Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

CARRERA DE ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

TRABAJO FINAL DE ESPECIALIZACIÓN

"La inteligencia criminal y su alcance en la sociedad:
Crimen organizado, terrorismo y nuevas tecnologías."

AUTOR: LIC EDUARDO JAVIER ARANCET

DIRECTOR DE ESPECIALIZACIÓN: DR RICARDO SPADARO

DOCENTE DEL TALLER: MAG JOSÉ LUIS PIBERNUS

MAYO DE 2024

RESUMEN

La importancia que ha adquirido en los últimos años las TIC ha llevado a los gobiernos del mundo a prestar real importancia a los delitos que pueden cometerse utilizando internet y nuevas tecnologías, siendo los delitos informáticos hechos ilícitos que van en aumento año tras año, evolucionando los métodos y profesionalizándose el criminal haciendo uso y abuso de factores que favorecen la ciberdelincuencia como la rentabilidad de ganancias, la velocidad que brinda internet en la comisión de los hechos, el anonimato y la fragilidad de las agencias estatales para abordar el tema. Los delitos cometidos mediante el uso de tecnologías desarrolladas involucran a los estados del mundo ya que una de las características principales de este tipo de delitos es la transnacionalidad. El desarrollo de este trabajo pretende realizar un breve recorrido y análisis descriptivo sobre la implementación de las TIC tanto en el ámbito delictivo como en el ámbito legal, los organismos encargados de la prevención y frustración del crimen en conjunto con la problemática económica que enfrentan los gobiernos para hacer frente a estos delitos. Las nuevas tecnologías representan un papel preponderante como herramientas auxiliares eficaces en la lucha y combate contra el crimen, aún es un medio que presenta cierto grado desconocimiento brindándole mayor facilidad a la impunidad. La implementación de estas nuevas herramientas presenta varios obstáculos que deben resolverse para garantizar al estado y a la comunidad la seguridad que se necesita. El alto costo que demanda la adquisición y desarrollo de softwares modernos en conjunto con la necesidad de incorporar personal capacitado, las filtraciones de información valiosa que ocurren en las diferentes áreas de trabajo y un débil marco legal representan la gran batalla para nuestro gobierno, lo que no significa que sea obsoleta la tarea que se lleva adelante si no que hay escollos por sortear aún. Conocer el modo, las conductas, los medios y métodos como así también las técnicas es primordial para construir un sistema eficaz.

PALABRAS CLAVES: delitos informáticos, TIC, inteligencia criminal, criminología.

ABSTRACT

The importance that ICT has acquired in recent years has led the governments of the world to pay real importance to the crimes that can be committed using the Internet and new technologies, with computer crimes being illicit acts that are increasing year after year, evolving the methods and professionalizing the criminal by making use and abuse of factors that favor cybercrime such as the profitability of profits, the speed provided by the Internet in the commission of acts, anonymity and the fragility of the fragility of state agencies to address the issue. Crimes committed through the use of developed technologies involve the states of the world since one of the main characteris TICS of this type of crime is transnationality. The development of this work aims to carry out a brief tour and descriptive analysis of the implementation of ICT both in the criminal field and in the legal field, the organizations in charge of the prevention and frustration of crime in conjunction with the economic problems faced by governments. to confront these crimes. New technologies represent a predominant role as effective auxiliary tools in the fight and combat against crime; it is still a medium that presents a certain degree of ignorance, making it easier for impunity. The implementation of these new tools presents several obstacles that must be resolved to guarantee the state and the community the security that is needed. The high cost demanded by the acquisition and development of modern software together with the need to incorporate trained personnel, the leaks of valuable information that occur in different work areas and a weak legal framework represent the great battle for our government, which It does not mean that the task being carried out is obsolete, but rather that there are still obstacles to overcome. Knowing the way, the behaviors, the means and methods as well as the techniques is essential to build an effective system.

KEYWORDS: computer crimes, ICT, criminal intelligence, criminology.

INDICE

INTRODUCCIÓN:

Las organizaciones criminales han ido evolucionando su estructura y actuar criminal en la medida que las nuevas tecnologías se lo han permitido logrando mejorar su capacidad de actuación. Las nuevas tecnologías facilitan la actividad criminal, eleva el grado de impunidad de los delincuentes y permite cometer varios ilícitos a la vez. En la mayoría de los casos quienes deben combatir la delincuencia, al tratarse de tecnologías nuevas y costosas, no cuentan con los recursos para su adquisición, desconocen su uso y aplicación, como así también las formas de proceder frente a estas novedades tecnológicas, incluso muchas veces no están receptadas en la ley tornando tedioso darle un encuadre legal.

Esta situación pone de manifiesto la necesidad que tienen las instituciones encargadas de realizar inteligencia criminal de adoptar nuevas tecnológicas que contribuyan a la labor ampliando el margen de información con la que cuentan. La información debe ser amplia, específica y detallada debiendo compartirse en las áreas competentes dedicadas a la lucha y combate del crimen organizado. Para trabajar el caudal de información de manera correcta se debe centralizar la misma bajo un mismo ente, que, con las herramientas adecuadas, pueda compartirla con los sectores y áreas especializadas que tienen la tarea de manejar esta información de datos sensibles con absoluta discreción.

Las nuevas tecnologías simplifican tareas, acortan los tiempos y proporcionan avances en la sociedad siempre que sean utilizadas correctamente a conciencia, la realidad es que estas tecnologías se encuentran al alcance de todos y cuando se realiza un mal uso o un uso indebido de las mismas comienzan a aparecer situaciones que hacen dudar de la confiabilidad de dichas tecnologías. Inicialmente muchas personas con conocimientos elevados de manejo de diferentes tecnologías vieron la posibilidad de adentrarse en el mundo de la delincuencia, primero se dio forma lenta y paulatina, realizaban sus trabajos de manera solitaria, actualmente han surgido y están en actividad bandas criminales y mafias organizadas que utilizan las nuevas tecnologías para realizar ataques a gran escala especialmente delitos involucrados con la ciberseguridad.

Se ha descubierto que estas bandas organizadas de criminales hacen captaciones de genios de la informática especialmente en foros y convenciones ofreciéndoles trabajos con remuneraciones cuantiosas que son difíciles de rechazar. La mayoría de las veces los delincuentes ofrecen trabajos bajo la fachada de empresas fantasmas que buscan crear y desarrollar nuevas tecnologías como softwares que utilizaran para la actividad criminal.

El internet es una de las TICS que en los últimos años ha revolucionado la industria criminal y ha traído consecuencias gravosas para las instituciones que se dedican a la seguridad nacional e inteligencia criminal. Bien es sabido que las operaciones de carácter económico se realizan en fracciones de segundos y pueden hacerse casi en simultáneo de una cuenta a otra, incluso viajar por el mundo a través de la red, hasta desaparecer por completo su rastro, esto es una de las características principales de lo que puede hacer el internet y contribuye al lavado de dinero ilícito sin dejar evidencias. Hoy en día una de las operaciones que lidera la punta en el ranking de delitos informáticos es la sustracción de información desde datos menores como cuentas bancarias y tarjetas de crédito hasta datos de grandes empresas que utilizan para extorsiones o simplemente vender la información al mejor postor.

Planteando así la relación estrecha entre las TICS (tecnologías de la información y las comunicaciones) y el crimen organizado.

Argentina cuenta con entes y organismos dedicados al control de los delitos cometidos por grupos criminales y terroristas: el Sistema de Inteligencia Nacional integrado por la Agencia Federal de Inteligencia, Dirección de Inteligencia Criminal, Ministerio de Seguridad Nacional, Dirección Nacional de Inteligencia Estratégica Militar. El marco normativo de la Agencia Federal de Inteligencia está conformado por la ley 25.520 y la ley 27.126 junto con decretos y resoluciones.

PLANTEAMIENTO DEL PROBLEMA:

La inteligencia nacional es un tema que presenta dificultades que aún deben resolverse. Resulta pertinente solucionar el problema de adquisición y aplicación de nuevas tecnologías, si se considera el efecto que tienen las agencias y entes estatales dedicados a la realización de inteligencia nacional y a los aportes que puede realizar en el ámbito internacional. La falta de presupuesto para la adquisición de nuevas tecnologías limita la correcta labor de las instituciones y permite que el crimen organizado siga expandiéndose haciendo un uso indebido de tecnologías de última generación. Ahora bien, ¿cómo puede mejorarse la efectividad de las instituciones encargadas de la inteligencia nacional mediante la adquisición y aplicación adecuada de nuevas tecnologías, considerando su impacto en la prevención y detección de delitos, especialmente en el contexto del crimen organizado?

Es importante que la comunidad comprenda el importante trabajo de la inteligencia criminal y lo elemental que resulta contar con los medios tecnológicos necesarios para una mejor comunicación y manejo de datos sensibles que puedan prevenir y evitar ilícitos.

Las instituciones dedicadas a la investigación de inteligencia criminal necesitan recopilar y tratar información que debe obtener de la implementación de nuevas tecnologías, convirtiéndolas en el medio idóneo para prevenir los hechos delictivos.

Investigamos sobre la organización de las instituciones y áreas especializadas en la detección y prevención del delito mediante el uso de las TICS. Es importante resaltar que las TICS ayudan e incitan al delito y también lo previenen, tanto el crimen organizado como quienes lo combaten se sirven de la tecnología para llevar adelante sus labores.

OBJETIVOS:

Objetivos generales:

Las TICS y los institutos de seguridad nacional que tienen la labor de prevenir y combatir la inseguridad y los hechos delictivos. Por ello nos planteamos el siguiente objetivo general:

Analizar el avance y desarrollo de las organizaciones criminales y terroristas como así también analizar la implementación de TICS y la íntima relación que existen entre ambas

partes con la comisión de hechos delictivos. Y para alcanzar esta meta, definimos los siguientes objetivos específicos:

Objetivos específicos:

- Identificar y analizar los grupos criminales y formas de actuar.
- Identificar los peligros del ciberespacio y las ventajas que ofrece el uso de la tecnología en la comisión de los hechos delictivos.
- Analizar la influencia de los hechos delictivos ligados a la tecnología en la sociedad actual y la pérdida de credibilidad a ciertas empresas y la falta de coordinación entre los agentes estatales para la prevención de dichos hechos junto a TICS eficaces que permitan combatir la delincuencia.

ASPECTOS METODOLÓGICOS:

Se utilizó un enfoque metodológico de investigación exploratorio-descriptivo para abordar el tema planteado. Este método permitió un análisis detallado de los institutos y ministerios responsables de detectar, prevenir y combatir el crimen organizado, especialmente en los delitos cometidos a través de las nuevas tecnologías y el internet. Se empleó un diseño de investigación exploratorio-descriptivo para comprender en profundidad la dinámica de trabajo de las instituciones mencionadas y su coordinación en la lucha contra el crimen organizado.

