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

Ciberseguridad Nacional en la República Argentina:

Concientización ciudadana

AUTOR: JANINA PEREYRA

DOCENTE DEL TALLER: JOSÉ LUIS PIBERNUS

MAYO 2023

Resumen

La ciberseguridad no solo se trata de asegurar la infraestructura, sino también de analizar tendencias globales, crear conciencia y establecer una infraestructura rápidamente recuperable ante posibles ataques. Por lo tanto, la investigación aborda la siguiente pregunta: ¿Qué información se proporciona a la población en general sobre ciberseguridad en Argentina para fomentar la conciencia, informar y desarrollar conductas preventivas frente a delitos informáticos?

Durante la investigación, se observó que Argentina cuenta con una estrategia nacional de ciberseguridad que aún tiene margen de mejora. Existen esfuerzos aislados pero no consolidados a nivel nacional, y mucho menos coordinados con el sector privado o con otras naciones. Además, se compara la estrategia nacional de ciberseguridad de Argentina y España, identificando los puntos importantes y destacados para responder a la pregunta planteada. También se analizó el estado actual de la estrategia nacional de ciberseguridad de Argentina según las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), que propone un ciclo de vida que un estado debe seguir para lograr una estrategia de ciberseguridad nacional sólida, así como el análisis normalizado de cinco factores importantes que deben ser desarrollados en una estrategia de ciberseguridad nacional.

Por lo tanto, se recomienda que el gobierno argentino revise el ciclo de madurez de una estrategia nacional de ciberseguridad recomendado por la UIT y siga las recomendaciones de la Agencia de Seguridad de la Red y la Información de la Unión Europea (ENISA) para fortalecer su plan completo de ciberseguridad nacional para así desarrollar una sólida cultura de ciberseguridad nacional.

Palabras claves: Estrategia Ciberseguridad Nacional – Concientización ciudadana – Coordinación nacional – Cultura ciberseguridad

Índice

1. Introducción 1

2. Marco teórico 2

3. Diagnóstico 8

3.1 La evolución de la ciberseguridad en Argentina y su comparación con un país relevante como el gobierno de España 10

3.2 Plan vigente de ciberseguridad nacional argentino 14

3.3 Estado actual de ciberseguridad nacional argentina en términos de ciberdefensa 16

3.4 Acciones de concientización por parte del estado a la sociedad argentina en materia de ciberseguridad. 18

4. Propuesta de intervención 20

5. Conclusiones 26

6. Referencias bibliográficas 29

7. Anexos 30

1. Introducción

La concientización de los usuarios es un factor clave en la ciberseguridad del sector privado, y su importancia se extiende también al ámbito nacional. En este sentido, es fundamental mantener al ciudadano como un foco de atención en la estrategia de ciberseguridad, y proporcionarle conocimientos relevantes para que pueda protegerse ante posibles amenazas cibernéticas.

Es responsabilidad del Gobierno nacional garantizar la seguridad del ciberespacio nacional, y para ello, se designa un Sistema Nacional de Ciberseguridad que involucra no solo a los actores gubernamentales tradicionales encargados de la protección de infraestructura crítica y sistemas internos, sino también al sector privado, académico, expertos y representantes de la ciudadanía en general. La participación de todos estos actores es fundamental para lograr una estrategia de ciberseguridad integral y efectiva en el país.

En este sentido, el Estado tiene la responsabilidad de fomentar la conciencia social sobre la importancia de proteger el ciberespacio, comenzando por el individuo. Para lo cual, resulta crucial la formación en la Ley de Protección de Datos Personales (25.326) y la normativa vigente relacionada con la ciberseguridad, así como la capacitación en las técnicas de posibles ataques. De esta forma, se busca que cada ciudadano esté consciente de su responsabilidad en la protección de la información sensible y personal en su identidad en línea y contribuya activamente a la prevención de incidentes de seguridad cibernética.

La presente investigación pretende contribuir a la estrategia nacional de ciberseguridad argentina, como así también realizar aportes académicos como fuente de consulta, generando una descripción del estado actual de la estrategia de ciberseguridad nacional y su espacio de mejora y evolución.

El tipo de abordaje que se utilizó es un enfoque exploratorio y se recopiló información a través de un análisis cualitativo. El enfoque inicial fue descriptivo, y se abordaron conceptos fundamentales de ciberseguridad, seguido por un análisis del estado actual del plan de ciberseguridad nacional argentino. Además, se realizó una comparación con la estrategia nacional actual de ciberseguridad del Gobierno de España, solo como punto de referencia.

Paralelamente se realizaron encuestas a algunos profesionales con trayectoria CISO (Chief Information Security Officer), con la finalidad de conocer sus opiniones respecto a la temática tratada, las mismas se realizaron en formato formulario de preguntas a completar (formato similar al de Google form).

Así mismo, para el desarrollo del diagnóstico se utilizó el siguiente esquema de capítulos:

- La evolución de la ciberseguridad nacional Argentina realizando comparaciones con un país relevante como ser el Gobierno de España para este caso en específico.
- Plan vigente de ciberseguridad nacional argentino
- Estado actual de la Ciberdefensa Nacional
- Acciones actuales de concientización por parte del estado a la sociedad argentina en materia de ciberseguridad.

El propósito de la presente investigación es realizar aportes concretos para mejorar el plan actual de ciberseguridad. La propuesta presentada en este trabajo se considerará como un punto de partida para futuras expansiones.

2. Marco teórico

Se deja enunciado el marco conceptual preliminar a utilizar y a desarrollar en el trabajo de investigación:

• Transformación digital:

> La irrupción de las nuevas Tecnologías de la Información y las Comunicaciones ha significado un punto de inflexión en la historia. Todos los aspectos de la vida humana están atravesados por este fenómeno. "Hoy las personas se comunican, se expresan, se educan, crean, comercian, investigan y desarrollan gran parte de su vida social y laboral en el Ciberespacio." (“ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA”) (Argentina.Gob, 2019, pág. 2)

En la última década, el desarrollo y la potenciación de un entorno de digitalización completa ha llevado a la necesidad de prestar atención a múltiples aspectos. Este proceso ha alcanzado a todos los niveles de ciudadanos, incluyendo aquellos que trabajan en instituciones del estado que interactúan con aplicaciones tecnológicas que manipulan datos de interés nacional. Además, hay sectores de sistemas que desarrollan los softwares de

operación nacional que el estado requiere. Por lo tanto, prestar atención al proceso de construcción y uso de datos se ha vuelto fundamental. La transformación digital ha generado una globalización de interacciones en muchos aspectos positivos, pero conlleva una gran responsabilidad para evitar que organizaciones criminales o terroristas saquen provecho de ella. Estas organizaciones han aumentado su desarrollo y expansión gracias a la globalización digital, que ha eliminado las fronteras.

• **Protección de datos personales**: "Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". ("PROTECCION DE LOS DATOS") (Argentina.Gob, Ley Nacional 25.326 - Art.2, 2000, pág. Art.2)

Actualmente en la Argentina se encuentra vigente la Ley Nacional de Protección de Datos Personales N° 25.326 la cual en su Artículo 1 establece su objeto, el cual tiene como finalidad:

> La protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. (Argentina.Gob, Ley Nacional 25.326 - Art.2, 2000, pág. Art.1)

Asimismo, en su Artículo 2 establece que los datos personales son ''Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables" (Argentina.Gob, Ley Nacional 25.326 - Art.2, 2000, pág. Art.2).

En un entorno de constante evolución tecnológica y globalización, se hace cada vez más necesario prestar atención a la protección de datos personales y a la seguridad del ciberespacio. Muchos países han desarrollado leyes que garantizan la protección de datos personales, pero estas medidas no son suficientes para proteger a la sociedad de posibles amenazas de organizaciones criminales o terroristas. Es importante concientizar a los ciudadanos sobre la importancia de proteger sus datos personales y complementar las leyes existentes con un marco legal amplio que brinde normas claras y accesibles para los ciudadanos en caso de ser necesario. Aunque se han realizado avances en este sentido, el marco legal de protección del ciberespacio nacional requiere ser robustecido para

garantizar una mayor seguridad y protección. En tal sentido, es importante mencionar que actualmente la Agencia de Acceso a la Información Pública presentó el Proyecto de Ley de Protección de Datos Personales en el cual el proyecto de ley introduce nuevas definiciones tales como datos genéticos y biométricos. Además, incorporando nuevas bases legales para el tratamiento de datos personales diferentes al consentimiento.

La actualización de la Ley 25.326 fue en parte como consecuencia de la antigüedad de dicha normativa, con el objetivo de modernizarla manteniendo los derechos y garantías de la Constitución Nacional, pero adaptándolos al contexto actual en medio de nuevas tecnologías y los cambios del derecho comparado, como así también a la inminente necesidad de dar respuesta a los nuevos desafíos que imponen las transformaciones tecnológicas y el desarrollo de la economía digital,

Por último, en los últimos tiempos en América Latina diversos países como Ecuador y El Salvador están avanzando en la construcción de una regulación integral de la privacidad. Brasil y Panamá han aprobado su nueva legislación, mientras que Chile y Uruguay, están trabajando en proyectos de ley acordes con la economía digital y la protección de datos personales (BNAmericas, 2020). Cada uno de los países se encuentra en etapas diferentes. Se espera que en conjunto lograrán contribuir a respetar la privacidad de los usuarios y otorgar seguridad jurídica en su uso.

