



UNIVERSIDAD DE LA DEFENSA NACIONAL

INSTITUTO DE INTELIGENCIA DE LAS FUERZAS ARMADAS

**POSGRADO “ESPECIALIZACIÓN EN GESTIÓN DE INFORMACIÓN
MILITAR AEROESPACIAL”**

TRABAJO FINAL INTEGRADOR

TEMA: Criptografía

TITULO: “Desarrollo de criptografía nacional en el ámbito militar,
para evitar la existencia de vulnerabilidades implantadas”

AUTOR: Primer Teniente MÓNACO, Gastón Nicolás

DIRECTOR: Ingeniero BORCHERT, Hugo Alejandro

AÑO: 2025

“Las ideas expuestas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia, la opinión del Instituto de Inteligencia de las Fuerzas Armadas y de la Universidad de la Defensa Nacional”.

RESUMEN

Este trabajo se enfoca en la importancia de la criptografía de desarrollo nacional para la protección de la información y los secretos en el ámbito militar, evitando así la posible existencia de vulnerabilidades implantadas, conocidas en el ámbito como “puertas traseras” (mecanismos para evadir la protección), en desarrollos adquiridos pertenecientes a terceros.

La metodología del mismo se basa en la investigación bibliográfica y el análisis de un caso de estudio, esto desarrollado en los párrafos subsiguientes.

Se analiza el contexto histórico y las posibles consecuencias para la Seguridad Nacional en cuanto a la afectación de la información sensible de sus Fuerzas Armadas. A su vez se busca definir conceptos básicos de criptografía, sus ventajas, desafíos, ejemplos en la actualidad y cómo esta puede ser aplicada para preservar cierta soberanía tecnológica en materia de seguridad de la información.

Además, se examina un caso puntual y sus respuestas, conocido como el escándalo protagonizado por la empresa suiza “Crypto AG”, la cual era controlada por agencias de inteligencia de Estados Unidos y Alemania permitiendo que estas espieran a todos sus clientes, mediante puertas traseras colocadas en los equipos de cifrado que la misma comercializaba.

Asimismo, propone recomendaciones para implementar una estrategia de desarrollo criptográfico nacional, a fin de evaluar una solución a esta problemática.

INTRODUCCIÓN

Fundamentos del Trabajo

Es de público conocimiento como a lo largo de la historia, sobre todo en la actualidad, la información es uno de los bienes más preciados que todo tipo de organización quiere proteger y a su vez obtener, tanto de su rival o enemigo como de sus aliados. De allí que se puede encontrar evidencia en uno de los libros de estrategia más antiguos del mundo, en donde el filósofo chino Sun Tzu (2020) argumentó “Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro”.

Esta afirmación permite corroborar la existencia de gran cantidad de ejemplos en el pasar de los años, evidenciando cómo grandes líderes se las han arreglado para proteger esta información, principalmente en lo que a mensajes y comunicaciones refiere. Un ejemplo puntual de la antigüedad es aquel que utilizaban los romanos, denominado en algunos libros como “El cifrado del Cesar”, el cual podemos encontrar mencionado en el libro “Historia de la Criptografía” en el siguiente fragmento, "Este método del que se atribuye su uso al emperador romano Julio César en el año 300 a. C., fue usado para enviar mensajes de carácter militar a los generales del ejército romano" (Urrea, 2020).

Durante el siglo XX, otro ejemplo de gran relevancia fue el que utilizaron las fuerzas del eje en la segunda guerra mundial, principalmente los alemanes, conocido como la maquina “Enigma”. Fue desarrollada en los años 20 por el ingeniero e inventor Arthur Scherbius y mejorada a posteriori. Durante los años 30, luego de ser mejorada y modificada, se convirtió en el dispositivo estándar que brindaba seguridad a las comunicaciones, siendo la más avanzada para la época y un gran problema para las fuerzas aliadas, ya que durante cierto periodo les otorgo una ventaja significativa (Anónimo, 2023).

Más cercano en el tiempo, es de gran relevancia para el desarrollo de este trabajo no pasar por alto un ejemplo, el cual es el puntapié inicial o disparador, aquel por cuyas consecuencias la República Argentina ha sido afectada y del cual se debería aprender, ya que como nos advierte Santayana, "Aquellos pueblos que olvidan su pasado están condenados a repetirlo" (Santayana,

1905, p. 284). El mismo se dio durante el Conflicto del Atlántico Sur en el año 1982, dándose por hecho, que el Reino Unido de Gran Bretaña, que ocupa las Islas Malvinas de manera ilegal desde el año 1833, recibió información valiosa suministrada por los Estados Unidos, su principal aliado. Esta era obtenida a través de la vulneración del secreto de las comunicaciones, a las cuales tenían acceso mediante la empresa a la que la República Argentina le había comprado dispositivos que en teoría debían protegerlas, lo que ha sido reflejado en artículos publicados, “Cómo la CIA espió a la Argentina durante la guerra de Malvinas y le pasó información a Gran Bretaña” (Infobae, 2020) o “¿Cuál fue la trampa que usó la CIA para espiar a Argentina durante el Plan Cóndor y la guerra de Malvinas?” (La Voz del Interior, 2023) por citar algunos ejemplos.

La soberanía tecnológica, precisamente en el ámbito de la criptografía, y la protección de la información crítica nacional no pueden depender de elementos desarrollados en su totalidad por entidades del extranjero. Partiendo de una perspectiva estatal actual, principalmente en lo que refiere a los conflictos entre estos y en los cuales se utilizan sus instrumentos militares, la protección de la información de carácter secreta se vuelve primordial, ya que, ante un potencial enfrentamiento armado, aquel que pueda hacerse de los secretos del enemigo tendrá una ventaja significativa.

La posibilidad de que existan puertas traseras implantadas en algoritmos o dispositivos criptográficos foráneos constituye una amenaza real, tal como demuestran numerosos antecedentes históricos. En este contexto, el desarrollo de criptografía nacional se vuelve imprescindible para garantizar la confidencialidad e integridad de las comunicaciones estratégicas, particularmente aquellas del instrumento militar.

Actores como Estados Unidos, China y Francia han adoptado políticas de control soberano sobre la criptografía. Existen legislaciones que regulan su uso, exportación e importación. También existen ejemplos de desarrollo nacional exitoso en Argentina, como el sistema Cryptocomm de ARSAT e INVAP, o algoritmos presentados al NIST. Sin embargo, estos esfuerzos son dispersos y carecen de una estrategia real unificada, tal como lo afirma el Ingeniero Daniel Edgardo Cortes, “En nuestras Universidades tenemos material humano suficiente para desarrollar con criterios particulares, nuestro propio esquema que nos identifique y que a su vez sea compatible con los

estándares internacionales. Para ello es necesario dar señales precisas que permitan encolumnar a la sociedad a tomar este desafío como lo han hecho en otros países” (Cortés, s. f., Opinión).

En lo que respecta a nivel regional, la Junta Interamericana de Defensa (2022) establece en una de sus guías que “Es necesario que las naciones desarrollen sus propias capacidades de ciberdefensa para evitar la dependencia de otros países.” entendiendo que la criptografía se encuentra mayormente ligada al ciberespacio en la actualidad y que por consecuencia “El establecimiento de una industria nacional de ciberdefensa es esencial para evitar la dependencia de otros países.”

Especialistas en el ámbito de la criptografía como Hugo D. Scolnik, uno de los mayores referentes de la República Argentina, ha remarcado que la dependencia tecnológica limita el control de la seguridad y por ende vulnera la soberanía del Estado (Ambrojo, 2004). A su vez otorga un gran énfasis en la necesidad de poder auditar la criptografía y que esta sea desarrollada por organismos nacionales para evitar la inserción de vulnerabilidades ocultas o “puertas traseras” (Huergo, 2023).

Se evidencia en el estado del arte actual un consenso sobre la importancia de la criptografía, el rol que ocupa para el estado y la necesidad de una estrategia nacional unificada que genere un efecto de sinergia para poder hacerle frente a potencias tecnológicas.