Se utilizaron fuentes secundarias y primarias. Las observaciones directas de las actividades realizadas por las instituciones, así como entrevistas semiestructuradas con funcionarios y expertos en tecnología y seguridad, fueron las principales fuentes. Los informes oficiales, los documentos institucionales, las investigaciones académicas y las noticias relevantes fueron fuentes secundarias. Los institutos y ministerios encargados de la seguridad y la lucha contra el crimen organizado, así como las organizaciones criminales y sus métodos delictivos, fueron la unidad de análisis principal.

Para comprender los procesos internos de las instituciones, se llevaron a cabo observaciones participativas y entrevistas semiestructuradas con funcionarios clave y expertos. Además, se realizó una revisión completa de la documentación y la literatura disponible. Se aplicó un enfoque cualitativo para analizar los datos recopilados, identificando patrones, tendencias y relaciones entre las acciones de las instituciones y la evolución del crimen organizado en el ámbito tecnológico. El análisis se llevó a cabo de

manera temática, identificando y analizando los temas clave que surgieron en las entrevistas y la revisión de la literatura.

MARCO TEÓRICO:

CAPITULO I: HISTORIA DE LA CRIMINOLOGÍA Y EL TERRORISMO.

La criminología surge a mediados del siglo XIX asociada principalmente a la antropología física, luego mudo con la intensidad por la biología, pero también estuvo comprometida por la geografía física, la psicología, la sociología, la ecología, la medicina, la ciencia política y la medicina:

No obstante, por años, esto fue percibido como un fenómeno que se encontraba vinculado a la peligrosidad (Bernal Castro: 2013).

En palabras de Miguel A. Lorite Moreno, en su trabajo Criminología: Estudio del terrorismo (2021), se define como "la ciencia empírica e interdisciplinar encargada del estudio del delito, del delincuente, de la víctima y de los medios de control social que trata de suministrar una información válida y eficaz sobre el hecho delictivo, sus formas de actuación y prevención" (p.4).

La criminología utiliza en sus estudios el método empírico, observa y analiza la realidad, elabora una hipótesis y la verifica a través de la recopilación exhaustiva de datos, se vale así mismo de otras ramas como lo son la medicina, psicología, derecho, etc. La finalidad es prevenir las conductas disvaliosas y frente a los ilícitos cometidos tratar este tipo de conductas antisociales.

Asimismo, el método empírico aporta información válida, fiable y contrastada sobre el problema criminal que se basa en el análisis y observación de la realidad (Lorite Moreno. 2021).

Los máximos y principales exponentes de la criminología fueron César Lombroso, Rafael Garófalo y Enrico Ferri.

Fue Lombroso, perteneciente a la escuela positiva, quien elaboró las primeras teorías del delincuente sustentado en su aspecto físico y biológico, estudió cráneos de delincuentes, determinando que los mismos tenían ciertos rasgos característicos como deformidades:

frente baja y salida, poca capacidad craneal, pómulos sobresalientes, orejas grandes, etc., surgiendo, así lo que definiría como “antropología criminal”. Garófalo sería otro gran positivista que adoptó las teorías de Lombroso con una visión más humanista, elaborando un esquema de penas para los delincuentes basado en una clasificación de los mismos en base a estudios antropológicos y no en el delito. Garófalo añadió a las teorías de Lombroso que los delincuentes tienen rasgos hereditarios comunes como deficiencias morales y psíquicas.

Fue Ferri quien va un paso más allá y planteó que el delincuente no sólo está determinado por características biológicas si no que está condicionado por su entorno, incorporando así elementos sociales, económicos y políticos planteando que el comportamiento disvalioso debe estudiarse en su dimensión individual y social conjuntamente (Parada Gamboa: 2009).

La criminología ha ido avanzando conforme la humanidad, en sus orígenes se centraba en el delincuente y sus rasgos físicos y psíquicos, luego comienza a ocuparse del delito en sí y posteriormente a la víctima para llegar a la actualidad estudiando los sistemas de control social (Parada Gamboa: 2009).

El terrorismo fue parte de la sociedad desde los primeros tiempos, son actos violentos e intimidatorios carentes de moral, que atentan sobre las personas y la libertad. Si bien el terrorismo se ha llevado adelante por grupos organizados como forma de conquistas o de protesta también los Estados lo han utilizado tras la cortina de defensa hacia la ciudadanía o intereses generales.

Al igual que la criminología el terrorismo ha ido avanzando conforme la sociedad y hoy en día el terrorismo utiliza un arma fundamental: la informática, buscando como objetivo desestabilizar el equilibrio del poder de nuestros sistemas (Lorite Moreno: 2021).

1.1 Criminología y terrorismo en Argentina:

En nuestro país los primeros trabajos sobre criminología fueron llevados adelante por José Ingenieros, creador del Instituto de Criminología en el año 1.907. Ingenieros (s.f) decía que la criminología es una ciencia multidisciplinaria que estudia la conducta disvaliosa en forma individual y en conjunto con otros individuos, determinando qué relación existe entre el individuo y el hecho delictivo, las causas que llevan a cometer un ilícito, las formas de prevenirlo y tratarlo.

El Estado considera que debe estar institucionalizada la lucha contra el terrorismo por lo que participa activamente en foros y congresos a nivel nacional e internacional, ratificando el compromiso asumido con todas las resoluciones y recomendaciones realizadas por la OEA y Naciones Unidas trabajando incansablemente en la capacitación y prevención del terrorismo (Organización de las Naciones Unidas ONU. S.f).

1.2 Estructuras criminales en Argentina:

Según Sampó y Quirós (2018) las estructuras criminales argentinas actualmente están conformadas en forma de clanes, en donde la violencia no es extrema como en países latinoamericanos, generalmente estos grupos suelen desarrollarse en áreas marginadas y humildes, como los son las villas miserias en nuestro país, siendo sectores sociales vulnerables en donde radica gran parte de la actividad delictiva. Normalmente estos clanes familiares inician en el mundo del narcotráfico, para terminar, cometiendo otros ilícitos que les permiten blanquear el dinero que obtienen de la venta de drogas, convirtiéndose el lavado de activos y los ciberdelitos en prácticas comunes de estas organizaciones.

Las nuevas tecnologías les han brindado la posibilidad a estas estructuras criminales de desarrollar múltiples actividades y expandirse más allá de los límites nacionales haciendo conexiones a nivel global con otras organizaciones obteniendo grandes beneficios económicos, hecho que limita a los Estados combatir y prevenir el crimen organizado, siendo el dinero uno de los factores claves, la corrupción se desarrolla a conveniencia, los delincuentes destinan grandes cantidades de dinero para evadir la intervención policial y judicial, sumado a que el desarrollo de nuevas tecnologías para la investigación y prevención de los delitos es sumamente costoso y generalmente los países no cuentan con las partidas presupuestarias necesarias (Ellis. s.f).

1.3 Iniciativas para combatir el avance de la actividad criminal y a sus organizaciones:

En nuestro país como complemento del Ministerio de Seguridad se han creado institutos tendientes a la prevención y desarticulación del crimen organizado y el terrorismo como el Observatorio de Seguridad Ciudadana, el Plan Federal de Abordaje del Crimen Organizado 2021-2023, el Centro de Estudios para la Prevención del Delito, la Dirección Nacional de Investigaciones, Secretaría de Gobierno de Modernización, Unidad Ejecutiva del Comité de Ciberseguridad, etc. (Ministerio de Seguridad de la Nación Argentina. s.f).

1.4 Marco normativo:

En su artículo primero el Código Penal Argentino (2022) establece “este código se aplicará: a) Por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción. b) Por delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo. c) Por el delito previsto en el artículo 258 bis cometido en el extranjero, por ciudadanos argentinos o personas jurídicas con domicilio en la República Argentina, ya sea aquel fijado en sus estatutos o el correspondiente a los establecimientos o sucursales que posea en el territorio argentino.

La ley de inteligencia nacional 25.520 (2001) establece las bases jurídicas, orgánicas y funcionales del Sistema de Inteligencia de la Nación, integrado por la Agencia Federal de Inteligencia, la Dirección de Inteligencia Criminal e Investigaciones del Ministerio de Seguridad, Dirección Nacional de Inteligencia Estratégica Militar. La inteligencia no se basa en “espiar” al ciudadano si no a observar y producir información relevante para la defensa y seguridad nacional (Poczynok: 2023).

La legislación referente a seguridad, crimen organizado, terrorismo, delitos informáticos, lavado de activos, narcotráfico, ventas de armas, etc., se recepta respetando la Constitución Nacional, tratados y acuerdos nacionales e internacionales a los que nuestra República a adherido (Constitución Nacional, cap. I y II. 2010).

A través de la resolución 75/2022 le asignan al Ministerio de Seguridad la facultad para llevar adelante la política criminal, elaborar planes y estrategias como así también programas destinados a prevenir el delito y garantizar la seguridad de los ciudadanos. Esta resolución surge luego de la pandemia que afecto a las sociedades a nivel mundial, este hecho generó que individuos y organizaciones criminales utilizaran cada vez más los servicios digitales creciendo exponencialmente los ciberdelitos y aumentando considerablemente los delitos transnacionales, frente a esta situación la mayoría de los estados, incluido nuestro país, quedaron desprovistos de legislación y marcos normativos acordes, personal especializado en TICS y servicios digitales modernos tendientes a la prevención de los ilícitos (Resolución 75/2022). Como respuesta a estos hechos surge el plan federal de abordaje del crimen organizado, tendiente a modernizar las políticas de seguridad, neutralizar el delito federal y el crimen organizado (Plan Federal del Abordaje del Crimen Organizado. 2021-2023).

Resolución 977/2019 Plan Federal de Detección de Delitos Tecnológicos y Ciberdelitos estableciendo bases y lineamientos sobre políticas públicas orientadas al ciberespacio y su impacto en la seguridad nacional (Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos. 2019).

Resolución 829/2019 Estrategia Nacional de Ciberseguridad tendiente a brindar un ciberespacio seguro a todos los ciudadanos, empresas, sector público y privado (Ministerio de Seguridad. 2019).

1.5 Prevención del delito:

Tal como expusimos ut-supra las resoluciones y planes mencionados tienden a prevenir el delito.

- Plan Federal del Abordaje del Crimen Organizado: hay delitos individuales que son cometidos por el crimen organizado y se interrelacionan entre sí, tales como narcotráfico, tráfico de armas, lavado de activos, trata de personas, contrabando, ciberdelitos, algunas veces con conexiones internacionales adentrándonos así en el mundo de la transnacionalidad. Estos delitos si bien en nuestro país no generan la inseguridad que impera en otros países latinoamericanos, afectan a la sociedad, sus derechos y provocan daños económicos. El programa fue diseñado para neutralizar la logística y economía de estos grupos criminales en Argentina, a través de la prevención de políticas anticipativas y herramientas para investigar, individualizar y neutralizar.
- Resolución 977/2019: este plan establece bases y prioridades de políticas públicas relacionadas con la inseguridad informática, ciberdelitos y TICS desarrollando trabajos de coordinación y cooperación entre sector público, sector privado, organizaciones gubernamentales y no gubernamentales como así también en diversas áreas académicas. El ciberespacio presenta demasiados peligros de inescrupulosos oportunistas y redes de organizaciones criminales que están al asecho de los más vulnerables: niños, adolescentes, ancianos y la población en general que no es debidamente precavida. La resolución busca prevenir y alertar sobre estos delitos a toda la comunidad reduciendo el riesgo de que se consuman. Se creó un Sistema Federal de Ciberdelitos para recabar y compartir información de delitos cometidos por medios tecnológicos. Creó áreas dentro de las fuerzas policíacas tendientes a la lucha contra estos delitos. Incorporó nuevas herramientas tecnológicas

y capacitó a personal calificado. Creó el Centro de Atención y Respuesta al Ciberdelito a través de la línea telefónica 134 que recepta denuncias y brinda información sobre este tipo de delitos.