La transformación digital está sucediendo, de manera que América Latina -como el resto del mundo- también se suma a la necesidad de construir marcos legales que brinden protección a las personas en lo referente al uso de sus datos por parte de las distintas instituciones tanto públicas como privadas.

• **Ciberseguridad:**

> El término "ciberseguridad" pretende describir el conjunto de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, aseguramiento y tecnologías que se pueden usar para proteger la disponibilidad, integridad y confidencialidad de los activos en las infraestructuras conectadas pertenecientes al gobierno, organizaciones privadas y ciudadanos; estos activos incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios digitales, sistemas de telecomunicaciones y datos en el entorno digital. (ITU, 2021, pág. 12)

En una sociedad altamente digitalizada, la seguridad en el ciberespacio adquiere una importancia crucial. Las medidas de seguridad deben abarcar desde el nivel individual de cada ciudadano hasta el nivel nacional e incluso internacional. Es fundamental crear una conciencia permanente en la población, que incluya la visibilización de los riesgos, la capacitación en temas tecnológicos y de seguridad, y la coordinación de acciones tanto a nivel interno como externo con otros países. Dado que el ciberespacio no tiene límites geográficos, contar con una estrategia coordinada entre organismos públicos, privados y de distintas naciones es fundamental para consolidar una estrategia madura de ciberseguridad.

• **Ciberdefensa:**

> El término ciberdefensa se refiere a los componentes militares del Estado que son utilizados para defender el ciberespacio. "En esta línea, la OTAN la define como la habilidad de salvaguardar los sistemas de comunicación y de información en respuesta a acciones potenciales e inminentes que hayan sido o no originadas en el ciberespacio." (“Ciberseguridad y Ciberdefensa en Argentina | CAPSI Arg. | CAPSI”) (Keticoglu, 2020)

A su vez la Directiva de Política de Defensa Nacional de Argentina emitido el 14 de julio de 2021 (Decreto 457/2021) establece las políticas y directrices generales para la defensa nacional, con el objetivo de garantizar la protección de la soberanía, la integridad territorial, la independencia y la libertad de los ciudadanos argentinos.

Entre sus principales objetivos, la Directiva de Política de Defensa Nacional establece el fortalecimiento de las capacidades de las Fuerzas Armadas, la promoción de la cooperación internacional en materia de defensa y seguridad, la implementación de un sistema de defensa integral y la modernización de la industria de defensa nacional. Además, la directiva aborda temas como la ciberseguridad, la protección de datos, la lucha contra el terrorismo y el narcotráfico, y la prevención de conflictos y crisis internacionales. En cuanto a la ciberseguridad, se establecen medidas para proteger la infraestructura crítica, los sistemas y las redes de información del Estado, así como para prevenir y responder a los ciberataques.

• **Ciberseguridad nacional:**

> Las estrategias nacionales de seguridad cibernética pueden tomar muchas formas y pueden entrar en diferentes niveles de detalle, dependiendo de los objetivos y niveles de preparación cibernética del país en particular. Por lo tanto, no existe una definición establecida y consensuada de lo que constituye una Estrategia Nacional de Ciberseguridad. (ITU, 2021, pág. 13)

En el marco Argentino, el Poder Ejecutivo Nacional estableció la segunda Estrategia Nacional de Ciberseguridad (RESOL-2023-1-APN-SDG#JGM) con el objetivo de fijar las previsiones nacionales para proteger el ciberespacio y brindar un contexto seguro para su aprovechamiento. Esta estrategia se llevará a cabo mediante la coordinación y cooperación entre diferentes entidades públicas y privadas. La ciberseguridad es importante porque muchos aspectos de nuestra vida cotidiana dependen de las tecnologías de la información y las comunicaciones, lo que nos expone a amenazas y potenciales daños a los derechos de las personas y las organizaciones. La ciberseguridad es un conjunto de políticas y acciones orientadas a elevar los niveles de seguridad de las personas y las organizaciones frente a amenazas, incidentes y delitos, entre otros, que utilicen como medio y/o fin un dispositivo informático.

Las complejidades que exhibe el ciberespacio y los desafíos que se presentan en la protección del entorno digital frente al avance de nuevas tecnologías, ponen de manifiesto la necesidad de actualización de las estrategias nacionales de ciberseguridad.

A su vez, la evolución del cibercrimen y las grandes organizaciones delictivas, junto con un contexto de ciberguerra sin límites fronterizos, ha aumentado la importancia de que un estado nacional cuente con un sólido desarrollo en ciberseguridad nacional. Esto es clave para proteger los recursos nacionales de posibles intrusiones no deseadas por parte de estas organizaciones criminales, así como para garantizar la seguridad de la nación. Además, es importante tener en cuenta que dentro de estas organizaciones delictivas también hay grupos terroristas que actualmente poseen la capacidad de desatar una ciberguerra con el objetivo de causar daño radical.

• **Ciberespacio:**

> Desde la perspectiva del Derecho Internacional, los Global Commons son aquellos espacios y recursos que se encuentran fuera de la soberanía de cualquier país, esto es, todo el mundo puede acceder a ellos y consecuentemente beneficiarse. Son

> reconocidos como Global Commons los océanos, el espacio aéreo, el espacio ultraterrestre, el Ártico y el ciberespacio. (Instituto Español de Estudios Estratégicos, 2017, pág. 70)

El control de los Global Commons se ha convertido en un objetivo estratégico de primer orden y entre todos ellos el ciberespacio ocupa el primer lugar. El ciberespacio se ha convertido en un objeto codiciado, no solo para los estados, sino también para grupos de crimen organizado y organizaciones terroristas. Estos actores encuentran que sus objetivos pueden lograrse a un costo mucho menor y con un riesgo significativamente reducido en el ciberespacio.

Es importante destacar que el impacto de un ciberataque es extremadamente difícil de medir. La evaluación del daño causado por un incidente de ciberseguridad resulta sumamente compleja debido a la variedad de tipos de ataques, actores y factores involucrados. Con el tiempo, se ha comprendido que no se puede abordar únicamente desde una perspectiva técnica, sino que es necesario considerar tanto el enfoque técnico-táctico como el político-estratégico, tal y como se hace en cualquier ámbito de seguridad.

Es común encontrar que las redes de crimen organizado, organizaciones terroristas e incluso los Estados son los autores detrás de los ciberataques. Sin embargo, las consecuencias de estos ataques pueden ser inesperadas y tener un gran impacto en los principales sectores económicos, las infraestructuras críticas y las administraciones.

Los grupos terroristas no pasan desapercibidos en el ciberespacio, ya que representan una importante amenaza a la seguridad internacional. El ciberterrorismo ha experimentado un salto cualitativo y cuantitativo importante. Los grupos terroristas (EsGlobal, 2016) aprovechan la navegación anónima en la web profunda y en particular, el llamado "internet oscuro" , donde se realizan actividades ilegales en el mercado negro. Desde hace algún tiempo se conocen foros extremistas pertenecientes a grupos terroristas, extremistas y radicales, que se utilizan principalmente para la captación de nuevos miembros o para que los usuarios ofrezcan su apoyo a sus causas.

En este sentido y a modo de ejemplo, la organización terrorista Dáesh ha sabido utilizar las oportunidades que le brinda el ciberespacio para: realizar actividades de propaganda, comunicaciones internas, formación, adoctrinamiento, financiación, reclutamiento y obtención de información como así también realizar ciberataques que causen terror. Como ejemplo específico, el portavoz de Dáesh, Abu Mohammad al-

Adnani, realizó en 2014 un llamamiento difundido a través de las redes sociales que incitaba a sus seguidores a cometer ataques individuales, indiscriminados y empleando cualquier vía. Este mensaje, que se convirtió en viral, ha servido de inspiración para muchos de los ataques que se han producido en el territorio europeo. Desde entonces, Dáesh ha difundido y distribuido, a través de las redes sociales, vídeos de ejecuciones de prisioneros con el objetivo de crear terror. Hasta finales de 2015, el Ministerio del Interior del Gobierno de España estimaba que Dáesh había difundido aproximadamente mil vídeos a través de sus cuentas de Twitter (en esa fecha se contabilizaban entre 35.000 y 75.000 cuentas gestionadas directamente por Dáesh). El 16 % de estos vídeos muestran la ejecución de rehenes y en total se habría mostrado al público el asesinato de más de mil quinientas personas.

3. Diagnóstico

Al examinar detenidamente la relevancia de contar con un plan nacional de ciberseguridad integral y completo, es importante considerar los últimos acontecimientos desde diversas perspectivas, especialmente tras la pandemia que ha resaltado la importancia de este tema.