Para el desarrollo de este trabajo se deben abordar ciertos conceptos fundamentales, los cuales otorgan un adecuado entendimiento sobre el tema que se investiga. Primeramente, el de criptografía, la cual se define como “el arte de escribir con clave secreta o de un modo enigmático” (Real Academia Española, s.f.) utilizada a lo largo de la historia para la protección de la información y las comunicaciones, sobre todo en lo que respecta a los conflictos o interacciones entre los estados.

La historia brinda ejemplos del uso de estos sistemas en contexto de guerra. El cifrado del César, utilizado por el imperio romano, y la máquina Enigma de Alemania durante la segunda guerra mundial, demostraron como el control o la vulneración de estos sistemas pueden otorgar una ventaja o una derrota total (Urrea, 2020; Anónimo, 2023).

En lo que refiere a una perspectiva estratégica, la criptografía cumple un rol fundamental dentro de las actividades de inteligencia y contrainteligencia, evitando que se comprometa información sensible, encontrándose enmarcado para la República Argentina dentro de Ley 25.520 de Inteligencia Nacional. En ella se define el sistema de inteligencia, el cual tiene dentro de su misión la protección de información con clasificación de seguridad, reforzando la necesidad de soluciones propias y la generación de capacidades de auditoría.

Por consiguiente, la soberanía tecnológica como concepto se vuelve eje de este análisis, ya que la completa dependencia de desarrollos en criptografía de origen extranjero aumenta el riesgo de que en ellos existan vulnerabilidades deliberadamente implantadas o “puertas traseras”, fiel ejemplo de esto es el caso de la empresa suiza Crypto AG. Este es un antecedente clave, donde organizaciones de inteligencia, pertenecientes a potencias extranjeras, manipularon equipos de cifrado para espiar a los gobiernos que los adquirirían, entre los cuales se encontraba Argentina (GPDel, 2020; Consejo Federal de Suiza, 2021).

Finalmente, es clave entender que la protección de la información y las comunicaciones en escenarios de conflicto no puede depender en su totalidad de proveedores foráneos. La criptografía nacional se convierte en una necesidad estratégica, permitiendo evitar la repetición de errores cometidos en el pasado en este ámbito y posicionar a la Argentina dentro de una doctrina parcial de independencia tecnológica, primordial para preservar la seguridad y por ende la soberanía.

Formulación del Problema y Enfoque Metodológico

Actualmente, la República Argentina continúa dependiendo en gran medida de tecnologías criptográficas desarrolladas por entidades extranjeras, incluso para la protección de información crítica en sectores sensibles como el militar. Esta situación representa un riesgo en términos de soberanía y seguridad nacional, ya que no se puede asegurar la inexistencia de puertas traseras intencionalmente colocadas en dichos dispositivos o algoritmos, lo cual podría comprometer la confidencialidad de las comunicaciones.

La carencia de una estructura nacional sólida en lo que respecta a criptografía, puntualmente en la fabricación y control de hardware, deja vulnerable al país frente a posibles filtraciones o

intervenciones en sus comunicaciones estratégicas, particularmente en contextos de conflicto. A partir de esto, surgen interrogantes que no deberían postergarse: ¿se puede seguir confiando en tecnologías completamente desarrolladas en el exterior para proteger información sensible? ¿Qué capacidades reales tiene el Estado para garantizar la integridad y seguridad de sus propios sistemas sin depender del exterior?

El trabajo se enfoca en los aspectos estratégicos y doctrinarios de la criptografía nacional.

Se analiza su aplicación en el ámbito militar, sin abordar detalles técnicos de implementación en dispositivos (hardware) o programas informáticos (software). No se propone una solución técnica concreta, sino los aspectos claves de una estrategia conceptual y organizacional.

En este trabajo se propone el diseño conceptual de una estrategia nacional para el desarrollo de criptografía militar con el fin de reducir la dependencia tecnológica extranjera y evitar la existencia de vulnerabilidades implantadas.

Para alcanzar este objetivo se parte de la definición de los conceptos básicos de la criptografía, así como del análisis de los antecedentes históricos y el enfoque internacional actual.

A su vez, se analiza la relación entre la criptografía y la actividad de inteligencia, y se evalúan las posibilidades de una solución a través de criptografía nacional. Se complementa con el análisis de un caso real de vulneración de sistemas criptográficos de uso militar: el caso Crypto AG y por último se proponen lineamientos para una estrategia nacional de criptografía militar.

En este marco, se parte de la hipótesis de que la existencia de una estrategia nacional de criptografía contribuye a disminuir los riesgos de afectación en la confidencialidad e integridad de las comunicaciones estratégicas, fortaleciendo el control soberano, particularmente en el ámbito del instrumento militar.

En lo que aportes al campo disciplinar refiere, el trabajo busca contribuir a la doctrina de defensa nacional proponiendo una visión estratégica de la criptografía como pilar de soberanía.

Asimismo, pretende servir como punto de partida para la elaboración de articulaciones coordinadas entre defensa, educación y ciencia.

El trabajo se basa principalmente en la metodología descriptiva, partiendo del análisis de documentos provenientes de distintas fuentes técnicas, legales y doctrinarias. Asimismo, se aplica una metodología exploratoria, mediante la cual se revisan las experiencias internacionales y nacionales en cuanto al uso, tratamiento y desarrollo de la criptografía.

Finalmente se opta por la metodología propositiva, a partir de la cual se formula una estrategia de criptografía a nivel nacional de manera conceptual.

INDICE

RESUMEN	1
INTRODUCCIÓN.....	2
Fundamentos del Trabajo	2
Formulación del Problema y Enfoque Metodológico	5
CAPITULO 1: Marco Conceptual y Contexto Estratégico	9
1.1. Definiciones, Antecedentes y Contexto Internacional	9
a) ¿Qué es la Criptografía?.....	9
b) Antecedentes Históricos y Nacionales	10
c) Enfoques Internacionales Actuales	12
1.2. Relación con la Inteligencia	14
CAPÍTULO 2: Propuestas y Estrategias para la Criptografía Nacional.....	17
2.1. Criptografía Nacional como Solución.....	17
CAPÍTULO 3: Estudio de Caso: El escándalo de la empresa internacional “Crypto AG” ..	20
CAPÍTULO 4: Desarrollo de una Estrategia Nacional de Criptografía.....	23
CONCLUSIONES:.....	27
BIBLIOGRAFÍA:.....	29

CAPITULO 1: Marco Conceptual y Contexto Estratégico

1.1. Definiciones, Antecedentes y Contexto Internacional

a) ¿Qué es la Criptografía?

Para comenzar a desarrollar este trabajo debemos centrarnos en definir ciertos conceptos claves, ya que son necesarios para la correcta interpretación del mismo y a su vez teniendo en cuenta que la temática es poco conocida o popular fuera de ámbitos como lo son las comunicaciones, actividades de inteligencia o matemáticas.

La criptografía según el diccionario se define como "el arte de escribir con clave secreta o de un modo enigmático" (Real Academia Española, s.f.), si bien esta definición es bastante abstracta, nos sirve para ir comprendiendo el porqué de su uso y ciertos elementos que participan, como lo es la clave y un modo de aplicación. Yendo hacia un camino con cierto nivel de tecnicismo vigente en la actualidad, encontramos que se define a la misma como “conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo.” (NIC Argentina, s.f.), dejándonos en claro su principal objetivo, que no obtenga la información nadie que no deba poseerla, más allá de donde esta se encuentre o por donde se transmita.

El modo en que se alteran esos archivos y vuelven a su estado normal es conocido como algoritmo, cuya definición formal es “Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.” (Real Academia Española, s.f.), en el ámbito de la criptografía estos están conformados por grandes cantidades de operaciones matemáticas, sumándole a eso una o varias claves, las cuales son utilizadas como llaves tanto para volver el mensaje ilegible o a su estado original. La fortaleza de estos se encuentra en la dificultad para obtener el mensaje original sin las claves. En un principio, el enfoque fue diferente, se buscaba proteger el algoritmo y así evitaban que el mensaje fuera descubierto, pero en la actualidad se ha demostrado que, si este posee la robustez necesaria (existen una serie de pruebas para poder afirmarlo), el conocimiento detallado del algoritmo no es una preocupación, es más, al estar publicado, es mayor la población que puede dar fe que el mismo es irrompible (computacionalmente hablando).

