continuidad del negocio.

Siempre se habló de habilidades duras y habilidades blandas, ahora esas habilidades deben ser específicas.

7-. ¿Qué importancia tiene la formación continua de los profesionales de la seguridad privada frente a amenazas emergentes como el terrorismo?

Es significativo, sin dudas. El terrorismo ya no es esa cosa terrible que sucede en países lejanos. Actualmente, los clientes, cada vez exigen más, cada vez tienen más requerimientos para conformar un equipo de protección. Recuerdo una excelente capacitación universitaria sobre Terrorismo que dictaba el Magister Alejandro Cassaglia sobre terrorismo, maras y pandillas, solo había dos alumnos que se dedicaban a la protección de personas. En Argentina hubo hechos terribles relacionados al terrorismo internacional que han cambiado la historia ¿Cómo no vamos a capacitarnos sobre terrorismo? Si formas parte de un equipo de protección de un empresario importante, tienes que viajar al exterior con él, ¿Cómo no vas a capacitarte sobre Terrorismo? Tienes que capacitarte sobre cuestiones geopolíticas, “pensar global”, entender como funciona la política internacional. De igual manera, sobre delitos tecnológicos. Un oficial de protección moderno debe estar capacitado también en delitos tecnológicos. Es importante saber disparar, saber pelear, saber conducir; pero hoy con eso solo no alcanza.

8-. ¿Cómo pueden los escoltas privados contribuir a la detección y prevención de actos terroristas?

Interesante pregunta. Con capacitación. En principio entendemos que es una actividad de los organismos de Estado, y volviendo a lo que hablamos anteriormente sobre la integración de lo público y lo privado en los servicios de seguridad, creo que se puede aportar mucho en la “detección” por ejemplo en un evento masivo, en un hotel, en una embajada, en un aeropuerto; en estado de alerta la visualización de las personas que están en su entorno sus acciones, su actitud, su vestimenta, los objetos que portan. Un buen sistema de seguridad puede llegar a ser disuasorio y ejercer efectos preventivos. Ser capaz de “leer” a las personas es muy importante. La comunicación no verbal constituye entre el 60 y el 65% de toda la comunicación interpersonal.



9-. ¿Qué papel juega la tecnología en la modernización de la seguridad privada y en la respuesta a posibles atentados terroristas?

Hoy todo pasa por lo tecnológico. No podemos imaginar un servicio de seguridad que no esté actualizado en cuanto al uso de tecnología, con una central de monitoreo eficiente, eficaz y efectiva, con equipos de comunicación que funcionen perfectamente, el uso de aplicaciones para teléfonos ha avanzado muchísimo, aplicaciones de rastreo y seguimiento, aplicaciones para grabar conversaciones, aplicaciones para monitorear vuelos, buques, el tránsito en una ciudad, monitorear publicaciones en redes sociales, monitorear noticias que se publiquen en los medios. Hoy todas las policías del mundo, en sus ciudades más importantes, tienen un departamento de delitos tecnológicos.

En el ámbito privado y con el cuidado de las leyes locales también existen centros de monitoreo y empresas que protegen a clientes de ataques cibernéticos que pueden afectar no solo su imagen personal, sino también la de la empresa que representa. Por eso debemos capacitar no solo a nuestro cliente, sino también a sus hijos, a sus familiares directos, a sus secretarías y asistentes, a las personas que colaboran en su casa, a quienes cuidan a sus hijos, porque siempre, quien filtra la información es alguien del entorno. ¿Cuántas veces vimos publicadas fotos de personas muy importantes en vacaciones? Muchas. Y vemos donde están vacacionando, vemos en que hotel están alojados, vemos con quién se reúnen, vemos en que vehículos se desplazan; ellos mismos nos envían información muy sensible que debe ser controlada por su jefe de seguridad para no ser publicada y que llegue a las manos que no debe llegar.

Recordemos en 2022 asesinaron al Fiscal Marcelo Pecci paraguayo, que investigaba casos de narcotráfico y estaba de vacaciones en Colombia, lo atacaron a balazos en plena playa de Cartagena, ¿Cómo sabían que estaba de vacaciones en Colombia? Una filtración, una foto publicada, un seguimiento de teléfonos, rastreo de mail, historial del navegador de su computadora, compras con tarjetas de crédito, alguien de migraciones que vendió información; cualquiera de estas hipótesis está relacionada con lo tecnológico.

10-. ¿Qué retos enfrenta actualmente el sector de la seguridad privada en la protección contra el terrorismo y cómo pueden superarse?

Adaptarse o morir, así de simple. A nadie le importa lo que hicimos ayer. Hoy no alcanza con tener un título universitario, o con haber sido 30 años miembro de una fuerza de seguridad o una fuerza armada. La seguridad evoluciona en forma constante y eso es muy bueno porque nos obliga a buscar algo más, siempre hay algo más. Tenemos un título universitario, busquemos otro. Tenemos una carrera de 30 años de policía, busquemos certificarnos internacionalmente en ASIS o IFPO.

Compremos libros, leamos, participemos de ferias, de eventos, de capacitaciones que dictan profesionales respetados. Seamos miembros de organizaciones reconocidas internacionalmente que nos permitan hacer networking con otros profesionales de otras partes del mundo, que pueden tener o haber tenido las mismas necesidades que nosotros. Estemos actualizados. Todo cambia, todo avanza. Tengamos ese espíritu de aprendizaje permanente, siempre vivo, que nos ayude a destacarnos, a ser diferentes, a ser distintos.