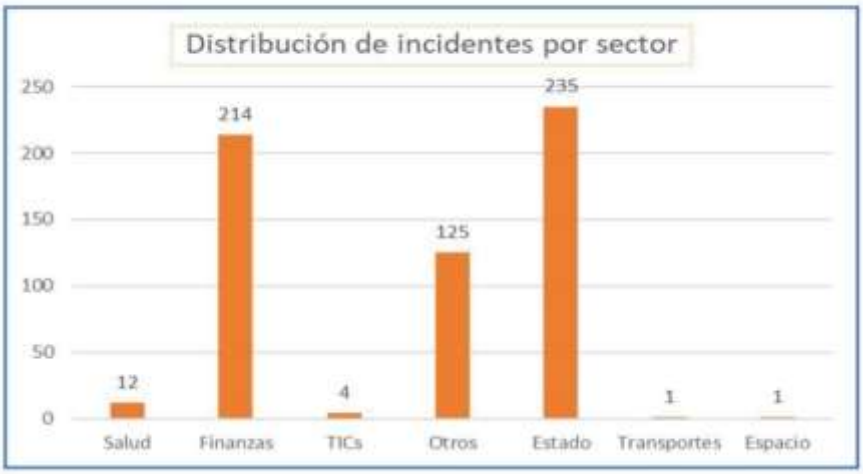
Por ejemplo, en el informe anual que elabora el Equipo de Respuesta ante Emergencias Informáticas nacional (CERT) destaca que durante el 2021 el ransonware y el phishing fueron los incidentes informáticos más reportados. Siendo el estado el más afectado por incidentes informáticos y segunda instancia el sector financiero. Como se puede apreciar en el siguiente gráfico:

Gráfico 0: Informe anual de incidentes de seguridad informática registrados en 2021

Fuente: CERT

Año de publicación: 2021

Distribución anual de incidentes por sector.



En el mismo informe destaca: “Haciendo un análisis anual, el sector más comprometido de acuerdo con los incidentes reportados fue el Estado con 235 incidentes, cifra que representa el 39,70% del total registrado en el 2021”. (CERT, 2021, pág. 3).

Los tipos de incidentes más reportados en el estado fueron:

- Modificación no autorizada de la información: 79 incidentes, cifra que representa el 33,62% del total de los casos estatales.
- SPAM: 54 (22,98%).
- Phishing: 39 (16,60%).
- Sistemas vulnerables: 24 (10,21%).

En este marco mencionado es que el estado toma conciencia para robustecer la estrategia nacional de ciberseguridad según menciona el mismo informe:

> En cuanto al del Estado, la inmediatez de implementar el teletrabajo y otras alternativas laborales surgidas por la pandemia, para continuar brindando servicios a la ciudadanía, no permitieron la preparación necesaria de los recursos de información para ser accedidos de esta forma online, ni la concientización adecuada, masiva, acerca de la posibilidad de incidentes de seguridad. (CERT.ar, 2021, pág. 2)

Si bien es positivo afirmar que se necesita una mayor concienciación y preparación en cuanto a recursos informáticos, es importante tener en cuenta que existen otros aspectos relevantes que serán abordados en los siguientes puntos.

3.1 La evolución de la ciberseguridad en Argentina y su comparación con un país relevante como el gobierno de España

La Estrategia Nacional de Ciberseguridad en España comenzó en el año 2013 (España P. d., 2013) basada en los siguientes principios:

- Un enfoque integral de la ciberseguridad, que implica la coordinación de todos los actores involucrados, tanto públicos como privados.
- La prevención, detección y respuesta temprana ante incidentes de ciberseguridad.
- La protección de la información clasificada y de los sistemas críticos.
- La promoción de la investigación, el desarrollo y la innovación en ciberseguridad.
- La cooperación internacional en la lucha contra las amenazas cibernéticas.
- El respeto a los derechos y libertades fundamentales en el ámbito digital.

Estos principios se han ido actualizando en las diferentes versiones de la Estrategia Nacional de Ciberseguridad de España para adaptarse a los cambios tecnológicos y a las nuevas amenazas.

El ciberespacio plantea desafíos que requieren no solo un liderazgo nacional, sino también una coordinación precisa de capacidades, recursos y competencias. En el marco de la responsabilidad compartida, resulta importante que todos se encuentren involucrados en esta estrategia de ciberseguridad nacional para coordinar iniciativas y generar los ámbitos requeridos para compartir información. Cuando se menciona todos, hace referencia a los múltiples organismos del ámbito público, privado, incluyendo también a los propios ciudadanos. El sentido de encontrarse todos involucrados resalta la importancia de gestionar los riesgos derivados del uso de la tecnología, equilibrando oportunidades y amenazas, asegurando la proporcionalidad en las medidas de protección adoptadas.

En al año 2019 el segundo documento sobre Estrategia Nacional de Ciberseguridad de España ampliará este concepto, al incluir:

> El ciberespacio es un espacio común global caracterizado por su apertura funcional y dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también

presenta serios desafíos a la seguridad. (“BOE-A-2019-6347 Orden PCI/487/2019, de 26 de abril, por la que se ...”) (España.Gob, 2019, págs. 17-18)

Y a su vez en este segundo documento refuerza y agrega el impacto de este riesgo en la estructura nacional:

"Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones." (“BOE-A-2019-6347 Orden PCI/487/2019, de 26 de abril, por la que se ...”) Afectan a la totalidad de los ámbitos de la Seguridad Nacional, como son la Defensa Nacional, la seguridad económica, o la protección de infraestructuras críticas, entre otros, y no distinguen fronteras" (España.Gob, 2019, págs. 23-24)

El objetivo IV de la Estrategia de Ciberseguridad Nacional de España es: sensibilizar a los ciudadanos, profesionales, empresas y administraciones públicas españolas de los riesgos derivados del ciberespacio. Asimismo, especifica claramente que: la gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere en los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios. Dentro del mismo plan, se ha aprobado el plan de cultura de ciberseguridad, concienciación, sensibilización y educación, cuyo objetivo es: promover la cultura de ciberseguridad entre ciudadanos, profesionales, empresas y administraciones públicas españolas mediante el desarrollo de actividades y mecanismos para la sensibilización, concienciación, formación y educación que renueven y doten de nuevos conocimientos sobre los riesgos derivados del ciberespacio y el uso seguro y responsable de las Tecnologías de la Información y las Comunicaciones (TIC). El Plan se articula en tres ejes de acción: sensibilización, concienciación y conocimiento; normativa y buenas prácticas. Cada eje tiene asignado un organismo de la Administración pública como responsable y otros como colaboradores. Asimismo, se contemplan unos recursos financieros y humanos para poderlo llevar a cabo.

En España, otra institución muy dinámica en el ámbito de la ciberseguridad es el Instituto Nacional de Ciberseguridad (INCIBE), el cual ha puesto en marcha diversas iniciativas dirigidas tanto a empresas como a ciudadanos. En el ámbito específico del programa de sensibilización, concienciación, educación y formación definido por el plan de confianza digital y la Estrategia de Ciberseguridad Nacional, desde el año 2015 INCIBE lleva a cabo el proyecto Servicio de Creación, mejora y soporte de contenidos de ciberseguridad y confianza digital dirigido a las empresas y ciudadanos. La Oficina de

Seguridad del Internauta (OSI) es una de sus principales iniciativas en este ámbito. Es una oficina que ofrece materiales, herramientas y buenas prácticas. Cabe destacar, por ejemplo, el kit de concienciación que INCIBE ha desarrollado y ha puesto a disposición de las empresas. Dicho kit propone una serie de prácticas y materiales a distribuir. La primera fase, por ejemplo, consistió en lanzar un ciberataque dirigido, dentro de la empresa, con un fichero infectado con malware inocuo y cuyo vector de infección sería el correo electrónico o una memoria USB. INCIBE incluso propone los mensajes y ficheros a utilizar. Una vez realizada esta primera fase, se pasó a una fase formativa en la que se distribuyen materiales como pósteres o trípticos, que también han sido preparados por INCIBE. Se dio continuidad posteriormente a esta tarea mediante consejos de ciberseguridad de periodicidad mensual.

Respecto a Argentina, comienza sus primeros pasos en el año 2011 con la creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad por medio de la resolución 580/201, por medio de la cual se sienta el marco para diseñar las leyes requeridas, se define ámbito de aplicación y la coordinación que requiere. Sin embargo en este sentido existe un foco en las infraestructuras críticas.

En los años subsiguientes se realizaron diversas resoluciones que organizaron los ámbitos de pertenencias y responsabilidades de diferentes secretarías y ministerios hasta llegar a la Resolución 829-2019 donde se aprueba la estrategia nacional de ciberseguridad Argentina.

Recientemente en enero de 2023 el Poder Ejecutivo Nacional Argentino aprueba mediante la resolución 1/2023 la segunda estrategia de ciberseguridad nacional establece mediante la misma cinco objetivos prioritarios:

- El primer objetivo es aumentar la conciencia y la capacitación en ciberseguridad a nivel nacional, desarrollando planes y recursos humanos especializados en el área.
- El segundo objetivo es actualizar el marco normativo para hacer frente a los desafíos que plantea el ciberespacio, protegiendo los derechos fundamentales.
- El tercer objetivo es fortalecer las capacidades de prevención, detección y respuesta frente a ciberataques y amenazas en el ciberespacio.
- El cuarto objetivo es garantizar un adecuado nivel de seguridad y recuperación de los sistemas de información del Sector Público.

