Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias. Exactas y Naturales e Ingeniería

Carrera de Maestría en Seguridad Informática

Trabajo Final

Título:

Marco para la generación de una Estrategia Nacional de Ciberseguridad en Argentina

Autor:

Facundo Mauricio

Tutora:

Patricia Prandini

Año de Presentación: 2018

Cohorte: 2017

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADA

FACUNDO NAHUEL MAURICIO

Resumen

Este trabajo final de maestría se construye sobre la base de una investigación descriptivo-explicativa a partir una fase exploratoria de bibliografía y se divide en cuatro partes para su desarrollo.

En la primera parte, se exploran los componentes teóricos y prácticos de la ciberseguridad, su evolución y las características esenciales que ponen de manifiesto su creciente importancia en el mundo y su correlación con el continuo desarrollo de nuevas tecnologías. En este marco se toman en cuenta los amplios desafíos y riesgos que estos desarrollos tecnológicos implican para las personas, las organizaciones y los gobiernos.

En la segunda parte, el foco está puesto en revisar estrategias de ciberseguridad publicadas e implementadas por otros países, a los fines de comprender sus tendencias, evaluar sus enfoques y formar las bases de un necesario aunque postergado desarrollo de la estrategia nacional de ciberseguridad en Argentina, a partir de las experiencias adquiridas por diversos países del globo como ser Estados Unidos, Alemania, Estonia y Turquía, entre otros.

La tercera parte se centra en el objetivo principal de este trabajo final, presentando la descripción de los elementos necesarios para la construcción de una estrategia de ciberseguridad. Dicho aporte describe los lineamientos de una propuesta concreta que busca acelerar y facilitar la creación de dicho documento por parte de las autoridades argentinas, con la esperanza de generar una Nación más próspera y segura en términos digitales y tecnológicos y lista para enfrentar los desafíos actuales de la ciberseguridad.

La cuarta y última sección describe las principales conclusiones el trabajo final de maestría y una serie de recomendaciones para la generación de una estrategia nacional de ciberseguridad en nuestro país.

Palabras Clave

Ciberseguridad | Estrategia | Riesgos | Argentina | Seguridad Informática

Índice

Prólogo

El presente documento no hubiera sido posible sin el aporte y el apoyo de los varios amigos, colegas, familiares y principalmente, profesores de esta maravillosa casa de estudios que es la Universidad de Buenos Aires. Con su conocimiento y experiencia, permitieron que podamos aprender y crecer como profesionales no solo en el ámbito académico, sino también en el plano ético y moral. En especial, me permito destacar la excelente labor de Pedro Hecht en acompañar y brindar su apoyo durante la confección del presente documento.

Adicionalmente es central destacar y agradecer enormemente la incansable y brillante labor de Patricia Prandini, destacándose no solo como una excelente tutora y experta en la materia, sino como una gran persona, siempre dispuesta a colaborar con los objetivos propuestos y manteniendo los más altos estándares de calidad durante toda la investigación y redacción del presente trabajo final de maestría.

Finalmente, mis más profundas palabras de agradecimiento para mis padres, quienes me apoyan desde hace años en todos mis proyectos personales y han sido determinantes para que hoy me encuentre nuevamente persiguiendo otro desafío académico.

PARTE 1 Entendiendo la ciberseguridad

Introducción

Con el crecimiento de la dependencia de la sociedad del uso de internet y las redes de comunicación para un gran número de actividades y servicios esenciales y para el desarrollo económico de las comunidades de nuestro país, se hace necesaria la construcción de una Estrategia de Ciberseguridad para la República Argentina. Efectivamente, como en otros países del mundo, el aumento exponencial del acceso a internet ha facilitado un desarrollo económico sostenido, acercando nuevas oportunidades de innovación y crecimiento. Sin embargo, este acelerado avance del nivel de conectividad ha traído aparejado nuevas amenazas y actores que representan una variedad de nuevos riesgos para las naciones del mundo y sus ciudadanos, quienes cada vez desarrollan más actividades en el ciberespacio y requieren en consiguiente, estrategias de protección.

Adicionalmente, la conectividad de las redes corporativas a redes industriales que proveen servicios esenciales, como electricidad, agua, transporte o salud entre otros, propone nuevos desafíos dadas las vulnerabilidades que continuamente son descubiertas en los sistemas que estas instituciones utilizan. El creciente número de dispositivos conectados a internet y el advenimiento de las tecnologías de Internet de las cosas (IoT) también propone mayores complejidades al ya incontrolable número de dispositivos vinculados a la red.

Con estos conceptos en mente, gobiernos y organizaciones deben considerar un panorama creciente y cambiante de amenazas que se presentan en el espacio digital y cuyo tratamiento corresponde a la disciplina conocida como ciberseguridad. [1]

¿Qué es ciberseguridad?

Ciberseguridad se ha convertido en los últimos años en un término que se escucha cada vez más habitualmente en los distintos medios de comunicación, espacios de discusión académica y científica y en múltiples discusiones políticas y

económicas entre especialistas y formadores de opinión, empresarios y políticos. La definición exacta de la ciberseguridad es aún motivo de discusión entre académicos e instituciones internacionales, y para su comprensión es necesario tomar varios aspectos asociados a la seguridad informática o de la información. A continuación, se presentarán distintas perspectivas de su definición, a fin de permitir una compresión amplia del fenómeno de la seguridad asociada al ciberespacio.

El NIST define la ciberseguridad como la habilidad de proteger o defender el uso del ciberespacio de ciberataques. A partir de este concepto, caracteriza los ciberataques como aquellos que tienen lugar en el ciberespacio con la intención de desestabilizar, debilitar, destruir o malintencionadamente controlar un equipo o una infraestructura informática, destruir la integridad de los datos o robar información. En cuanto al ciberespacio, el NIST lo define como el dominio global donde la interconexión de redes interdependientes, de sistemas de información e infraestructura, incluyendo internet, redes de telecomunicaciones, sistemas computarizados, procesadores y controladores embebidos, gestionan información en formato digital. [2]

La ISO/IEC 27032:2012 describe la ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo luego el ciberespacio como el complejo ambiente resultante de la interacción de personas, software y servicios en internet, por medios tecnológicos y de redes. Según esta norma, el ciberespacio no tiene existencia física. [3]. Se aprecia que la ISO/IEC parte de la definición de seguridad de la información, contenida en la ISO/IEC 27000, que es aceptada internacionalmente.

Por último, se puede considerar también, la definición provista por la empresa Kaspersky, que conceptualiza la ciberseguridad como la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos. [4]Esta definición no se encuentra alineada con las anteriormente descriptas, faltando en ella una interpretación más amplia del campo de estudio de la ciberseguridad y que parece coincidir con visiones más clásicas de la seguridad informática, presentando un esquema limitado de la materia. En cuanto al

resto de las definiciones, puede apreciarse que la práctica de la ciberseguridad normalmente refiere a la protección de sistemas de información y comunicación en conjunto con los datos, y de otras tareas vinculadas a la gestión de la información, generalmente refiriéndose a uno o más de los siguientes aspectos:

- Actividades y medidas destinadas a proteger del ataque, disrupción u otras amenazas, a computadoras, equipos informáticos, redes, hardware, software y otros dispositivos que contengan o comuniquen información a través del ciberespacio o por medios digitales.
- El estado de sentirse protegido de las amenazas descriptas en el punto anterior
- El esfuerzo enfocado en implementar medidas que mejoren las actividades descriptas en el primer punto y fomenten su seguridad [5]

Por otro lado, según el diccionario de Oxford [6], la ciberseguridad es definida como: el estado de estar protegido contra actividades criminales o el uso no autorizado de datos electrónicos, o de actividades que busquen ese objetivo. Podemos apreciar aquí que la definición propuesta por el mencionado Diccionario no acaba por construir una idea holística de la ciberseguridad, que ayude a comprender la necesidad de los distintos países de trabajar activamente en diseñar estrategias de ciberseguridad.

Un camino posible es explorar la definición de ciberseguridad por el lado de las amenazas que actualmente están en amplio crecimiento. Entre ellas podemos destacar la penetración de actores maliciosos en infraestructuras críticas de información, entendiendo por tales al soporte tecnológico que facilita la provisión de un servicio considerado esencial para los ciudadanos, la economía o el correcto funcionamiento del Estado, la afectación de computadoras y equipos electrónicos, el espionaje industrial, el robo de información personal, los ataques al sector financiero, el *ransomware* y el robo de identidad, entre tantos otros delitos. Algunos de estos problemas impactan en la esfera personal de los individuos, pero otros lo hacen en organizaciones privadas, Estados o directamente en la sociedad en su conjunto

La proliferación y sofisticación de los delitos informáticos ha generado que los gobiernos comiencen a considerar estos delitos no como cuestiones aisladas, sino como amenazas crecientes a las sociedades de las cuales son responsables. Es en este marco que la generación de estrategias de ciberseguridad se vuelve una necesidad para todos aquellos países que busquen defender su soberanía y proteger a las personas, no solo en el plano físico sino en el digital, con frecuencia haciendo énfasis en los miembros de la sociedad más vulnerables, como ser los niños y los adultos mayores. [7]

Continuando con la revisión del concepto de ciberseguridad, un error habitual es contemplar solamente los casos más extremos, considerando incidente de ciberseguridad a una interrupción masiva de la provisión de energía o de agua, producto del acceso no autorizado a los sistemas que controlan su distribución. Si bien esta situación ha sucedido ya, por ejemplo, en Ucrania, sería un error enfocarse solamente en estas acciones masivas y perderse la cotidianeidad de la ciberseguridad, que normalmente se manifiesta en delitos de menor alcance y, por lo tanto, mayor dificultad para identificar, pero que tienen (en conjunto) terribles consecuencias económicas para las organizaciones y las personas afectadas.

De hecho, gran parte de los delitos asociados a la ciberseguridad tienen motivaciones puramente económicas y no políticas, observación que puede apreciarse en los reportes anuales de cibercrimen de Accenture [8]. Sin embargo, su impacto representa una amenaza para los países en distintos ámbitos, que abarca por ejemplo, desde el robo de la propiedad intelectual hasta socavar la confianza en medios de pago electrónico. Esto no significa que los países no deban enfocarse en escenarios de destrucción total, como los asociados a la pérdida de infraestructura crítica, sino que algunos delitos asociados a la ciberseguridad son el resultado directo de estímulos económicos de los diferentes actores de la economía y pueden ser reducidos trabajando en los incentivos y costos para las organizaciones, como los mencionados anteriormente.

Una mirada histórica de la ciberseguridad nos lleva a considerar que los primeros problemas comienzan a surgir con el crecimiento de los llamados programas

de *time-sharing* (*ver Glosario*) que permitían que múltiples usuarios se conecten en simultáneo a una computadora para compartir los entonces limitados recursos disponibles. En ese momento surge la necesidad de proteger los datos de los usuarios que compartían el uso de un mismo equipo. En aquellos tiempos, los ingenieros buscaron solucionar esta situación con el marco de herramientas disponibles, en este caso a través de programas que protegían los datos de los usuarios. Sin embargo, cuando la tecnología fue evolucionando exponencialmente a la vez que los accesos a datos a través de las redes se volvieron más frecuentes, quedó en evidencia que esta situación no es solo un problema técnico, sino que debía ser revisada por las autoridades en búsqueda de regulación y legislación que permita proteger la información de individuos y organizaciones en el nuevo espacio digital que se estaba gestando.