Evidentia
University
of Behavioral & Forensic Sciences

Master of Science in Criminal Profiling

Profesores del FBI, Policía Nacional Española, Guardia Civil Española, Policía Nacional de Ecuador, Fiscalía de México y los mejores profesores internacionales en la materia.

100% online con clases semanales en vivo.

Tutorización y seguimiento continuo.



Programa en español o inglés.
Tú eliges.

www.evidentiauniversity.com

111 E Monument Av. Kissimmee, Florida. USA



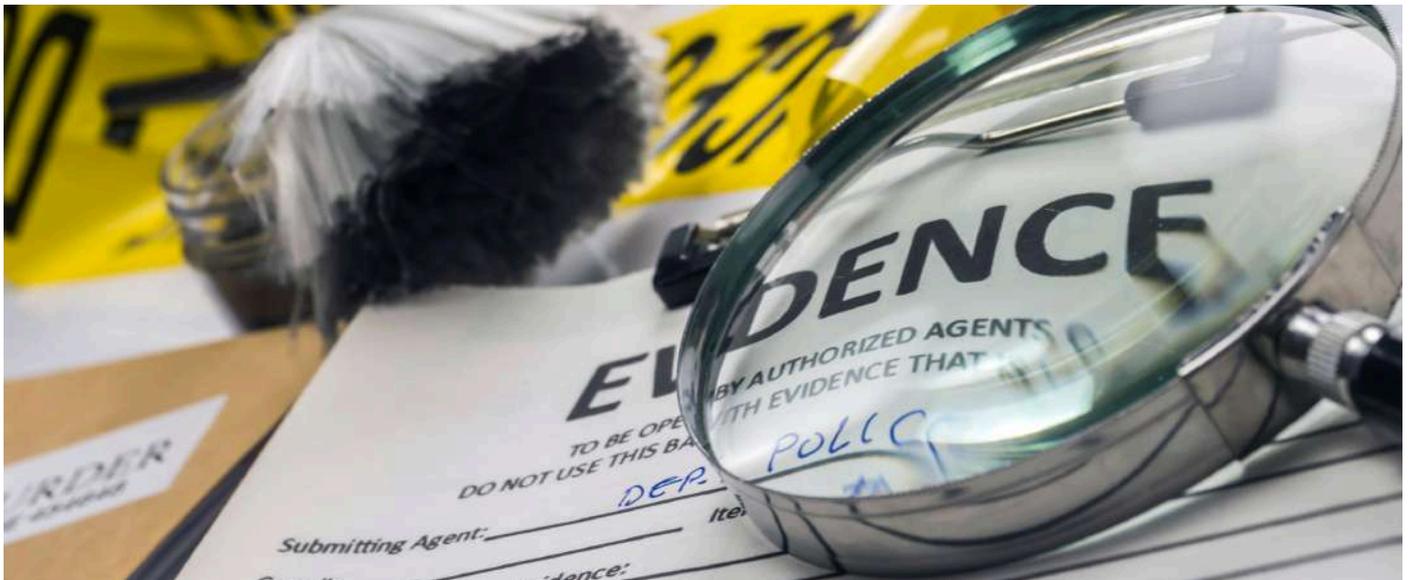
CRIMINOLOGÍA

WWW.ALGHURABA.ORG

LA IMPORTANCIA DE LA AUDITORIA FORENSE CONTABLE

EN LA INVESTIGACIÓN CRIMINAL FINANCIERA MUNDIAL

Francisco Javier Ramos.
Perito Forense Contable.



Introducción

En los tiempos que estamos viviendo, cada día que pasa en el ámbito profesional forense contable, se van experimentando cambios inherentes a las investigaciones criminales financieras de las que indudablemente se desprenderán evidencias graves causadas al patrimonio económico de las entidades o personas físicas. Derivado de lo anterior, al experto forense contable se le exigirá mayor preparación y experiencia forense criminal en el área en materia de Contabilidad, pues los procesos contables hoy ya son digitales, coadyuvando en tener la información en el menor tiempo y esfuerzo, obteniéndose un producto de mayor calidad y presentación que le permita al Órgano Jurisdiccional, es decir, al Juez, valorarlo y emitir su sentencia correspondiente.

Ahora bien, las entidades, sean estas públicas o privadas, sectores gubernamentales o empresariales, no están exentos de la delincuencia criminal financiera, sus sistemas contables digitales pueden ser vulnerados por estos grupos delictivos afectando su patrimonio económico o financiero a nivel mundial. Por ello, hoy día se cuenta con el apoyo de los profesionales en las mate-

-rias del Derecho y Auditoría Forense Contable, así como la Auditoría Forense en informática, las cuales de manera conjunta intervendrán en la solución del caso elaborando el Informe Pericial Contable así como el Informe en Informática Forense, o en su caso, el Dictamen Pericial Contable o de Informática Forense.

La Auditoría Forense Contable vinculada a la Auditoría de Informática Forense, coadyuvará de manera muy importante en la investigación criminal en los sistemas de informática rastreando y encontrando las evidencias en los registros digitales contables e información financiera aunque hayan sido encriptadas en otros archivos no contables, o incluso al ser desechados o borrados del sistema financiero contable por el responsable o los responsables del manejo financiero dentro de la empresa o negocio particular.