- El quinto objetivo es promover el desarrollo de la industria nacional en los sectores relacionados con la ciberseguridad.

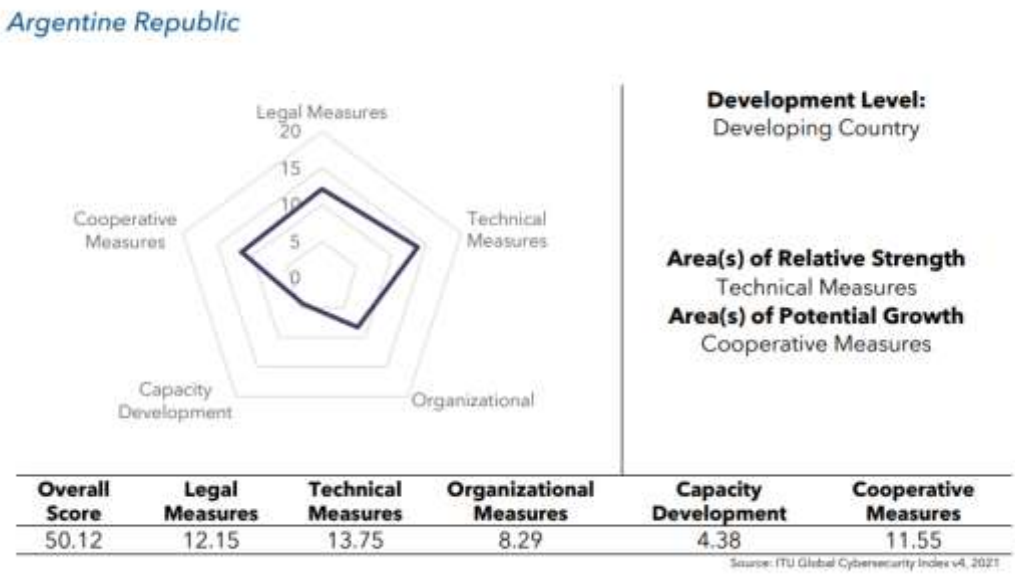
El informe Global Cybersecurity Index v4, 2021 desarrollado por International Telecomunication Union (ITU), comenta la metodología y pasos importantes a seguir para desarrollar una estrategia de ciberseguridad del estado. Se tomaron solo datos vinculados a España y Argentina a modos de comparación y ejemplo a los efectos de la presente investigación. En el informe queda definido el margen de mejora existente en la estrategia Nacional Argentina en términos de capacidades y por otra parte mejorar el resto de aristas como ser: mayor generación de medidas en el marco legal, cooperación internacional, entre otros. Argentina categorizado como Developing Country en el informe posee un Score 50,12, en cambio España categorizado como Developed Country cuenta con un score de 98,52.

Gráfico 1: Informe Global Cybersecurity Index v4

Fuente: International Telecomunication Union

Año de publicación: 2021

El siguiente gráfico muestra el estado de madurez de los países en su estrategia nacional de ciberseguridad analizado por la International Telecomunication Union (ITU). Para evaluar el estado de madurez se analizan 5 dimensiones importantes. Las mismas lanzan un puntaje que deja visible en datos concretos el estado de madurez de cada país.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
50.12	12.15	13.75	8.29	4.38	11.55

Source: ITU Global Cybersecurity Index v4, 2021

Spain

Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development, Technical Measures

Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

La principal diferencia entre ambas estrategias nacionales de ciberseguridad radica en el marco de comunicación y en la asignación de recursos para la ejecución.

3.2 Plan vigente de ciberseguridad nacional argentino

Las acciones primarias que tiene la Dirección Nacional de Ciberseguridad comprenden tanto aquellas que fueron creadas para entender en los aspectos relativos a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional. (“Objetivos de la Dirección Nacional de Ciberseguridad”)
(Argentina.Gob, s.f.) (Argentina.Gob, s.f.)

- "Diseñar políticas de ciberseguridad, en coordinación con los organismos del Estado Nacional con competencia en la materia." (“Objetivos de la Dirección Nacional de Ciberseguridad”)
- Elaborar planes, programas y proyectos con perspectiva federal en materia de ciberseguridad, en el ámbito de competencia de la Secretaría de Innovación Pública.
- Participar en las acciones destinadas a implementar los objetivos fijados en la Estrategia Nacional de ciberseguridad, articulando proyectos con las diferentes áreas del Estado Nacional involucradas.

- Asistir a la Secretaría en su participación ante el Comité de Ciberseguridad creado por Decreto N° 577/17 y sus modificatorios y colaborar en la ejecución de las decisiones que se adopten.
- Proponer proyectos de normas relacionados con la ciberseguridad en la República Argentina, en coordinación con las áreas con competencia en la materia.
- Analizar las vulnerabilidades de software en la Administración Pública Nacional, así como también definir las Infraestructuras Críticas de Información, incluyendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes cibernéticos y de seguridad informática.
- Desarrollar el Programa Nacional de Infraestructuras Críticas de la Información, así como incorporar en la Administración Pública Nacional buenas prácticas y experiencias internacionales exitosas en la materia.
- Impulsar y promover la resiliencia de los sistemas definidos como críticos en el Sector Público Nacional.
- Intervenir en la formulación y ejecución de planes de capacitación en materia de ciberseguridad en el ámbito de la Administración Pública Nacional.
- Colaborar, junto a organismos y centros de investigación públicos y privados, en la promoción de planes, programas y proyectos de innovación tecnológica en materia de ciberseguridad, en coordinación con los organismos competentes en la materia.
- "Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL)." (“Texto completo ”)
- Administrar el registro de equipos de respuesta ante incidentes de seguridad informática.

Se realizaron y dieron curso a varios de los objetivos planteados por la dirección nacional de ciberseguridad como ser el CERT NACIONAL, un registro de incidentes de seguridad informática, colaboración directa en propuesta de normas, entre otros. Pero aún queda profundizar, para crear una consolidación total de la estrategia de ciberseguridad nacional Argentina.

Por otra parte se destaca la normativa vigente a la fecha relacionada a la estrategia de ciberseguridad (Argentina.Gob, 2022):

Leyes relacionadas a la ciberseguridad:

- Ley 26.388 de Delito informático

- Ley 25.326 de Protección de Datos Personales
- Decreto Reglamentario N° 1558/2001
- Ley 25.506 de Firma Digital
- Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming

Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras críticas de la información y ciberseguridad:

- Decisión Administrativa 641/2021. "Establece los requisitos mínimos de seguridad de la información para organismos públicos" (“Normativa - Ciberseguridad ”)
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.

Otras normativas relacionadas a la ciberseguridad

- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Decreto 480/2019. Modificación del Decreto 577/2017.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad.

3.3 Estado actual de ciberseguridad nacional argentina en términos de ciberdefensa

El Decreto 1714/2009 (Boletín Oficial, 2009) de Argentina establece el régimen de protección de la seguridad de la información en el ámbito del Sector Público Nacional. Este decreto establece que los organismos del Sector Público Nacional deben implementar medidas de seguridad de la información en sus sistemas, procesos y operaciones que permitan proteger la confidencialidad, integridad y disponibilidad de la información que manejan. Además, el decreto establece la obligación de los organismos públicos de designar un Responsable de Seguridad de la Información, quien será el encargado de

planificar, coordinar y supervisar la implementación de las medidas de seguridad de la información en el organismo. También se establecen medidas específicas de seguridad que deben ser implementadas, como la protección de los sistemas informáticos, la gestión de contraseñas, la protección de la información clasificada, entre otras.

En las últimas décadas, el ciberespacio se ha convertido en un aspecto crucial para las operaciones militares. Varios países han redirigido sus esfuerzos y recursos hacia la protección no solo de los espacios tradicionales como el terrestre, marítimo y aeroespacial, sino también del espacio cibernético. En este sentido, el Decreto 457/2021 establece la importancia de considerar la dimensión de la defensa relacionada con el ciberespacio, introduce cuestiones conceptuales y precisas sobre la Tecnología de la Información, la operación y la comunicación, el ciberespacio y la ciberdefensa como dimensiones a considerar en la Defensa Nacional. El ámbito del ciberespacio ha generado cambios en las categorías tradicionales de la "guerra real", lo que ha requerido una rápida adaptación por parte de los sistemas de defensa. En las últimas décadas, muchos países han redirigido sus esfuerzos y recursos para proteger su espacio ciberespacial. Una de las principales características del ciberespacio es que, aunque tiene sus propios medios y reglas, no es un "espacio en sí mismo", sino una dimensión que atraviesa todos los espacios tradicionales (tierra, mar, aire y espacio). Las acciones de ciberguerra pueden tener impacto en el mundo físico, lo que se evidencia en precauciones en áreas como el tráfico aéreo y terrestre, el control de infraestructuras críticas, el abastecimiento de energía y agua potable, las comunicaciones militares y la capacidad de comando y control, entre otros.