- Resolución 829/2019 enumera principios rectores de ciberseguridad y establece objetivos de Estrategia Nacional de Ciberseguridad, dentro de la cual se desarrolla un marco normativo (Estrategia Nacional de Ciberseguridad de la República Argentina. 2019).

El reporte de ciberseguridad 2020 elaborado por el Banco Interamericano de Desarrollo (2020) y la Organización de los Estados Americanos (2020) arrojó que América Latina en general es un foco para el fraude cibernético, aumentando exponencialmente los delitos a través de internet por lo que todas las políticas públicas que se desarrollan son tendientes a difundir el desarrollo de estos nuevos delitos de la era digital.

1.6 Conductas criminales:

Los hechos delictivos en el ámbito de las TICS engloban conductas que deben ser reconocidas, los protagonistas de estos hechos son los criminales y sus víctimas, inicialmente los primeros en aparecer fueron los reconocidos *"hackers"* en su mayoría adolescentes tímidos e introvertidos con problemas sociales recluidos en el mundo de la informática para llegar a las bandas criminales que existen actualmente. Estas conductas delictivas no siempre tienen trasfondo económico, también atacan la intimidad, la libertad sexual, el honor, encontramos también los cibercrimenes políticos realizados con intención de desestabilizar al gobierno o a los estados (Blanco: s.f).

Las empresas siguen siendo las principales víctimas, el robo de datos para vender al mejor postor o extorsionar a la empresa misma son los principales problemas de estos ataques cibernéticos (Blanco: s.f).

Las conductas criminales han ido evolucionando, los primeros ataques comenzaron en las décadas de los sesenta y setenta utilizando sólo ordenadores para alterar hardware y software, luego con la aparición del internet comenzaron a utilizar la red para realizar diversos ataques y actualmente han surgido las TICS que en conjunto con el internet son los medios para la comisión de delitos (Sain en Parada y Errecaborde: 2018).

1.7 Criminología informática:

La criminología informática es el estudio de los delitos informáticos, las herramientas y los programas que se utilizan para prevenir, identificar, investigar y recabar la información necesaria para combatir estos delitos (Sain en Parada y Errecaborde: 2018).

Los delitos informáticos forman parte del Código Penal a través de la ley 26.388, cuyo objetivo es regular las nuevas tecnologías como medio para la comisión de hechos delictivos (Ley 26.388: 2008).

Los delitos que se han incorporado a nuestro código penal (2022) son: a) pornografía infantil por internet u otros medios electrónicos, b) violación, apoderamiento y desvío de la comunicación electrónica, c) intercepción o captación de comunicaciones electrónicas o telecomunicaciones, d) acceso a un sistema o dato informático, e) publicación de una comunicación electrónica, f) acceso a un banco de datos personal, g) revelación de información registrada en un banco de datos e inserción de datos falsos en un archivo informático, h) fraude informático, i) daño o sabotaje informático.

1.8 Nuevas tecnologías:

Las TICS son las tecnologías de la información y la comunicación, son el resultado de la fusión entre las tecnologías informáticas y las telecomunicaciones y las utilizamos para comunicarnos y manejar datos e información. En las décadas de los `60 `70 comienzan a aparecer los primeros ordenadores de dimensiones gigantescas, luego surgen los primeros ordenadores personales y teléfonos celulares. En los `90 la revolución llega de la mano de la invención del "internet", esto permitió una comunicación a nivel mundial y la era de los *smartphones* termina de revolucionar e irrumpir con esta evolución tecnológica al permitir manipular gran cantidad de información (Sain en Parada y Errecaborde: 2018).

1.9 Inteligencia Artificial:

La inteligencia artificial, de ahora en adelante IA, comenzó a ganar terreno, dejó de ser algo que se veía en las películas de ciencia ficción para instalarse en la sociedad causando igual o más impacto que el internet cuando apareció.

La IA surge como una combinación de algoritmos aplicados en máquinas para tomar decisiones y ejecutar situaciones como el ser humano. Hay diversidad de tipos de IA, encontramos aquellos sistemas que automatizan actividades y resuelven problemas, es decir que piensan como humanos, ejemplificamos con las redes neuronales artificiales, también

hay máquinas o computadoras que realizan diversas actividades como lo son los robots, hay sistemas expertos que piensan racionalmente y sistemas que actúan racionalmente. La IA está presente cotidianamente en la detección facial, bots, asistentes virtuales de voz y se posiciona como la tecnología esencial de los próximos años (Gobierno de España: 2023).

1.10 Contrainteligencia:

La contrainteligencia es un conjunto de actividades organizadas estratégicamente llevadas a cabo por un grupo o servicio de inteligencia a través de medidas defensivas y ofensivas para confundir y engañar a quien se considera el "enemigo". Dentro de las actividades de contrainteligencia podemos mencionar: entrevistas a testigos, interrogatorios de sospechosos, investigación de espionaje y sabotaje, preparar informes sumarios, observación, detectar y neutralizar blancos. La función principal es proteger a los estados de otros estados u organizaciones criminales.

En Latinoamérica las actividades de contrainteligencia utilizan doctrina militar norteamericana a partir de planes estratégicos se pueden prevenir, detectar y neutralizar amenazas de origen interno o externo provenientes de grupos teorista o de otros estados. La contrainteligencia protege los derechos y libertades de los ciudadanos como así también la soberanía y la integridad de un estado (Ugarte: 2019).

1.10.1 Contrainteligencia nacional:

El art. 2 inc. 2 de la ley nacional 25.520 (2001) de inteligencia nacional establece "se entenderá por contrainteligencia a la actividad propia del campo de la inteligencia que se realiza con el propósito de evitar actividades de inteligencia de actores que representan amenazas o riesgos para la seguridad del Estado Nacional".

DIAGNÓSTICO:

El servicio de inteligencia argentino enfrenta desafíos significativos que han persistido a lo largo de los años. Estos desafíos incluyen la falta de políticas sólidas a largo plazo, la escasez de personal capacitado en diversas áreas, presupuestos limitados que obstaculizan la adquisición y desarrollo de nuevas tecnologías para prevenir y combatir los delitos tecnológicos, así como la corrupción dentro del ámbito de la inteligencia.

La recolección de datos para este análisis se llevó a cabo mediante una combinación de métodos cualitativos y cuantitativos. Entre los métodos cualitativos se incluyeron entrevistas a funcionarios y expertos en el campo de la seguridad y la inteligencia, así como análisis de documentos oficiales y literatura académica relevante.

Además, se realizaron observaciones directas de las actividades llevadas a cabo por las instituciones de inteligencia. Por otro lado, se emplearon métodos cuantitativos para analizar datos estadísticos y financieros relacionados con el presupuesto y el personal asignado a las agencias de inteligencia. Estos métodos permitieron obtener una comprensión amplia y detallada de los desafíos que enfrenta el servicio de inteligencia argentino.

Asimismo, los sueldos mediocres pueden inducir a que el personal filtre información a bandas criminales, lo que eventualmente compromete la efectividad de los esfuerzos de inteligencia. Es crucial reconocer la necesidad de que todas las instituciones involucradas en el servicio de inteligencia manejen y coordinen la información de manera precisa y sin filtraciones.

Este enfoque permitirá un análisis más detallado de los problemas y desafíos identificados en el servicio de inteligencia argentino. Es esencial reconocer que la calidad de los datos recopilados influirá directamente en la comprensión de la situación y en la formulación de recomendaciones efectivas para abordar los problemas identificados.

La combinación de métodos cualitativos y cuantitativos proporcionó una visión integral de la situación, permitiendo no solo explorar las percepciones y experiencias de los actores clave, sino también obtener datos concretos sobre aspectos financieros y operativos del servicio de inteligencia. Estos datos son fundamentales para comprender los desafíos y oportunidades que enfrenta la institución y para informar el diseño de políticas y estrategias efectivas.

A continuación, desarrollaremos la inteligencia criminal en nuestro país, las organizaciones encargadas de realizar inteligencia, los aspectos normativos y como las TICS se involucran en el delito y en la prevención del mismo.

CAPITULO II: INTELIGENCIA CRIMINAL.

2.1 Evolución de la inteligencia criminal en Argentina:

La inteligencia criminal en nuestro país es una actividad organizada en ministerios llevando adelante políticas que permiten combatir el crimen y brindar seguridad a la

población. Se utilizan métodos a nivel estratégico trabajando en conjunto la seguridad pública y policial. La finalidad es disminuir al accionar delictivo de organizaciones criminales y delincuentes individuales a través de planes de manejo y control de información, accionar táctico eficiente y eficaz a través del aprovechamiento óptimo de los recursos policiales. Mención de esto hace la página web del Ministerio de Seguridad de la Nación Argentina.

2.2 Ciclo de la inteligencia criminal:

El informe elaborado por el Centro de Estudios Legales y Sociales (CELS: 2021) acerca de la inteligencia criminal en Argentina nos dice que la inteligencia criminal conforma un ciclo de información que se analiza desde los principios de utilidad, pertenencia, legalidad, necesidad y proporcionalidad. Cada ciclo tiene un proceso previo de planificación que lo motiva, garantizando tanto su control interno como externo y la discrecionalidad.

1) Obtención: primera dimensión del ciclo en donde se recolecta la información para elaborar un reporte que pasará a formar parte de la base de datos de información criminal, la obtención de dicha información se realiza a través de técnicas y fuentes diversas. Se debe organizar de donde se reunirá la información, que programas se utilizarán y quienes serán las personas que llevarán adelante dicha actividad (agentes encubiertos, tareas de observación, intervenciones a líneas telefónicas, etc.). Se utilizan medios humanos, tecnológicos, señales que recopilan información a través de sistemas de comunicación y digitales abiertas que son de acceso público. Las acciones que se lleven adelante en esta dimensión deben asegurar las garantías constitucionales y deben adecuarse a un marco normativo respetando los principios de proporcionalidad, necesidad, utilidad y legalidad.