En esta línea, el crecimiento del sector tecnológico impulsó esta compleja situación, pues la economía estaba impulsando un flujo acelerado de información a través de las redes y su limitación por cuestiones de seguridad podría haber comprometido seriamente el crecimiento de las naciones más desarrolladas. En este marco, la tecnología comienza a estar cada vez más presente en la vida de los individuos, trayendo nuevas implicancias a la gestión y protección de la información. Con el rápido crecimiento e interrelación de la información de las diferentes entidades que conforman una sociedad, es que en la actualidad nos encontramos en la discusión de cómo gestionar la ciberseguridad y cuál es el compromiso que cada nación va a tomar en cuenta para cuestiones asociadas a las libertades individuales como el respeto de la privacidad, el anonimato y otros valores sociales que han crecido en importancia con el desarrollo de las discusiones en la materia. [9]

Detalle de ataques

Se presenta a continuación una breve descripción de los ataques más comunes que se registran en el ciberespacio, como base para el entendimiento de los riesgos a los que se enfrentan las instituciones que prestan servicios a través de internet. Los

tipos de ataques que se han incluido aquí son aquellos que se dan con mayor frecuencia, o bien tienen el mayor impacto [10]:

- Denegación de Servicio (DDoS)
    - Estos ataques implican la coordinación de un gran número de dispositivos que intentan acceder a un determinado recurso en forma simultánea. El recurso, normalmente un sitio web, al ser incapaz de procesar tanta demanda, cae, denegando el servicio a los usuarios legítimos.
- Herramientas de Explotación
    - Son programas creados por desarrolladores para encontrar y explotar vulnerabilidades existentes en los sistemas.
- Bombas lógicas
    - Hacen referencia a código generado por programadores maliciosos que cuando es ejecutado por un programa en particular, lo hacen fallar inesperadamente y generalmente, de forma catastrófica.
- Phishing
    - Consiste en la generación de correos electrónicos y sitios web que son diseñados para parecer válidos pero que en realidad, fueron creados para capturar ilegalmente credenciales de usuarios y afectar su patrimonio.
- Sniffer
    - Es un programa que intercepta datos en la red y examina cada paquete en búsqueda de información valiosa que pueda ser utilizada para luego atacar al usuario o para obtener información privilegiada.
- Caballo de Troya (Troyano)
    - Refiere a software que en principio parece válido y útil al usuario, pero que en su interior esconde código malicioso que permite a su creador tomar control de la PC que lo ejecuta. Puede ser considerado dentro de la familia de código malicioso.

- Virus
    - Son programas que infectan las computadoras y que replican su código en otras computadoras a través de la intervención (por desconocimiento) del usuario. A diferencia de los gusanos, los virus siempre requieren que el usuario intervenga en su ejecución y diseminación. Puede ser considerado dentro de la familia de código malicioso.
- Gusano
    - Se trata de un programa que infecta computadoras y se reproduce en una red de forma automática. Son similares a los virus, pero no requieren intervención del usuario, sino que se basan en vulnerabilidades existentes en la red o en los sistemas donde se propagan. Puede ser considerado dentro de la familia de código malicioso.
- Ingeniería Social
    - Es el arte de convencer a los usuarios para que entreguen información voluntariamente a personas malintencionadas. Esto se logra mediante el engaño del usuario usando distintos métodos, más cercanos a la psicología que a la tecnología, pero no por ello menos efectivos a la hora de conseguir información privilegiada.
- Ransomware
    - Es un tipo de software diseñado para bloquear el acceso a la información que existe en una computadora, normalmente obligando al usuario a pagar una suma de dinero para recuperar sus archivos. Puede ser considerado dentro de la familia de código malicioso.

Esta enumeración no pretende incluir todos los ataques existentes sino dar una lista ejemplificativa de los vectores más usados para atacar organizaciones e individuos. La realidad, como siempre, es notablemente más compleja y presenta manifestaciones

mixtas de estos ataques, combinando varios en sucesión, siempre con fines malintencionados o delictivos. [10]

Amenazas: principales actores

Al igual que con la evaluación de los potenciales ataques vistos en la sección anterior, a continuación se realiza una revisión de los principales actores detrás de las amenazas y ataques, a fin de luego comprender las motivaciones e incentivos que pueden tener para cometer actos delictivos. Veamos entonces algunos de los orígenes más comunes de las amenazas de ciberseguridad:

- Grupos Criminales
    - Son organizaciones que funcionan igual que las organizaciones criminales ya conocidas, pero cuya organización y accionar está en el ciberespacio.
- Servicios de inteligencia extranjera
    - Son organismos financiados por los Estados que tienen una agenda propia y pueden operar a través de distintos medios para adquirir información o infiltrarse en las redes de otros países con el propósito de acceder a datos protegidos por cuestiones de soberanía nacional.
- Hackers
    - Se trata de un término de definición compleja y sujeta a debate, pues los hay en diferentes variedades e inclinaciones. En este contexto nos referimos a los individuos que utilizan su conocimiento para infiltrarse en redes ajenas y robar información o afectar el normal funcionamiento de las organizaciones.
- Empleados disconformes (usuarios internos)
    - Aquí nos referimos a usuarios que pertenecen a la organización y atacan desde adentro. Normalmente se trata de empleados que utilizan sus credenciales o brindan información crítica a terceros que cometen delitos.

- Phishers
    - Se hace referencia a individuos que generan esquemas para robar identidades o delitos de orden financiero con el objetivo de ganar dinero mediante la manipulación de los usuarios.
- Spammers
    - Se consideran en esta categoría a aquellos individuos que distribuyen contenido no solicitado a los usuarios u organizaciones, también pudiendo enviar virus u otro tipo de contenido malicioso que puede afectar a quienes lo reciben.
- Desarrolladores de Virus/Malware/Spyware
    - Son aquellos programadores que usan sus talentos para la construcción de aplicaciones que tienen consecuencias negativas para la sociedad, organismos o individuos.
- Terroristas
    - Grupos o individuos que buscan destruir, incapacitar o afectar estados u organizaciones. Estos grupos pueden utilizar diversas técnicas para alcanzar sus fines, ente ellas la explotación de vulnerabilidades como vector de ataque o el aprovechamiento del ciberespacio para reclutar personal o difundir su ideología.
- Operadores de Botnets
    - Las Botnets son redes desarrolladas por terceros y operadas por actores maliciosos, que capturan diversos dispositivos o equipos informáticos para su uso en ataques coordinados. La idea es contar con gran poder de ataque sin invertir en recursos propios, ni comprometer la identidad del hacker al utilizar su propia infraestructura.

Este listado no es exhaustivo en cuanto a los orígenes de ataques, pero orienta respecto a los grupos más reconocidos a nivel global. Cabe destacar que estas listas son dinámicas y muchos ataques puede surgir de una combinación directa o indirecta de varios de los grupos mencionados, utilizando una variedad de vectores de ataque que cambia día a día. [10]

Infraestructuras críticas

En todo análisis de ciberseguridad es necesario detenerse a contemplar el rol de las llamadas infraestructuras críticas y su impacto en el mundo digital, dados los nuevos paradigmas propuestos por la tecnología y la expansión de las redes globales. Para ello, corresponde definir como infraestructura crítica a todo aquel soporte tecnológico que permite o facilita la provisión de un servicio considerado esencial o de gran importancia para la vida del ciudadano, la economía o el correcto funcionamiento del Estado. Por lo general, los países incluyen en esta lista a servicios como: transporte, electricidad, telecomunicaciones y agua, entre otros. Sin embargo, cada país puede por cuestiones estratégicas, identificar distintos servicios como de vital importancia para su supervivencia.

En este marco es interesante establecer un paralelismo con la guerra clásica, puesto que la discusión con respecto a la infraestructura crítica surge del análisis que se realiza en los años posteriores a la Primer Guerra Mundial. Es en ese momento histórico cuando el desarrollo de la Fuerza Aérea pone a los gobiernos de Europa y el mundo por primera vez, a considerar su infraestructura desde el punto de vista de su vulnerabilidad a ataques aéreos. En este contexto, se realizan numerosos análisis sobre el alcance de una infraestructura crítica y cuáles son las opciones para protegerla, siendo curiosamente la premisa del momento el de evitar la concentración, para que la destrucción de un punto concreto no destruya el sistema completo. El paralelismo es curioso porque años después, toda esta planificación y análisis sería puesta a prueba en la Segunda Guerra Mundial donde diversos países utilizaron su Fuerza Aérea para propinar bombardeos estratégicos en la infraestructura más crítica de cada país enemigo, como ser la electricidad, el agua, las principales plantas de manufactura, rutas, aeropuertos, etc. Notablemente mucha de la literatura en materia de ciberseguridad, refiere a los mismos tipos de ataques y los mismos blancos, solo que en lugar de bombas aéreas, utilizan los hoy llamados ciberataques. [11]

Es interesante notar que durante la Segunda Guerra Mundial los aliados fueron incapaces de destruir infraestructura crítica alemana de forma definitiva en un solo ataque. Fue necesario el ataque reiterado y coordinado para debilitar la estructura

productiva y de servicios de Alemania, que probó ser un rival extremadamente resistente. Sin embargo, muchos expertos afirman que esta no será la naturaleza de los ciberataques a la infraestructura crítica en la actualidad, pues la mayoría de ellos solo puede funcionar una vez, ya que luego de ser ejecutado el primer ataque, las vulnerabilidades serán seguramente encontradas y al menos por ese vector, no será posible atacar nuevamente. Esto obliga a los atacantes a buscar constantemente nuevas vulnerabilidades y eleva el costo de futuros ataques, siendo en este sentido muy distinto al paralelismo histórico presentado. Sin embargo, en cuanto a lo que costos refiere, el valor invertido y la infraestructura requerida para propiciar un ataque a un país son cada vez menores, mientras que las vulnerabilidades van en aumento. Esta situación fuerza a gobiernos a estar constantemente a la búsqueda de nuevas formas de proteger no solo su soberanía, sino también los bienes y la calidad de vida de sus ciudadanos.

Con estas consideraciones, los gobiernos tienden a preocuparse por ciberataques que provoquen daños más allá del software o los sistemas de control, afectando físicamente equipos costosos o muy complejos de reparar que facilitan servicios de importancia para la población. El poder del ciberataque, más allá de la mera interrupción de un servicio, es la posibilidad de una profunda repercusión negativa en la percepción de las personas u organizaciones con respecto a la capacidad de dichos organismos de protegerlos y garantizar la provisión de servicios críticos. En este sentido, tanto la duración de la interrupción, como la capacidad de respuesta ante incidentes serán de gran importancia para ponderar el impacto social de un ciberataque, y junto con el costo económico de reparar los equipos dañados, terminaran por definir el costo total del incidente que afrontará la nación víctima.

Otro factor a considerar con respecto a ciberataques a la infraestructura crítica es la escala del impacto. En este sentido, los países deben analizar cuán distribuidos son sus servicios básicos y cuántas personas se van a ver afectadas. Siendo que las diferentes empresas y organismos que controlan los servicios están normalmente diseminados y en diferentes manos, construidos en diferentes épocas y con variada tecnología, es complejo imaginar un escenario coordinado donde todos estos objetivos

sean atacados al mismo tiempo y sean incapacitados con éxito, dejando a un país completo sin la totalidad de sus servicios esenciales. Sin embargo, la complejidad de dejar a una parte importante de la población sin servicios, no debe limitar el entendimiento del enorme impacto psicológico y social que podría tener en una sociedad un ataque a las principales ciudades donde reside la mayoría de la población o donde tiene lugar la mayor parte de la actividad económica. [11]

Rol del terrorismo

En la actualidad se habla con bastante frecuencia del rol del terrorismo como una de las principales amenazas para la ciberseguridad y se vislumbran grupos de hackers escondidos en algún país atacando naciones con un par de clics y comandos en una computadora. Esta imagen, aunque pintoresca, es raramente correlacionada con la realidad, pues se requiere una infraestructura y habilidades que generalmente solo están a disposición de grupos respaldados por algún gobierno o centro de poder, permitiéndoles coordinar ataques masivos que afecten a naciones enteras. Desde luego que las organizaciones terroristas utilizan internet y las redes en general de diversas maneras y dicha situación debe ser una preocupación para cualquier gobierno. Normalmente estas organizaciones usan las redes para contactarse, reclutar nuevos miembros, coordinar ataques, encontrar seguidores, difundir su mensaje, publicar noticias falsas, generar terror en la población o financiar sus actividades mediante actividades ilícitas en la red, entre otros.