En este contexto, el mismo decreto menciona que la disolución de la Unión de Naciones Suramericanas (UNASUR) y el Consejo de Defensa Suramericano (CDS) ha dejado vacíos importantes en cuanto a la cooperación, el diálogo y la coordinación en la región. Destaca también que es crucial fomentar la reconstrucción de mecanismos similares para restablecer los intercambios y la formación profesional combinada de las fuerzas armadas de la región, promover la creación de espacios que estimulen los consensos doctrinarios y operativos, y aumentar la interoperabilidad entre las fuerzas armadas.

La Resolución Nro. 105/2023 firmada en enero de 2023 se enmarca en la Directiva de Política de Defensa Nacional (DPDN), que establece los lineamientos de orientación y planeamiento estratégico de la Política de Defensa y de la Política Militar de la República

Argentina. (“Actualización de la Política de Ciberdefensa y creación de dos áreas ...”) entre los considerandos de esta disposición, se destaca la importancia de:

> La ciberdefensa debe minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del ciberespacio en las operaciones militares que realice el instrumento militar en cumplimiento de la normativa vigente en materia de Defensa Nacional. (“Actualización de la Política de Ciberdefensa y creación de dos áreas ...”) (Boletín Oficial, 2023)

Mediante la resolución mencionada se han creado dos instrumentos clave para proteger el ciberespacio de la Defensa Nacional en Argentina. El primero es el Comité de Infraestructuras Críticas de la Información de la Defensa, encargado de identificar los Activos Digitales Críticos que soportan el funcionamiento normal de las Infraestructuras Críticas del Sistema de Defensa Nacional. (“Actualización de la Política de Ciberdefensa y creación de dos áreas ...”) El segundo es el Centro de Supervisión y Control de Gestión de Ciberdefensa, que tiene como objetivo centralizar y gestionar la información y prevención de incidentes cibernéticos en la jurisdicción. Para garantizar una implementación eficaz de estas políticas, estas nuevas áreas estarán bajo la órbita de la Subsecretaría de Ciberdefensa, que coordinará y supervisará los trabajos de los organismos correspondientes del Estado Mayor Conjunto de las Fuerzas Armadas y de los Estados Mayores del Ejército, Armada y Fuerza Aérea en materia de seguridad en el ciberespacio. (“Actualización de la Política de Ciberdefensa y creación de dos áreas ...”)

3.4 Acciones de concientización por parte del estado a la sociedad argentina en materia de ciberseguridad.

Según menciona (Vaninetti, 2021) desde que los delitos son cada vez más violentos y las organizaciones criminales se encuentran cada vez más constituidas junto con la amenaza latente de actos terroristas, hacen pensar que para encontrar más seguridad se debe tolerar tener menos libertad y/o privacidad. En este sentido hace difícil vislumbrar la peligrosidad de esta limitación. Ya que un estado de hipervigilancia avasallante que no cuenta con un debido respeto a los derechos personalísimos cumpliendo estrictos controles sobre las restricciones legales correspondientes pueden generar un efecto no deseado.

Incorporando la cita textual de la (Ley N°25.326 /Decreto Reglamentario 1558, 2001) “Los ciudadanos tienen derecho a la libertad de expresión, al acceso a la información, a la privacidad de las comunicaciones y a la seguridad de sus datos. Poseen

además todos los derechos y libertades contemplados en los tratados internacionales en materia de derechos humanos y comunicaciones personales reconocidos por la Constitución Nacional de la República Argentina.” Si complementamos los derechos de la ciudadanía declaradas desde el poder nacional (Derechos de la ciudadanía, s.f.) encontramos más ensuciados específicos como ser: poder denunciar un delito informático, libertad para acceder a la web y a las distintas plataformas digitales, libertad de expresión, información y comunicación digital, entre otras.

Indagando en las acciones del estado nacional en lo que respecta a concientización nacional ciudadana en términos de ciberseguridad encontramos en la página nacional (Recomendaciones, s.f.) como acciones visibles del estado nacional informes desarrollados como por ejemplo:

- Guía de recomendaciones para compras seguras por Internet
- Resguardo de información personal
- Protege tu cuenta en redes.
- Grooming: acoso infantil
- Extorsiones digitales
- "El ransomware, el software malicioso usado para atacar a las organizaciones" (“El Ransomware El Software Malicioso Usado para Atacar A Las ... ”)
- Botnets. Una guía y un glosario para entender su funcionamiento
- Phishing. Una guía y un glosario para conocer sus modalidades y prevenirlas.
- Delitos informáticos relevados durante la pandemia, descripción y recomendaciones para evitarlos
- Recomendaciones generales de ciberseguridad

Avanzando en ciudades específicas como ser la Ciudad Autónoma de Buenos Aires para conocer también el contenido de concientización ciudadana se encuentra el BA-Csirt – Centro de ciberseguridad ciudadana https://bacsirt.buenosaires.gob.ar/. El cual se encuentra bastante nutrido, con información variada, desde cómo reportar un incidente, conocer las novedades de la semana en términos de ciberseguridad, hasta capacitaciones específicas para consolidar conceptos importantes.

4. Propuesta de intervención

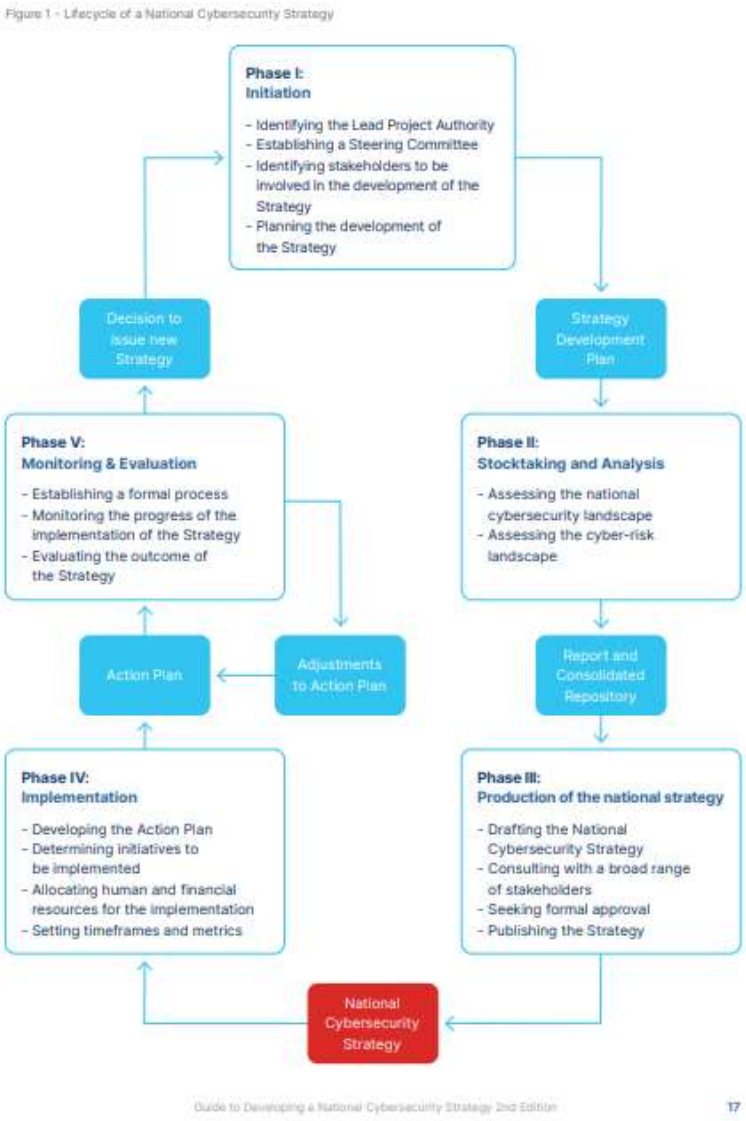
Dado que el plan de ciberseguridad nacional argentino aún contaría con espacio para robustecerse entonces existe margen de mejora en las estrategias de concientización ciudadana masiva tal como se fue recorriendo en los puntos anteriores. Ante este evento resulta de vital importancia realizar una reevaluación del estado actual del plan de ciberseguridad nacional, tomando de guía los procesos para el desarrollo de una estrategia de ciberseguridad nacional planteados en NCS Guide el cual se deja expresado el proceso que define la (ITU, NCS-Guide – Page 17, 2021):

Gráfico 2: NCS-Guide

Fuente: International Telecomunication Union

Año de publicación: 2021

A continuación se presenta el gráfico que ilustra el ciclo de vida que debería ser seguido por un país para desarrollar una estrategia de ciberseguridad nacional sólida:



Si se revisa el informe (ITU, NCS-Guide – Page 28, 2021), se encontrarán nueve principios generales para una estrategia de ciberseguridad nacional:

- Establecer una visión clara de todo el gobierno y toda la sociedad.
- Debe ser el resultado de una comprensión y un análisis integrales del entorno digital general, pero debe adaptarse a las circunstancias y prioridades del país.
- Debe desarrollarse con la participación activa de todas las partes interesadas relevantes, y debe abordar sus necesidades y responsabilidades.
- Debe fomentar la prosperidad económica y social y maximizar la contribución de las TIC al desarrollo sostenible y la inclusión social.
- Debe respetar y ser coherente con los derechos humanos fundamentales

- Debe permitir una gestión eficiente de los riesgos de ciberseguridad e impulsar la resiliencia de las actividades económicas y sociales.
- Debe utilizar los instrumentos de política disponibles más apropiados para lograr cada uno de sus objetivos, considerando las circunstancias específicas del país.
- Debe establecerse al más alto nivel del gobierno, que luego será responsable de asignar las funciones y responsabilidades pertinentes y asignar suficientes recursos humanos y financieros.
- Debería ayudar a construir un entorno digital en el que los ciudadanos y las organizaciones puedan confiar.