En esta primera dimensión encontramos ciertas limitaciones, una de ellas es el costo que tiene el desarrollo de softwares y programas tendientes a la recopilación de información como así también el costo de adquisición que tienen los mismos y el vacío legal existente con relación a las nuevas tecnologías y medios digitales específicamente lo que respecta a la intimidad y privacidad de las personas, es imperante establecer las regulaciones necesarias para operar a nivel de tecnologías y automatización digital.

2) Registro: es la segunda dimensión del ciclo, aquí se clasifica y organiza la información recopilada en la primera dimensión. Se evalúa la eficacia de

los métodos utilizados en la recopilación de la información determinando que porcentaje de dicha información es relevante y cual no.

3) Sistematización: tercera dimensión del ciclo, en donde se ordena la información de tal manera que los analistas accedan a ella sencillamente. Aquí se desarrollan y construyen variables para el entrecruzamiento de datos y se seleccionan las tecnologías que se utilizarán para tal fin. En esta fase se evita repetir datos, se elimina información irrelevante e impertinente y de baja calidad.

4) Recuperación: aquí se establecen niveles de acceso a la información para el personal ya sean del organismo de origen u otras dependencias determinando quienes pueden acceder y utilizar la información como así también en qué medida.

5) Análisis: último filtro de la información, se analiza, se interpreta y se construyen hipótesis que llevarán a la toma de decisiones por parte de analistas expertos en la materia. En este punto el cuerpo de analistas debe estar conformado por sujetos de diversas disciplinas y especializaciones enfocándose en el capital humano, tecnológico y computacional. Deben ser personas idóneas que se capacitan constantemente.

6) Reporte: se confecciona un informe sobre el objeto de estudio y la persona. Estos reportes tienen diversas características: son sintéticos y concisos, resaltan la información relevante, son precisos libres de ambigüedades y contribuyen a la toma de decisiones. Se elaboran en formato papel y/o digital.

7) Difusión: última fase del ciclo. Se entrega el reporte a la persona encargada de la toma de decisiones. La ley nacional de inteligencia establece categorías para clasificar y divulgar la información: i) secreta, ii) confidencial, iii) pública de acuerdo a lo comprometido de la información y cómo puede afectar la seguridad ciudadana y el orden público. Esta clasificación sirve para un correcto control interno y externo y para brindar transparencia al estado con respecto a la información que se maneja.

Dicho informe reconoce que para desarrollar de forma eficiente y eficaz este ciclo resulta necesario que haya legislación adecuada como así también protocolos y reglamentos con la finalidad de resguardar derechos constitucionales y amplía lo establecido por nuestra carta magna al decir que más allá de las disposiciones constitucionales y la normativa internacional la legalidad de la inteligencia criminal debe estar delimitada por la organización que la lleva adelante (CELS: 2021).

2.3 Como funciona la inteligencia criminal:

Actualmente la ley de inteligencia nacional (2001) establece que la Agencia Federal de Inteligencia (AFI) requiera y solicite información a todos los organismos de la administración pública tanto nacional como provincial, estos organismos y áreas encargadas de realizar inteligencia criminal desarrollan protocolos que permiten el desarrollo de las actividades, dentro de estas actividades destacamos la observación, el seguimiento, acciones encubiertas por agentes secretos, interceptar comunicaciones, captar imágenes, realizar entrevistas, solicitar información a diversos organismos. Las acciones de inteligencia pueden afectar ciertos derechos por lo que estas acciones deben estar controladas ejemplo de ello son las numerosas denuncias realizadas por diversas organizaciones sociales y sindicales de derechos humanos en contra de la policía bonaerense que realiza seguimiento y espionaje ilegal a través de fotografías, registros audiovisuales y tareas de seguimiento vestidos de civil a personas que participan en actividades de movilización.

2.4 Inteligencia criminal en el mundo y sus modelos:

La inteligencia criminal tiene objetivos específicos, a través de ella los estados repelen amenazas y previenen delitos, por lo que con el correr de los años diseñaron y ejecutaron diversos métodos y modelos. Los institutos y áreas especializadas trabajan con niveles tácticos y estratégicos. Los diferentes modelos de inteligencia criminal están orientados a mantener el orden, actualmente hay métodos que por su efectividad son reconocidos a nivel mundial y son implementados y seguidos por las organizaciones dedicadas a realizar inteligencia.

Destacamos algunos modelos a nivel mundial desarrollados por Barcat (s/f) en su informe Inteligencia Criminal:

- Modelo Scanning Analysis Response Assessment (SARA) o Detección, Análisis, Respuesta, Evaluación (DARE): son los sistemas que se utilizan en Gran Bretaña y Estados Unidos, basado es cuatro etapas o principios:
    1. Inteligencia precisa y oportuna.
    2. Tácticas efectivas.
    3. Despliegue rápido de personas y recursos.
    4. Seguimiento insistente y valoración de la táctica.

  Con este método se busca reducir los ataques específicos en lugares y tiempos determinados.

- Modelo utilizado por el área de Alta Densidad en Tráfico de Drogas: se aplica inteligencia en base a amenazas.
- Modelo Nacional de Inteligencia del Reino Unido: utiliza programas de inteligencia estándares que comparten entre las agencias destinadas a inteligencia. Investigan y detectan amenazas, particularmente a empresas que pueden ser objetivos o víctimas del crimen virtual, redactan informes y elaboran planes de actuación y control de las amenazas.

En cuanto a la inteligencia que realizan los estados para garantizar el orden público y la seguridad ciudadana, se rigen por ciertos principios: la inteligencia que se realiza tiene una naturaleza preventiva, para poder actuar no dependen del sistema judicial, se utilizan instituciones y entidades que no pertenecen a la policía pero que la acompañan, se realiza con el apoyo de privados y la comunidad en general (Barcat: s/f).

2.5 Modelos guía y técnicas especiales de investigación:

Los principios que rigen las técnicas de investigación tienen la función de orientar estas técnicas y convertirlas en eficaces dentro de un marco normativo legal respetando la constitución y los tratados y pactos internacionales. Dichos principios son: de legalidad, de subsidiariedad, de celeridad, de excepcionalidad, de especialidad, de proporcionalidad, de pertenencia, de reserva y debido proceso, la ley de inteligencia nacional (2001) garantiza estos principios. El sitio web Seguridad en América reconoce al método científico como la base para realizar todo tipo de tareas e investigaciones, dicho método irá conjugándose con otros ya que comienza con información general hasta llegar a la información particular y de alta relevancia en el estudio que llevan adelante.

- Método científico: se emplea la observación, clasificación y descripción del problema como así también la hipótesis y la conclusión.
- Método inductivo: se parte de un razonamiento particular y se formula una hipótesis.
- Método deductivo: se parte de conocimientos generales y se aplica al caso específico.
- Técnica clínica: se vale de estudios clínicos para conocer el perfil de los delincuentes.

- Método histórico: se hace un estudio particular del delincuente, se analiza toda su vida y se determina si hubo hechos claves que lo llevaran a cometer ilícitos.
- Técnica de exploración: analizan componentes biológicos que derivan en hechos violentos y agresivos.
- Método sociológico: hay variadas teorías sociológicas que el investigador deberá implementar en el caso particular.
- Método estadístico: se elaboran estadísticas a partir de la recolección de datos sobre un determinado hecho arrojando resultados sobre un lugar, un año o la característica específica en la que está orientada la estadística.
- Cuestionarios: se utilizan para recolección de datos, pueden ser cerrados o abiertos.
- Encuestas de victimización: a través de estas encuestas se pueden conocer datos reales sobre hechos no denunciados, es decir conocemos las cifras ocultas detrás del delito.

2.6 Estructura organizacional del Sistema de Inteligencia Nacional:

El artículo 5 de la ley nacional 27.126 (2015) establece "la agencia federal de inteligencia (AFI) será el organismo superior del sistema de inteligencia nacional y dirigirá el mismo, abarcando los organismos que lo integran". Y el art. 6 establece cuáles son sus funciones, a saber, se realiza inteligencia a través de obtener, reunir y analizar la información sobre hechos riesgosos que puedan afectar la seguridad nacional y se realiza inteligencia criminal sobre delitos federales complejos como narcotráfico, ciberdelitos, terrorismo y delitos de orden público.

La AFI es la encargada de proporcionar toda la información relevante para contribuir a la toma de decisiones por parte del poder ejecutivo con respecto a seguridad nacional.

Las áreas especializadas en inteligencia criminal son la policía federal argentina, gendarmería nacional, prefectura naval, policía de seguridad aeroportuaria y de inteligencia penitenciaria del servicio penitenciario federal.

Las actividades policiales que realizan las fuerzas especializadas deben estar dentro de un marco legal establecido, la actividad de recolectar datos e información de diversas fuentes abiertas se corresponde la actividad de inteligencia criminal por lo que su regulación debe ser sobre seguridad e inteligencia, una deuda pendiente de nuestro sistema: una ley que

regule el alcance de la inteligencia criminal, cuáles son las herramientas tecnológicas y controles permitidos.

2.6.1 El acceso de la información y sus inconvenientes:

Si bien el acceso a la información es un derecho reconocido en nuestra constitución, en muchas leyes provinciales y en el decreto 1172/03 en donde se garantiza el derecho de acceso a la información pública con el objetivo de fortalecer, a través de la transparencia de datos, las relaciones entre el estado y la sociedad, aún se carece de una ley nacional que regule y establezca de manera clara el acceso a la información pública. Estudios llevados a cabo por la Asociación Civil por la Igualdad y la Justicia (ACIJ) y la Asociación por los Derechos Civiles (ADC) (2012) arrojaron irregularidades y falencias por parte del poder ejecutivos respondiendo pedidos de acceso a la información, algunos de los inconvenientes que sucedieron fueron la falta de respuestas, demoras injustificadas o respuestas incompletas por ello infiero que la respuesta a estos inconvenientes es la sanción de una ley nacional que garantice el derecho de acceso a la información pública.

CAPITULO III: NUEVAS TECNOLOGÍAS.

3. Evolución de las TICS en el mundo:

En los últimos años los gobiernos han utilizado y manipulado las TICS para llevar adelante operaciones gubernamentales, realizar inteligencia y mantener contacto con la comunidad, así es como la AFI junto con los demás organismos de la administración pública nacional y provincial desarrollan sus tareas, ejemplificamos esto con uno de los tantos programas y softwares que las TICS proporcionan y es a través del uso de plataformas predictivas del delito con las que cuenta la policía bonaerense basados en algoritmos probabilísticos avanzados que brindan una aproximación de donde y cuando ocurrirá un hecho delictivo (Ciberprisma: s.f).