Hasta el momento, y al menos en lo que se conoce públicamente, el rol del terrorismo en la ciberseguridad tiene más que ver con su propaganda y financiación que con su real capacidad de ataque a naciones desarrolladas. Hasta el momento no hay un ciberataque terrorista confirmado que haya logrado comprometer seriamente la infraestructura o funcionamiento de un país. Además, si un terrorista está buscando un acto de violencia que genere un estado de shock y miedo en la sociedad, es más eficiente una bomba que un corte masivo de luz, que si bien traumático, no tiene el impacto publicitario que normalmente buscan con ataques en lugares públicos. [11]

Rol de la economía

La economía es un actor principal en la evaluación de la ciberseguridad y esto puede comprenderse desde múltiples ángulos. Por un lado, está la desproporcionada relación entre el costo de un ataque y su impacto y por otro, la diversa lista de repercusiones económicas que puede tener un ciberataque. A continuación, se analizan ambas consideraciones:

El costo de generar un ciberataque es relativamente menor, pues en principio solo requiere talento por parte de un experto en seguridad informática que sea capaz de encontrar una vulnerabilidad o bien el desarrollo de código que tenga consecuencias desastrosas para personas u organizaciones. Sin embargo, la realidad muestra que este escenario es el menos común, siendo mucho más frecuente la necesidad de inversión por parte de organizaciones tanto en infraestructura como en la compra de vulnerabilidades (principalmente las conocidas como *0-days*) y la incorporación de software diseñado para realizar ciberataques. Existe en el mercado un número creciente de actores cuyo trabajo es la generación de programas informáticos con fines nefastos que venden estos productos principalmente en la *DarkWeb* y ofrecen sus servicios de hacking a quien pueda y quiera pagarlos. También existen numerosos individuos vendiendo redes de bots para ataques a gran escala, siendo los más comunes aquellos usados para la denegación distribuida de servicio (DDoS). Además, existen mercados de *brokers* de vulnerabilidades que compran y venden debilidades de sistemas al mejor postor. En resumen, el costo total de un ciberataque puede variar dependiendo del talento del personal de sistemas, la infraestructura, el tiempo y el presupuesto disponible de quien genera la actividad maliciosa. Sin embargo, queda en evidencia que más allá de su costo inicial, el potencial daño puede ser desproporcionado respecto a dicho valor, haciendo de los ciberataques un arma muy efectiva y económicamente rentable.

Por otro lado, el impacto económico de un ataque puede ser muy variado dependiendo de su tipo, magnitud y efecto en los diversos procesos económicos o

sociales que afecta. Por ejemplo, los ataques de denegación distribuida de servicio (DDoS) a una empresa en particular constituyen un ciberataque pero su impacto puede extenderse más allá del tiempo en el que la empresa no pudo operar, por ejemplo afectando su reputación, ocasionando una situación de lucro cesante o mostrando consecuencias en términos de costo de oportunidad de clientes perdidos o por el impacto en la cadena de producción, donde una demora en alguna parte del circuito puede afectar el desarrollo de todo el ciclo productivo. [11] [7]

Para analizar las consecuencias económicas en mayor detalle, se listan a continuación algunas de las principales ciberamenazas que de materializarse, pueden dar lugar a los ataques descriptos anteriormente:

- Robo de identidad
    - Constituye uno de los fenómenos más frecuentes, donde actores maliciosos obtienen las credenciales bancarias o de tarjetas de crédito que les permiten operar en nombre de sus víctimas. Desde que los bancos han invertido fuertemente en convencer a sus usuarios que realicen cada vez más transacciones en línea reduciendo significativamente costos operativos, los clientes han quedado expuestos a mayores riesgos de robo de identidad.
- Espionaje industrial
    - Con empresas guardando un número creciente de documentos confidenciales en medios digitales y más recientemente en la nube, los riesgos de interceptar esa información crecieron drásticamente. La información robada puede ir desde una fórmula secreta, a planes de marketing para el siguiente año o la lista de costos internos de la empresa. Esta información de caer en manos de competidores, puede tener un efecto devastador en el mediano y largo plazo para las finanzas y el futuro de las compañías.
- Sabotaje a infraestructura crítica

- La mayor conectividad de los dispositivos asociados a la infraestructura crítica favorecen la posibilidad de nuevos ataques en forma de sabotajes e interrupciones, apuntando principalmente a los equipos que controlan servicios esenciales. Un creciente tipo de sabotaje se manifiesta mediante el uso de comandos SCADA que son enviados a través de la red, para ser interpretados por los dispositivos electrónicos industriales que controlan la provisión de servicios.

- Botnets
  - En este caso consideramos las implicaciones económicas del crecimiento de las botnets, que son utilizadas no solo para realizar ataques de denegación distribuida de servicio, sino también para enviar spam, cometer fraudes asociados con la publicidad online, ataques de phishing y finalmente, para anonimizar el tráfico de los atacantes, dificultando su detección y captura. [7]

El problema de la atribución

La ciberseguridad en la actualidad se enfrenta a un sinnúmero de amenazas que crecen constantemente con el desarrollo de las nuevas tecnologías. Sin embargo, más allá de la escalada en la existencia de nuevos vectores de ataque, la complejidad ante un ataque también está dada por lo que se conoce como el problema de atribución.

En las interacciones que se manifiestan a través de las redes, es notablemente complejo atribuir un ataque a un individuo u organización en particular en forma precisa. La atribución refiere al proceso por el cual se puede identificar efectivamente al ejecutor de un determinado acto, generalmente un ataque, a través de diversas técnicas forenses y del monitoreo de redes. Existe un gran número de técnicas que pueden ayudar a los investigadores a encontrar a los culpables, pero generalmente la

evidencia es de tipo circunstancial, pues es con el uso de inferencias que se puede ir acercando al individuo, grupo, país u organización detrás del acto criminal.

Los objetivos de este proceso son generalmente:

- Obtener un mejor entendimiento de las causas y el origen del ataque en cuestión
- Caracterizar amenazas emergentes desde un punto de vista general, que permita contrarrestar o minimizar la posibilidad de nuevos ataques [12]

El problema de la atribución tiene grandes consecuencias desde el punto de vista de la legislación y la posibilidad de los gobiernos de imponer políticas de ciberseguridad efectivas. El inconveniente es que, si no se puede encontrar al culpable, la legislación tiene limitada eficacia, al menos la que apunta a la sanción de los actores maliciosos que originaron el daño.

Muchas de las vulnerabilidades presentes en los sistemas actuales tienen que ver con la posibilidad de hacerse pasar por otro usuario o esconder de alguna forma la identidad verdadera de quien se encuentra detrás del teclado. Estas vulnerabilidades, que en principio parecen tener menor relevancia que aquellas que permiten acceder a sistemas ajenos, toman particular valor cuando son usadas en combinación con otros ataques y vulnerabilidades que dificultan la atribución. [13]

Por otro lado, cabe destacar que contrario a lo normalmente asumido, el costo del anonimato en el ciberespacio no es menor si el ataque a realizar es a gran escala. Es relativamente económico y sencillo ocultar la identidad del atacante si la agresión es menor y focalizada. Sin embargo, las mismas herramientas que facilitan el anonimato, reducen la eficacia y agregan complejidad al ataque en sí. Esta condición limita la capacidad de ataques a gran escala, quedando esta habilidad reducida principalmente a gobiernos u organizaciones que permiten gestionar los recursos y las herramientas que permiten el anonimato a gran escala.

PARTE 2 Análisis comparativo

Estrategias nacionales de ciberseguridad

Basado en la información planteada en la primera parte, queda en evidencia que los países deben tomar medidas para proteger su soberanía y a sus ciudadanos en el marco de los nuevos desafíos digitales que propone un mundo cada vez más globalizado e interconectado. Es en este contexto que varios países han desarrollado y publicado sus estrategias nacionales de ciberseguridad, comúnmente referidas por sus siglas en inglés como NCSS (*National Cibersecurity Strategies*).

Estos países difieren en la exacta definición de lo que debe incluir una estrategia de ciberseguridad, y es por ello que el presente documento propone un análisis inicial de estrategias pertenecientes a varios países a fin de comparar los contenidos y comprender las consideraciones, para seleccionar aquellas más aplicables a la República Argentina, país que al momento de escribirse este documento (último trimestre de 2018) no dispone de una estrategia nacional de ciberseguridad. Para proporcionar una perspectiva más amplia en el foro internacional, cabe destacar que de los 194 Estados miembros de Unión Internacional de Telecomunicaciones (ITU) [14], solo 70 países (aproximadamente el 36%) no disponen de una estrategia publicada [15], encontrándose entre ellos la Argentina.

El primer paso es definir dicha estrategia como el documento que detalla los aspectos de liderazgo, dirección y principalmente el camino a seguir para alcanzar una visión y objetivos concretos para generar un ciberespacio más seguro, concretándose a través de una serie de actividades asociadas a la seguridad, la soberanía y la protección de la nación en el espacio digital. Las estrategias buscan alinear las distintas áreas de gobierno y los sectores académico, privado y de las Organizaciones No Gubernamentales (ONG) en un esfuerzo coordinado para maximizar la adopción de medidas de protección del ciberespacio y minimizar la exposición a riesgos de la Nación en materia de ciberseguridad. [16]

Países elegidos y criterio de selección

El siguiente mapa representa los países cuyas estrategias de ciberseguridad fueron evaluadas para la generación del presente trabajo final de maestría:

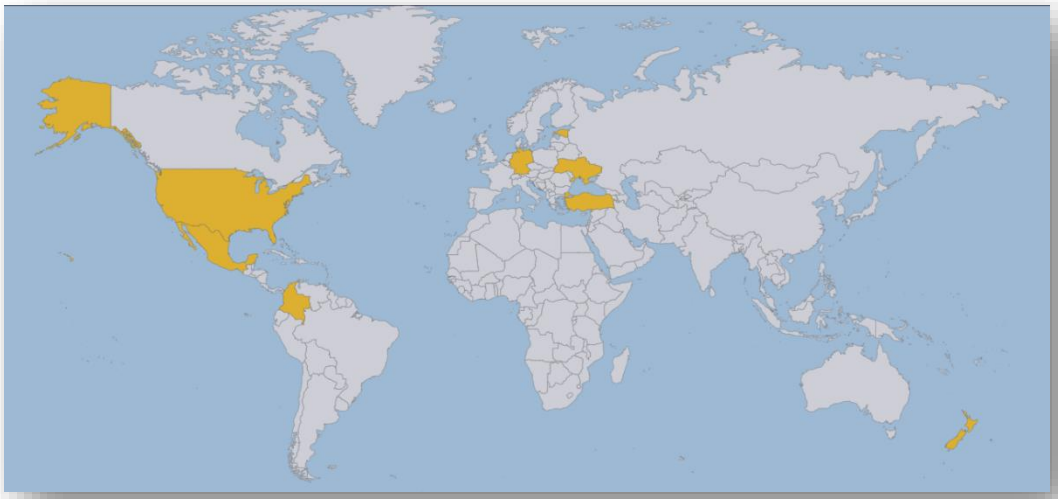

Figura 1. Países cuyas estrategias de ciberseguridad han sido seleccionadas para ser evaluadas: Estados Unidos, Estonia, Nueva Zelanda, Alemania, Colombia, Ucrania, México y Turquía. (Imagen generada con: https://www.amcharts.com/visited_countries/#EE,DE,TR,UA,MX,US,CO,NZ)

En el mapa se pueden observar los siguientes países:

1. Estados Unidos [1]
2. Estonia [17]
3. Nueva Zelanda [18]
4. Alemania [19]
5. Colombia [20]
6. Ucrania [21]
7. México [22]
8. Turquía [23]

La siguiente tabla presenta información general sobre los países seleccionados, considerando las variables que fueron tenidas en cuenta para su elección.

	Población	Superficie	Gasto Militar (% del PBI)	Usuarios de Internet	PBI (2017)
Estados Unidos **[1]**	325,719,178	9,833,520 km2	3.29%	246,809 Millones	$19.390 Billones
Estonia **[17]**	1,319,133	45,227 km2	2.17%	1,097 Millones	$44.177 Mil millones
Nueva Zelanda **[18]**	4,900,880	268,021 km2	1.13%	3,958 Millones	$220.89 Mil millones
Alemania **[19]**	82,800,000	357,386 km2	1.19%	72,365 Millones	$3.685 Billones
Colombia **[20]**	49,913,668	1,141,748 km2	3.39%	27,452 Millones	$327.978 Mil millones
Ucrania **[21]**	42,418,235	603,628 km2	3.50%	23,202 Millones	$112.154 Mil millones
México **[22]**	123,675,325	1,972,550 km2	0.58%	73,334 Millones	$1.250 Billones
Turquía **[23]**	80,810,525	783,356 km2	1.73%	46,838 Millones	$909 Mil millones

Tabla 1 - Variables de orden general que fueron consideradas como insumos para la selección de los países [24]. Todos los datos son presentados usando la escala numérica larga [25].

En busca de fomentar una mayor diversidad en el análisis, los países a evaluar fueron seleccionados en principio, en base a aquellos que tienen publicada una estrategia de ciberseguridad en los últimos 10 años. Este criterio tiene que ver con la actualidad y validez de las estrategias publicadas, especialmente teniendo en cuenta el vertiginoso avance tecnológico y un panorama creciente y cambiante de amenazas cibernéticas. También se buscó aquellas estrategias que fueron publicadas en inglés o español, evitando la necesidad de traducciones externas que pueden contener errores de interpretación.