Existen dos grandes tipos de cifrados (basándonos en la utilización de claves para cifrar y realizar el proceso contrario) el Simétrico y el Asimétrico, la gran diferencia que radica en ambos es, que el primero, utiliza la misma clave tanto para cifrar como para descifrar, y el otro, utiliza dos claves diferentes (pública y privada), solo es necesario poseer la clave pública (la cual puede estar publicada al alcance de todos) del receptor para cifrar el documento y que este solo sea abierto por el mismo (INCIBE, 2021). Un ejemplo de criptografía simétrica es Microsoft BitLocker, una aplicación que cifra por completo el disco duro y protege su contenido mediante una contraseña única. En cambio, un ejemplo de criptografía asimétrica es la firma digital, donde se utiliza la clave privada para firmar y la clave pública para verificar la autenticidad del mensaje.

Los conceptos anteriormente detallados, logran evidenciar el porqué del cambio de enfoque en cuanto a la protección, donde hoy solo se debe mantener oculta la clave (en caso de algoritmos simétricos) o la clave privada (algoritmos asimétricos) y no el algoritmo en sí.

b) Antecedentes Históricos y Nacionales

A través del tiempo se han encontrado numerosos ejemplos en donde el ser humano a tratado de ocultar un mensaje o hacerlo legible solo para quienes conocieran ese “código”, en la biblia se encuentran referencias a un sistema denominado Atbash, el cual constaba en la sustitución de letras, aproximadamente en el año 600 a.C. (Juan Jesús Velasco, 2014). jeroglíficos encontrados en Egipto en el año 1900 a.C., los cuales no eran los utilizados con frecuencia y buscaban transformar de algún modo el texto original (Sidhpurwala, 2023). Luego aproximadamente en el año 100 a.C., mencionado en la introducción y uno de los más famosos ejemplos, el cifrado utilizado por Julio Cesar, conocido como cifrado del César, en donde se desplazaban los caracteres del alfabeto una cantidad X de posiciones, dando así una nueva letra, la cual debía ser intercambiada en el mensaje original, en este caso la seguridad se basaba en mantener oculto el “algoritmo”, o en palabras comunes, la forma de cifrar. Avanzando en el tiempo encontramos el primer algoritmo de cifrado que utilizo una clave, por ende, su fortaleza no residía en mantenerlo oculto, sino que debía custodiarse la misma, este era nombrado Cifrado de Vigenere, cuyos comienzos como tal son provenientes del siglo XVI.

En lo que respecta al siglo XVIII y XIX, la criptografía fue de la mano con los conflictos que se desarrollaron, el obtener información a través de las comunicaciones del enemigo daban a lugar a grandes ventajas y esto quedó evidenciado en disputas tales como la guerra de independencia de las colonias americanas (se desarrolló la rueda de cifrado de Jefferson) en donde era un objetivo primordial interceptar los mensajes británicos, o en la guerra de Crimea (Maquina Analítica de Charles Babbage) en donde Gran Bretaña tuvo una gran ventaja sobre el Imperio Ruso y el Reino de Grecia (Velasco, 2014).

Durante el siglo XX, sumado a la aparición de la electrónica y las dos guerras mundiales, los avances en criptografía fueron notables, uno de los hechos históricos de mayor relevancia fue la invención de la conocida “Maquina Enigma”, la cual trabajaba con una serie de rotores mecánicos y utilizaban como clave inicial la posición de estos (Sidhpurwala, 2023). Esta otorgó a las fuerzas del eje, principalmente a Alemania, una ventaja sobre los Aliados. Sin embargo, esta situación se revirtió cuando se logró descifrar su funcionamiento, y se plantea que, gracias a ello, logró acortar la duración del conflicto.

Con la aparición de las computadoras, la criptografía fue abandonando el ámbito militar y de a poco se incorporó a las empresas privadas, si bien en lo que respecta a Estados Unidos, por mucho tiempo la investigación y desarrollo de algoritmos estuvo monopolizado por la Agencia de Seguridad Nacional (NSA), con el tiempo esto fue cambiando, prueba de ello fue la aparición de los algoritmos Data Encryption Standard (DES), desarrollado por la empresa IBM en 1975 y posterior a este en el año 2001, el Advanced Encryption Standard (AES), al cual le tomo 5 años convertirse en un estándar y logro reemplazar a su anterior (Velasco, 2014).

En la actualidad, han surgido nuevas temáticas y desafíos en el ámbito de la criptografía. Uno de ellos es la aparición de la computación cuántica, la cual podría vulnerar la principal fortaleza de los algoritmos criptográficos actuales: la complejidad matemática de los cálculos y el tiempo necesario para realizarlos. Estos quedarían obsoletos y abrirían la puerta a la denominada criptografía poscuántica (ANIMUS, 2023), la cual en esta investigación solo será mencionada.

A nivel nacional, son muy pocos los ejemplos documentados que se pueden mencionar, ya que la mayoría de la información en cuanto a la temática tratada, haciendo foco en el ámbito militar,

ha sido secreta. Durante la guerra de la Independencia, el General José de San Martín utilizaba diferentes métodos criptográficos para las comunicaciones de gran importancia que debían mantenerse secretas, entre ellos estaban las denominadas “Tintas Simpáticas” o “Tintas Invisibles”, los métodos “Rejilla Simple” (dibujar una cuadrícula de letras y luego, mediante una rejilla con agujeros, seleccionar ciertas letras para formar el mensaje cifrado), Cifras Mono alfabéticas (también conocido como el Cifrado del César o método de sustitución, reemplaza letras por números previamente elegidos), Nomenclátor (combinan métodos de sustitución con el reemplazo de palabras o la utilización de códigos, sumando a eso símbolos sin sentido) y Diccionario (utiliza un libro común entre el emisor y el receptor, codificando un mensaje a través de tres números que indican la página, renglón y columna de las palabras seleccionadas) (Carlos & Díaz, n.d.).

Otro, de gran relevancia para el enfoque de este trabajo, fue la utilización del lenguaje “guaraní” durante el conflicto de las Islas Malvinas en el año 1982, este permitió que las comunicaciones se mantuvieran seguras e indescifrables para el enemigo. Un caso diferente fue el de los dispositivos “CAG 500” pertenecientes a la empresa Crypto AG, los cuales podían ser fácilmente vulnerados por los británicos y de los cuales la Argentina poseía una gran cantidad de unidades (Sciaroni, 2024).

En la actualidad, se sigue trabajando en el área, apuntando a la actualización y modernización de nuestras Fuerzas Armadas, haciendo foco en la necesidad e importancia de la criptografía en los sistemas de información y comunicación e incentivando el desarrollo propio (Morales Rins, 2018).

c) Enfoques Internacionales Actuales

Para poder entender la relevancia de la temática, es pertinente considerar las diferentes posturas a nivel internacional, las cuales nos sirven como elementos de juicio a la hora de realizar una comparación con nuestra situación actual y el manejo de esta.

En lo que respecta a países del continente americano, Estados Unidos tiene una postura clara sobre el tema, si bien en un principio la criptografía solo estaba limitada al ámbito militar y el ente responsable era la Agencia de Seguridad Nacional, como lo mencionamos con anterioridad esta fue liberada para el ámbito civil y comercial (Velasco, 2014), pero se debe aclarar que existen ciertas

restricciones, por ejemplo, esta es clasificada como munición de guerra, por ende, su comercialización dependería de autorizaciones y esto le permite tener un control soberano sobre lo que se produce dentro del territorio (Niss & Compilador, n.d.).

La República Popular de China puso en vigencia en el año 2020 una ley que regula la criptografía (Portaltic & Portaltic, s. f.), esto le permite al estado controlar como se desarrolla, utiliza y comercializa los elementos referidos a esta temática y a su vez hace foco en velar siempre por la seguridad nacional.