3.1 Las TICS en las estructuras criminales y los aportes para la comisión de hechos delictivos:

Las nuevas tecnologías han permitido que los delincuentes encuentren una nueva forma de cometer ilícitos, se llevan a cabo delitos comunes y tradicionales ahora a través de un medio no tradicional con la ventaja de que estos hechos pueden ser cometidos desde

cualquier parte del mundo hacia cualquier otra parte, volviendo la transnacionalidad un escollo difícil de sortear para las autoridades que combaten este tipo de delitos. La falta de normativas acordes a la evolución de las TICS y de los ilícitos que puedan cometerse mediante el uso de estas tecnologías también se ha vuelto un gran inconveniente para la seguridad. El desarrollo de estas tecnologías produce un impacto económico negativo en las personas que son víctimas de estos delincuentes y a la inversa, resulta demasiado rentable para quienes desarrollan este tipo de actividades. El negocio de las TICS económicamente hablando es costoso, el desarrollo de nuevos programas y softwares cada más sofisticados tiene su costo y frente a esta realidad nuevamente los gobiernos quedan un paso detrás de las bandas y organizaciones criminales, ya que no cuentan con el presupuesto necesario para combatir estos hechos delictivos.

Estudios recientes han demostrado que la ciberdelincuencia va en aumento y ha crecido exponencialmente en los últimos años. Sus inicios se dieron con los famosos *"hackers"* y delitos comunes como estafas y robos de datos a empresas, hasta hoy en día en donde estos ciberdelitos son llevados a cabo por organizaciones criminales que operan a nivel mundial cometiendo ilícitos en masa, dentro de los cuales podemos mencionar, lavado de activos, estafas, robo de datos, pornografía infantil. Estas bandas de criminales utilizan e invierten cada vez más en recursos informáticos que les permitan seguir desarrollando sus actividades (El Fisco: s/f).

3.2 Las TICS en los organismos gubernamentales para combatir los delitos:

Las nuevas tecnologías no sólo se utilizan para cometer ilícitos, con el tiempo las han implementado las fuerzas de seguridad, brindando a los cuerpos policiales y especialistas en inteligencia criminal herramientas para prevenir y combatir el delito, se utilizan equipamientos de alta tecnología, softwares y plataformas digitales. La seguridad informática no sólo utiliza nuevas tecnologías tendientes controlar sistemas operativos, la seguridad de las aplicaciones y desarrollo de softwares, sino que también hay controles físicos como cámaras de seguridad, accesos biométricos, administrativos destinados a la política de seguridad las organizaciones y técnicos orientados a la seguridad de los softwares (Ciberprisma: 2021).

En Argentina es baja la tasa de denuncias referidas a delitos informáticos, el equipo de respuesta ante emergencias informáticas nacional (CERT.ar) de la Dirección Nacional de

Ciberseguridad realiza anualmente los registros de estadísticas y métricas, el informe del año 2.022 arrojó 335 incidentes que fueron reportados a lo largo del año, la mayoría de los ataques fueron destinados a los organismos públicos y en menor medida a entidades y usuarios privados. El 72.2% de los casos reportados fue de *phishing* a través de redes sociales y *spam* en donde se envían enlaces invitando a los usuarios a acceder al mismo, siendo el sector finanzas uno de los más comprometidos con 185 incidentes reportados, representando 55.2% de total. Los correos electrónicos son las herramientas más utilizadas para cometer estos hechos, reportando 232 denuncias, la segunda herramienta más utilizada fueron los *feed* en los cuales el CERT.ar participa y la tercera fue el formulario web, registrando 27 incidentes. Del total de los casos 323 fueron resueltos y 12 continúan en proceso de análisis. Los incidentes registrados se categorizaron en:

1. Indicio de fraude: 244.
2. Compromiso de la información: 63.
3. Contenido abusivo: 14.
4. Contenido dañino 4.
5. Intrusión no autorizada: 3.
6. Disponibilidad: 3.
7. Vulnerable: 3.
8. Otros: 1.

El indicio de fraude representa el 72.8% de los incidentes reportados, se incluyen dentro de esta categoría la suplantación de identidad, phishing y uso no autorizado de recursos. El impacto que causan estos incidentes se catalogan en cuatro niveles según la severidad: bajo, medio, alto y crítico. 305 incidentes fueron de severidad alta, 18 de severidad media, 11 de severidad crítica y 1 de severidad baja. De este informe deducimos que no se denuncia al CERT.ar la totalidad de los incidentes, 335 casos es un número ínfimo de incidentes en una era digital en donde los delitos informáticos van en alza (CERT.ar: 2022).

En nuestro país en el año 2.011 se creó Infraestructuras Críticas de Información (ICIC) que es un programa nacional dependiente de la administración pública (Disposición 1/2021: 2021) que cuenta con un certificado de Computer Emergency Response Team (CERT), que son modelos de seguridad desarrollado por los Estados Unidos. El objetivo fundamental del ICIC es la protección de activos críticos del país a través de organizaciones

públicas y privadas y organismos interjurisdiccionales. Las tareas vinculadas a ICIC son las de prevención, detección, recupero y respuestas a diversos ataques informáticos que sufren los sistemas, elabora reportes diarios sobre incidentes de seguridad en el sector público y brinda soluciones, asesoramiento técnico, alerta sobre virus y ciberataques. Frente a solicitudes de asistencia el ICIC debe poner en resguardo la información de la organización u organismo que solicita sus servicios y realizar una investigación para encontrar a los culpables. ICIC tiene estrecho contacto con el Ministerio Público Fiscal y las agencias de seguridad. En líneas generales cada país cuenta con un organismo de oficia de CERT cuyo trabajo es brindar asesoramiento a los usuarios, compartiendo recomendaciones de seguridad, informes sobre amenazas intentando concientizar a la población en general del uso responsable y seguro de la tecnología (Disposición 1/2021: 2021).

CAPITULO IV: INTELIGENCIA ARTIFICAL

4 Impacto e influencia de la IA en la sociedad:

La IA se ha instalado en la sociedad, comenzando por los teléfonos celulares con su tecnología avanzada hasta la forma de organizar las comunidades a través de la automatización de procesos y toma de decisiones. La IA ya está presente en la salud, industria automotriz, servicios al cliente y no ha sido indiferente con la seguridad y defensa en la forma de organizar y actuar de los servicios de inteligencia de nuestro país a cargo del gobierno y las fuerzas de seguridad (Gobierno de España: 2023).

4.1 Riesgos y beneficios de la IA:

Dentro de los beneficios que ofrece la IA podemos mencionar la eficiencia, aprendizaje, razonamiento, innovación, automatización, análisis de información y la experiencia personalizada que ofrece a los diferentes usuarios. En el campo de la seguridad la IA ofrece las herramientas para identificar, prevenir y actuar eficazmente contra las ciberamenazas permitiendo una menor intervención humana. La IA ha demostrado ser eficiente en la detección y neutralización de amenazas como spam, malware y phishing. La poderosa capacidad de procesar grandes flujos de datos en tiempo real, procesando información proveniente de satélites y sensores que le permiten detectar amenazas es una de las características más notable de la IA (Gobierno de España: 2023).

Dentro de los riesgos que plantea la IA encontramos los vacíos legales y los desafíos éticos que se deben resolver. La capacidad que tiene la IA de tomar decisiones que deberían realizar los humanos nos hace preguntarnos ¿quién es responsable?, la posibilidad de delegar

decisiones que se le da a un algoritmo ciertamente es un desafío ético, una máquina no posee la suficiente capacidad de discernimiento ni tiene empatía o capacidad de relacionarse como lo hacemos los humanos. En cuanto a lo legal son los gobiernos los que deben desarrollar un marco legal en relación a la IA que existe y se utiliza actualmente, disminuyendo al máximo los vacíos legales imperantes, estableciendo límites a la responsabilidad y regulando el uso y aplicación de la IA.

En nuestro país se lanzó el programa de regulación sobre el uso de la IA "Programa de Transparencia y Protección de Datos Personales en el Uso de la Inteligencia Artificial" (Resolución 161/2023: 2023) cuyo objetivo es establecer y fijar pautas como así también proporcionar información sobre el uso de la IA. La ley nacional 25.467 de Ciencia, Tecnología e Innovación del año 2001, tiene aspectos que han quedado obsoletos actualmente, considerando que la implementación de la IA de forma masiva se ha llevado a partir del año 2.015, existe un proyecto que solicita modificar tres puntos de esta ley: 1) esta tecnología de regirse por dos principios; paz y justicia y por dos valores; diversidad e inclusión. 2) se deben registrar los sistemas de IA según lo establecido por el gabinete científico y tecnológico. 3) toda persona ya sea física o jurídica debe poder radicar una denuncia si es amenazado o afectado por la IA. Dicho proyecto surgió luego de que la Argentina adoptara el Marco Ético Mundial sobre Inteligencia Artificial (2021) siguiendo las recomendaciones de la UNESCO y la ONU.

CAPITULO V: CONTRAINTELIGENCIA

La AFI es el organismo encargado de "proporcionar información para la toma de decisiones relacionadas a la seguridad de los argentinos" (AFI: s/f).

En nuestro país hay una falta de control sobre las actividades de inteligencia que realiza la policía lo que lleva prácticamente al fracaso de la contrainteligencia, poniendo en riesgo la democracia, Alberto Binder presidente del Instituto Latinoamericano de Seguridad y Democracia (ILSED) en una entrevista radial (Crisis en el aire: 2023) se expresó sobre esta problemática "la Dirección Nacional de Inteligencia Criminal no tiene control sobre la inteligencia que realiza la policía... la inteligencia llevada a cabo por estos grupos puede utilizarse a fines espurios y a la venta… las políticas de contrainteligencia tienen que evitar cualquier tipo de inteligencia ilegal".

Existe una zona gris entre las actividades de inteligencia criminal llevadas a cabo por la policía nacional, provincial y gendarmería, y las actividades de inteligencia de otros organismos. Los controles sobre los agentes informales no son efectivos, lo que permite que estos "espías" desvíen la inteligencia a fuentes externas a la AFI. Se ha ejemplificado esta problemática con las actividades de inteligencia ilegal realizadas por la policía bonaerense, dirigidas hacia miembros de organizaciones sociales, sindicales y de derechos humanos, así como a miembros de partidos opositores. Esto sugiere un manejo arbitrario de la AFI y otros entes gubernamentales para sus propios intereses.

Desde la sanción de la ley nacional 25.520 en el año 2001, se han realizado sucesivas reformas e intervenciones sin lograr cambios estructurales profundos en los procesos de inteligencia y la supervisión necesaria. La falta de una política de estado efectiva sobre el desarrollo de las actividades de contrainteligencia en Argentina es evidente. Se requiere un sistema democrático y transparente que garantice el acceso a la información pública. Las irregularidades en las prácticas de inteligencia han permitido la manipulación y comercialización de información fuera del Ministerio de Seguridad, poniendo en peligro la democracia y los derechos de los ciudadanos.

CAPITULO VI: CRIMINOLOGÍA Y SEGURIDAD.