El criterio fundamental utilizado fue la diversidad de variables que caracterizan a los países seleccionados con relación a nuestro país (ver Tabla 1 y Tabla 2) haciendo

foco en una visión global y diversa de las implementaciones que otras naciones han realizado, y utilizando la variabilidad para evitar sesgos típicos de países ricos, pobres, grandes o pequeños. Las variables elegidas permiten una mejor comprensión del fenómeno de la ciberseguridad y siendo que nuestro país presenta características particulares que dificultan incorporarlo en grupo específico, se eligió entonces un enfoque basado en la diversidad en consonancia con la transversalidad de la ciberseguridad en las actividades que se lleva a cabo en las sociedades modernas.

Según lo descripto, podemos ver que se han elegido países con más habitantes que la Argentina (EEUU), países con menos habitantes (Nueva Zelanda) y países con similar cantidad de habitantes (Ucrania). También se seleccionó considerando países con mayor PBI (México), similar (Estonia) y menor PBI (Colombia). Adicionalmente se consideró la superficie y la ubicación en el globo, como países en Europa (Alemania) o en Asia (Turquía) y en Oceanía (Nueva Zelanda), además de algunos en América (EEUU, Colombia y México). Según la información publicada por la Unión Internacional de Telecomunicaciones (ITU) existen 124 países con estrategias de ciberseguridad aprobadas [15]. Sin embargo, cabe destacar que no todas se encuentran públicamente disponibles o en algunos casos, sus textos están publicados en un idioma distinto al inglés o español, por lo cual no pueden ser utilizadas a los fines de este trabajo.

Nótese que podría haberse utilizado otros criterios de selección, como por ejemplo las estrategias pertenecientes a países cercanos geográficamente o la pertenencia a una misma región, la similitud cultural o países con dimensiones comparables. Sin embargo, se descartaron estos criterios por limitar la diversidad de análisis en lugar de expandirla y para evitar la consideración de puntos de vista ajenos a nuestra economía y situación geopolítica como único criterio.

Como cierre de lo mencionado anteriormente, se agregan a continuación algunos criterios de selección destacables respecto a los países elegidos:

1. Estados Unidos [1]

- Por ser una de las principales potencias en materia de ciberseguridad y cuyas políticas son frecuentemente consideradas como estándares internacionales
- Por su ubicación geográfica en el continente americano

2. Estonia [17]
   - Por su PBI de tamaño similar al de Argentina
   - Por su historia reciente, habiendo sido víctima en el año 2007 de uno de los mayores ciberataques conocidos
3. Nueva Zelanda [18]
   - Por su ubicación geográfica alejada de nuestra región
   - Por ser conocida como una nación avanzada y segura según estándares internacionales
4. Alemania [19]
   - Por ser conocida como una nación avanzada y segura según estándares internacionales
   - Por su posición como eje de innovación en materia de tecnología y referente de los países industrializados
5. Colombia [20]
   - Por poseer un PBI comparable al nuestro
   - Por su ubicación en el continente americano, especialmente en América del Sur, compartiendo aspectos culturales y procesos históricos
6. Ucrania [21]
   - Por su historia reciente, habiendo sido víctima en el año 2015 de unos de los mayores ciberataques de los que se tiene registro
   - Por su ubicación geográfica alejada de nuestra región y por estar en el medio de un conflicto armado
7. México [22]
   - Por poseer un PBI mayor al nuestro
   - Por su ubicación en el continente americano, especialmente en Norte América donde limita con Estados Unidos

8. Turquía [23]
    - Por su ubicación geográfica alejada de nuestra región
    - Por encontrarse en una zona de conflicto con naciones vecinas y grupos terroristas

La siguiente tabla presenta las variables mencionadas con anterioridad, pero en el marco de nuestro país:

	Población	**Superficie**	**Gasto Militar (% del PBI)**	**Usuarios de Internet**	**PBI (2017)**
Argentina	43,847,430	2,780,400 km2	0.95%	30,786 Millones	$625.921 Mil millones

Tabla 2 - Variables de referencia con respecto a nuestro país. Todos los datos son presentados usando la escala numérica larga [25].

Este análisis busca fomentar una sólida base de estudio en esta sección para luego poder plantear las bases de una posible ENCS para la República Argentina, habiendo considerado una serie de países con condiciones socio-culturales diversas y con un amplio espectro de realidades tecnológicas, con el objeto de generar un espacio muestral que intersecte distintas miradas, distintos grados de madurez y distintas concepciones socio-políticas.

La siguiente tabla presenta algunos datos básicos sobre las estrategias de los países seleccionados:

	Año de publicación	**Cantidad de Paginas**	**Idioma de Publicación**	**Idioma de la versión revisada**	**Organismo responsable de su redacción**
Estados Unidos **[1]**	2018	30	Inglés	Inglés	Departamento de Seguridad Interior
Estonia **[17]**	2014	14	Estonio	Inglés	Ministerio de Asuntos económicos y de comunicación

	Año de publicación	Cantidad de Paginas	Idioma de Publicación	Idioma de la versión revisada	Organismo responsable de su redacción
Nueva Zelanda **[18]**	2015	8	Inglés	Inglés	Ministerio de Comunicaciones
Alemania **[19]**	2011	16	Alemán	Inglés	Ministerio Federal del Interior
Colombia **[20]**	2014	15	Español	Español	Ministerio de Tecnologías de la Información y las Comunicaciones
Ucrania **[21]**	2016	8	Ucraniano	Inglés	Decreto Presidencial
México **[22]**	2017	30	Español	Español	Gobierno de México
Turquía **[23]**	2016	26	Turco	Ingles	Ministerio de Asuntos de Transporte Marítimo y Comunicaciones

Tabla 3 - Datos básicos de las estrategias de ciberseguridad elegidas

Comparación de estrategias de ciberseguridad

La siguiente tabla detalla un análisis comparativo de la información contenida en los textos de las estrategias de ciberseguridad seleccionadas. Para facilitar su entendimiento, se propone la siguiente escala para los aspectos considerados:

1. Expresamente incluida
2. Indirectamente especificado
3. No incluido

	Visión, Misión, Metas	Objetivos	Principios	Contexto Internacional, Tendencias	Riesgos y Amenazas
Estados Unidos	1	2	1	1	1
Estonia	1	1	1	1	1
Nueva Zelanda	1	2	1	1	2
Alemania	3	1	1	2	3
Colombia	3	3	1	1	3
Ucrania	2	2	2	1	1
México	2	1	1	1	3
Turquía	1	1	1	1	1

Tabla 4 - Análisis comparativo de los textos de las estrategias de ciberseguridad seleccionadas

A continuación, se analiza cada uno de los aspectos mencionados precedentemente.

Revisión de visiones, misiones y metas

La mayoría de las estrategias de ciberseguridad analizadas incluye algún nivel de definición de visión, de misión y de metas que permiten definir hacía donde debe apuntar la Nación al momento de proteger el ciberespacio y a sus ciudadanos frente a los riesgos de las tecnologías de la información.

Visión, Misión, Metas

Estados Unidos	Para el 2023 haber mejorado la gestión del riesgo de ciberseguridad nacional al aumentar la seguridad y resiliencia en las redes gubernamentales e infraestructura crítica, reduciendo ciber actividades ilícitas, mejorando la respuesta a ciber incidentes y creando un ecosistema más seguro y confiable mediante la creación de uno basado en la unión de varios departamentos, un fuerte liderazgo y acuerdos con agencias federales y no federales.
Estonia	Estonia es capaz de asegurar la seguridad nacional y proveer el funcionamiento de una abierta, inclusiva y segura sociedad. Mejorar las capacidades de ciberseguridad y aumentar el conocimiento público respecto a las ciberamenazas, forma asegurando una continuidad en la confianza en el ciberespacio.
Nueva Zelanda	Nueva Zelanda segura, resiliente y prospera en línea, buscando: • Que prosperen los neozelandeses y sus negocios • Que el daño por ciber amenazas y ciber crimen se reduzca • Que los derechos fundamentales sean respetados y protegidos • Que la infraestructura critica sea defendida • Que Nueva Zelanda sea respetado internacionalmente como un lugar seguro para hacer negocios y almacenar información
Alemania	*No definido*
Colombia	*No definido*
Ucrania	Crear condiciones para el funcionamiento seguro del ciberespacio y su uso para el beneficio de los individuos, la sociedad y el Estado.
México	En 2030 ser una nación resiliente ante los riesgos y amenazas en el ciberespacio que aprovecha con responsabilidad el potencial de las TIC para el desarrollo sostenible en un entorno confiable para todos.
Turquía	Determinar, coordinar e implementar políticas eficientes y sustentables para garantizar la ciberseguridad nacional.

Podemos apreciar la diferencia de criterios respecto a la selección y redacción de la misión, visión y metas en las distintas estrategias analizadas. Alemania y Colombia, por ejemplo, no incluyen una definición concreta, mientras que países como

México y Estados Unidos definen hasta una fecha específica como plazos para las metas a cumplir.

Revisión de objetivos

La siguiente tabla representa la lista de los distintos objetivos que son principalmente definidos por las distintas Estrategias Nacionales de Ciberseguridad seleccionadas:

	Objetivos
Estados Unidos	• Evaluar la evolución de los riesgos de ciberseguridad • Proteger los sistemas de información del Gobierno Federal • Proteger la infraestructura crítica • Prevenir el uso criminal del ciberespacio • Responder efectivamente a ciber incidentes • Fortalecer la seguridad y la confianza del ecosistema de ciberseguridad • Mejorar la gestión de las actividades de ciberseguridad
Estonia	• Asegurar la protección de los sistemas de información que proveen servicios críticos • Mejorar la lucha contra el cibercrimen • Desarrollar capacidades de ciberdefensa nacional • Gestionar la evolución de amenazas de ciberseguridad • Desarrollar actividades entre diferentes sectores
Nueva Zelanda	• Ciber resiliencia • Ciber capacidad y competencia • Enfrentar el cibercrimen • Cooperación internacional
Alemania	• Protección de la infraestructura crítica • Proteger sistemas de tecnologías de la información (TI) • Fortalecer la seguridad de los sistemas de TI en la administración publica • Centro nacional de respuesta al cibercrimen • Concejo nacional de ciberseguridad • Control efectivo del crimen en el ciberespacio • Acciones coordinadas efectivamente para proteger la ciberseguridad de Europa y del mundo

	• Uso de tecnologías de la información confiables y seguras • Desarrollo de personal en autoridades federales • Herramientas para responder a ciberataques
Colombia	*No definido*
Ucrania	• Establecer un sistema nacional de ciberseguridad • Mejorar las capacidades de las entidades de defensa y el sector de seguridad para la lucha efectiva contra las ciber amenazas, espionaje, terrorismo y crimen, desarrollando la cooperación internacional en estos aspectos • Asegurar la protección de los recursos informáticos y de la infraestructura que de ellos depende
México	• Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC (Tecnologías de la Información y Comunicación) de manera responsable para el desarrollo sostenible del Estado.
Turquía	• Asegurar la seguridad, confidencialidad y privacidad de todos los servicios, transacciones e información provista a través de las TIC junto con los sistemas que se utilizan para proveerlos y cubren el ciber espacio en su totalidad • Determinar acciones de ciberseguridad para minimizar los efectos de los incidentes de ciberseguridad • Desarrollar localmente tecnologías críticas y productos para asegurar la ciberseguridad, confidencialidad y privacidad

Podemos apreciar que la mayoría de los objetivos se encuentra presentada en forma de lista, con la excepción de México que prefirió un formato más tradicional. Por otro lado, la estrategia de Colombia no menciona objetivos concretos para su estrategia, sino que la información se encuentra diseminada a lo largo del texto sin definiciones específicas. En este sentido, Colombia parece haber buscado un enfoque implícito para la definición de los objetivos de su Estrategia.

Revisión de principios

Las estrategias de ciberseguridad evaluadas incluyen en su mayoría, una lista de principios que permiten definir las bases y los elementos fundacionales que los redactores tuvieron en cuenta a la hora de su redacción.