El último principio enunciado es uno de los más importantes y relevantes para el marco argentino.

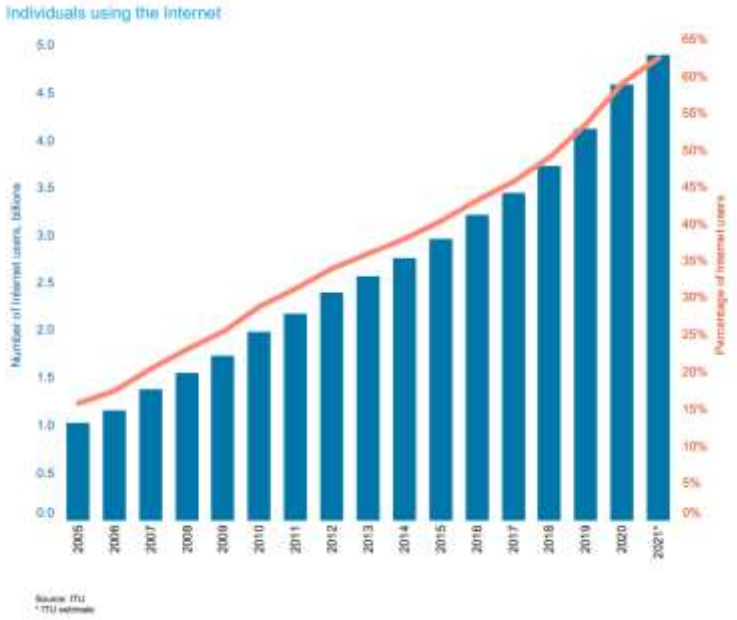
Durante mucho tiempo, Internet ha sido considerado una fuente de innumerables oportunidades para el desarrollo personal, profesional y la creación de valor. Con la pandemia de COVID-19, se ha convertido en una necesidad vital para trabajar, aprender, acceder a servicios básicos y mantenerse en contacto. Tal como se menciona en el informe, es evidente el aumento en el uso de Internet por parte de la ciudadanía en general a nivel global. (ITU, Measuring digital development Facts and figures - Page 1, 2021):

Gráfico 3: Measuring digital develpment Facts and Figures

Fuente: International Telecomunication Union

Año de publicación: 2021

El siguiente gráfico muestra como ha evolucionado la cantidad de usuarios de internet en los últimos 15 años, medidos en billones de personas.



Dentro de los informes elaborados por la ITU, existe un punto de gran importancia para el Estado Argentino que aún no se encontraría consolidado. El informe (ITU, NCS-Guide – Page 46, 2021) menciona una de las buenas prácticas marcadas dentro de la guía para una estrategia nacional de ciberseguridad:

> Implementar un programa coordinado de concientización sobre seguridad cibernética. Las entidades responsables de las campañas y actividades de concientización sobre seguridad cibernética a nivel nacional deben colaborar con las partes interesadas relevantes para desarrollar e implementar programas de concientización sobre seguridad cibernética que se centren en difundir información sobre los riesgos y amenazas de seguridad cibernética, así como sobre mejores prácticas para contrarrestarlos. Un programa de concientización sobre ciberseguridad podría incluir campañas de concientización dirigidas al público en general, niños, programas de educación centrados en el consumidor con desafíos digitales e iniciativas de concientización, entre otros, dirigidas a ejecutivos de los sectores público y privado. Los programas de concientización deben incluir KPI y métricas relevantes para medir el impacto y la efectividad. (ITU, NCS-Guide – Page 46, 2021)

Para dar otro ejemplo relacionado con un grupo específico de alto riesgo y exposición, el informe (ITU, Global Cybersecurity Index - Page 16, 2020) señala lo

siguiente: realizar campañas de concientización pública para personas con discapacidad y personas mayores. Por mucho que Internet y el mundo digital brinden oportunidades sin precedentes, la mayoría de las veces las personas con discapacidad y las personas mayores no son consideradas cuando se toman decisiones operativas y opciones tecnológicas. Se estima que hay 752 millones de personas de 65 años o más en 2021. Al comparar esta cifra con la cantidad de países con campañas de concientización enfocadas en personas con discapacidad y personas mayores, el resultado es significativamente bajo. De 194 países, solo el 18 % estaba creando conciencia sobre las personas con discapacidad y el 25 % realizaba campañas para las personas mayores. El pequeño número de países comprometidos en crear conciencia sobre estas dos poblaciones específicas es alarmante, ya que crea una brecha digital significativa, teniendo presente que se insta a las personas con discapacidad y a las personas mayores a utilizar los servicios digitales, como las aplicaciones de rastreo de contactos de COVID-19.

La esencia de las personas es a menudo olvidada en las estrategias de concientización. En general, estas estrategias se enfocan en los empleados o ciudadanos, sin visualizar que son lo mismo. Todos los individuos establecen patrones de comportamiento que influyen tanto en su vida personal como en la profesional. Por lo tanto, es esencial que las personas (en sentido completo) comprendan el problema y adopten estándares de comportamiento que mejoren su nivel de seguridad cibernética, y con ello, el de las organizaciones en las que participan.

La tecnología de los hogares conectados en la actualidad es cada vez más compleja. Las previsiones con el despliegue masivo de IOT es que se multipliquen los dispositivos útiles gestionados por cada unidad familiar, llegando incluso según previsiones recientes a tener que manejar cientos de direcciones IP en una red de un hogar avanzado. Las previsiones hablan de 500 IP. Actualmente, de manera intuitiva y a nivel casero, uno de los miembros de la unidad familiar ejerce labores que ejercería un jefe de la información y un jefe de la seguridad (CIO y CISO), desplegando la tecnología que el hogar necesita y vigilando de la forma que puede y sabe la seguridad de su entorno tecnológico. Ese CIO y CISO en funciones no tiene especial formación tecnológica y, si bien puede ser un usuario de la tecnología, actualmente no tiene suficiente formación o conocimiento para ejercer de manera responsable de seguridad de su hogar. Muchas veces no sabe realmente a lo que se enfrenta.

A continuación, se mencionan unos pocos ciberataques que tomaron estado público (Threatpost / ZDNet/ Cybersecurity Ventures, 2021). Estos son solo algunos ejemplos de los ciberataques recientes en Argentina, pero desafortunadamente hay muchos más casos de ataques exitosos o intentos de ataques que no se hacen públicos:

- Enero 2021: se produjo un ataque a la página web de la Ciudad de Buenos Aires, que fue hackeada y se mostró un mensaje en el que se pedía la liberación de una persona detenida.
- Febrero 2021: hubo un ataque de ransomware que afectó a la empresa alimentaria Molinos Río de la Plata, que tuvo que cerrar temporalmente sus operaciones.
- Marzo 2021: se produjo un ataque de ransomware contra la compañía de transporte y logística Andreani, que también se vio obligada a detener temporalmente sus operaciones.
- Marzo 2021: se reportó un ataque cibernético masivo en Argentina y otros países de América Latina, que afectó a varias empresas, incluyendo bancos, aerolíneas y servicios de telecomunicaciones. El ataque consistió en un ransomware que cifraba los archivos de los sistemas afectados y pedía un rescate para su liberación.
- Abril 2021: el sitio web de la Cámara Argentina de Empresarios Mineros (CAEM) fue hackeado y se publicaron datos de usuarios.
- Abril 2021: el Ministerio de Desarrollo Social de la provincia de Buenos Aires sufrió un ataque de phishing que resultó en la filtración de información de los beneficiarios del programa alimentario.
- Abril 2022: el Banco de la Ciudad de Buenos Aires sufrió un ataque cibernético que afectó a su sistema de banca online, resultando en la exposición de información de sus clientes.
- Abril 2021: se detectó un ataque cibernético contra el Ministerio de Salud de Argentina, en el que se accedió a información confidencial relacionada con la pandemia de COVID-19.
- Mayo 2021: la plataforma educativa virtual del Ministerio de Educación de la Nación sufrió un ataque que afectó a la información de los estudiantes y docentes.

- Mayo 2021: se produjo un ataque a la empresa de telecomunicaciones Telecom Argentina, que afectó a su servicio de internet y causó problemas de conectividad en todo el país.