Así mismo, es importante observar que el experto en Auditoría Forense en Informática en la actualidad es de suma importancia su experiencia profesional, pues la mayor parte de la Investigación Criminal Financiera está digitalizada en los sistemas y programas computacionales y deberán ser revisados de manera profunda y completa al cien por ciento todo lo almacenado digitalmente, aplicando la normativa forense digital y lo concerniente a lo establecido en las leyes vigentes, de tal manera que dichas evidencias o pruebas le sean turnadas al experto en Contabilidad Forense.

Una vez que el experto Forense en informática le entregue dicha información financiera al experto contable, este procederá a analizar dichos archivos del que se desprenderá un informe pericial contable o a su vez un dictamen pericial contable.

Es importante mencionar que el avance de la IA (INTELIGENCIA ARTIFICIAL) de la informática y lo digital en el mundo, ha causado una gran revolución y avance tecnológico, y esto aparejadamente al avance de los criminales digitales o informáticos, quienes han causado fraudes cibernéticos a instituciones financieras, gobiernos, ciudadanos, etc... logrando obtener grandes recursos económicos de manera deshonestamente





socavando el patrimonio de los afectados. De ahí, la necesidad de la intervención de los expertos en las materias del derecho, de la auditoría forense contable y de la auditoría forense en informática, para la investigación de los hechos, obtención de las evidencias digitales y contabilidad financiera las que a través del Informe Pericial de informática o del Dictamen de Auditoría Forense Contable se presente la denuncia penal por medio del abogado al Órgano Jurisdiccional es decir, el Juez.

Evidentemente, cada país tiene su sistema de justicia y órganos judiciales, los cuales deberán observar de manera obligatoria los procedimientos a seguir en materia de Auditoría Forense Contable y en materia de Auditoría Forense en informática, por lo que siempre habrá que tener presente los requisitos a observar en la elaboración tanto del Informe Pericial Contable y el Informe Pericial en materia de Informática así como lo del Dictamen Pericial Contable y el Dictamen Pericial en Informática.

Informe pericial, contable y de informática forense

- Autoridad a quien se dirige el Informe Pericial.
- Planteamiento del Problema.
- Metodología Científica.
- Conclusiones.

Dictamen pericial contable y de informática forense

- Autoridad a quien se dirige.
- Planteamiento del problema.
- Metodología Científica.
- Cuestionario/ampliación del Cuestionario.
- Fundamentación y Motivación de las respuestas.
- Conclusiones y la razón de su dicho/ lugar y fecha.
- Firma del experto.

Cabe mencionar que generalmente esta es la información que debe contener dichos elementos de prueba judiciales como lo son el INFORME PERICIAL Y EL DICTAMEN PERICIAL.

Finalmente, estos documentos de carácter probatorios en materia del derecho penal, contribuyen de manera profesional a que el Órgano Jurisdiccional pueda obtener clarificación en el análisis de las evidencias en materia financiera contable así como en materia de informática, es decir, información digital, esclareciendo su Teoría del Caso y poder emitir su sentencia correspondiente.

Cada día que pasa observamos que los avances en materia de informática y en lo digital, van a pasos agigantados en el mundo, así como la criminalidad digital, el delito con instrumentos o equipos digitales, software o hardware, entre ellos computadoras, tablets, teléfonos, lentes digitales, relojes inteligentes (IA) así como programas muy actualizados de informática. Por ello, a los gobiernos les obliga a aprobar nuevas leyes con mayores penas judiciales a quien violente dichas normas en materia digital o de informática que contribuya a aminorar dicha problemática en la era de la IA en el mundo.



TRIBUNA DE OPINIÓN

WWW.ALGHURABA.ORG

SIRIA EN TRANSICIÓN

RETOS Y OPORTUNIDADES BAJO EL LIDERAZGO DE AHMED AL-SHARAA

CISEG.

Analistas de CISEG.