	Principios
Estados Unidos	• Priorización de riesgos • Eficiencia de costos • Innovación y agilidad • Colaboración • Enfoque global • Balancear patrimonios • Valores nacionales
Estonia	• Ciberseguridad es una parte integral de la seguridad nacional • Ciberseguridad es garantizada mediante el respeto de derechos fundamentales y libertades • Ciberseguridad es asegurada en base a los principios de proporcionalidad • Ciberseguridad es asegurada en una manera coordinada entre el sector público, privado y terceras partes. • La ciberseguridad empieza con el uso responsable de herramientas de ICT • Anticipar y prevenir potenciales amenazas y responder efectivamente a amenazas que se materializan • La ciberseguridad es apoyada por investigación y desarrollo internacional • La ciberseguridad es asegurada mediante la cooperación internacional
Nueva Zelanda	• Los acuerdos son esenciales • Potenciar el desarrollo económico • Defender la seguridad nacional • Proteger los derechos humanos en la red
Alemania	• Promover la prosperidad económica y social de Alemania • Proteger la disponibilidad de información y comunicación • Asegurar la integridad, autenticidad y confidencialidad de los datos • Cooperación con EEUU, NATO, Consejo de Europa, G8, OSCE (Organización para la Seguridad y Cooperación en Europa) y otros organismos multilaterales

Colombia	• Generación de legislación que permita el intercambio de información entre las entidades del Estado, buscando garantizar la integridad, la confidencialidad y la disponibilidad de información • Generación de legislación para proteger el ciberespacio de amenazas que atenten contra la soberanía nacional y los principios constitucionales • Incorporación de los delitos cibernéticos en la legislación • Generación de directrices de protección de confidencialidad, integridad y disponibilidad de los datos del Estado • Dimensionamiento de políticas de seguridad de la información y ciberseguridad para la incorporación de software en las entidades del Estado • Generación de legislación para fortalecer las alianzas y los acuerdos de cooperación internacional en la lucha contra el cibercrimen • Generación de legislación para la adecuada identificación de los ciudadanos y la protección de su identidad.
Ucrania	• Proteger la ley y el respeto por las personas, los derechos humanos y las libertades • Proteger los intereses nacionales • Apertura, accesibilidad, estabilidad y seguridad en el ciberespacio • Acuerdos entre el sector público y privado • Adecuación y proporcionalidad entre medidas de seguridad y riegos • Priorizar medidas preventivas • Inevitabilidad de castigo por comisión de cibercrímenes • Prioridad en el desarrollo científico, tecnológico y productivo. • Cooperación internacional para la construcción de confianza mutua en el ciberespacio • Aseguramiento del control civil y democrático sobre unidades militares legalmente establecidas y agencias de seguridad que operan en el área de la ciberseguridad
México	• Perspectiva de derechos humanos • Enfoque basado en la gestión de riesgos • Colaboración multidisciplinaria y de múltiples actores
Turquía	• La ciberseguridad es asegurada por medios y métodos basados en un eficiente y continuo análisis y mejora de la gestión de riesgos • Todos los stakeholders deben saber sobre riesgos de ciberseguridad y estar atentos a cómo gestionar esos riesgos para que dichos riesgos no afecten a otros • La gestión de riesgos implica una rápida remoción de vulnerabilidades técnicas, previniendo y respondiendo ante ataques y amenazas y minimizando potenciales daños • La ciberseguridad requiere cooperación internacional y de los distintos sectores que intercambian información y generar confianza • Todos los stakeholders deben cumplir con la ley, respetar la libertad de expresión, los derechos humanos y otras libertades en sus esfuerzos por asegurar la ciberseguridad

- Los stakeholders deben actuar con transparencia, responsabilidad y valores éticos mientras gestionan riesgos en el ciberespacio
- Las medidas implementadas deben ser proporcionales al riesgo en cuestión y los impactos negativos y positivos deben ser analizados y balanceados
- Se promueve el uso de productos y servicios nacionales.

Podemos apreciar la variabilidad y granularidad en la presentación de los principios listados en las distintas estrategias, siendo el caso de Turquía, Estonia, Ucrania y Colombia las que aportan mayor detalle.

Revisión de contextos y tendencias

En la mayoría de las estrategias evaluadas, se encuentra un análisis del contexto, del marco nacional e internacional y de las tendencias que dan una idea de la situación en la cual la estrategia fue redactada, a manera de diagnóstico. Estos contextos o tendencias guardan un marco común que normalmente refiere al crecimiento de la conectividad y a los distintos impactos en la sociedad y la economía que genera la ciberseguridad. Sin embargo, a los fines de incluir un resumen en esta sección, se ha realizado un análisis general, resumiendo los contextos y tendencias de cada estrategia, si bien cada uno de los documentos analizados muestra un distinto nivel de detalle.

	Contexto internacional, tendencias
Estados Unidos	El extraordinario crecimiento del acceso a internet y la mayor dependencia de muchos servicios provistos a través de la red, junto con el incremento en el riesgo de ciber ataques por parte de otros Estados o terroristas, motivan la creación de este NSCC. También el desarrollo económico asociado al ciberespacio y la necesidad de gestionar los riesgos generados por las nuevas tecnologías.
Estonia	El rápido desarrollo de TI y el creciente número de dispositivos conectados a la red. La creciente importancia de la tecnología en la cotidianeidad de la vida de los ciudadanos, y su utilidad para que el estado provea servicios a través de internet. La creciente habilidad de los criminales para utilizar el ciberspacio

	como método para actividades ilícitas. La creciente complejidad en la identificación de los criminales y si estos operan en conjunto con Estados u organizaciones con diversas motivaciones políticas o financieras.
Nueva Zelanda	El incremento de la conectividad, el impacto de los cibercrimenes que pueden causar daño real, más allá de lo digital.
Alemania	*No definido*
Colombia	La conversión de las TIC en aspectos claves de la sociedad actual y socio estratégico del estado dentro de las políticas nacionales e internacionales.
Ucrania	La rápida transformación del mundo en términos de tecnología de la información. Avances en el uso de nuevas tecnologías y la creación de nuevas amenazas. El conflicto con la Federación Rusa que requiere acción inmediata de parte del Estado nacional para proteger la seguridad del país
México	La vulnerabilidad de los sistemas de información puede afectar gravemente a las personas, su información, su patrimonio, su reputación e incluso su dignidad.
Turquía	Las TIC se han vuelto componentes integrales de la sociedad y la economía y contribuyen significativamente a su desarrollo.

Podemos apreciar como Estados Unidos y Estonia hacen mayor foco en el contexto internacional en sus estrategias, mientas que Alemania no incluye este tipo de información y pone mayor foco en su situación y necesidades internas.

Revisión de riesgos y amenazas

La mayoría de las estrategias de ciberseguridad analizadas incluye algún nivel de definición riesgos, pero no todas los hacen con igual detalle. Generalmente se listan algunas de las amenazas más comunes, pero según lo encontrado, se busca mantener una visión global y estar preparado para los cambios y las nuevas amenazas del futuro. Por lo tanto, los riesgos se describen más a modo de ejemplo, que como lista que busca comprender todas las posibles ciberamenzas.

Riesgos, amenazas y desafíos

Estados Unidos	• Espionaje • Intereses en ideologías políticas • Riesgos financieros • Ataques a agencias federales • Interconexión entre el espacio físico y el virtual • Infraestructura critica • Ransomware • DarkWeb (pasaportes falsos, drogas, armas, malware) • Lavado de dinero
Estonia	• Dependencia de las TIC • Extensión del uso de la Infraestructura crítica (nacional e internacional) • Reducción de la confianza en servicios digitales • Pérdida de vidas
Nueva Zelanda	• Pérdidas financieras • Daño a la reputación del país o las empresas • Robo de propiedad intelectual • Daño a servicios u operaciones • Interrupción de los servicios críticos
Alemania	*No definido*
Colombia	*No definido*
Ucrania	• Discrepancia en la infraestructura nacional de comunicaciones • Insuficiente nivel de protección de la infraestructura crítica • Falta de sistematización en las medidas de protección de la infraestructura crítica • Falta de desarrollo organizacional y técnico para proteger la infraestructura crítica de las ciberamenazas • Falta de efectividad en las actividades de protección contra ciberamenazas • Inadecuado nivel de coordinación, cooperación e intercambio de información entre entidades asociadas a la ciberseguridad
México	*No definido*
Turquía	• Interrupción de la energía, trasporte u otros servicios críticos • Robo, publicación, modificación o destrucción de información personal y confidencial • Robo, publicación, modificación o destrucción de información sensible

o comercialmente valiosa
- Perjuicio a la reputación de varias instituciones u organismos por información obtenida como consecuencia de un ciberataque
- Daño material como consecuencia de la falla de un servicio
- Pérdida de reputación de compañías asociadas al comercio electrónico o al sector financiero
- Pérdida de continuidad en las operaciones de pequeñas y medianas empresas de servicios por falta de gestión de sus sistemas
- Exposición a malware y ataques de phishing, fraude u otros ciberdelitos que puedan robar, manipular o destruir la información de personas u organizaciones
- Fraude a instituciones u organizaciones
- Interrupción de servicios y operaciones provistos por sistemas informáticos

En el caso de los riesgos, amenazas y desafíos, se observa en las estrategias analizadas que Alemania, Colombia y México decidieron no incluir riesgos ni amenazas y, por el contrario, países como Turquía, Ucrania y Estados Unidos han puesto gran foco en listar los posibles riesgos y amenazas que fundamentan la creación de sus respectivas estrategias de ciberseguridad. En este sentido, dada la velocidad con que las amenazas y riegos mutan en consonancia con la rápida evolución tecnológica, podría inferirse que resulta complejo incluir este tipo de información en la estrategia de ciberseguridad, ya que requeriría una actualización casi permanente.

Aspectos en común

Hoy las estrategias de ciberseguridad reconocen en sus textos que la economía, la sociedad y los gobiernos necesitan de internet para muchas de sus funciones esenciales y que las ciberamenazas son un riesgo enorme que está creciendo a gran velocidad. La mayoría de las estrategias contemplan la idea de coordinación de políticas a través de distintos niveles de gobierno, definiendo roles y responsabilidades. Todas manifiestan y profundizan la necesidad de cooperación entre el sector público y el sector privado, destacando la necesidad de respetar valores fundamentales como privacidad, la libertad de expresión y el libre flujo de información entre individuos, organizaciones y países. [26]

A continuación, se enuncian algunos conceptos que se destacan en la mayoría de las estrategias revisadas:

- Mejorar la coordinación entre distintas áreas de gobierno, generando políticas y legislación que permitan trabajar las distintas facetas de la ciberseguridad y proveer un marco donde se defina la responsabilidad y la posibilidad de accionar sobre los delitos informáticos con herramientas modernas, acordes a los desafíos actuales.
- Mejorar la cooperación internacional con otros países, buscando fortalecer alianzas y comprendiendo que la ciberseguridad es un problema global que debe ser trabajado en conjunto para obtener resultados.
- Trabajar en la gestión de los valores fundamentales de la sociedad para balancear la seguridad con derechos esenciales como la privacidad y la libertad de expresión.
- Promover el trabajo en equipo entre el sector privado y el sector público, siendo clave el desarrollo conjunto de soluciones y legislación que permita a ambos el desarrollo sustentable y la mitigación de riesgos.
- Fomentar el desarrollo económico y productivo del país mediante el desarrollo de nuevas tecnologías y servicios de TI, incluyendo aspectos de seguridad en los productos y servicios que se generen. [26]

Tendencias en estrategias de ciberseguridad

La siguiente lista presenta tendencias que pueden apreciarse con la evaluación realizada, siendo la dirección que varios gobiernos parecen estar tomando.

- Discusiones y consideraciones sobre la evolución y consideración de la soberanía nacional en el ciberespacio.

- Políticas y legislación más amplia y flexible para adaptarse al constante cambio de las amenazas y las tecnologías del ciberespacio.
- Valor central de la economía en todos los aspectos asociados a la ciberseguridad y búsqueda de maneras de evitar impactos en la economía real, fomentando el desarrollo de nuevas tecnologías como ventaja competitiva.