Por otra parte el último informe del CERT.ar publicado en 2022 (CERT.ar, 2022) informa que durante el año 2022 el registró un total de 335 incidentes informáticos. La cifra da cuenta de una disminución del 46% respecto a la del año 2021, en el que se registraron 591 incidentes de los cuales:

- El phishing como intento de fraude representó el 72% del total de incidentes reportados, siendo el delito informático que más se registró en 2022. De esta manera, el sector Finanzas fue el más comprometido de acuerdo a los reportes: hubo un total de 185 incidentes (el 39% del total registrado en 2021). (“Informe de Gestión CERT.ar 2022 ”)
- "El Estado continúa siendo uno de los más atacados con un total de 71 incidentes críticos reportados" (“Informe de Gestión CERT.ar 2022 ”)

Existe una recomendación que realiza la European Union Agency for Network and Information Security (ENISA), la misma es formar una Public Private Partnership (PPP) según su definición:

> “Una PPP queda definida como una relación organizada entre organizaciones públicas y privadas, en la que se establece un ámbito y objetivos en común y define unos cometidos y metodología de trabajo para alcanzar la finalidad compartida” (Instituto Español de Estudios Estratégicos, 2017, pág. 241)

En una organización de este estilo es requerido definir su marco legal, por ejemplo en España la ley que dá marco a esta organización es la Ley 40/2015.

5. Conclusiones

Dada la situación actual, se puede confirmar que el Estado argentino tiene un largo camino por recorrer en términos de consolidar un plan de ciberseguridad efectivo. La pandemia ha expuesto las vulnerabilidades en sistemas críticos y la falta de preparación y conciencia del personal del Estado y la ciudadanía para trabajar de manera remota. Es vital realizar una reevaluación general de la madurez para fortalecer los puntos débiles de manera coordinada. El estado argentino mostró en el último año señales concretas de evolución del plan nacional de ciberseguridad, resta camino de coordinación y articulación

entre los ámbitos estatales y privados para lograr cohesión y efectividad con evolución continua.

La concientización ciudadana es un área crítica que necesita mucha atención. Para mejorar la gestión de los recursos disponibles a nivel nacional, es necesario crear un catálogo nacional de ciber ejercicios que identifique las áreas deficitarias y las potencie tanto en el sector público como en el privado. Estos ejercicios deben promover la participación de ambos sectores a través de una planificación coordinada a nivel nacional. En este sentido, es esencial generar mecanismos más visibles, como propaganda y canales de mensajería en línea para comunicar eventos relevantes de ciberamenazas, posibles intrusiones, últimos ciberataques, siempre incluyendo mensajes de cómo el ciudadano puede colaborar y protegerse fomentado el desarrollo de una cultura de la ciberseguridad. La estrategia de concientización nacional debe ser homogénea y abordar las diferencias entre el contenido nacional y local. También debe tener una gestión coordinada y existir comunicación fluida entre ámbito público, privado y también escuelas.

El Estado debe ser el gran sponsor y facilitador en consolidar tres puntos clave: difundir mensajes a las personas (en todos sus roles: ciudadano-empleado), brindar el apoyo institucional y asignar los recursos necesarios para desarrollar planes alineados con los intereses del Estado. En este sentido la presente investigación propone que el estado impulse el armado de un organismo PPP (Public Private Partnership), definiendo su marco legal de acción con el objetivo de definir las líneas de trabajo requeridas para la concientización ciudadana que garanticen el éxito.

De esta manera se fomenta el desarrollo de una cultura de ciberseguridad[1] a nivel nacional. Se trata de crear una mentalidad de seguridad informática en todas las áreas de la vida y motivar a las personas a tomar medidas proactivas para protegerse y proteger su información personal, siendo parte responsable e involucrada.

Esta investigación es un punto de partida para fortalecer el plan vigente, tomando en cuenta procedimientos internacionales recomendados. La gestión de vulnerabilidades nacionales, la revisión frecuente y la prueba de sistemas críticos nacionales son otros aspectos importantes de la estrategia nacional de ciberseguridad que se deben explorar. Los

[1] La cultura de ciberseguridad refiere a la conciencia, conocimiento y prácticas relacionadas con la seguridad informática en una organización o sociedad. Para fomentarla, se deben educar a las personas sobre las mejores prácticas de seguridad informática, implementar herramientas de seguridad y políticas de seguridad, y fomentar una cultura de transparencia y responsabilidad.

informes y guías de ITU son una fuente sólida para obtener más información sobre estos temas.

6. Referencias bibliográficas

Argentina, B. O. (2019). *Resolución 829/2019*. Obtenido de Estrategia Nacional de Ciberseguridad de la República Argentina : https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528

Argentina.Gob. (s.f.). Obtenido de Objetivos - Dirección nacional Ciberseguridad: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/objetivos-de-la-direccion

Argentina.Gob. (2000). Ley Nacional 25.326 - Art.2.

Argentina.Gob. (2019). *Estrategia Nacional de Ciberseguridad de la República Argentina* .

Argentina-Gob. (2001). Ley N°25.326 /Decreto Reglamentario 1558. Boletin Oficial - Argentina.

Argentinas, F. A. (2022). *Boletines de Noticias de Ciberseguridad de la subsecretaría de de ciberdefensa*. ("Instituto de Ciberdefensa - Fuerzas Armadas") Obtenido de https://www.fuerzas-armadas.mil.ar/Instituto-Ciberdefensa-FFAA/boletinesNoticias2022.html

Argentino, D. N. (2014). *Decreto 2645/2014.* Boletín Oficial - Argentina.

CASI. (2022). *Consejo Argentino para la seguridad integrada*. Obtenido de https://capsi-ar.org/

CERT. (2021). *Informe anual de incidentes de seguridad informática registrados en 2021*. Argentina: CERT.

CERT.ar. (2021). *Informe anual de incidentes de seguridad informática registrados en 2021.* Argentina: CERT.

Confidencial. (08 de 2022). Comparación estrategia nacional Argentina vs España. (Pereyra, Entrevistador)

Decreto Nacional. (2018). *Decreto Nº 703/2018* . Argentina: Boletín Oficial.

Derechos de la ciudadanía. (s.f.). Obtenido de Argentina.gob.ar: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/derechos-de-la-ciudadania

España, M. S. (2021). *Ministerio de la presidencia*. Obtenido de Estrateigia Nacional de Ciberseguridad de España 2021: https://www.mpr.gob.es/prencom/notas/Paginas/2022/290322-ciberseguridad.aspx

España.Gob. (2019). Estrategia Nacional de Ciberseguridad. España.

España.Gob. (2019). Estrategia Nacional de Ciberseguridad. España.

Instituto Español de Estudios Estratégicos. (2017). *Ciberseguridad: La colaboración público-privada.*

Instituto Español de Estudios Estratégicos. (2017). *Ciberseguridad-La cooperación público-privada.*

ITU. (2020). *Global Cybersecurity Index - Page 16.*

ITU. (2021). *Guide to Developing a National Cybersecurity Strategy.*

ITU. (2021). *Guide to Developing a National Cybersecurity Strategy - Page13.*

ITU. (2021). *Guide to Developing a National Cybersecurity Strategy 2nd Edition 2021*. Obtenido de https://www.itu.int/pub/D-STR-CYB_GUIDE.01

ITU. (2021). *Measuring digital development Facts and figures - Page 1.*

ITU. (2021). *NCS-Guide – Page 17.*

ITU. (2021). *NCS-Guide – Page 28.*

ITU. (2021). *NCS-Guide – Page 46.*

Keticoglu, E. a. (2020). Ciberseguridad y Ciberdefensa en Argentina CAPSI. (M. Ana, Entrevistador)
Recomendaciones. (s.f.). Obtenido de Argentina.Gob.Ar: https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/recomendaciones
Resolución 343/14. (May de 2014). Argentina.
Vaninetti, H. A. (2021). Derecho a la intimidad en la era digital.

7. Anexos

- **Cuestionario encuesta:**

Se deja adjunto el cuestionario utilizado. El mismo fue creado y enviado vía Google Form y solicitado a cada uno de los contactos seleccionados. En el mismo formulario se incluyó un apartado para que el entrevistado decida si quería que su identidad sea revelada. Del mismo respondió 1 entrevistado que prefiere mantener su identidad en reserva.

Pregunta 1

¿Considera que existen planes efectivos de concientización ciudadana como parte de la estrategia nacional de ciberseguridad nacional? Comente su visión, agregue si considera los puntos de mejora que considere

Respuesta Encuestado N1: No... hay acciones aisladas de algunos organismos pero no es suficiente ni efectivo.

Pregunta 2

Si conoce el plan de ciberseguridad nacional de España ¿Que diferencias observa entre el plan nacional de ciberseguridad de España vs el plan de ciberseguridad nacional Argentino? ¿Observa diferencias en el estado de evolución de ambos?

Respuesta Encuestado N1: Considero que entre ambos existen varios puntos a tener en cuenta como diferencias pero para destacar la principal diferencia está dada en el marco de comunicación y en la asignación de recursos para la ejecución del plan.

Pregunta 3

¿Cuánto conoce del plan vigente de ciberseguridad nacional argentino?

Respuesta Encuestado N1: Bastante, mi especialidad profesional es ciberseguridad. Si bien mi ámbito de pertenencia y trayectoria se desempeña en el sector privado, observo de cerca el plano público y su evolución.

Pregunta 4

Comente su opinión respecto al estado actual de ciberseguridad nacional en términos de ciberdefensa

Respuesta Encuestado N1: Sin duda ha evolucionado respecto a los últimos 10 años pero claramente la falta de recursos se evidencia en la lentitud del desarrollo del plan.