La República de Francia también posee ciertas restricciones con respecto a la criptografía, su uso, exportación e importación, las cuales son menos restrictivas para cuestiones exclusivas de comprobación de integridad (característica que nos permite saber si un archivo fue modificado o no) o en caso de estar involucrados países miembros de la Unión Europea, de lo contrario las restricciones son mayores y necesitan de autorizaciones (República Francesa, s. f.).

El Reino Unido posee ciertas legislaciones referidas a esta temática, entre las que se destaca la Ley de Seguridad Nacional e Inversión (Reino Unido, 2021). Esta ley establece que ciertos elementos a adquirir deben ser notificados al gobierno, incluyendo aquellos vinculados a la criptografía para autenticación.

Existen otros grupos de países, donde la exigencia de autorizaciones o licencias para la producción o venta de servicios relacionados a la criptografía es obligatoria, dentro de ellos se encuentra Turquía, Etiopía, Túnez y Mali, con algunas excepciones cuando se trata para uso personal. Existen algunos países con legislación vigente pero no han dado crédito de que se esté aplicando, donde podríamos mencionar a Bahamas y Barbados (Ciberseg, 2021).

En cuanto a exportación e importaciones de este tipo, el número de países aumenta, en el caso de Armenia, Bielorrusia, Kazajstán, Kirguistán y Rusia, estos demandan una licencia con múltiples exigencias como lo pueden ser longitud de claves, tipos de algoritmos, tipos de datos, entre otras.

Referido a normativas internacionales, existe el Acuerdo de Wassenaar, el cual regula el control de exportaciones de armas convencionales y de bienes y tecnologías de doble uso, donde

se encuentra incluida la criptografía y la República Argentina ha ratificado mediante el Decreto N° 437/2000 Modificación del Decreto N° 603/92, en relación con la integración de la Comisión Nacional de Control de Exportaciones Sensitivas y Material Bélico. Listado de Materiales y Tecnologías de Doble Uso (República Argentina, 2000).

En términos generales, considerando las diferentes perspectivas de abordaje que posee la temática, se puede concluir que es un asunto de gran relevancia para los diferentes estados. Si bien algunos lo abordan con mayor seriedad que otros, el mismo no puede ser ignorado.

1.2. Relación con la Inteligencia

Para abordar este capítulo es necesario en primera instancia, definir ciertos conceptos. Argentina define a la Inteligencia como “la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, amenazas, riesgos y conflictos que afecten la seguridad exterior e interior de la Nación” (República Argentina, s. f.), asimismo es de utilidad mencionar que se suele utilizar dentro del ámbito, la palabra Inteligencia, para hacer mención al producto (se obtuvo inteligencia), la actividad (se realizó inteligencia) y la organización (proviene de inteligencia).

Dentro de una organización tendremos otra área o función a la que se denomina Contrainteligencia, la cual según la legislación vigente es definida como “actividad propia del campo de la inteligencia que se realiza con el propósito de evitar actividades de inteligencia de actores que representen amenazas o riesgos para la seguridad del Estado Nacional” (República Argentina, s. f.). Por lo tanto, puede afirmarse, en términos generales, que los Organismos de Inteligencia tienen como responsabilidad la obtención de inteligencia de los actores de interés, así como también la protección de la información propia del accionar de la inteligencia de otros estados.

Existe una sub-clasificación de la contrainteligencia por parte de la ley, la cual mencionamos con anterioridad, esta categoría es denominada como Contrainteligencia Militar y esta “destinada a prevenir, detectar y contrarrestar acciones de inteligencia de actores que intenten afectar el propio poder militar” (República Argentina, s. f.).

Establecidos los conceptos principales, queda explícita la necesidad y obligación de desarrollar capacidades de almacenamiento, procesamiento y transmisión de información de forma segura, más allá del tipo de soporte o medio que se utilice (si bien en la actualidad la mayoría de estas se realiza con medios digitales a través de internet o redes privadas) por lo cual esto otorga protagonismo una vez más a la criptografía y en función de la naturaleza de los roles asignados, los organismos de contrainteligencia serán los más interesados en su aplicación, ya que colabora de forma directa con su responsabilidad primaria, evitar que actores no autorizados se hagan de nuestros datos o información.

El trabajo de las organizaciones de inteligencia es continuo, y la criptografía es su aliado, pero desde el punto de vista de un actor adversario u oponente es el enemigo o uno de sus grandes obstáculos, por lo cual es lógico que una de las tecnologías más importantes a las que tienen como objetivo los servicios de inteligencia sea el cifrado (TechRepublic, 2023). Esto se ve reflejado en los esfuerzos que se realizan para vulnerar los diferentes algoritmos que existen, existiendo múltiples formas, como por ejemplo las mencionadas a continuación “Una solicitud de presupuesto de la NSA 2013 — revelada en otro de los documentos de Snowden — muestra que los planes de la NSA incluían crear puertas traseras en sistemas de cifrado comerciales e influir en los estándares y especificaciones utilizados como fundamentos de las tecnologías de privacidad con la intención de facilitar su acceso”, “Los recursos en este proyecto se utilizan para... insertar vulnerabilidades en sistemas de cifrado comerciales, sistemas de TI, redes y dispositivos de comunicaciones de punto final utilizados por los objetivos” (TechRepublic, 2023).

Por lo tanto, es un desafío de grandes dimensiones para las áreas de contrainteligencia militar, el poder cumplir de manera eficaz sus responsabilidades, para ello debe utilizar todos los medios que se encuentren disponibles por lo cual, la criptografía es una de las opciones por excelencia a la cual se debe recurrir, pero no se debe dejar de lado lo riesgoso que sería depositar toda la confianza en una empresa extranjera a la hora de adquirir dispositivos, programas o algoritmos, cuya probabilidad de estar modificados para permitir el acceso a su desarrollador es enorme, esto no responde a especulaciones, supuestos o hipótesis sino a filtraciones de operaciones en curso por parte de los grandes servicios de inteligencia del mundo mencionadas al principio y al final del este trabajo. Entonces es correcto plantearse las siguientes posibilidades, un escenario en

el que la seguridad de las comunicaciones yace sobre un tercero, desarrollos puramente nacionales con gran control por parte del estado y las agencias propias o un tipo de modelo híbrido en donde se puedan aprovechar los desarrollos no nacionales, pero se le agreguen modificaciones o capas de seguridad extra desarrolladas con capacidades y bajo control nacional.

CAPÍTULO 2: Propuestas y Estrategias para la Criptografía Nacional

2.1. Criptografía Nacional como Solución

Partiendo de las ideas ya desarrolladas, entendemos que nuestras Fuerzas Armadas están transitando un camino de mayor dependencia tecnológica y uso de sistemas informáticos complejos, hecho por lo cual se abren nuevas posibilidades a la existencia de diferentes tipos de vulnerabilidades antes desconocidas. La utilización de dispositivos móviles es mayor por lo que el riesgo se incrementa exponencialmente, ya que nos acompañan en todo momento y suelen ser plataformas donde se relacionan las cuestiones laborales o profesionales y la vida privada, por lo cual muchas veces, por comodidad o falta de recursos, se termina recurriendo al uso de dispositivos propios, para atender o resolver cuestiones oficiales. Sumado a esto, gran parte de esta tecnología es de origen extranjero dando lugar a que exista vulnerabilidades deliberadamente colocadas o comúnmente definidas como puertas traseras.

Las problemáticas a las que se ven expuestas nuestras comunicaciones e información en la actualidad son de diversa naturaleza, ya no solamente debe preocuparnos la interceptación de las comunicaciones en tiempo real o el descifrado de las mismas a posterior por vulnerabilidades implantadas, sino que existe un concepto aún más peligroso que debemos agregar a la lista, *Cosecha Ahora Descifra Después* (Harvest Now, Decrypt Later) “se basa en la premisa de que, aunque actualmente no sea posible romper el cifrado utilizado, la evolución de la tecnología eventualmente hará que estos datos sean accesibles” (Redacción IT NOW, 2024) por lo cual es necesario generar alternativas en el corto, mediano y largo plazo para lograr mitigar el uso de tecnología extranjera en ámbitos tan sensibles como lo son la defensa y seguridad nacional, así como también la inteligencia.