Tendencias en planes de acción

La siguiente lista presenta tendencias encontradas en el análisis de varias estrategias de ciberseguridad y que delinean diferentes planes de acción propuestos a partir de ellas:

- Protección de infraestructuras críticas
- Desarrollo de leyes para combatir y sancionar los ciberdelitos
- Iniciativas para que el público en general tome conocimiento de los riesgos asociados a la ciberseguridad
- Planes de educación para formar capacidades en los ciudadanos en aspectos relacionados a la ciberseguridad desde jóvenes
- Grupos de gestión de incidentes, conocidos como Equipos de Respuesta de Incidentes de Ciberseguridad o CSIRTs por sus siglas en inglés (*Computer Security Incident Response Teams*)
- Investigación y desarrollo de nuevas tecnologías en el ámbito local

Otras consideraciones sobre las estrategias

Algunos *stakeholders* (interesados) en el mercado internacional han expresado cierta preocupación con respecto a algunas de las estrategias generadas por los distintos gobiernos, destacando inconvenientes que los afectan principalmente en el aspecto comercial, ante el temor de verse comprometidos por las políticas que los Estados implementan en materia de ciberseguridad y su impacto en el mercado tecnológico. Por lo tanto, este análisis no estaría completo sin la visión del mercado,

que lamentablemente no siempre está alineada con los intereses de las naciones extranjeras o a las cuales pertenece su casa central. Entre la bibliografía revisada pueden encontrarse las siguientes opiniones y comentarios:

- Los requerimientos y especificaciones de seguridad de algunos países no son estándar y complican el diseño de productos y servicios, al momento de ser comercializados en otras naciones.
- Los múltiples consorcios de certificaciones de seguridad y sus diferentes reglas complican la validación de dispositivos electrónicos.
- Las crecientes preocupaciones de seguridad informática limitan la posibilidad de innovación y aumentan el costo de lanzar un nuevo producto a la venta [26].

La presente lista expresa la opinión de parte de la industria, que debe balancear el costo de incorporar seguridad en sus productos con el precio que los usuarios están dispuestos a pagar por sus dispositivos. Adicionalmente los usuarios en su mayoría todavía no reclaman avanzadas medidas de seguridad en sus productos o servicios y es más común escuchar que se quejan por la cantidad de mecanismos de seguridad que deben sortear para llevar adelante las tareas, que por lo inseguras que son las aplicaciones que usan. Desde luego, esta visión suele cambiar para todos aquellos que han sido víctima de un delito informático, más allá de su tipificación en cada país.

En un último apartado, con respecto a las complejidades que los *stakeholders* del sector privado vislumbran en las estrategias de ciberseguridad, es posible considerar la falta de incentivos adecuados o en su defecto, la falta de consecuencias en caso de que algo salga mal. Debe considerarse que algunos problemas de seguridad cibernética existen porque la empresa responsable de diseñar el sistema normalmente no sufrirá significativas consecuencias si el mismo falla o es vulnerable. Por lo general, la experiencia muestra que el mayor afectado es el usuario, quien tiende a sufrir por los efectos negativos de los ciberataques, mientras que los cuerpos directivos de las organizaciones suelen enfrentar consecuencias civiles o penales proporcionalmente menores por las vulnerabilidades de los sistemas que producen.

Adicionalmente muchas empresas encuentran incentivos en la convergencia tecnológica, siendo el uso de los mismos protocolos y programas un escenario deseado pues baja las inversiones iniciales y reduce los costos operativos. Sin embargo, esta práctica ha probado exponer a todas las empresas a los mismos riesgos de TI ya que en lugar de diseñar protocolos seguros y acordes a sus necesidades, reutilizan algo ya existente principalmente porque es económicamente más rentable, ya que baja los costos de desarrollo y producción. [7]

PARTE 3 Ciberseguridad en la Argentina

Preparación

La presente sección propone lineamientos de base para el diseño de una estrategia nacional de ciberseguridad para la República Argentina en el marco del trabajo final de maestría, sobre la base de los conocimientos adquiridos mediante la revisión de otras estrategias y del material consultado, según se describió en el capítulo anterior.

El propósito de las siguientes secciones es proponer un modelo de estrategia nacional, que pueda ser utilizado para la construcción de la Estrategia Argentina de Ciberseguridad. Como se desarrolla a continuación, las autoridades solo han manifestado la creación de un Comité de Ciberseguridad [27] que busca crear dicha estrategia, sin embargo se desconoce el estado la misma, pudiendo solo afirmar que hasta la presentación de este Trabajo Final de Maestría, no ha sido difundida, aprobada o publicada en el boletín oficial.

Antecedentes locales

En la República Argentina existe como precedente a la generación de una Estrategia Nacional de Ciberseguridad, el Decreto Nº 577 publicado en el Boletín Oficial de la República Argentina el 31 de julio de 2017 [28], que crea el Comité de Ciberseguridad y en cuyo artículo 1 º y 5º el Presidente de la Nación dispone:

ARTÍCULO 1°.- Créase el COMITÉ DE CIBERSEGURIDAD en la órbita del MINISTERIO DE MODERNIZACIÓN, que estará integrado por representantes del citado Ministerio, del MINISTERIO DE DEFENSA y del MINISTERIO DE SEGURIDAD, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

ARTÍCULO 5°.- Encomiéndase al MINISTRO DE MODERNIZACIÓN, o a quien ese designe, impulsar los actos administrativos y demás acciones necesarias para la implementación de la Estrategia Nacional de Ciberseguridad que apruebe el COMITÉ DE CIBERSEGURIDAD, así como de los objetivos en ella contenidos.

Este esfuerzo inicial, propuesto en julio de 2017 por el actual Presidente muestra la necesidad de trabajar en una estrategia de ciberseguridad y la visión política que comienza a alinearse con concepciones globales sobre riesgos cibernéticos latentes en el sector tecnológico.

Previo al Decreto Nº 577/2017, la defensa del ciberespacio se incorpora en la agenda política y muestra intenciones de progreso, según lo denota la prioridad de gobierno número 74: "Ciberseguridad", enmarcado en el objetivo V: "Combate al Narcotráfico y mejora de la Seguridad", presentado por la Presidencia de la Nación al principio de la administración actual. Esta lista de objetivos centrales fue fijada como resultado de la Reunión de Trabajo del Gabinete en Chapadmalal, con el fin de establecer un rumbo definido para el futuro de su gestión. [29]

Adicionalmente y ya con posterioridad a la creación del Comité de Ciberseguridad, el 5 de Noviembre de 2018 se publicó en el Boletín Oficial la Agenda Digital Argentina [30], la cual registra la voluntad del Poder Ejecutivo Nacional de alinear el progreso de la nación con la transformación digital, presentando en lo referente a ciberseguridad el objetivo VII, el cual como parte de su artículo segundo, plantea: "desarrollar capacidades en ciberseguridad para generar confianza en los entornos digitales".

A nivel nacional es posible apreciar un crecimiento en la importancia del sector tecnológico y en ese marco, es esperable un mayor número de inversiones asociadas con la transformación digital del Estado en búsqueda de eficiencias, mejora en los servicios al ciudadano, modernización y reducción de costos. El gobierno actual ha invertido fuertemente en lo que se propone como el Gobierno Digital [31], una de las propuestas fomentadas por el ex Ministerio de Modernización creado el 10 de Diciembre de 2015, según lo dispuesto en el Artículo 23 de la Ley de Ministerios, recientemente convertido en la Secretaria de Gobierno de Modernización de la Jefatura de Gabinete de Ministros, según lo dispuesto en los decretos 801/2018 y 802/2018 [32] [33]. Esta dependencia se ocupa de la implementación de nuevas tecnologías para la función pública, la transparencia de la gestión y de procesos de formación de empleados públicos.

Según la legislación vigente podemos destacar los siguientes objetivos relacionados con la ciberseguridad en el ámbito de dicha Secretaría de Gobierno, si bien no se la nombra expresamente:

14. Intervenir en la definición de estrategias y estándares sobre tecnologías de información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información de la Administración Nacional.

15. Diseñar, coordinar e implementar la incorporación y mejoramiento de los procesos, tecnologías, infraestructura informática y sistemas y tecnologías de gestión de la Administración Pública Nacional.

16. Proponer diseños en los procedimientos administrativos que propicien sus simplificación, transparencia y control social y elaborar los desarrollos informáticos correspondientes.

17. Actuar como Autoridad de Aplicación del régimen normativo que establece la infraestructura de firma digital para el sector público nacional.

18. Intervenir en el desarrollo de sistemas tecnológicos con alcance transversal o comunes a los organismos y entes de la Administración Pública Nacional, Centralizada y Descentralizada.

Adicionalmente el Ministerio de Seguridad de la Nación también tiene competencia en el área de la ciberseguridad, si bien como en el caso anterior, sin mencionarla expresamente, pues el artículo 22 bis de la Ley de Ministerios indica que le compete al Ministerio de Seguridad asistir al Presidente de la Nación y al Jefe de Gabinete de Ministros, en orden a sus competencias, en todo lo concerniente a la seguridad interior, a la preservación de la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías en un marco de plena vigencia de las instituciones del sistema democrático. [32] [33] [34]

Finalmente otro organismo que podría tener un rol en la estrategia de ciberseguridad de la Nación es la Agencia Federal de Inteligencia (AFI) y cuya

incorporación en el mundo de la ciberseguridad es un poco tardía con respecto a otros países, pero que en los últimos años ha puesto énfasis en desarrollar sus capacidades de defensa en la materia, mediante la incorporación de nuevos cursos de formación (principalmente a través de la Escuela Nacional de Inteligencia - ENI) y la contratación de profesionales especializados. [35]

Con la intención de contribuir al avance del tema, el presente trabajo busca aportar los lineamientos de base que, en función del análisis realizado sobre las estrategias de otros países, faciliten el desarrollo de la Estrategia Nacional para nuestro país, a manera de contribución a los esfuerzos nacionales en esa dirección. Dichos lineamientos de base se describen a continuación, bajo el título: "Lineamientos para una Estrategia Nacional de Argentina" y conforman lo que podría ser una propuesta de texto para el documento correspondiente.

Lineamientos para una Estrategia Nacional de Argentina

1. Introducción

En el marco de la creciente interconectividad entre dispositivos de distinta índole y del ritmo vertiginoso de la incorporación de nuevos usuarios a Internet, es vital comenzar a considerar el ciberespacio como un área en la que el Estado debe estar presente, en su rol regulatorio y velando por el bienestar de los ciudadanos y las organizaciones. El uso del ciberespacio no solo está creciendo en América Latina en términos de cantidad de usuarios, sino también respecto a la inversión. En efecto, el retraso que los distintos países tienen en materia de transformación digital, está obligando a las naciones a realizar fuertes inversiones en la digitalización de servicios que hasta el momento se encontraban completamente fuera de la órbita de las tecnologías de información.

Estas rápidas transformaciones, que van desde la ampliación de los servicios de banca digital, hasta la digitalización de los procesos burocráticos del Estado, se

producen a gran velocidad y en muchos casos, sin el acompañamiento del debido análisis de riesgos o de implementaciones acordes a los estándares internacionales. En este contexto, América Latina, incluyendo a nuestro país, progresa hacia mayores grados de madurez en términos de tecnologías de la información e indirectamente, con respecto a la ciberseguridad.

En efecto, la ciberseguridad se ha convertido en un desafío para la soberanía de los países y los gobiernos están obligados a extender la protección de sus ciudadanos al ciberespacio, buscando proteger la confidencialidad, integridad y disponibilidad de los datos que se encuentran en poder del Estado, de las organizaciones y de los individuos. Esta protección no solo debe considerarse desde el punto de vista social, sino también desde el económico, ya que el desarrollo de las naciones está atado a sus capacidades tecnológicas y aquellos países que no estén dispuestos a financiar y profundizar su transformación digital, verán mermada su capacidad de crecer en el mediano y largo plazo.

Por otro lado, las organizaciones criminales asociadas a la ciberseguridad se encuentran en franco crecimiento y las herramientas que utilizan para perpetrar sus ataques son cada vez más sofisticadas. Adicionalmente nuevos actores se incorporan en el ya complicado panorama de la ciberseguridad, formando un conjunto de amenazas que deben ser evaluadas y gestionadas por los gobiernos, con el fin de proteger a los ciudadanos y las organizaciones que habitan y ejercen sus actividades en el territorio soberano.

2. Contexto internacional

En el marco internacional existe una constante presión para los países, las empresas, las organizaciones y todas las entidades que manejan información sensible, gestionan servicios críticos o tiene a su cargo la mitigación de riesgos en el área de la ciberseguridad, con respecto a diseñar estrategias que permitan reducir la posibilidad de verse afectadas por ataques cada vez más complejos y difíciles de prevenir.

Muchas de las dificultades y desafíos que se presentan en el contexto internacional, como por ejemplo la interdependencia de infraestructura crítica, los vínculos entre empresas nacionales y extranjeras, las relaciones entre los distintos países y organizaciones gubernamentales y no gubernamentales, tiende a complicar la implementación de acciones que puedan afectar las relaciones geopolíticas en las que se encuentra inmersa nuestro país.