6. Los delitos concretados con la ayuda e implementación de TICS:

Los delitos informáticos son delitos tradicionales que han mutado su forma de llevarlos a cabo con la introducción de la era informática y digital. Las TICS brindan nuevas herramientas para cometer estos delitos como virus y programas maliciosos. Este tipo de delitos va en constante aumento y expansión, las nuevas tecnologías permiten la comisión de hechos delictivos poniendo en riesgo a la sociedad, son los estados y gobiernos lo que deben brindar las herramientas necesarias para mantener y asegurar la seguridad de los ciudadanos y sus bienes, por lo que los delitos informáticos están en la agenda de los gobiernos del mundo (El fisco. s/f). En Argentina muchos de estos hechos no están contemplados en el código penal ni en ninguna normativa, lo cierto es que afectan la propiedad y los bienes jurídicos de las personas. La ley de delitos informáticos Nº 26.388 del año 2.008 ha incorporado figuras penales relacionadas con los ciberdelitos dotando de marco legal a figuras que carecían de regulación. Las TICS crecen a pasos agigantados y constantemente surgen nuevas formas o facilidades para concretar este tipo de hechos

delictivos en un entorno virtual y los marcos normativos van perdiendo efectividad ante la falta de actualizaciones.

Según CELS (2021) el gobierno debe impulsar políticas públicas enfocadas en ciberseguridad y crear leyes que regulen el funcionamiento de internet dentro del país, ya que actualmente hay muchas leyes que regulan diversas actividades, pero en sus formas tradicionales no contemplando que esas mismas actividades pueden realizarse en línea desde cualquier parte hacia cualquier parte, un ejemplo es la ley de los juegos de azar que busca regular la ludopatía en espacios físicos pero no regula los juegos en línea, el uso de internet por parte de sectores vulnerables como son los niños, niñas y adolescentes debe estar regulado y controlado por la autoridad competente, para así reducir riesgos de ser víctimas de cualquier delito informático. Es una tarea compleja que debiera estar más aceitada en los gobiernos brindando asistencia y asesoramiento constante a los organismos encargados de cibercrimen.

6.1 Delitos informáticos:

Como dice Sain y Azzolin en su obra Delitos Informáticos (2017) nos referimos a los delitos informáticos "como aquellas conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo".

Siguiendo a Sain y Azzolin (2017) este tipo de delitos los clasificamos en:

- Delitos que requieren de programas maliciosos desarrollados por "*hackers*", que dañan dispositivos electrónicos o redes con finalidad económica, para la comisión de estos ilícitos se utiliza lo que se denomina como ingeniería técnica.
- Delitos que utilizan aplicaciones sencillas para engañar, estafar, amenazar, no siempre con finalidades económicas, para la comisión de estos ilícitos se utiliza lo que se denomina como ingeniería social.
- Delitos relacionados a la violación de privacidad de los Estados o gobiernos: tienen injerencia sobre la privacidad de las personas, como los espionajes ilegales de las agencias de seguridad.
- Delitos relacionados a la violación de privacidad y datos personales de los usuarios por parte de empresas que comercializan servicios de internet: utilización de datos sin el consentimiento de los usuarios para establecer ventas de productos y servicios.

- Delitos relacionados a la violación de privacidad en el ámbito laboral: acceso ilícito por parte de las empresas a información personal de los empleados.

Las disciplinas que abordan estas temáticas son el derecho y la seguridad informática. Actualmente los gobiernos crearon áreas específicas y especializadas para combatir este tipo de delitos adaptando marcos normativos tendientes a proteger los bienes jurídicos afectados y grupos especiales que utilizan dispositivos tecnológicos y automatizados para mejorar los procedimientos administrativos, al igual que los delitos tradicionales incorporaron las TICS como medios para ser concretados, las fuerzas destinadas a la detección y prevención también debieron adoptar TICS para combatirlos (El fisco: s/f).

Este tipo de delitos presenta dificultades a la hora de prevenirlos y combatirlos: requiere de tecnología costosa que debe ir actualizándose constantemente, personal capacitado e idóneo, la información que poseen los agentes muchas veces se termina filtrando o vendiendo a beneficio de organizaciones criminales, el bajo índice o nivel de denuncias judiciales, etc.

Algunos de los motivos del bajo índice de denuncias son: lo difícil que suele ser en términos judiciales la resolución de estos ilícitos, el desconocimiento por parte de los usuarios que están siendo víctimas de un delito informático, el temor de públicos y privados de ver afectada su imagen frente al conocimiento público de haber sido víctima de estos tipos de delitos, las pruebas informáticas son endebles, fáciles de manipular, adulterar, ocultar y perderse (CERT.ar: 2022)

El artículo 128 del Código Penal (2022) sanciona los delitos informáticos contra la integridad sexual, la novedad y lo que interesa es que se incorpora la posibilidad castigar a quien utilice medios electrónicos para llevar adelante una conducta delictiva típica que anteriormente se realizaba de forma tradicional, es decir el delito es el mismo, el medio empleado es diferente y esta receptado en la norma. También se incorporó al *"grooming*[1]*"* como un delito informático en donde las víctimas son menores de edad en el artículo 131 del Código Penal (2022).

Según lo publicado por Infobae (2021) datos de la línea 137 del Ministerio de Justicia y Derechos Humanos, el total de violencias en entornos digitales aumentó, durante el 20 de marzo y el 20 de septiembre de 2020, un 195,3% respecto al mismo período de 2019. La

[1] Grooming: Este delito consiste en tomar contacto con una persona menor de edad a través de medios de comunicación electrónica (redes, mail, chat, etc.) para cometer alguno de los delitos contra su integridad sexual.

utilización de niños, niñas y adolescentes en pornografía se disparó un 522,5% y el Grooming, 124%. Estos delitos se conocen como delitos impropios ya que se utiliza el internet como medio para cometer ilícitos y se diferencia de los delitos propios en donde los ilícitos se cometen utilizando datos informáticos.

Los delitos informáticos contra la libertad son sancionados por el Código Penal (2022) cuando se cometen las siguientes conductas: apoderarse o desviar comunicaciones electrónicas que están dirigidas a otra persona, acceder de manera ilegítima a sistemas o datos informáticos de organismos públicos o privados, publicar comunicaciones electrónicas que no estén destinadas a publicidad cuando este acto causare perjuicios a terceros, revelar documentos oficiales que deben ser secretos, acceder a bases de datos personales revelando información o modificando la existente, según un informe de la Unidad Fiscal Especializada en Ciberdelincuencia en 2.019 se detectaron 229 accesos ilegítimos a sistemas públicos y privados y durante la pandemia mundial de Covid-19 estos casos aumentaron a 1.220 (UFECI: 2020).

El art. 173 inc. 15 del Código Penal (2022) incorporó a los delitos informáticos contra la propiedad, dentro de los cuales mencionamos las estafas mediante el uso de tarjetas magnéticas cuando se defraudare utilizando indebidamente los datos de tarjetas de créditos y débitos de terceras personas.

La defraudación informática es otro delito penado por ley, en este ilícito se contempla la defraudación a través de cualquier manipulación informática que altere sistemas informáticos.

Se contemplan en nuestro Código Penal (2022) los delitos informáticos contra la seguridad pública: entorpecimiento de comunicaciones electrónicas y resistencia a su restablecimiento, delitos informáticos contra la administración pública: violación de pruebas, registros y documentos electrónicos, *phishing*[2], *pharming*[3], sustitución de identidad digital con destino a cometer ilícitos o causar perjuicios, difusión no autorizada de material de audio y/o imágenes sexuales de carácter privado, hurto de datos informáticos.

Estos hechos delictivos tienen características que los diferencian de otros delitos, particularmente su investigación es más compleja, el medio virtual que utilizan abre un

[2] Phishing deriva de la expresión password harvesting fishing, significa obtener y manipular información y datos personales de la víctima a través del uso de técnicas de ingeniería social.
[3] Pharming: manipulación de sitios web para que parezcan reales.

abanico de oportunidades en cuanto a las acciones que se pueden cometer. Una de las particularidades más complejas y difíciles de resolver es la transnacionalidad que manejan estos delitos, es decir a través de la web o de la virtualidad se pueden cometer ilícitos desde cualquier parte del mundo hacia cualquier destino, dándoles una ventaja a los criminales específicamente redes de pedofilia y lavado de dinero, el anonimato es otra de las características que vuelve compleja la investigación, el uso de redes virtuales y softwares les permite a los delincuentes actuar desde el anonimato prácticamente sin dejar huellas, la *dark web* es inmensa y muy complicada, y por último mencionamos lo tedioso a nivel técnico y normativo adicionando el dinamismo con el que evoluciona la virtualidad. Estos factores dificultan enormemente la tarea del legislador y la justicia de ahí la necesidad de contar con cooperación internacional y un convenio que siente las bases para que los gobiernos puedan darle un marco legal eficiente a esta cuestión. En el año 2.001 en Budapest, se creó el primer tratado internacional orientado a la protección de la sociedad frente a delitos informáticos y delitos de internet, se elaboraron leyes, mejoraron las técnicas de investigación y se sumó la colaboración internacional de los gobiernos y empresas privadas de seguridad. Argentina ha adherido a este convenio.

En palabras del autor Fernando Tomeo (2014):

> Esta nueva modalidad 2.0 fue bien recibida por los cibercriminales, que cuentan con múltiples herramientas tecnológicas para infringir la ley; no por casualidad muchos consideran que el cibercrimen constituye una actividad más rentable que el narcotráfico. La tecnología los invita a cometer cibercrimenes donde se delinque con armas mucho más eficaces que las tradicionales, dado que a simple vista no parecen armas; son gratuitas. Además, cuentan con adicionales claves como el anonimato, la difícil persecución y en varios casos corren con la ventaja de que aún no existen leyes que tipifiquen sus conductas dolosas en la web (p.206).

6.2 Facilitación en el lavado de activos:

Las nuevas tecnologías profundizan los delitos informáticos como el lavado de activos, y son estas mismas tecnologías las que debemos utilizar para prevenir estos ilícitos.

Los crímenes financieros mutan conforme modalidades tecnológicas nuevas se suman y las mafias o bandas de crímenes organizados utilizan el lavado de activos como la forma de darle curso legal al dinero que produce la delincuencia. Las herramientas para combatir estos delitos están ligadas a las TICS: IA, machine learnig, la nube, robótica.

En nuestro país el terrorismo está íntimamente ligado a este tipo de delitos, bien es sabido que todos los actos terroristas deben ser financiados.