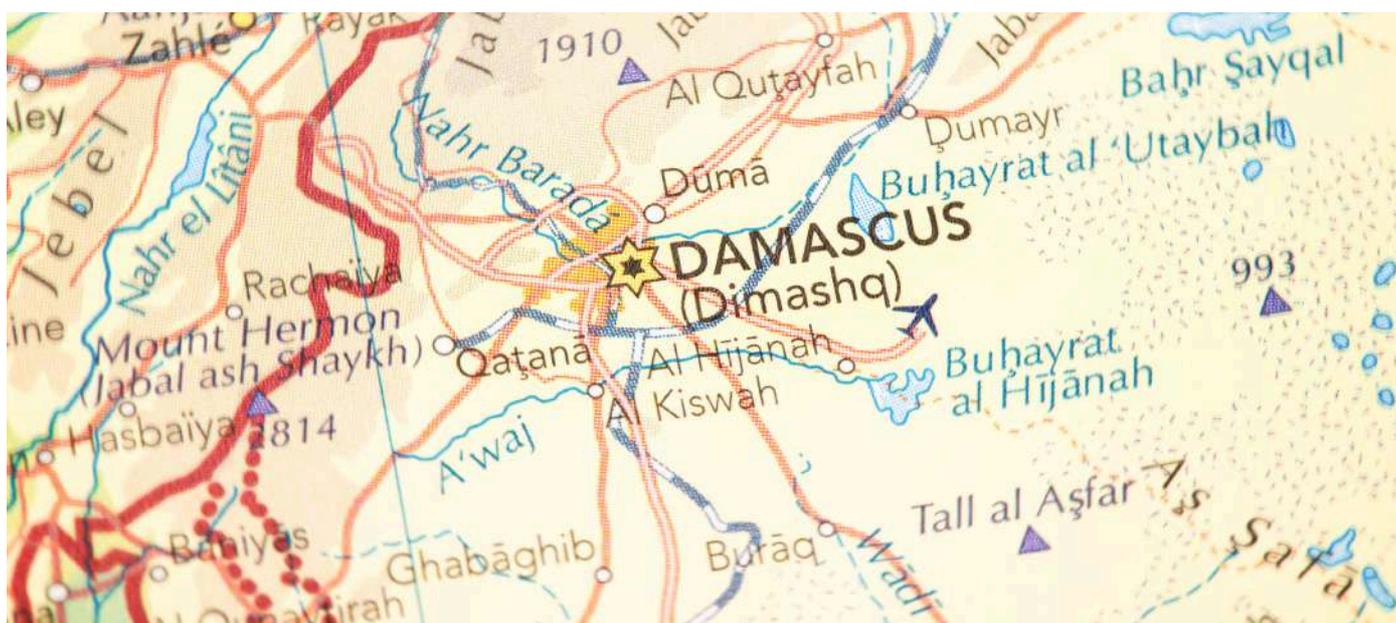
Tras la caída del régimen de Bashar al-Assad en diciembre de 2024, Siria se encuentra inmersa en una delicada fase de transición liderada por Ahmed al-Sharaa, más conocido como Abu Mohammed al-Golani, antiguo dirigente del grupo Hayat Tahrir al-Sham. Este cambio de liderazgo supone un momento crucial en la historia reciente del país, que tras años de conflicto devastador enfrenta la tarea monumental de reconstruirse en lo político, económico, social y diplomático. A partir de marzo de 2025, se perfilan diversos escenarios que abarcan desde la consolidación del poder y la estabilización interna hasta la reconfiguración de las relaciones internacionales y la implementación de una transición democrática.

La consolidación del poder por parte de al-Golani será un paso inicial imprescindible para intentar traer estabilidad tras más de una década de guerra civil. Entre las medidas que su gobierno podría implementar, se encuentra la suspensión de la actual Constitución para instaurar un marco legal temporal que permita gobernar mientras se elabora una nueva carta magna. Este movimiento estaría orientado a evitar el colapso institucional, aunque podría ser interpretado por algunos sectores como una señal de autoritarismo.

Paralelamente, al-Golani podría buscar neutralizar a sus opositores, tanto armados como políticos, mediante estrategias de cooptación, represión o acuerdos estratégicos. También será fundamental fomentar la unidad nacional a través de alianzas con grupos tribales y otras facciones, utilizando su experiencia como líder de HTS para presentarse como un garante de la estabilidad. Sin embargo, estas acciones conllevan riesgos considerables, pues si son percibidas como medidas autoritarias podrían alimentar tensiones internas y externas que comprometan el proceso de transición.

En el ámbito económico, Siria enfrenta una devastación sin precedentes tras años de conflicto armado, lo que requerirá un enfoque integral para la reconstrucción. La prioridad será atraer inversión extranjera, un objetivo que demandará esfuerzos diplomáticos significativos para normalizar relaciones con actores clave en el Golfo y Asia, quienes podrían mostrar interés en participar en la reconstrucción del país. Al mismo tiempo, el gobierno deberá trabajar para obtener el levantamiento de sanciones internacionales, un desafío que implicará demostrar una ruptura clara con vínculos previos con grupos yihadistas y un compromiso con reformas políticas significativas. En el plano interno, la reconstrucción económica deberá enfocarse en rehabilitar infraestructuras críticas como el suministro de agua, electricidad y transporte, además de revitalizar sectores clave como la agricultura y la industria. Asimismo, será crucial abordar las necesidades humanitarias de millones de desplazados internos y refugiados en el extranjero, cuyo retorno seguro e integración serán factores determinantes para la estabilidad a largo plazo.

La legitimidad internacional del nuevo gobierno de al-Golani será otro de los grandes desafíos en este escenario de transición. Su estrategia podría centrarse en presentarse como un líder moderado, pragmático y necesario para estabilizar Siria, adoptando un discurso que priorice la lucha contra los extremismos residuales y el progreso del país hacia una mayor normalidad. Las relaciones con potencias regionales como Turquía, Qatar, Arabia Saudita y Emiratos Árabes Unidos jugarán un papel crucial, ya que estos países podrían actuar como mediadores para facilitar la aceptación de su liderazgo en el ámbito internacional. Sin embargo, la relación con Occidente será probablemente más compleja, ya que Estados Unidos y la Unión Europea podrían mostrarse cautelosos y exigir pruebas contundentes de reformas políticas, respeto a los derechos humanos y avances democráticos antes de otorgar reconocimiento pleno o apoyo económico.





El tejido social de Siria, caracterizado por su diversidad étnica y religiosa, plantea un desafío adicional para la cohesión interna. Al-Golani podría intentar garantizar la inclusión ofreciendo representación a minorías como kurdos, drusos y cristianos en el gobierno, promoviendo un mensaje de unidad y confianza en su administración. Además, la implementación de procesos de justicia transicional para abordar los crímenes cometidos durante la guerra podría ser una herramienta clave para cerrar heridas y fomentar la reconciliación nacional. No obstante, si el gobierno no responde adecuadamente a las demandas y necesidades de estas comunidades, corre el riesgo de enfrentarse a levantamientos locales o incluso a un resurgimiento de conflictos internos.