Debido a la dependencia tecnológica en aumento, lo cual es algo coherente si se quiere tener un estado moderno con instituciones a la altura de los tiempos que corren y principalmente, ya que es el foco de este trabajo, Fuerzas Armadas modernas con capacidad de interoperabilidad entre ellas y con otras naciones, el oscurantismo tecnológico, en el cual se contemple la opción de no usar estas herramientas o solamente aquellas que se desarrollen dentro del contexto nacional, no es una opción viable en su totalidad. Debe ser evaluada una postura flexible, en donde se aprovechen las

bondades de desarrollos por parte de empresas que han invertido importantes recursos para su obtención, y que nos llevaría años alcanzar o, por lo contrario, no se cuenta con el conocimiento en ese rubro, cosa que lo haría imposible. Esta debería estar orientada a agregar diferentes capas de seguridad con desarrollos propios o modificaciones que nos permitan personalizar estas tecnologías o poseer cierto control, y en paralelo, hay capacidades que deben ser mejoradas o fomentadas para crear y controlar este tipo de tecnologías.

En lo que refiere a la República Argentina, en donde el presupuesto para ciencia, investigación y desarrollo suele ser uno de los primeros en ser recortado ante alguna crisis, son variados los ejemplos de implementaciones originadas por especialistas en la temática, lo cual hace factible la idea de un aprovechamiento de la tecnología que nos ofrecen otros países, pero sin confiar en estos de modo exclusivo, cuestión que ha tenido lugar en el pasado, con elevados costos y consecuencias. Un claro ejemplo de la capacidad intelectual existente en nuestro país fue la presentación, en el concurso de algoritmos de criptografía ligera realizado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, por parte del Ingeniero Miguel Montes perteneciente al Instituto Universitario Aeronáutico dentro de la Universidad de la Defensa y Daniel Penazzi, licenciado y doctor en matemática, criptógrafo y profesor en la Facultad de Matemática, Astronomía, Física y Computación (Universidad Nacional de Córdoba), el mismo fue llamado “Yarar’a and Coral v1” (Montes & Penazzi, 2019).

Otro ejemplo de gran relevancia es el caso del señor Hugo D. Scolnik, “Licenciado en Ciencias Matemáticas (UBA, 1964) y Doctor en Matemática por la Universidad de Zurich (1970)” (Troop Software Factory, 2020) el cual “trabaja en ARSAT SA, es consultor en seguridad informática e investigador con una importantísima trayectoria en criptografía, optimización no lineal y modelos matemáticos. Es uno de los investigadores que más sabe de criptografía en Argentina” (El Fundador Del DC En Primera Persona, 2023). En su entrevista detalla la problemática que tienen ciertos algoritmos en su necesidad de compartir claves y como ciertas naciones como por ejemplo China o Israel, centran sus esfuerzos en la obtención de estas. Además se detalla el trabajo realizado entre empresas con ciertas relaciones con el estado como lo es ARSAT (Empresa Argentina de Soluciones Satelitales S.A) e INVAP (Investigaciones Aplicadas Sociedad del Estado propiedad de la Provincia de Río Negro) en donde afirmó “Lo que hicimos en ARSAT

fue un método para que dos partes lleguen a una clave común pero el espía que está escuchando no pueda deducirla, y este algoritmo forma parte de un sistema general llamado Cryptocomm que implementa nuevas formas post cuánticas de claves público/privadas, certificados digitales, autoridades certificadoras, encriptación simétrica, etc. Es decir que Cryptocomm resiste los ataques de las computadoras clásicas y de las cuánticas. Cuando decidimos hacer todo esto, formalizamos un convenio con INVAP, por el cual vamos a desarrollar unas máquinas de encriptación no solo para abastecer a Argentina sino para situarnos en un escenario mundial, o sea exportar.” siendo esto prueba irrefutable de la necesidad de formalizar una coordinación entre todos los esfuerzos individuales que se encuentran actualmente vigentes en la República Argentina.

Los recursos humanos propios no solo se encuentran radicados en el país, sino que hay ejemplos de mentes argentinas desempeñando funciones claves en el extranjero, así lo detalla el diario El Cronista en su artículo “Este genio argentino es el responsable de que no te hackeen WhatsApp todos los días” (Garabetyan, 2019).

Si bien el desarrollo netamente nacional no es algo a lo que podamos aspirar en el mediano plazo y tal vez ni siquiera en el largo plazo (dimensionados para nuestra cultura), ya que naciones con inversiones descomunales no logran aplicarlo, el lograr una postura híbrida en donde se logre aprovechar el potencial propio en la materia, en combinación con implementaciones extranjeras consolidadas, debe ser algo que requiera de nuestra atención en el corto plazo.

CAPÍTULO 3: Estudio de Caso: El Escándalo de la Empresa Internacional “Crypto AG”

Es común, como hemos visto a lo largo de la historia, que la investigación y el avance tecnológico estén relacionados con el ámbito militar, mayormente las innovaciones provienen en parte de proyectos que surgen en dicho entorno, en el caso de la criptografía podemos decir que no es algo ajeno a esto. Como se mencionó con anterioridad, esta fue abandonando de a poco el secreto militar para ser desarrollada por diferentes organizaciones del sector privado.

Con el cambio de conceptos, empezaron a emerger cada vez más empresas que ofrecían sistemas de cifrado robustos. Estas normalmente ofrecían ciertas garantías en cuanto a confidencialidad y calidad del producto en los acuerdos de confidencialidad que se firman durante la compra, lo que nos debería generar cierto interrogante, ¿cómo compruebo técnicamente las prestaciones del elemento y el cumplimiento del contrato?

Siendo consientes acerca del trabajo que realizan los servicios de inteligencia, conceptos que han sido desarrollados en otro capítulo, la sensación que perciben los estados en cuanto a la inseguridad de sus comunicaciones puede llegar a ser percibida como paranoia haciendo parecer a aquellos que buscan evitarla como personas que tienen ideas sacadas de la ficción, este es el momento donde el caso de la empresa suiza Crypto AG materializa, por fuera de cualquier guion u obra literaria de espías, una de las operaciones de espionaje a gran escala de la Agencia de Inteligencia de los Estados Unidos.

En el año 2020, debido a una revelación del diario The Washington Post y BDZ (cadena de televisión alemana) se conoció que “los servicios de inteligencia de los gobiernos de EE. UU. y Alemania espionaron durante décadas las operaciones de cerca de 100 países, mediante un dispositivo de encriptación que producía la empresa suiza Crypto AG” (Redacción, 2020), cabe recalcar que la República Argentina estuvo incluida en el grupo de estados afectados. La Agencia de Inteligencia de los Estados Unidos, como se aprecia en el siguiente extracto, “con el Servicio Federal de Inteligencia de Alemania (BND) compró la empresa, a través de intermediarios”, permitiéndole mediante diversos métodos descifrar las comunicaciones interceptadas que utilizaban dispositivos de la marca.

En primeras instancias, la empresa fundada por Hagelin “fabricó máquinas con buenos algoritmos criptográficos para Suiza, Suecia y los miembros de la OTAN, y otros, que eran muy fáciles de descifrar, para los demás países, especialmente, los países árabes. Esto facilitó al servicio secreto estadounidense poder descifrar las transmisiones de radio encriptadas” (Landwehr, 2024). Luego de la compra por parte de las agencias y el retiro de su fundador, estas tuvieron injerencia directa sobre las decisiones que se tomaban dentro de la compañía en cuanto a la fabricación.

En cuanto a las repercusiones a nivel nacional, podríamos decir que la República Argentina fue uno de los países más perjudicados si hacemos hincapié en el espionaje de las comunicaciones propias de las operaciones militares, pasando por alto el espionaje a los cables diplomáticos, cosa que quedó documentada y fue revelada tal como detalla el diario MDZ “La inteligencia estadounidense monitoreó activamente, durante décadas, las comunicaciones diplomáticas y militares de numerosas naciones latinoamericanas, a través de máquinas de cifrado suministradas por la compañía suiza Crypto AG” (Mundo, 2020).