Pregunta 5

¿Qué acciones de concientización ciudadana en términos de ciberseguridad, considera deberían incluirse en una estrategia de ciberseguridad nacional?

¿Considera que sus sugerencias se encuentran incluidas en el plan nacional del país que reside?

Respuesta Encuestado N1: Existen múltiples acciones que pueden desarrollarse, el estado actual de la estrategia nacional de ciberseguridad argentina, no radica en que acciones se podrían implementar. Radica, primeramente en que debe existir una estrategia clara, coordinada, asignación de recursos y una comunicación eficiente. Esto último aplica entre varios otros temas a la concientización ciudadana.

- **Ejemplo Estados unidos, concientización en ciberseguridad:**

Un ejemplo interesante para el lector será el caso de estados unidos y su estrategia de iniciativas para concientización ciudadana:

En Estados Unidos se han lanzado algunas iniciativas interesantes en cuanto a concienciación en ciberseguridad, como son: el mes de la concienciación en ciberseguridad, la campaña Stop. Think. Connect, el día de la privacidad de los datos (Data Privacy Day) y la campaña Re: Cyber para directivos. En 2001 se fundó la Alianza Nacional de Ciberseguridad (National Cyber Security Alliance, NCSA). Fue

conformada por un grupo de líderes visionarios de la industria que se dieron cuenta de que no se había hecho lo suficiente para formar al público sobre cómo protegerse en las redes. Desde el principio los principios reguladores incluían que: aunque en algunas esferas los socios miembros podían competir todos tenían un interés compartido en un internet más seguro y confiable y el éxito final vendría garantizado si trabajaban juntos y próximos al Gobierno, quien también compartía este interés. Hoy en día la misión de la NCSA es educar una sociedad digital de tal manera que puedan utilizar internet de manera segura en la casa, el trabajo y la escuela, protegiendo la tecnología que utilizan las personas, las redes a las que se conectan y los medios compartidos. Sus actividades están financiadas por los miembros asociados y por el Departamento de Seguridad. Algunas empresas asociadas a esta iniciativa son: ADP, AT & T, Bank of America, Comcast, EMC, ESET, Facebook, Google, Intel, Leidos, McAfee, Microsoft, Symantec, Verizon and VISA. En el año 2009 la política del ciberespacio del presidente Obama recomendaba que: El Gobierno Federal, en cooperación con educadores e industria, debería conducir un esfuerzo común de concienciación pública en ciberseguiridad y esfuerzo en educación. Como respuesta, en una iniciativa sin precedentes, la NCSA junto con el grupo de trabajo Anti Phising trajeron consigo veinticinco empresas y siete agencias gubernamentales para explorar la posibilidad de una campaña nacional de concienciación. El grupo rápidamente tomó la tarea y en los siguientes catorce meses trabajando en estrecha cooperación y por consenso investigó y desarrolló un conjunto de mensajes que deberían estar disponibles y ser usados por todos. Este es el origen del programa clave desarrollado por la NCSA y conocido como Stop.Think.Connect (Para. Piensa. Conecta). El trabajo desarrollado ha sido reconocido al proclamar el presidente Obama Stop. Think.Connect como la campaña nacional de concienciación durante su anuncio del Mes Nacional de Ciberseguridad en 2010. Algunos de los beneficios de esta campaña incluyen:

– Más de ciento cincuenta socios firmaron la campaña para utilizar el mensaje de la campaña. Grandes y pequeñas empresas, departamentos de policía e instituciones educativas y el mismo Gobierno entre ellas.

– La campaña se ha expuesto en transportes públicos de importantes ciudades de Estados Unidos como Washington, Boston y Chicago.

– Se han desarrollado pequeñas campañas en torno a mensajes clave de la campaña.

– Muchas empresas lo han utilizado para demostrar al público su política interna de seguridad en las redes.

– Mucho material ha sido desarrollado para escuelas. Aunque esta campaña inicialmente solo iba dirigida a los Estados Unidos, esta campaña creció internacionalmente y se ha expandido hacia otras organizaciones regionales e incluso otros países.

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

Solicitud de evaluación de TRABAJO FINAL DE ESPECIALIZACIÓN (TFE)	Código de la Especialización
Nombre y apellido del alumno	Tipo y N° de documento de identidad
Año de ingreso a la Especialización - Ciclo	Fecha de aprobación del TFE en el Taller

Título del Trabajo Final

Solicitud del docente a cargo del Taller

Comunico a la Dirección de la Especialización que el Trabajo Final bajo mi tutoría se encuentra satisfactoriamente concluido. Por lo tanto, solicito se proceda a su evaluación y calificación final.

Firma del docente ……

Aclaración……

Lugar y fecha……

Datos de contacto del Tutor	
Correo electrónico	Teléfonos

Se adjunta a este formulario:

- Trabajo Final de Especialización impreso (indicar cantidad de copias presentadas)
- CD con archivo del Trabajo Final en formato digital (versión Word y PDF)
- Certificado analítico

Fecha	Firma del alumno

Form. TFE v1
PRESENTAR EN LA RECEPCIÓN DE LA ESCUELA DE ESTUDIOS DE POSGRADO

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

ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

EVALUACION TRABAJO FINAL INTEGRADOR

DOCENTE EVALUADOR: Ing Exp Carlos Amaya – Docente de la materia Tecnologías de la Información y de las Comunicaciones.

.

TEMA: " Ciberseguridad en la República Argentina: Concientización ciudadana. "

ALUMNO: Janina Pereyra

CRITERIOS DESARROLLADOS:

1. Conocimiento del tema:
   El tema elegido es por demás interesante (concientización ciudadana) y la autora inicialmente encaró su estudio de investigación desde un punto de vista más hacia lo cognitivo y sociológico, incluyendo y mencionando casos de ciberdelitos, producto de esa falta de concientización por parte del usuario y no desde la posición de propuesta al ESTADO NACIONAL. Posteriormente, aportó esta perspectiva, con la inclusión de las normativas vigentes en nuestro país, contextualizando su investigación.

2. Actualización del Diagnóstico:
   Como parte de la actualización de situación en materia de prevención de ciberdelitos, realizó un buen análisis de la situación en España, que constituye un excelente ejemplo de políticas de seguridad en esta materia. Completando su indagación sobre nuestro país, donde exhibió las necesidades y carencias, que facilitan el avance de la criminalidad mediante las tecnologías y las redes sociales. Si bien cumplió con los estándares, se observó algunas opiniones que merecen ser fundamentadas mediante el uso de citas y referencias que la sostengan, y mejorar la redacción académica en sus futuras investigaciones como especialista.

3. Pertinencia y coherencia de la propuesta de intervención

   Como se expresó, el tema es muy interesante, pertinente y coherente con los objetivos del posgrado, también así la propuesta de intervención. El avance de la criminalidad organizada usa las debilidades de la población, por lo tanto, el desarrollo de programas de concientización en distintos niveles, son considerados elementales para la prevención de los ciberdelitos.

4. Breve juicio del TFI.
   Buen trabajo descriptivo, fundamentalmente por la dedicación de la autora en organizar la información en torno a sus objetivos y que le permitieron sostener y avalar su propuesta de la necesidad de concientización como base de la ciberseguridad.

5. Propuesta de calificación numérica: SIETE (7). –

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.

- Se advierte el uso de numerosas fuentes, principalmente secundarias para la construcción de un diagnóstico real con relación a la cibercriminalidad, que le permitió construir una propuesta, que resulta evidentemente necesaria como contribución para la prevención de los delitos cometidos mediante las TICs, por lo tanto un aporte más de esta carrera al sistema vigente.

- Cumple con la Guía de la Facultad de Ciencias Económicas (UBA) establecida para los trabajos finales de especialización y con el Reglamento de Estudios de Posgrado de la Universidad de Buenos Aires.

TFI: APROBADO. JUICIO: BUENO, CALIFICACIÓN PROPUESTA: OCHO (8).

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

Consideraciones: La cursante ha desarrollado un aporte sintético, de fácil lectura y comprensión, respecto de cuestiones en plena discusión vinculados al ciberespacio y sus incumbencias en la seguridad y defensa atinentes en el mismo.
Su recorrido por España le permite acceder a los avances europeos, que la lleva a una excelente revisión de las normas argentinas que la inducen a describir vacíos y necesidades de respuesta por el Estado Nacional.
Ha centrado su mirada en las prácticas estatales de concientización sobre riesgos y amenazas al ciudadano, con interesantes referencias para eventuales consultas.
Más allá de esta presentación, debo destacar como director de la carrera, que no ha pasado desapercibida la permanente intervención de la Licenciada Pereyra en el desarrollo de la carrera, donde su constante participación y significativas observaciones en el aprendizaje de la especialidad, la ubican indudablemente en el mejor plano de la excelencia profesional.
Finalmente, este trabajo puede y debe ampliarse para promover una publicación destinada precisamente a lo que la motiva en todo momento:

Difundir conocimiento accesible a un usuario alejado del tecnicismo que suele oscurecer el mundo digital. ¡Adelante!
Calificación final : Excelente (9).-

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