En el ámbito de la seguridad, Siria seguirá enfrentándose a la amenaza de milicias armadas y grupos extremistas. El gobierno deberá negociar el desarme y la reintegración de estas facciones, ofreciendo alternativas económicas como su incorporación en un ejército nacional o en programas civiles de empleo. Además, persistirá la necesidad de combatir células extremistas activas, como remanentes del Estado Islámico, especialmente en áreas desérticas y de difícil acceso. Un componente esencial de este esfuerzo será la creación de unas fuerzas armadas unificadas y profesionalizadas que garanticen el control estatal y disuadan posibles intervenciones extranjeras.

Por último, el proceso político dependerá de la credibilidad de la transición democrática. La redacción de una nueva Constitución será un paso crucial, en el que se debatirá el carácter laico o religioso del Estado y se buscará garantizar derechos fundamentales para todas las comunidades. Paralelamente, el gobierno interino podría comprometerse a celebrar elecciones en un plazo de cuatro años, aunque su éxito dependerá de la transparencia y seguridad del proceso, así como de la participación de observadores internacionales que otorguen legitimidad. No obstante, algunos actores globales podrían mantener reservas sobre el gobierno de al-Golani, lo que añadiría presión a su administración.

En este contexto, el futuro de Siria bajo el liderazgo de al-Golani presenta tanto oportunidades como riesgos. Si el nuevo gobierno logra equilibrar la consolidación del poder con avances hacia la inclusión, la reconstrucción económica y la reconciliación social, podría estabilizar el país y sentar las bases para una paz duradera. Sin embargo, errores como la exclusión de minorías, el incumplimiento de promesas democráticas o una gestión autoritaria podrían perpetuar el ciclo de violencia y crisis humanitaria, dificultando la recuperación de una nación que ha sufrido profundamente durante años de conflicto.

ALGHURABA



WWW.ALGHURABA.ORG

**¿QUIERES
ANUNCIARTE EN LA
REVISTA AL-
GHURABÁ?**

¿Quieres promocionar tu próximo evento? Contacta con
alghuraba@intelciseg.com

WWW.INTELCISEG.ORG



Seguridad, terrorismo y contra-terrorismo

Curso Universitario

225 horas / 9 Créditos ECTS

890€

21 Abril 2025

a

29 Junio 2025

CURSO UNIVERSITARIO

Descuento: SOCIOS CISEG

Info: info@intelciseg.com



UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES



Diplomatura de Especialización Profesional en Crimen Organizado y Delitos Trasnacionales

Coordina Mg. en Defensa Nacional Alejandro Cassaglia

Inicio Abril 2024 Pre-inscripción:
https://bit.ly/crimen_organizado

Más info (L a V de 9 a 14hs) en:
tel: 4867 7657 | Wpp:1138614395
utn.seguridad.frba@gmail.com



DIPLOMATURA DE ESPECIALIZACIÓN PROFESIONAL en CRIMEN ORGANIZADO Y DELITOS TRASNACIONALES

Info: utn.seguridad.frba@gmail.com
LINK: https://bit.ly/crimen_organizado

DIPLOMADO INTERNACIONAL TERRORISMO DE ETIOLOGÍA YIHADISTA



INICIO: VIERNES 14 DE JUNIO DE 2024

5PM México - 6PM Ecuador - 8PM Argentina

Titulación: Centro de Estudios en Estrategia y Políticas Públicas (Argentina) / Comunidad de Inteligencia y Seguridad Global (España)
Institute for Executive Education IEXE (México)



Norberto Emmerich

Presidente del Centro de Estudios en Estrategia y Políticas Públicas – CEEYPP. Profesor de Seguridad Ciudadana y Política Criminal en la Licenciatura en Seguridad y Políticas Públicas, Universidad Autónoma de Ciudad Juárez – México. Coordinador de la Maestría en Relaciones Internacionales, Coordinador General de Investigaciones y Decano del Centro de Seguridad y Defensa del

Instituto de Altos Estudios Nacionales – IAEN, Quito, Ecuador. Asesor Editorial y miembro del Consejo Directivo del periódico Norte Digital, Ciudad Juárez, México. Investigador del Ministerio de Seguridad, Argentina.

Alejandro Gabriel Cassaglia

Licenciado en Relaciones Internacionales – IUPFA Argentina. Magister en Defensa Nacional – Facultad para la Defensa. Maestría en Inteligencia Estratégica Nacional – Universidad Nacional de La Plata. Máster Certificate of Risk Management - The University of Texas at Arlington. Fue miembro de la Policía Federal Argentina. Área de Investigaciones Criminales, Inteligencia y Antiterrorismo.

Comisario de la Policía Metropolitana, Buenos Aires. Área de Investigaciones Criminales. Fue Comisario Inspector en el área de Investigaciones, fundador y responsable del Departamento Antiterrorismo.



DIPLOMADO INTERNACIONAL TERRORISMO DE ETIOLOGÍA YIHADISTA

Info: info@intelciseg.com



Fecha: 05/02/2024 BOLETÍN N.º 01/2024 <https://aimcse.org>

PROTEGENS MUNDI



1

BOLETÍN PROTEGENS MUNDI

Info: <https://aimcse.org>

A black and white photograph of a woman in a library, reaching up to a high shelf to retrieve a book. The shelves are filled with books, and the scene is dimly lit, with a large, faint circular light source visible in the background. The woman is wearing a dark turtleneck and a plaid skirt.