El desarrollo de las operaciones militares durante el Conflicto del Atlántico Sur en la Islas Malvinas, Georgias y Sandwich del Sur, archipiélagos pertenecientes a la República Argentina invadidos por Gran Bretaña el 3 de enero de 1833, se vio afectado de gran manera ya que a través de la CIA (Central Intelligence Agency) los ingleses se hicieron de información valiosa “se conocían los equipos Crypto argentinos y las claves de estos, ya que CIA (por el acuerdo UKUSA antes citado) compartía con los servicios de inteligencia británicos toda la información” (Sciaroni, 2024), cosa que fue fundamental a la hora de la toma de decisiones para la planificación. Se pueden destacar dos hechos en particular, en donde el tener las comunicaciones interceptadas permitió al enemigo realizar acciones desequilibrantes durante el conflicto, la avería del submarino Santa Fe y el hundimiento del crucero ARA General Belgrano, tal como describe Sciaroni en su artículo “al emitir por radio (el 23 de abril) el submarino Santa Fe un mensaje dirigido a su comando, el mismo fue interceptado por el HMS Endurance, descifrado en el Reino Unido y, al volver al Teatro de Operaciones (24 horas después), se tomó conciencia que el submarino argentino se dirigía hacia las Georgias, lo que hizo que se hiciera una operación de vigilancia que terminó con el submarino argentino atacado y dañado” por su parte “la posición e intenciones del Grupo de Tareas que lideraba el ARA General Belgrano fue obtenida también descifrando comunicaciones argentinas,

lo que posibilitó que el submarino británico HMS Conqueror lo hundiera”(2024). Ambas situaciones generaron efectos significativos en el posterior desarrollo de las operaciones.

Cabe destacar que las complicaciones a la hora de interceptar y descifrar los mensajes argentinos provenían de la variedad de equipos que se poseían y la utilización de otras capas, como por ejemplo el uso del guaraní “heredera de la familia lingüística Tupi-Guaraní que dominaba la mayor parte de América del Sur en la época precolombina. Llegó a ser una de las “Lenguas generales” durante la Colonia y fue el objeto de la primera planificación lingüística que acompañó la experiencia social y económica de las Misiones jesuíticas en la región” (La Lengua Guaraní, Un Eslabón Patrimonial Para Fortalecer Los Lazos Bilaterales Y Multilaterales En Nuestra Región - Memorial Da América Latina, 2020), ejemplo similar a métodos utilizados por parte de los Estados Unidos en la Segunda Guerra Mundial.

Luego del conflicto, especialistas de la empresa Crypto AG se hicieron presentes en Argentina a pedido de las autoridades, ya que había grandes sospechas de que las comunicaciones fueron interceptadas y descifradas, pero ante la incapacidad técnica propia de poder demostrarlo ya que “eso estaba hecho “con una prominencia técnica” que garantizaba que el hackeo fuera “imposible de detectar mediante las pruebas estadísticas habituales” y que, en caso de que se los descubriera, se podían “enmascarar fácilmente como errores de implementación o errores humanos”” (Infobae, 2020), no se tomó decisión alguna y se mantuvieron los contratos con la empresa suiza.

En el año 1995, tras publicaciones del diario The Sun, las cuales afirmaban que había distintos tipos de dispositivos para países del tercer mundo, diferentes países cancelaron sus contratos con la firma, entre ellos la República Argentina. Por último, como mencionamos al principio de este capítulo, en el año 2020 se dieron a conocer los pormenores de la operación, lo cual desató un gran escándalo a nivel mundial, forzando a replantear el tratamiento de esta temática por parte de los estados.

CAPÍTULO 4: Desarrollo de una Estrategia Nacional de Criptografía

El área de la criptografía es un sector en donde el personal que interviene necesita un nivel avanzado de conocimientos técnicos, lo cual conlleva un prolongado periodo de educación previa y en la República Argentina, si bien existen, no abundan. Sumado a ello, como en otras áreas de características específicas similares, las ofertas del sector privado o del extranjero suelen ser ampliamente superadoras en comparación al mercado local o estatal. Otro factor determinante es el tiempo que demandan los proyectos en el ámbito, por ejemplo, como detalla el siguiente artículo “El NIST lanza las primeras herramientas de cifrado para resistir la computación cuántica” (Resility, 2024) permitiendo dimensionar cuánto cuesta abordar una problemática y encontrar posibles soluciones.

Realizando una sumatoria de las premisas anteriormente mencionadas, observamos un ambiente complejo en donde las características no permiten desaprovechar los recursos finitos con los que se puede llegar a contar, de ahí que teniendo en cuenta la relación directa del área con la seguridad nacional, haciendo hincapié en el sector de la defensa nacional, es menester de la conducción estratégica nacional abordar un modo de acción que permita extender los esfuerzos coordinados en largos periodos de tiempo, lo cual es necesario para poder abordar y solventar las problemáticas propias del desarrollo tecnológico dentro del ambiente de la criptografía.

La estrategia en primera instancia, como ya se ha hecho mención, debe emanar desde el más alto nivel del estado y debe trascender a las distintas administraciones, de ahí que necesitaría un sustento legal en el cual apoyarse, como lo podría ser una ley. En dicha normativa se debe definir, objetivos, alcance, el organismo responsable y aquellos que deben contribuir, las diferentes articulaciones entre estos, presupuesto y su modo de financiamiento, la clasificación de seguridad de los proyectos abordados, tratamiento de la información, diferenciación entre desarrollos para los distintos sectores críticos (defensa, inteligencia, comunicaciones) y aquellos que se pueden utilizar para comercializar, la relación entre el ámbito estatal y el privado, entre otras cuestiones.

Profundizando en el objetivo de esta estrategia, la misma debería buscar obtener la capacidad de desarrollar criptografía y criptoanálisis nacional a nivel teórico y práctico,

permitiendo la creación de sistemas propios, agregar niveles de seguridad a desarrollos de terceros y auditar ambos, todo esto tanto en programas (software) como así también dispositivos físicos (hardware).

Teniendo en cuenta las modificaciones en la legislación vigente, una opción válida, en cuanto al organismo responsable refiere, sería la Agencia Federal de Ciberseguridad (AFC) perteneciente al órgano de inteligencia de mayor nivel de nuestro país, la Secretaría de Inteligencia del Estado, en tal sentido, a este ente se lo faculta para “Desarrollar y aplicar sistemas de ciberseguridad, encriptación y todo otro mecanismo de seguridad informática a los fines de resguardar y proteger toda información y comunicación de cualquier tipo de ciberamenazas y actividades de inteligencia de terceros” (República Argentina, 2024), lo cual no implica que deba tener dentro de su órbita a todo el personal docente y técnico necesario, sino que debería ser aquel que oriente, ordene y controle los esfuerzos en el área. En lo que respecta al resto de los organismos, no caben dudas que los Ministerios de Capital Humano (Educación) y Defensa, en una primera instancia, deben ser tenidos en cuenta a la hora de coordinar esfuerzos, aprovechar conocimientos y recursos humanos, lo cual no es excluyente para otras dependencias que puedan llegar a tener cierta injerencia o capacidad de colaboración en la temática.

Para lograr el efecto sinérgico necesario, se debe poder articular mecanismos de obtención y perfeccionamiento de recursos humanos. Allí es donde las diferentes universidades y sus facultades, a través de la orquestación del área de educación del Ministerio de Capital Humano, serían de gran utilidad. Estas mediante incentivos tales como contratos, becas, ciertos beneficios en el ámbito estatal o convenios con empresas de capitales mixtos, podrían captar la atención de alumnos destacados dentro de las carreras afines.

En lo que refiere al Ministerio de Defensa, se destaca la necesidad de su participación dentro de esta estrategia, ya que probablemente sea uno de los usuarios con mayor demanda debido a la criticidad de la información que forma parte de las operaciones militares y a la multiplicidad de sistemas que se utilizan, los cuales dependen de la criptografía para su seguridad y por lo cual es el organismo que solicitaría la mayor cantidad de proyectos críticos junto a los entes de inteligencia, en una primera instancia.