Argentina debe encarar esta estrategia de ciberseguridad con un marcado interés en la formulación de acuerdos de cooperación internacional, no solo en términos de prevención y sanción del ciberdelito sino con respecto a la cooperación extranjera en caso de ataques, herramienta fundamental para disuadir posibles atacantes y factor crítico para poder identificar y perseguir a los culpables que habitan otros países.

3. Marco institucional

La ciberseguridad, al igual que la seguridad física, requiere coordinación entre los distintos niveles de gobierno y sus organismos descentralizados, así como también con el público en general. No existe política de ciberseguridad que funcione por sí misma o en aislamiento, pues parte de la complejidad del problema radica en la interconexión que existe entre los diversos sistemas que procesan la información. Esta interconexión se extiende también al sector privado, responsable en nuestro país de proveer gran parte de los servicios públicos, a través de equipamiento y recursos tecnológicos normalmente conocidos como infraestructura crítica.

Es absolutamente necesario que la política de ciberseguridad se defina a nivel nacional y que se coordine con los distintos gobiernos provinciales y municipales con respecto a cómo implementar políticas que permitan proteger a los ciudadanos o a las organizaciones, ya que la Argentina ha adoptado para su funcionamiento un esquema federal.

Es necesario también considerar modificaciones en la legislación que permitan la coordinación entre diferentes organismos reguladores gubernamentales y el sector privado a los fines de proteger la infraestructura crítica, que permite a la provisión de servicios esenciales para la Nación, entre los que se pueden considerar, por ejemplo: agua, electricidad, telecomunicaciones y transporte.

Por otro lado, la historia de la República Argentina y su registro en materia de derechos humanos obligan a incluir consideraciones adicionales con respecto a la creación de normas de ciberseguridad que garanticen los derechos individuales en el ciberespacio. Dichas consideraciones deben permitir un escrutinio por parte del público en general, garantizando un nivel de transparencia tal que permita un control responsable del accionar de las fuerzas de seguridad, en este caso para todo lo vinculado al ciberespacio. El mencionado control busca minimizar la posibilidad de excesos por parte de estos organismos en sus habilidades de control y monitoreo de los ciudadanos, principalmente garantizando su privacidad y balanceando las medidas preventivas con los potenciales riesgos que dichas medidas proponen mitigar.

Finalmente es necesario considerar el desarrollo de organismos y especialistas responsables de la prevención, detección y respuesta coordinada ante incidentes de seguridad a nivel nacional. Es vital que el país desarrolle las capacidades y habilidades necesarias para gestionar de forma eficaz y eficiente el creciente volumen de incidentes asociados a la ciberseguridad que afectan a los habitantes y organizaciones de la nación.

4. Misión

Para el año 2025 y como parte de su proceso de transformación digital, que la Argentina sea capaz de brindar mecanismos de protección a sus ciudadanos y organizaciones frente a las ciberamenazas, fomentar el desarrollo productivo y económico en materia de telecomunicaciones y tecnologías de la información seguras, adoptar medidas de protección de su infraestructura crítica y de los servicios que de ella dependen, entablar acuerdos internaciones y de cooperación entre el sector

público y privado con el objeto de minimizar los riesgos asociados a la ciberseguridad y hacer de nuestra Nación un lugar reconocido por sus políticas de ciberseguridad y su absoluto respeto por los derechos y garantías individuales de sus ciudadanos en el ciberespacio.

5. Objetivos

La presente propuesta de Estrategia de Ciberseguridad para la República Argentina abarca los siguientes objetivos:

- Evaluar, gestionar y monitorear el ciberespacio y las ciberamenazas buscando proteger a los habitantes y organizaciones del país.
- Acompañar con una adecuada capacidad de gestión de riesgos la transformación digital del Estado, con la incorporación responsable de nuevas tecnologías, buscando balancear el avance tecnológico con la necesidad de protección en el ciberespacio en nuestro país.
- Apoyar el desarrollo nacional de tecnologías de la información y telecomunicaciones (TICs), particularmente a aquellas aplicadas a la ciberseguridad, en el marco del desarrollo de la Nación en el ciberespacio, buscando multiplicar el impacto de este crecimiento no solo en la ciberseguridad, sino como motor de crecimiento en lo económico y social de la ciudadanía y base de mayores inversiones tecnológicas en el país.
- Generar políticas, normas, leyes y otros instrumentos legales y administrativos junto con acciones concretas que permitan coordinar las distintas áreas de gobierno para mitigar los riesgos asociados a la ciberseguridad, investigar y sancionar las conductas delictivas y la cooperación entre organismos públicos de control y el sector privado con respecto al monitoreo y la gestión de riesgos en materia de infraestructura critica.
- Fomentar la cooperación municipal, provincial, nacional e internacional en busca de la reducción del ciberdelito, la minimización de las

vulnerabilidades y la detección temprana de amenazas que se presentan en el ciberespacio.

- Fortalecer el centro de respuesta ante ciberincidentes a nivel nacional permitiendo gestionar y responder de forma rápida y coordinada ante eventuales ciberataques, y trabajando en conjunto con equipos multidisciplinarios para dar pronta respuesta a los incidentes que tengan a nuestro país como blanco.
- Fortalecer la infraestructura de telecomunicaciones y de la información a nivel nacional, para que empresas, organismos e individuos puedan confiar en los servicios e información provista por el estado y los privados, fomentando el desarrollo económico y social de la nación.
- Generar acuerdos de cooperación internacional en la lucha contra el cibercrimen, fomentando su prevención y asegurando la cooperación de los mismos en caso de ser nuestro país atacado.
- Desarrollar procesos de concientización y diseminación de información relacionada a la ciberseguridad al público en general y a los sectores más vulnerables, en particular en el caso de niños, niñas, adolescentes y adultos mayores.
- Invertir en el desarrollo, formación y capacitación de recursos humanos, trabajando en distintos convenios con la comunidad educativa, el sector público y el sector privado para aumentar la disponibilidad de talento interno en ciberseguridad.

6. Principios

La presente propuesta de Estrategia de Ciberseguridad para la República Argentina contempla los siguientes principios, como base sobre la cual todas las actividades en el ciberespacio deben fundarse:

- Proporcionalidad entre las acciones de mitigación y sus consecuencias. Es necesario que se evalúen los riesgos y sus potenciales impactos con respecto a las medidas que se van a tomar para prevenirlos. Debe

buscarse siempre la proporcionalidad entre los costos, en términos sociales como ser derechos, libertades individuales y privacidad, como también en términos económicos, buscando balancear y siempre justificar las decisiones con profundos análisis respecto de las potenciales consecuencias de las medidas tomadas sobre individuos, organizaciones y la sociedad en general.

- Innovación de tecnologías de la telecomunicación y la información seguras a nivel local, desarrollando no solo la capacidad nacional de producción de bienes y servicios de alto valor agregado, sino también reduciendo la dependencia en tecnologías y recursos extranjeros que limitan la capacidad de acción soberana de la Nación
- Preservación de derechos y libertades individuales y en particular de la privacidad y la protección de la información que los mismos generan y gestionan, contribuyendo a la preservación de su integridad, disponibilidad y confidencialidad.
- Integración internacional con otros países y organismos internacionales para convertirse en un actor clave en ciberespacio, colaborando activamente con los esfuerzos transnacionales en materia de ciberseguridad.
- Integración entre el sector público y privado para gestionar en conjunto los riesgos que presenta el uso intensivo de las tecnologías y diseñar procesos que promuevan el bienestar ciudadano y el beneficio mutuo y aceleren el progreso en materia de TICs aplicadas a la ciberseguridad.

7. Lineamientos para la implementación de un plan de acción

La presente propuesta de Estrategia Nacional incorpora la formulación de un plan coordinado entre las distintas áreas de gobierno, organismos no gubernamentales, el sector privado y la población en general, basado en las siguientes acciones:

<u>Protección de la Infraestructura crítica y de los servicios esenciales</u>

- **Asegurar la protección de la infraestructura critica.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la provisión de servicios esenciales para la población y el desarrollo económico, estableciendo acuerdos público-privados para fomentar la cooperación con la industria en materia de ciberseguridad.
- **Generar alternativas para los servicios esenciales**. El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la creación y el fomento de fuentes alternativas de provisión de servicios críticos, reduciendo la dependencia de un grupo pequeño de empresas y minimizando los puntos únicos de falla.
- **Administrar la interdependencia entre infraestructuras críticas.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará las distintas interdependencias y relaciones que existen entre la gestión, el suministro y la provisión de servicios críticos para sus habitantes, a fin de comprender y mitigar posibles daños que pueden extenderse de una industria en otra, limitando la onda expansiva de un potencial ciberataque o falla generalizada.

Coordinación y cooperación

- **Coordinar iniciativas entre el sector público y el privado.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la colaboración público-privada entre distintas organizaciones, agencias gubernamentales y ONGs, y a la vez, fomentará espacios de difusión y debate entre empresas privados y el sector académico, con el objeto de promover y coordinar esfuerzos entre los distintos actores.
- **Fomentar la participación de expertos en ciberseguridad y el público en general.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la promoción de espacios de discusión, divulgación académica, científica y difusión general para que la población se involucre en la protección del ciberespacio y participe en la elaboración de nueva normativa, con el objetivo de generar una cultura de ciberseguridad.

- **Promover la cooperación internacional en la lucha contra el crimen.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la adhesión a acuerdos internacionales para colaborar con organismos supranacionales y otros países en la lucha contra el crimen organizado, el terrorismo y los ciberdelitos.

Promoción de la investigación y el desarrollo

- **Desarrollar tecnologías e infraestructura nacional asociadas a la ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará el fomento, la financiación y el otorgamiento de beneficios que promuevan la generación de las tecnologías que protejan a la Nación ante incidentes y ciberataques.
- **Promover la innovación en materia de ciberseguridad**. El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará instrumentos de promoción y financiación, con el objeto de maximizar el desarrollo de profesionales y empresas del sector tecnológico para la investigación y el desarrollo en áreas asociadas a la ciberseguridad.
- **Generar un fondo nacional de ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la utilización de un porcentaje del presupuesto nacional en un fondo para la inversión en desarrollo y prevención de riesgos de ciberseguridad, para ser utilizado especialmente, en caso de emergencia ante ciberataques.
- **Generación de capacidades para la detección, prevención de ciberamenazas y ciberincidentes.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la creación de grupos de respuesta a incidentes que monitoreen, prevengan, brinden las alertas necesarias y documenten las amenazas y vulnerabilidades con impacto en nuestro territorio, buscando contar con información confiable que permita tomar decisiones respaldadas por información cuantitativa y cualitativa, orientada a la gestión y prevención de los incidentes que pudieran afectar a la población y a los intereses nacionales.

Desarrollo de instancias de educación y concientización

- **Fomentar el conocimiento público en ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la difusión en diversos medios de comunicación y otros espacios de divulgación de información sobre los potenciales riesgos de ciberseguridad a los que está expuesta la población.
- **Fomentar la formación de profesionales en ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la creación y expansión de los programas universitarios de grado y posgrado para fomentar la generación de nuevas carreras y cursos de especialización que formen profesionales en las diversas áreas asociadas a la ciberseguridad.
- **Inclusión del tema en los programas de formación primaria y secundaria.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la creación y expansión de la formación en ciberseguridad en espacios para alumnos de primaria y secundaria, con actividades y contenidos orientados a minimizar los riesgos a los que están expuestos y fomentar el interés en la ciberseguridad desde temprana edad.
- **Fomentar el desarrollo de profesionales en ciberseguridad en el extranjero.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la continua educación en materia de ciberseguridad, promoviendo su continua formación en los riesgos de las nuevas tecnologías mediante cursos en el extranjero y acuerdos de cooperación con universidades de otros países.

<u>Desarrollo de legislación y fuerzas de seguridad</u>

- **Legislar sobre las responsabilidades civiles y penales asociadas a la ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará las responsabilidades civiles y penales que enfrentarán los responsables de empresas y organismos gubernamentales en caso de producirse un ciberataque. Se contemplarán las responsabilidades, obligaciones y sanciones que les caben a quienes debieron velar por la seguridad de los datos y la infraestructura y fallaron en sus tareas. Se incluirá

un esquema muy estricto de penalidades que fomente la inversión en tecnologías y buenas prácticas de protección de datos e información.