Hemeroteca

Todos los números de
Al-Ghurabá a un golpe de click



AMENAZA GLOBAL

un programa de Radio 4



¡ESCÚCHANOS!



ACCEDE A TODOS LOS PODCAST



PROGRAMA 1

CRIMINOLOGÍA Y SEGURIDAD



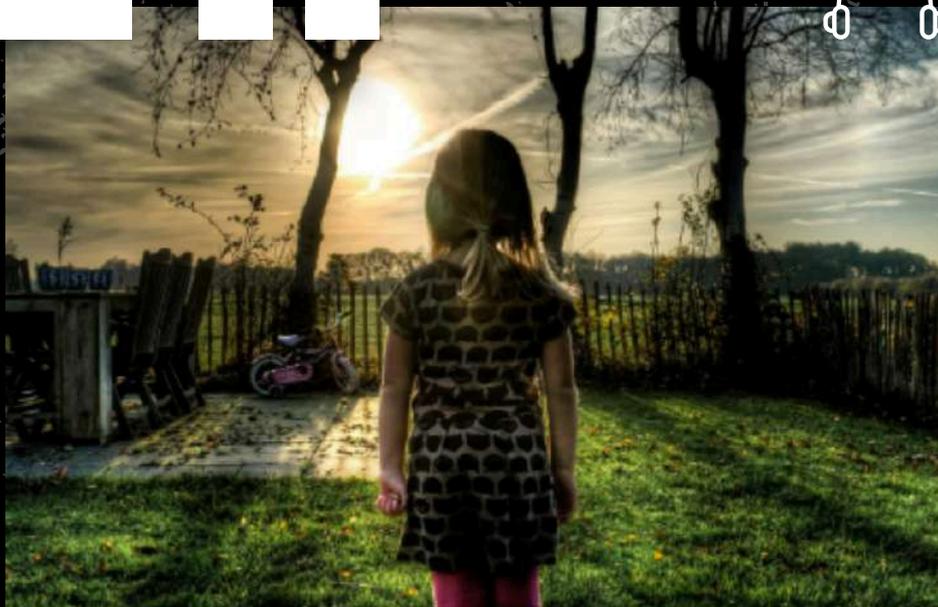
Amenaça Global - Ciberseguretat, amb Vicente Aguilera, ciber-analista

Treballem i estudiem a través del portàtil, tenim oci, serveis, relacions, però: és tan innocent i maco com sembla?

[rtve](https://www.rtve.es) RTVE.es / Feb 11, 2022

PROGRAMA 2

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Segrest de menors, amb Xavier Llaveries, criminòleg i Mosso d'Esquadra

Emisión del programa Amenaça Global titulado Segrest de menors amb Xavier Llaveries, criminòleg i Mosso. Todos los contenidos de RNE los tienes aquí, en RTVE...

[rtve](https://www.rtve.es) RTVE.es / Feb 11, 2022

PROGRAMA 3
CRIMINOLOGIA Y SEGURIDAD



Pornografia infantil

Pornografia Infantil amb Miguel Ángel Soria, doctor en Psicologia y professor de Psicologia Jurídica, Criminal y Criminología Avanzada en la Universidad de Barcelona...

rtve RTVE.es / 25 feb

PROGRAMA 4
CRIMINOLOGIA Y SEGURIDAD

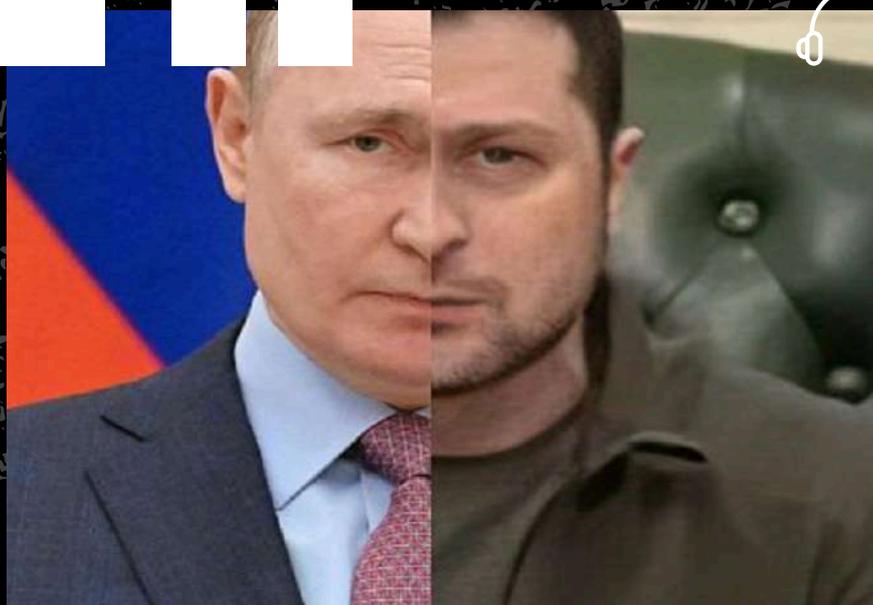


Amença Global - Síria després del DAESH

Gabriel Garroum, Graduat en Ciències Polítiques i de l'Administració i Màster en Política d'Orient Mitjà.

rtve RTVE.es / Mar 23, 2022

PROGRAMA 5
CRIMINOLOGÍA Y SEGURIDAD



Rússia i Ucraïna, un crit, dues trinxeres

Rússia i Ucraïna, un crit, dues trinxeres, amb Jesus M. Pérez, analista de seguretat i defensa. Ha escrit per vèri...