Entendiendo lo sensible de la materia y en los sectores que se aplica, dentro de la estrategia debe estar definido el nivel de clasificación de conocimientos, desarrollos, proyectos, presupuestos, personal, organismos, entre otros. Teniendo en cuenta las definiciones de clasificación seguridad utilizadas en el ámbito militar, las cuales se comparten a nivel nacional, todo lo relacionado a la actividad criptográfica debe ser SECRETO, la cual es definida como “aquellos asuntos que por su carácter e importancia necesiten una protección de seguridad máxima, ya que su divulgación causaría daño excepcional a la Nación o perjudicaría la ejecución de los planes del Estado” (REGLAMENTO PARA LA ESCRITURA y CORRESPONDENCIA, 2013) y dentro de los cuales se incluye:

- a) Codificación, documentación y material criptográfico para comunicaciones secretas.
- b) Estudios, investigaciones, experiencias e inventos de importancia vital.
- c) Adquisiciones, fabricaciones y construcciones en los casos en que se justifique tal carácter, así como ciertas características fundamentales de establecimientos y obras militares, buques, aeronaves y material de guerra en general.

Si bien se detallan más opciones, estas son las de mayor pertinencia que justifican la clasificación establecida. En cuanto al tratamiento de dicha información, será manipulada y conservada como lo establece el reglamento y en concordancia con las restricciones nacionales, debiéndose incluir al personal que interactúa de forma indirecta con esta, para lo cual se deberán establecer diferentes mecanismos para que los actores involucrados sean conscientes de las restricciones y cuidados que se deben tomar, así como también la no divulgación y confidencialidad del ámbito.

La asignación de recursos no es un tema arbitrario que pueda ser pasado por alto, es necesario que la normativa prevea un presupuesto y su fuente de financiamiento, de forma alternativa puede ser designado un porcentaje del total ya asignado a los organismos intervinientes, lo cual sería provisorio hasta lograr un nivel en donde los desarrollos no críticos o aquellos previamente autorizados puedan ser comercializados en diferentes sectores o países.

Otro punto para tener en cuenta es la relación estado – privados, en donde se deberían establecer los diferentes mecanismos para lograr sumar a este esfuerzo sinérgico los recursos de terceros, tomando todas las precauciones correspondientes al caso, en lo que refiere a la criticidad para la seguridad nacional, ya que prescindir de ellos sería un despropósito, sobre todo en las primeras instancias de desarrollo de esta estrategia.

Definiendo la estrategia en instancias temporales, en el corto plazo se buscaría generar y obtener todo el sustento legal y normativo necesario para permitir a los organismos comenzar con los trabajos iniciales (es por esto la importancia de permitir a los privados su interacción) que permitan generar los conocimientos y la experiencia básica necesaria para establecer una línea base, la cual, en el mediano plazo daría lugar a desarrollos y análisis nacionales iniciales. Por último, en el largo plazo, se obtendrían por completo las capacidades de desarrollar criptografía y criptoanálisis nacional a nivel teórico y práctico, permitiendo la creación de sistemas propios, agregar niveles de seguridad a desarrollos de terceros y auditar ambos, todo esto tanto en programas (software) como así también dispositivos físicos (hardware).

CONCLUSIONES

A lo largo de este trabajo hemos evidenciado la complejidad del escenario internacional actual y futuro en cuanto a la protección de la información de carácter crítico para un estado, si bien la tecnología (haciendo foco en la informática o sistemas informatizados y el ciberespacio) es una herramienta que ha otorgado grandes beneficios, ha abierto la posibilidad a nuevas amenazas, las cuales se multiplican en igual o mayor velocidad que el avance y la actualización tecnológica. Sumado a los adversarios convencionales como lo podrían ser otros estados mediante sus servicios de inteligencia o criminales comunes que buscan obtener información de las diferentes naciones, hoy se suman el aumento de la dependencia tecnológica (sobre todo en sectores críticos de un país como lo es la defensa) y la incapacidad de entender y controlar su correcto funcionamiento, entre otras cuestiones. Debido a esto podemos afirmar que la criptografía es una herramienta que nos permite dar seguridad a los sistemas que se utilicen, pero no es ajena a poseer vulnerabilidades (como todo aquello desarrollado por el ser humano) ya sean estas, voluntarias o involuntarias.

La historia nos ha enseñado, de la forma menos deseada, que existen temáticas que una nación no puede dejar libradas al azar y en donde no puede confiar ciegamente en un tercero, la criptografía es un claro ejemplo de eso. Desde un punto de vista negativo, resulta evidente nuestra pésima experiencia con la empresa suiza Crypto AG, experiencia en la que se obtuvo información secreta de nuestras comunicaciones a través de equipos de dicha firma, previamente, durante y después del Conflicto del Atlántico Sur y por lo cual quedaron significativamente afectados tanto el desarrollo de las operaciones militares como la misma defensa nacional.

Así mismo en simultaneo como experiencia positiva, pese a tener los equipos de cifrado vulnerados, otra capa de “protección criptográfica”, como lo fue el uso del lenguaje guaraní, permitió mantener a estas fuera del entendimiento del enemigo. No transformar estas experiencias en lecciones aprendidas sería un error de una magnitud grosera y nos pone en una situación adversa descomunal.

La capacidad criptográfica nacional existe, pero se encuentra en esfuerzos desorganizados e individuales que no logran explotar su capacidad en su máximo exponente, parte de materializar

las lecciones aprendidas es lograr establecer una Estrategia Nacional de Criptografía, que nos permita mitigar o eliminar los errores cometidos anteriormente, reduciendo la necesidad de confiar ciegamente en terceros, generando la capacidad de auditar o implementar nuestros propios desarrollos a través de la organización de todos los recursos disponibles, a fin de determinar si estos poseen vulnerabilidades existentes o implantadas.

Si bien es un aspecto que se aclaró no iba a ser profundizado en este trabajo, cabe destacar que la amenaza a la criptografía tradicional próxima o presente es la computación cuántica, la cual dejaría obsoletos los desarrollos actuales. Abordarla con toda una estructura ya establecida, presentaría un escenario favorable y nos colocaría en un lugar privilegiado a nivel internacional en caso de contar con desarrollos propios que aborden dicha cuestión. Tal cual fue el objetivo que se propuso la presente investigación, al delinear una estrategia que emane del más alto nivel de conducción nacional, de manera tal de poder gestionar los recursos necesarios para el logro de dicho objetivo, en los horizontes de mediano y largo plazo.

BIBLIOGRAFÍA

¿Sabías que existen distintos tipos de cifrado para proteger la privacidad de nuestra información en Internet? | Ciudadanía | INCIBE. (2021). Incibe.es.<https://www.incibe.es/ciudadania/blog/sabias-que-existen-distintos-tipos-decifradopara-proteger-la-privacidad>

Ambrojo, J. C. (2004, 12 de febrero). *Hugo Scolnik: “La criptografía debe pensar en la gente común para aplicar la seguridad”*. El País. Recuperado de https://elpais.com/diario/2004/02/12/ciberpais/1076553622_850215.html

ANIMUS. (2023, January 24). Comunicaciones seguras: Métodos Cuánticos y Poscuánticos 2022 - Arsat. Arsat. <https://www.arsat.com.ar/multimedia/comunicaciones-seguras/>

Anónimo. (2023). Máquina Enigma: comunicación codificada. Espacio Fundación Telefónica. Recuperado de <https://espacio.fundaciontelefonica.com/evento/maquina-enigma-comunicacioncodificada/>

Carlos, J., & Díaz, G. (s.f.). Sistemas criptográficos empleados en Hispanoamérica. Recuperado el 21 de septiembre de 2024, de <https://core.ac.uk/download/pdf/38839858.pdf>

Ciberseg. (2021, 16 noviembre). Leyes de cifrado: países con mayores restricciones al cifrado. Ciberseguridad.https://ciberseguridad.com/guias/recursos/leyes-cifrado-paisesmayoresrestricciones/#Estados_Unidos

Consejo Federal de Suiza. (2021, 26 de mayo). Stellungnahme des Bundesrates – Fall Crypto AG.