Ahora bien, en el año 2020 en Argentina el Comité de coordinación para la prevención y lucha contra el lavado de activos y la financiación del terrorismo y la proliferación de armas de destrucción masiva formó la Evaluación Nacional de Riesgos de Lavado de Activos (ERN-LA) para elaborar el primer diagnóstico del país, para realizar este diagnóstico se crearon mesas de trabajo con diferentes objetivos (ENR-LA-FT-PADM: 2022):

1. Amenazas: analizar el contexto criminal local e internacional identificando amenazas criminales con incidencia para el lavado de activos. Obtener y clasificar la información. Analizar volumen de fondos ilícitos provenientes del exterior cuyo objetivo es el lavado de activos en el país y viceversa. Se trabajó coordinadamente con el Ministerio de Seguridad, DaJuDECO y PROCELAC.
2. Vulnerabilidades: revisar y analizar la legislación sobre lucha y prevención de lavado de activos. Analizar si las agencias públicas y poderes del estado cumplen Hay efectivamente su finalidad. Analizar el contexto social y económico del país distinguiendo entre economía informal y economía criminal. Se trabajó coordinadamente con AFIP.
3. Sector Financiero: elaborar un mapa completo del sistema financiero nacional. Elaborar mapa financiero de las relaciones internacionales. Analizar los programas de supervisión de las autoridades competentes en relación con el sector financiero. Analizar políticas preventivas del sector financiero. Identificar los sectores vulnerables y los productos financieros. Se trabajó coordinadamente con BCRA, la SSN, la CNV y el INAES.
4. Sector No Financiero: elaborar mapa del sistema no financiero nacional identificando las actividades y sectores vulnerables. Realizar mapa de las relaciones internacionales del sistema no financiero. Analizar los programas de supervisión de las autoridades del sector no financiero. Analizar políticas preventivas del sector no financiero. Se trabajó coordinadamente con la UIF.
5. Inteligencia: revisar el ciclo de inteligencia financiera, táctica, operativa y estratégica. Revisar el ciclo de inteligencia no financiera. Se trabajó coordinadamente con la UIF, AFI, Ministerio de Seguridad y Ministerio Público Fiscal.

En nuestro país no predominan los grupos criminales de gran importancia. Los grupos criminales u organizaciones están conformados por clanes familiares dedicados a los negocios ilícitos, jerárquicamente son lideradas por uno o pocos líderes, las más grandes e importantes tienen niveles de organización compleja con diversas funciones bien establecidas y delimitadas, las zonas geográficas que abarcan son reducidas (barrios, zonas de barrios), se conectan criminalmente con países limítrofes, recurren a la coerción y corrupción, generalmente manejan un perfil bajo ante la sociedad (Sampó y Quirós; 2018).

Se ha realizado un relevamiento y arrojó un resultado de 41 organizaciones criminales dedicada al narcotráfico, trata de personas, contrabando de estupefacientes y mercadería y todas operan con lavado de activos (ERN-LA: 2022).

Entre los años 2.017 y 2.020 se iniciaron 1.386 causas de lavados de activos (ERN-LA: 2022) vinculados a delitos tributarios, narcocriminalidad, delitos contra la propiedad, delitos aduaneros, secuestros y trata de personas con finalidad de explotación sexual, delitos contra la administración pública, delitos contra el orden económico y financiero, delitos contra la fe pública.

PROPUESTA:

A lo largo del desarrollo del presente trabajo hemos establecido como las TICS han ido ganando terreno con el correr de los años, las nuevas tecnologías están a la vanguardia del delito y estas mismas tecnologías son las encargadas de llevar adelante la prevención, frustración y combate del delito. Es una realidad que no se puede ignorar, nuestro país debe ser capaz de desarrollar políticas eficaces, confiables y seguras, el internet se ha convertido en un área bajo responsabilidad del Estado. Actualmente se debe brindar ciberseguridad a los individuos, a las organizaciones y a todas las operaciones de Estado.

El gran meollo de la cuestión es la limitación económica que presenta el gobierno nacional para llevar adelante los organismos encargados de la seguridad estatal y de la sociedad en general. Hemos detectado que no es el único problema que se presenta hay además falta de personal idóneo y capacitado, no existe una correcta coordinación entre AFI que es el organismo encargado de producir inteligencia criminal y nacional y los demás organismos de la administración pública ya sea nacional o provincial, la filtración de información valiosa que cae en poder de bandas criminales, carencia de políticas

competentes, espionaje ilegal, junto con la falta de credibilidad y fraude hacen que el servicio de inteligencia federal no sea bien aceptado por la comunidad.

Frente al mayor inconveniente que surge de un presupuesto acotado se debe organizar a todas las instituciones de manera tal que funcionen como un gran engranaje, debiendo llevar adelante tareas específicas eliminando áreas inoperantes, contratando personal idóneo y capacitado, eliminando a aquellas personas que no tienen un papel relevante, con respecto a la información recabada debiera ser centralizada es decir que el organismo encargado de coordinar la tarea de inteligencia que es la AFI pueda acceder a ella de manera precisa e instantánea, es decir toda la información que se considere crítica más allá de que sea un interés provincial debe compartirse con la AFI para que esta pueda contribuir en la toma de decisiones, realizando de esta forma un trabajo en conjunto. La finalidad de contar con un número de personal adecuado, eliminado los extras, resulta relevante fundamentalmente en el manejo de la información tornando más complicado que se realicen filtraciones y más fácil determinar quién pudo haber filtrado o vendido dicha información, con un número más reducido de personal que sea idóneo, capacitado, competente, eficiente y eficaz los salarios pueden ser mejores.

Si bien el acceso a softwares modernos requiere de grandes inversiones, existen programas y plataformas más económicos e igualmente eficaces. Debería existir un conjunto de programas base que el personal utilice para planificar a futuro, determinar variables, posibles escenarios, factores y diagramar los planes de acción, para que esta propuesta sea factible se debe ser más estrictos y rigurosos al momento de seleccionar el personal y cubrir vacantes.

No debemos dejar de lado la ley, el gobierno debe constantemente realizar un equilibrio de prioridades se deben llevar adelante políticas de combate al cibercrimen en conjunto con la protección de los derechos fundamentales, nuestro país cuenta con una política de ciberseguridad definida que debe ir evolucionando conforme a la tecnología, existen leyes y organismos encargados de brindar protección. En base a esta política, sustento mi propuesta de adecuarnos al presupuesto existente:

1) Definiendo una estrategia de ciberseguridad en donde se contemplen principios y prioridades una estrategia adecuada nos permitirá gestionar mejor los recursos.

2) Estableciendo y reestructurando a la AFI como un único organismo transparente y efectivo, que sea la única autoridad y maneje toda la información relevante generando un trabajo conjunto con las demás administraciones que realizan tareas de inteligencia. Eliminando áreas innecesarias tendientes a la filtración de información. Y poniendo al frente de dicho órgano una persona competente e idónea, con una trayectoria que avale su designación.

3) Actualización constante de leyes, los marcos legales deben ampliarse y llevar una concordancia con la actualidad.

4) Llevar adelante políticas y estrategias de ciberseguridad a nivel internacional, hemos visto que una de las características de los delitos informáticos en la transnacionalidad, por lo que el Estado debe trabajar en conjunto con otros países.

CONCLUSIONES

A lo largo del trabajo desarrollado hemos podido apreciar como las TICS han revolucionado el mundo brindando soluciones, facilidades, rapidez a los quehaceres cotidianos de las personas y a la vez han abierto infinitas puertas para la delincuencia, comenzando con pocos y pequeños *"hackers"* hasta conformarse bandas y organizaciones criminales que operan a nivel mundial convirtiendo esta situación en temas generales en los gobiernos de todo el mundo, es así como comienzan a surgir las primeras organizaciones y áreas dependientes de los gobiernos destinadas a la prevención y frustración de los delitos informáticos.

La AFI en nuestro país es el órgano encargado de producir inteligencia y manejar la información crítica y relevante, como así también de establecer las políticas con las que trabajará en conjunto con otros órganos nacionales y provinciales. La realidad es que en Argentina la contrainteligencia, una de las funciones exclusivas de la AFI, no está vista con buenos ojos, denuncias de espionaje y corrupción son motivos para la desaprobación social en general.

Al concluir esta investigación, es esencial evaluar si hemos abordado de manera efectiva la pregunta problema que planteamos inicialmente. Nuestro análisis ha revelado que si bien la falta de presupuesto y los altos costos asociados con las nuevas tecnologías son

desafíos significativos en el ámbito de la inteligencia nacional, no son los únicos obstáculos que enfrentamos.

Las TICs presentan una amplia gama de problemas adicionales que requieren una atención cuidadosa y políticas bien desarrolladas. Desde la protección de la infraestructura crítica hasta la lucha contra el cibercrimen, es evidente que la seguridad del Estado y sus ciudadanos depende en gran medida de una estrategia integral que aborde estos desafíos de manera efectiva.

Por lo tanto, al reflexionar sobre nuestra investigación, podemos concluir que hemos identificado y analizado adecuadamente los problemas relacionados con la falta de presupuesto y los desafíos asociados con las nuevas tecnologías en el ámbito de la inteligencia nacional. Sin embargo, también reconocemos que hay una serie de problemas adicionales que merecen atención y acción por parte de los responsables de la formulación de políticas y los líderes de seguridad.

En consecuencia, nuestra conclusión responde afirmativamente a la pregunta problema planteada, al tiempo que destaca la complejidad del panorama y la necesidad de seguir abordando estos problemas de manera proactiva y estratégica en el futuro.

BIBLIOGRAFÍA:

Barcat, E. (s.f.). *Reconciliando mundos.* Obtenido de Inteligencia criminal: https://reconciliandomundos.com.ar/inteligencia-criminal/

Bernal Castro, C. (2013). *Bienes jurídicos o protección de la vigencia de las normas. Una lectura desde la historia social del derecho penal.* Bogotá: Universidad Católica de Colombia.

Blanco, B. (s.f.). *El crimen organizado y las nuevas tecnologías.* Obtenido de Revista Digital El Fisco Nº 151: http://el fisco.com/articulos/revista-no-151-el-crimen-organizado-y-las-nuevas-tecnologias

CELS, C. d. (2021). *Iniciativa Ciudadana para el Control del Sistema de Inteligencia ICCSI.* Obtenido de Acerca de la inteligencia criminal en Argentina - Apuntes para su discusión: https://www.cels.org.ar/web/wp-content/uploads/2021/11/Inteligencia-criminal-Arg-FINAL-3.pdf.

Ciberprisma. (17 de Septiembre de 2021). *Ciberprisma - Alianza por la ciberseguridad*. Obtenido de Delitos en Tiempo Real: Las Tecnologías y la Prevención del Delito: https://ciberprisma.org/2021/09/17/delito-en-tiem-po-real-las-tecnologias-y-la-prevencion-del-delito/

Código Penal de la Nación Argentina. (2.022). Buenos Aires: Erreius.

Comite de coordinación para la prevención y lucha contra el lavado de activos y financiación del terrorismo y la proliferación de armas de destrucción masiva. (2.022). *Evaluaciones Nacionales de Riesgos de Lavado de Activos y de Financiación del Terrorismo y de la proliferación de Armas de Destrucción Masiva.* Obtenido de https://www.argentina.gob.ar/sites/default/files/2022/11/evaluaciones_nacionales_de_riesgos_de_lavado_de_activos_y_de_financiacion_del_terrorismo_y_de_la_proliferacion_de_armas_de_destruccion_masiva_1.pdf

Constitución de la Nación Argentina. (2010). Buenos Aires: Eudeba.