[rtve RTVE.es](https://www.rtve.es) / 5 abr

PROGRAMA 6
CRIMINOLOGÍA Y SEGURIDAD



Amença Global - Homicides: què hi ha darrera de l'homicidi?

Què sabem sobre les víctimes? Realment tenim assassins serials al nostre país o més aviat són homicidis únics?

PROGRAMA 7

CRIMINOLOGÍA Y SEGURIDAD



Amenança Global - Suplantació d'identitat digital

Hi ha alguna manera d'evitar aquesta suplantació d'identitat virtual? Què hem de fer si la patim?

[rtve RTVE.es](https://www.rtve.es) / May 2, 2022

PROGRAMA 8

CRIMINOLOGÍA Y SEGURIDAD



Amenança Global - Som una societat insegura?

Què fa que les persones ens sentim més o menys segures? Què són els esclats d'inseguretat?

[rtve RTVE.es](https://www.rtve.es) / May 15, 2022

PROGRAMA 9

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Assetjament escolar

Com podem saber que un noi/a està en un procés d'assetjament? Què podem fer?

[rtve RTVE.es](https://www.rtve.es) / Jul 11, 2022

PROGRAMA 10

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Passat, Present i Futur de l'Afganistán

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Jul 11, 2022

PROGRAMA 11

CRIMINOLOGIA Y SEGURIDAD



Amenança Global - Confiem en la policia?

Quins models policials tenen una bona rebuda social?

rtve RTVE.es / Jul 26, 2022

PROGRAMA 12

CRIMINOLOGIA Y SEGURIDAD



Amenança Global - Delictes contra el Patrimoni

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

rtve RTVE.es / Jul 26, 2022

PROGRAMA 13

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Seguretat infantil

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Sep. 20, 2022

PROGRAMA 14

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Què es la Unitat Hospitalària Psiquiàtrica Penitenciària (UHPP)?

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Oct. 28, 2022

PROGRAMA 15

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Terrorisme i mediació: recosint ferides

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Nov 5, 2022

PROGRAMA 16

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Prevenció de la radicalització violenta a través de l'esport

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Dec 27, 2022

PROGRAMA 17

CRIMINOLOGÍA Y SEGURIDAD



Amença Global - Dark Web

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es / Jan 2, 2023](https://www.rtve.es/jan_2_2023)

PROGRAMA 18

CRIMINOLOGÍA Y SEGURIDAD



Amença Global - El suïcidi: quines son les senyals d'alerta?

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es / Jan 11, 2023](https://www.rtve.es/jan_11_2023)

PROGRAMA 19

CRIMINOLOGÍA Y SEGURIDAD



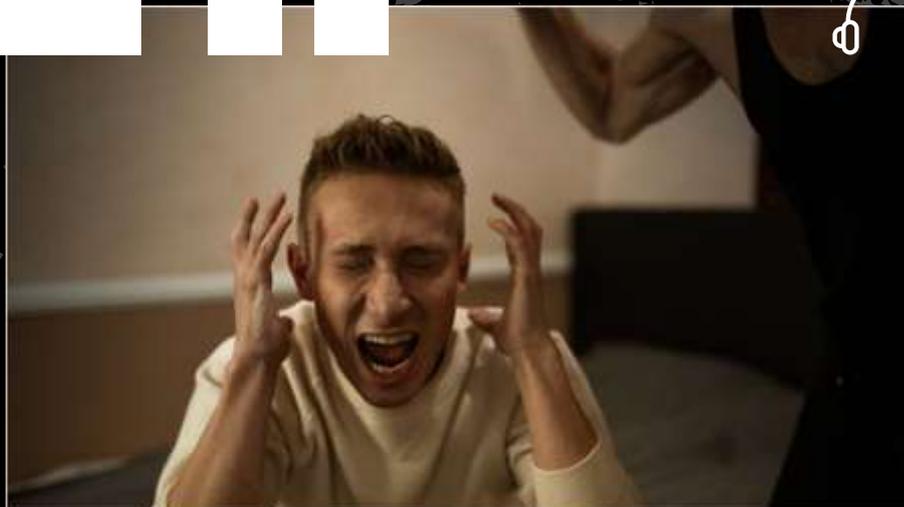
Amenança Global - Què és la psicopatia? - Primera Part

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Feb 13, 2023

PROGRAMA 20

CRIMINOLOGÍA Y SEGURIDAD



Amenança Global - El psicòpata violent (2ª Part)

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Feb 17, 2023

PROGRAMA 21

CRIMINOLOGÍA Y SEGURIDAD



Amença Global - Marc Marginedas

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve.es](https://www.rtve.es) / May 8, 2023

PROGRAMA 22

CRIMINOLOGÍA Y SEGURIDAD



Amença Global - Víctimes de la yihad negra del Daesh

Emisión del programa Amença Global titulado Víctimes de la yihad negra del Daesh. Todos los contenidos de RNE los tienes aquí en RTVE Play