Cortés, D. E. (s. f.). *Identificación virtual y sociedad* [Opinión]. *Revista Comunicaciones*, N.º 10.

Instituto de Derecho de las Comunicaciones, Facultad de Derecho, Universidad de Buenos Aires. Recuperado de https://www.derecho.uba.ar/rev_comunicaciones/ed010/opinion.htm

El fundador del DC en primera persona. (2023). Departamento de Computación. <https://www.dc.uba.ar/el-fundador-del-dc-en-primera-persona/>

Garabetyan, E. (2019, February 4). Este genio argentino es el responsable de que no te hackeen WhatsApp todos los días. Cronista.com; El Cronista.
<https://www.cronista.com/infotechnology/online/Este-genio-argentino-es-el-responsable-de-queno-te-hackeen-WhatsApp-todos-los-dias-20190204-0014.html>

GPDel. (2020, 2 de noviembre). Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte – Fall Crypto AG. Consejo Federal de Suiza.

Huergo, H. (2023, 21 de abril). *Hugo Scolnik: Una entrevista que me hicieron en el Departamento de Computación de la UBA*. Bit40 Dinos. Recuperado de
<https://bit40dinos.blogspot.com/2023/04/21042023-hugo-scolnik-una-entrevista.html>

Infobae. (2020, 14 de febrero). Cómo la CIA espío a la Argentina durante la guerra de Malvinas y le pasó información a Gran Bretaña. Infobae. <https://www.infobae.com/politica/2020/02/14/como-la-cia-espio-a-la-argentina-durante-laguerrade-malvinas-y-le-paso-informacion-a-gran-bretana/>

Juan Jesús Velasco. (2014, May 20). Breve historia de la criptografía. ElDiario.es.
https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html

Junta Interamericana de Defensa. (2022). *Guía de Ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*. Recuperado de
<https://jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf>

La Voz del Interior. (2023, 22 de junio). ¿Cuál fue la trampa que usó la CIA para espiar a Argentina durante el Plan Condor y la guerra de Malvinas? La Voz del Interior.
<https://www.lavoz.com.ar/politica/cual-fue-trampa-que-uso-cia-para-espiar-a-argentinaduranteplan-condor-y-guerra-de-malvina/>

Landwehr, D. (2024, January 24). El caso Crypto AG: un ‘thriller’ de espionaje durante la Guerra Fría. SWI swissinfo.ch. <https://www.swissinfo.ch/spa/politica/el-caso-crypto-ag-un-thrillerdeespionaje-durante-la-guerra-fr%C3%ada/46218942>

Montes, M., & Penazzi, D. (2019). Yarará and Coral v1. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/specdoc/yarara_and_coral-spec.pdf

Morales Rins, J. (2018). Argentina: Estrategia de Seguridad Nacional y roles de las Fuerzas Armadas. Revista de Estudios en Seguridad Internacional, 4(1), 73–88. <https://seguridadinternacional.es/resi/html/argentina-estrategia-de-seguridad-nacional-y-rolesdelas-fuerzas-armadas/>

Mundo, M. (2020). Informe revelador: El Plan Cóndor fue obra de EEUU en Latinoamérica. MdzOnline; MDZ Online. <https://www.mdzol.com/mundo/2020/2/18/informe-revelador-elplancondor-fue-obra-de-eeuu-en-latinoamerica-63967.html>

NIC Argentina. (s.f.). ¿Qué es criptografía? Recuperado de <https://nic.ar/es/enterate/novedades/que-es-criptografia>

Niss, O., & Compilador. (n.d.). Ciberdefensa y el Ciclo Evolutivo del Ciberespacio. Recuperado el 21 de septiembre de 2024, de <https://citeus.org/ltenv/6-cylcdc-undef.pdf>

Portaltic, & Portaltic. (s. f.). China aprueba una ley nacional de criptografía para regular su uso y gestión. europapress.es. <https://www.europapress.es/portaltic/ciberseguridad/noticiachinaaprueba-ley-nacional-criptografia-regular-uso-gestion-20191028105703.html>

Real Academia Española. (s.f.). Algoritmo. En Diccionario de la lengua española. Recuperado de <https://dle.rae.es/algoritmo?m=form>

Real Academia Española. (s.f.). Criptografía. En Diccionario de la lengua española. Recuperado de <https://dle.rae.es/criptograf%C3%ADa>

Redacción IT NOW. (2024, September 6). Recolección hoy, descifrado mañana: la nueva estrategia de los adversarios. IT NOW. <https://www.itnow.connectab2b.com/post/recoleccionhoy-descifradoamanana-la-nueva-estrategia-de-los-adversarios#:~:text=%C2%BFQu%C3%A9%20es%20Harvest%20Now%2C%20Decrypt,les%20permitir%C3%A1n%20descifrar%20estos%20datos>.

Redacción. (2020, February 19). Crypto AG: la máquina espía suiza que fue utilizada por los regímenes militares de Sudamérica para coordinar el infame Plan Cóndor. BBC News Mundo. <https://www.bbc.com/mundo/noticias-america-latina-51549644>

REGLAMENTO PARA LA ESCRITURA Y CORRESPONDENCIA: NORMAS GENERALES PARA ESCRITURA Y CORRESPONDENCIA (EXPERIMENTAL): Vol. I PARTE (2013.^a ed.). (2013).

Reino Unido. (2021). National Security and Investment Act 2021. <https://www.legislation.gov.uk/ukxi/2021/1264>

República Argentina. (2000, 21 de junio). Decreto N° 437/2000: Modificación del Decreto N° 603/92 en relación con la integración de la Comisión Nacional de Control de Exportaciones Sensitivas y Material Bélico. <https://www.argentina.gob.ar/normativa/nacional/decreto-4372000-63378>

República Argentina. (2024, 16 de julio). Decreto de Necesidad y Urgencia N° 614/2024: Creación de la Secretaría de Inteligencia de Estado y de sus órganos desconcentrados. Boletín Oficial de la República Argentina. <https://www.boletinoficial.gob.ar/#!DetalleNorma/310495>

República Argentina. (s.f.). Ley de Inteligencia Nacional N° 25.520. <https://www.argentina.gob.ar/normativa/nacional/ley-25520>

República Francesa. (s. f.). Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT0000000801164>

Resility. (2024, 14 de agosto). El NIST lanza las primeras herramientas de cifrado para resistir la computación cuántica. LinkedIn. <https://www.linkedin.com/pulse/el-nist-lanza-lasprimerasherramientas-de-cifrado-para-resistir-uzmbe>

Santayana, G. (1905). *The life of reason: Reason in common sense*. New York, NY: Scribner's.

Sciaroni, M. (2024, 2 abril). El arma más letal de los ingleses en Malvinas: cómo descifraban los mensajes en clave de Argentina casi en tiempo real. Infobae. <https://www.infobae.com/sociedad/2024/04/02/el-arma-mas-letal-de-los-ingleses-en-malvinascomo-descifraban-los-mensajes-en-clave-de-argentina-casi-en-tiempo-real/>

Sidhpurwala, H. (2023, noviembre 12). Una breve historia de la criptografía. Red Hat. <https://www.redhat.com/es/blog/brief-history-cryptography>

Sun Tzu. (2020). *El Arte de la Guerra*. Biblioteca Virtual Universal. Recuperado de <https://biblioteca.org.ar/libros/656228.pdf>

TechRepublic. (2023). Big Data: Latest Articles, News & Trends. TechRepublic <https://www.techrepublic.com/topic/big-data/>

Troop Software Factory. (2020). Hugo D. Scolnik | Fundación Konex. Fundacionkonex.org. <https://www.fundacionkonex.org/b2573-hugo-d-scolnik>

Urrea, L. F. (2020). *Historia de la criptografía*. Universidad Católica de Costa Rica. Recuperado de <http://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2130/LEC%20IG%20SIST%200074%202020.pdf?sequence=1&isAllowed=y>