Convenio sobre la Ciberdelincuencia - Budapest. (23 de Noviembre de 2.001). Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Dirección Nacional de Ciberseguridad. (2.023). *Incidentes informáticos.* Obtenido de https://www.argentina.gob.ar/sites/default/files/2023/02/informe_cert_2022.docx.pdf

Ellis, E. (s.f.). *Las drogas, las pandillas, el crimen organizado transnacional y los "Espacios mal gobernados" en las Américas.* Obtenido de https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-27_Issue-3/2015_3_04_ellis_s.pdf

Fernández Camacho, M. (4 de Septiembre de 2.021). *Infobae.* Obtenido de Durante la pandemia, la utilización de menores en pornografía creció más del 500% en Argentina: https://www.infobae.com/sociedad/2021/09/04/durante-la-pandemia-la-utilizacion-de-menores-en-pornografia-crecio-mas-del-500-en-argentina/

Gobierno de España. (19 de Abril de 2023). *Qué es la inteligencia artificial*. Obtenido de Plan de recuperación, transformación y resiliencia.: https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr#:~:text=La%20inteligencia%20artificial%20(IA)%20es,el%20razonamiento%20y%20la%20percepci%C3%B3n.

Instituto Superior de Seguridad Pública. (2020). *Geopolítica de seguridad y crimen organizado.* Buenos Aires: s/e.

Ley Nacional Nº 25.467. (2.001). Ciencia, tecnología e innovación. Buenos Aires: Boletín Oficial de la Nación Argentina.

Ley Nacional Nº 25.520. (2001). Inteligencia Nacional. Buenos Aires: Boletín Oficial de la Nación Argentina.

Ley Nacional Nº 26.388. (2008). Delitos Informáticos. Buenos Aires: Boletín Ofical de la Nación Argentina.

Ley Nacional Nº 27.126. (3 de Marzo de 2015). CREACION - MODIFICACION LEY N° 25.520. Buenos Aires: Boletín Oficial de la Nación Argentina.

Ley Nacional Nº 27.126. (25 de Febrero 2.015). *Agencia Federal de Inteligencia.* Bs. As: Boletín Oficial de la Nación Argentina.

Lorite Moreno, M. A. (2021). *Criminología: Estudio del terrorismo.* Obtenido de https://escuelapolicia.com/wp-content/uploads/2021/12/CRIMINOLOGIA-ESTUDIO-DEL-TERRORISMO.pdf

Ministerio de Seguridad. (2023). Obtenido de Plan Federal de Abordaje del Crimen Organizado 2021 - 2023: https://www.argentina.gob.ar/seguridad/abordaje-crimen-organizado

Noetinger & Armando. (30 de Agosto de 2023). Obtenido de Programa de transparencia y proteccion de datos personales en el uso de la IA - Resolución 161/2023: https://noetingeryarmando.com/la-argentina-lanza-el-programa-de-transparencia-y-proteccion-de-datos-personales-en-el-uso-de-la-inteligencia-artificial/

Parada Gamboa, M. (28 de Noviembre de 2009). *La criminología italiana durante el siglo XIX: su consolidación y sus autores.* Obtenido de https://derechopenalonline.com/la-criminologia-italiana-durante-el-siglo-xix-su-consolidacion-y-sus-autores/

Parada Ricardo Antonio, Errecaborde José Daniel . (2018). *Compilado - Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet.* Buenos Aires: Erreius.

Parada Ricardo Antonio, Errecaborde Jose Daniel. (2018). *Cibercrimen y delitos informáticos.* Obtenido de Los nuevos tipos penales en la era de internet: https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Poczynok, I. (2023). *Política y servicios de inteligencia - Hoja de ruta para un sistema legítimo y efectivo*. Obtenido de https://fund.ar/wp-content/uploads/2023/07/Fundar_Politica_y_servicios_de_inteligencia-1.pdf: FUNDAR.

Poder Ejecutivo de la Nación (PEN). (6 de Diciembre de 2021). Decreto 832/2021. *AGENCIA FEDERAL DE INTELIGENCIA.* Buenos Aires: Boletín Oficial de la Nación Argentina.

Poder Ejecutivo Nacional (P.E.N). (2019). *Resolución 977/2019*. Obtenido de PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS: https://www.argentina.gob.ar/seguridad/abordaje-crimen-organizado

PODER EJECUTIVO NACIONAL (P.E.N.) . (4 de Marzo de 2020). Decreto DNU 214 / 2020 . *LEY DE INTELIGENCIA NACIONAL LEY N° 25.520 - MODIFICACION*. Buenos Aires: Boletín Oficial de la Nación Argentina.

PODER EJECUTIVO NACIONAL (P.E.N.). (06 de Julio 2.015). *Decreto 1311/2015 - AGENCIA FEDERAL DE INTELIGENCIA - NUEVA DOCTRINA DE INTELIGENCIA NACIONAL - APROBACION.* Buenos Aires: Boletín Oficial de la Nación.

PODER EJECUTIVO NACIONAL (P.E.N.). (18 de Octubre de 2015.). Decreto 2415 / 2015. *AGENCIA FEDERAL DE INTELIGENCIA - DECRETO N° 1311/15 - MODIFICACION.* Buenos Aires: Boletín Oficial de la Nación Argentina.

Resolución 75/2022. (10 de Febrero de 2022). *Boletín oficial de la República Argentina*. Obtenido de Ministerio de Seguridad - Congreso de la Nación: https://www.boletinoficial.gob.ar/detalleAviso/primera/257535/20220215?busqueda=1

Resolución 829/2019 "Estrategia Nacional de Ciberseguridad". (24 de Mayo de 2019). *Secretaría de Gobierno de Modernización*. Obtenido de https://www.marval.com/publicacion/estrategia-nacional-de-ciberseguridad-de-la-republica-argentina-13372#:~:text=El%2024%20de%20mayo%20de,Ejecutiva%20del%20Comit%C3%A9%20de%20Ciberseguridad.

Sain Gustavo, Azzolin Horacio. (2017). *Delitos Informáticos: investigación criminal, marco legal y peritaje.* Montevideo-Buenos Aires: BdeF.

Sampo Carolina, Quiros Ludmila. (Noviembre 2.018). Las estructuras criminales en Argentina y las iniciativas de cooperación estatal para combatir su avance. Revista S.A.A.P. ISSN: 1666-7883.

Seguridad en América. (29 de Agosto de 2020). Obtenido de Métodos de investigación criminal: https://www.seguridadenamerica.com.mx/noticias/articulos/25302/mEtodos-de-investigaciOn-criminal

Sistema Nacional de Información Criminal (SNIC) - Ministerio de Seguridad, Presidencia de la Nación - UNODC - Información estadística del Gobierno. (2017). *Plan de mejoras Agosto 2019- Agosto 2022* . Obtenido de IF-2019-79722408-APN-SSEC-MSG

Tomeo, F. (2.014). *Redes sociales y tecnología 2.0.* Bs. As.: Astrea.

Ugarte, J. M. (2.019). *Desarrollo, situación y probable evolución de la inteligencia criminal en Latinoamérica.* Obtenido de https://alacip.org/cong19/285-ugarte-19.pdf

Unidad Fiscal Especializada en Ciberdelincuencia - UFECI. (2.021). *Informe de gestión 2.020.* Obtenido de https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf

ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

EVALUACION TRABAJO FINAL INTEGRADOR

DOCENTE EVALUADOR: Mg MARCELO LUIS MARTINENGO – PROFESOR DE CRIMEN ORGANIZADO Y TERRORISMO – CONTRAINTELIGENCIA.

TEMA: LA INTELIGENCIA CRIMINAL Y SU ALCANCE EN LA SOCIEDAD: CRIMEN ORGANIZADO, TERRORISMO Y NUEVAS TECNOLOGIAS. -

ALUMNO: EDUARDO JAVIER ARANCET. -

CRITERIOS DESARROLLADOS:

1. Conocimiento del tema
   El trabajo desarrolla aspectos específicos de la innovación que caracterizó al Crimen Organizado y al Terrorismo el uso de las Nuevas Tecnologías (TICs), enmarcando así a la Ciberdelincuencia o Cibercriminalidad, que demanda una especial atención por parte de las autoridades estatales para neutralizar esa gran amenaza criminal a la sociedad en su conjunto. -

2. Actualización del Diagnóstico
   El autor del TFI realiza una descripción acertada y actualizada sobre las actividades que se desarrollan para combatir el avance las organizaciones criminales a través de las Nuevas Tecnologías, como ha evolucionado la Inteligencia Criminal en la República Argentina para conjurar los delitos informáticos, en particular las técnicas que facilitan el lavado de activos. -

3. Pertinencia y coherencia de la propuesta de intervención
   El TFI es pertinente y coherente con los aspectos centrales de la Especialización, ya que trata un tema importante de la Inteligencia Criminal y el Crimen Organizado que es uno de los objetivos centrales para la actividad de un Especialista en Inteligencia Estratégica. -
   Es un trabajo que se encuentra organizado de manera objetiva y clara. Tiene una correcta redacción, ortografía y prolijidad en la presentación. Presenta un análisis reflexivo. -

4. Breve juicio del TFI.
   Además de realizar un excelente diagnóstico de la Ciberdelincuencia y los avances de la Inteligencias Criminal, efectúa una propuesta adecuada para la reformulación de la Contrainteligencia como una actividad esencial de la Agencia Federal de Inteligencia, para normalizar rápidamente esa actividad en pos de proteger la infraestructura critica de Internet que posee la República Argentina. -

5. Propuesta de calificación numérica: OCHO (8). -

INTERVENCIÓN DEL PROFESOR DE TALLER DE TRABAJO FINAL INTEGRADOR, Mg JOSE LUIS PIBERNUS.

- El TFI evaluado, reúne los procedimientos de metodología de investigación exigidos para el nivel académico de la carrera.
- Cumple con la Guía de la FCE establecida para TFE y con el Reglamento de Posgrado de la UBA.
- El trabajo presentado, ha logrado integrar adecuadamente distintas áreas estudiadas como partes de la especialización.
- TFI: APROBADO.
- Calificación propuesta: OCHO (8) MUY BUENO.

INFORME FINAL DE EVALUACIÓN DEL DIRECTOR DE LA ESPECIALIZACIÓN EN INTELIGENCIA ESTRATEGICA Y CRIMEN ORGANIZADO:

Juicio sintético: Coincido con las evaluaciones de los docentes intervinientes. Se trata de una vista concisa de algunos de los avances en tecnología aplicada a la Inteligencia Criminal, que representa un esquema útil para el desarrollo de trabajos ulteriores de investigación y de mayor profundidad, respecto de los desafíos que representan esos avances y en especial la IA, que se menciona tangencialmente, aunque ciertamente representa el mayor desafío estará en su empleo prudente y sin riesgos en el futuro incierto que la misma anticipa. El trabajo de integración indica un esfuerzo de coordinación temática importante, que merece la aprobación y reconocimiento.

Calificación: OCHO . (8). – ***MUY BUENO.***

Prof Dr José Ricardo Spadaro
Dir Esp en Icia Est y Crim Org
(097) – ENAP-FCE-UBA