PROGRAMA 23

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Delictes d'odi LGTBIQ+

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Jun 13, 2023

PROGRAMA 24

CRIMINOLOGÍA Y SEGURIDAD



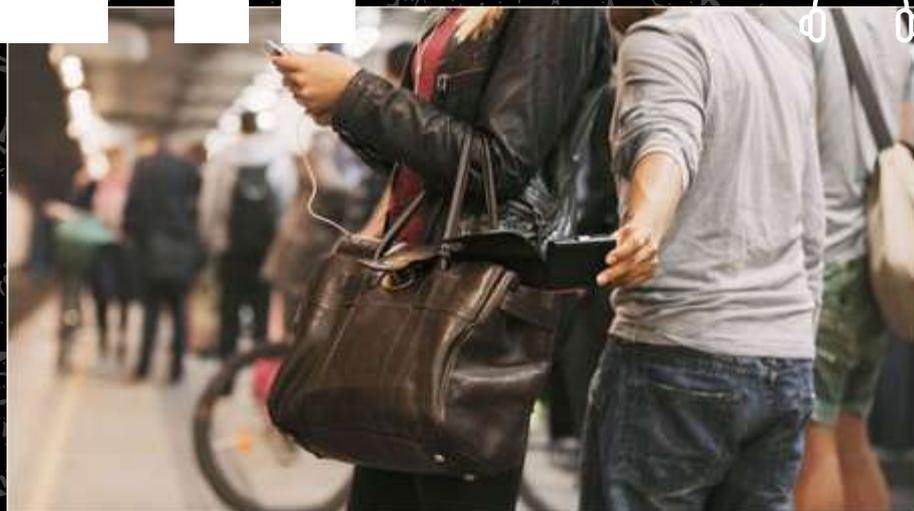
Amenaça Global - Victimes indirectes del Daesh: les mares de joves radicalitzats

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve RTVE.es](https://www.rtve.es) / Jun 19, 2023

PROGRAMA 25

CRIMINOLOGÍA Y SEGURIDAD



Amença Global - Xarxa Europea de Prevenció de la Delinqüència

Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve.es](#) / Jun. 29, 2023

PROGRAMA 26

CRIMINOLOGÍA Y SEGURIDAD



Amença Global - L'ús de la pornografia en menors

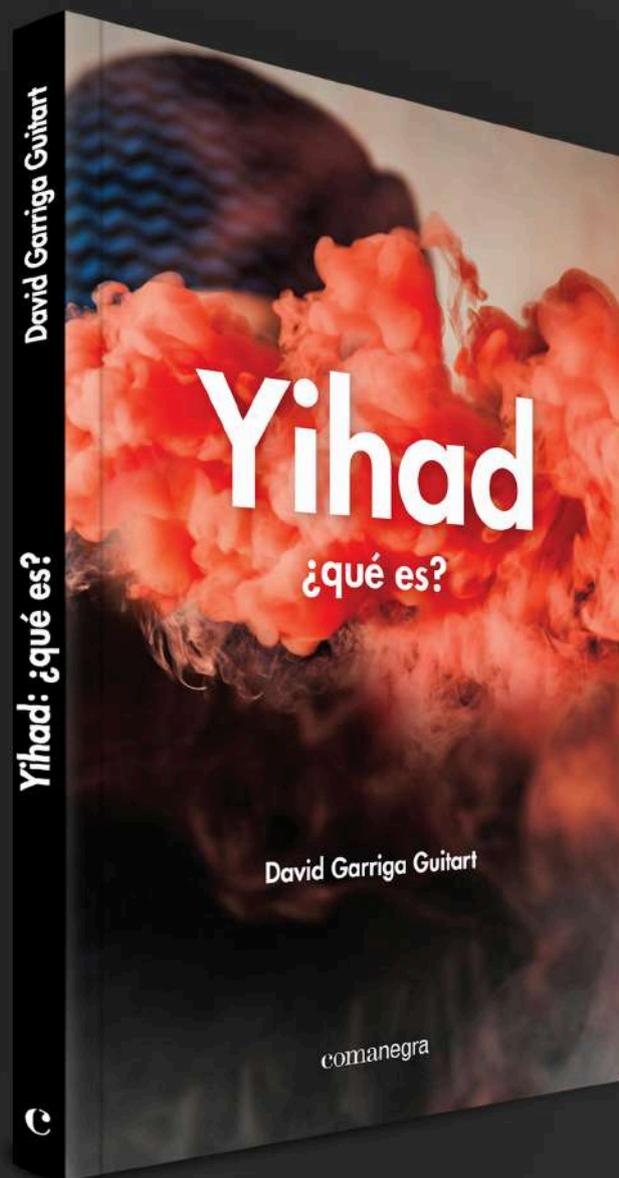
Ràdio 4 Extra a RTVE Play. Gaudeix de nous continguts i dels programes, sèries, pel·lícules, podcast i informatius gratuïts a la plataforma de RTVE

[rtve.es](#) / Dec. 4, 2023

YIHAD, ¿QUÉ ES?

David Garriga Guitart

UNA GUÍA PARA ENTENDER QUÉ ES EL YIHADISMO.



cómpralo con un 5% de descuento en:

www.comanegra.com

*Código de descuento: YHD-17

comanegra

**Revista indexada en Revistas Científicas de
América Latina, el Caribe, España y Portugal
(LATINDEX)**



www.alghuraba.org



Comunidad de Inteligencia y Seguridad Global

COLABORADORES