- **Legislar sobre transparencia de las políticas en ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la promoción de mecanismos para la supervisión pública y la transparencia de las actividades que el gobierno realiza en materia de ciberseguridad.
- **Regular la notificación a los afectados en caso de ciberincidentes.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la obligación de notificar ciberincidentes por parte de empresas y organismos, cuando estos pongan en riesgo la información y seguridad de terceros, como clientes, proveedores, usuarios y empleados, entre otros posibles afectados.
- **Tipificar delitos informáticos**. El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la legislación existente con el objeto de tipificar y describir los delitos asociados a la tecnología y en particular, a la ciberseguridad, que no se encuentran aún cubiertos por el marco normativo actual.
- **Desarrollar capacidades en el Poder Judicial en materia de ciberseguridad**. El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará el desarrollo y la formación de profesionales del Poder Judicial en aspectos jurídicos, procesales y en las mejores prácticas internacionales con respecto a la investigación y judicialización de ciberdelitos y ciberincidentes.
- **Definir procesos de captura y tratamiento de evidencia digital.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará la promoción de buenas prácticas de captura, gestión, manipulación y presentación de evidencias digitales, con el fin de facilitar y acelerar los procesos de investigación y las causas judiciales.
- **Desarrollar capacidades forenses en las fuerzas de seguridad en materia de ciberseguridad.** El Estado analizará, legislará, diseñará, implementará, evaluará y monitoreará las capacidades de las fuerzas de seguridad para proveerlos de conocimientos, herramientas y procesos que les permitan investigar con efectividad aquellos delitos vinculados al ciberespacio y a las nuevas tecnologías.

PARTE 4 Conclusiones

Conclusiones

La ciberseguridad no solo se vincula a la capacidad de los Estados al momento de proteger a los habitantes y organizaciones del país de los riesgos del ciberespacio, sino que se extiende al tejido social y a las interacciones de poder entre múltiples y diversos actores nacionales e internacionales. Las tecnologías de la información y las telecomunicaciones constituyen una herramienta de desarrollo económico y social de avance creciente que sin embargo, por su naturaleza dual, podrían tener un impacto negativo en la vida de las personas y en el destino de las organizaciones y los países, si no se protegen debidamente.

Según se explicó en la primera parte de este trabajo final de maestría, la ciberseguridad vuelve a traer a la superficie discusiones y tensiones entre la tecnología, el progreso, la vida privada de los individuos, el desarrollo económico y las capacidades de los sujetos económicos que, motivados por intereses incorrectos, podrían poner su inteligencia, creatividad y recursos al servicio de actividades malintencionadas. Lamentablemente, para muchos el cibercrimen es un medio de vida mucho más lucrativo y menos riesgoso que otras alternativas disponibles.

Estas tensiones e incentivos junto con la creciente interconectividad y el explosivo incremento de los dispositivos conectados, ponen constantemente a prueba las estrategias y planes de ciberseguridad de los países, dando lugar a nuevos vectores de ataque. En efecto, el rápido crecimiento tecnológico generalmente no disminuye su marcha, lo que impide o dificulta la revisión de las políticas de seguridad, una adecuada identificación y evaluación de riesgos y el control de los productos y servicios que lanzan, para que estén libres de vulnerabilidades antes de salir al mercado. Lamentablemente y como fue destacado previamente en este documento, la República Argentina no cuenta actualmente con una Estrategia Nacional de Ciberseguridad, lo que la expone de sobremanera a los riesgos que presenta el ciberespacio y propicia la pérdida de oportunidades frente a las promesas de bienestar que traen las tecnologías.

Con el fin de realizar una propuesta respecto a los principales contenidos que debería incluir una Estrategia Nacional de Ciberseguridad adecuada para la realidad

nacional, la segunda parte de este documento se enfocó en revisar las estrategias que varios países del mundo están implementando y sus convergencias en términos de gestión de riesgos, principios rectores, objetivos, contextos y misiones. Este trabajo incluyó la revisión de las estrategias de ciberseguridad de Estados Unidos, Estonia, Nueva Zelanda, Turquía, Colombia, México, Alemania y Ucrania. A partir del análisis, se generó un marco teórico y práctico para encarar la tercera parte de este documento sobre la base de los distintos enfoques en materia de protección del ciberespacio, para proponer una estrategia de ciberseguridad acorde a las necesidades de Argentina, pero alineada con las implementaciones realizadas por otros países, de manera de propender a la integración internacional en un mundo virtual que no reconoce fronteras para el flujo de datos.

Por último, en el tercer capítulo se propuso un modelo de estrategia de ciberseguridad para nuestro país, que contempla lo aprendido en la revisión de las estrategias de los países arriba mencionados, para producir un documento fundado que puede ser utilizado por los organismos con competencias y responsabilidades en la materia, como base para su redacción y como una posible vía para acelerar el proceso. La sección incorpora las bases necesarias para la tan necesaria generación de una estrategia de ciberseguridad y pone a disposición un marco para su creación, constituido por los pilares de la investigación a partir de la revisión de lo que ha sido efectivo en otras naciones del mundo.

El modelo de Estrategia Nacional de Ciberseguridad propuesto comienza por una introducción al estado actual de la ciberseguridad, describe el contexto internacional, explica el marco institucional, desarrolla una misión, objetivos y principios, para finalmente culminar con una serie de lineamientos para la implementación de la estrategia a través de planes de acción específicos.

La ciberseguridad se ha vuelto una cuestión esencial no solo de la vida de los ciudadanos del mundo, sino un aspecto fundamental para el desarrollo económico y social de una población. Es estratégico invertir en ciberseguridad no solo para minimizar los riesgos ya descriptos, sino como política de desarrollo económico.

Para considerar el impacto económico de la investigación y desarrollo en materia de seguridad informática, es posible mirar y aprender del caso de Israel, país que de la mano de Isaac ben Israel [36], fue capaz de diseñar una estrategia de ciberseguridad que no solo ha servido para proteger a la Nación de amenazas externas, sino que ha desarrollado el mercado de la ciberseguridad como uno de los grandes impulsores del crecimiento del PBI y actual hub internacional y de prestigio con respecto a la ciberseguridad. En este sentido, el desarrollo se produce mediante la unión de dos estrategias bien concretas. Por un lado, la formación de los jóvenes en el secundario (e incluso en el primario) en materia de protección de la información y la posibilidad de extender esa formación como título de grado, dando la posibilidad a muchas especialidades ya existentes en el país a focalizarse en la ciberseguridad (por ejemplo, abogacía, psicología, ingeniería, etc.), trayendo nuevos enfoques multidisciplinarios al problema y formando las nuevas generaciones que protegerán a la nación en caso de ataque. Por otro lado, este país ha fomentado la inversión del Estado en proyectos y emprendimientos relacionados con la ciberseguridad para el desarrollo de talento y tecnologías locales que conviertan al país en un centro internacional de producción de nuevas tecnologías.

El caso de Israel pone en evidencia la imperiosa necesidad de que nuestro país desarrolle una Estrategia Nacional de Ciberseguridad, que refleje su realidad y articule los esfuerzos que se están realizando en algunos sectores, para potenciar los beneficios de la tecnología para el bienestar y el desarrollo económico e institucional y al mismo tiempo, genere capacidades para enfrentar los riesgos que esto representa para las personas, organizaciones y la sociedad en su conjunto.

Recomendaciones para la generación de una estrategia

Es recomendable que los responsables de llevar adelante una política pública en materia de ciberseguridad tomen en cuenta las siguientes consideraciones al momento de desarrollar la Estrategia Nacional correspondiente:

- Generar en forma imperiosa las instancias necesarias para el desarrollo de un documento de carácter estratégico en materia de ciberseguridad con el fin de reducir la brecha con otros países que hace años cuentan con estrategias y habilitan así la mitigación de los riesgos a los que se encuentran expuestos.
- Utilizar en su desarrollo un lenguaje claro y carente de términos técnicos, de manera que pueda ser entendido por aquellos involucrados que no necesariamente pertenezcan al mundo de las tecnologías de la información y las comunicaciones. Como se explicó, una Estrategia Nacional de Ciberseguridad debe abarcar a toda la sociedad y a la economía en su conjunto y no solo al sector tecnológico.
- Revisar las estrategias creadas por otros países en busca de adquirir el conocimiento y las experiencias que los mismos tienen para aportar, tomando siempre en cuenta las distintas realidades y variables que afectan a cada nación y considerando aquellas que mejor se aplican a la situación de nuestro país. Con esto se favorecerá una rápida integración nacional en una dimensión que como se mencionó, no reconoce fronteras ni jurisdicciones.
- Tomar contacto con expertos del sector público y privado para que participen y revisen la propuesta, incorporando sus experiencias, motivaciones e intereses con objeto de crear una estrategia que aporte el mayor beneficio posible a todos los habitantes de la Nación.
- Someter una versión preliminar a la consulta pública, como lo han hecho varios países de la región, aportando transparencia al proceso y fomentando la amplia participación de diversos sectores con puntos de vista diversos.
- Involucrar especialistas en aspectos legales, técnicos y económicos que maximicen el valor agregado y las posibilidades de implementar rápidamente planes de acción concretos que respondan a la Estrategia en el contexto político y socioeconómico de la Argentina.

Mirada hacia el futuro

Es difícil predecir qué dirección tomará la ciberseguridad en los próximos años. Tecnologías como la inteligencia artificial y Big Data son grandes candidatas a generar una sinergia que revolucione nuevamente el mundo de la ciberseguridad. Desde el punto de vista del hardware, la computación cuántica tiene el potencial de cambiar completamente nuestro entendimiento con respecto a las capacidades actuales de las computadoras tradicionales de proteger la información que procesan y almacenan. Es posible que los próximos años se modifique drásticamente el concepto de identidad digital, cambiando la forma en la que interactuamos en el mundo digital, trayendo nuevos desafíos a nuestra existencia digital y su manera de representarnos en un mundo cada vez más conectado y sin fronteras.

Adicionalmente, cuestiones como la privacidad y los derechos individuales están cada vez más en puja con los intereses de los gobiernos de utilizar el poder estatal para aumentar el control sobre la sociedad en nombre de la seguridad y la protección de los ciudadanos. Cabe acotar que este esquema de permanente monitoreo, donde las acciones de los individuos son constantemente registradas, no son ejercidas solo por los gobiernos, sino también por empresas, quienes utilizan similares mecanismos de seguimiento con la excusa de proveer mejores servicios a sus usuarios o vender más productos.

En base a lo antedicho, resulta difícil predecir cuál será el futuro de los conflictos internacionales, la identidad y la misma soberanía nacional en el ciberespacio, por solo nombrar algunos temas. Sí es posible vislumbrar que esta tendencia no muestra ninguna señal de aminorar su marcha y por el contrario, la aceleración de la interconexión de personas, servicios y dispositivos es una de las más grandes amenazas a la ciberseguridad, a la vez que uno de los mayores cambios tecnológicos de la historia de la Humanidad.

Como cierre final de este documento y propuesta de futuras investigaciones, es dable mencionar que el Estado, en su rol de máximo responsable del presente y futuro de la Argentina, debe desarrollar un plan de continuidad digital y calidad del ciberespacio, que maximice las posibilidades de supervivencia en caso de ciberataque,

falla generalizada o desastre natural. Según la experiencia provista por Estonia, una alternativa a dicha continuidad puede materializarse a través de embajadas digitales que operen fuera del territorio nacional, preferentemente en locaciones neutrales, como podrían ser en la actualidad Suiza o Luxemburgo, proveyendo de ese modo servicios esenciales a los habitantes del país en situaciones extremas, protegiendo la soberanía y la información y maximizando así las posibilidades de reconstrucción de la nación frente a los desafíos que representa un mundo cada vez más interconectado. De ese modo se alcanzaría una nación resiliente que aproveche a pleno los beneficios del ciberespacio. El modelo planteado es uno de los posibles a seguir. El desarrollo de este tipo de soluciones es un camino a explorar para un ciberespacio más seguro.

Glosario

Término	Definición
Time-sharing software	Es un tipo de software que se utiliza cuando los recursos de hardware son muy limitados, de esta forma varios usuarios comparten un mismo equipo, teniendo tiempos asignados para su uso
Sponsor	Persona u organización que apoya un determinado proyecto con dinero, tiempo, experiencia o influencias, y que generalmente tiene un particular interés en el resultado del proyecto.
DarkWeb, DeepWeb, DarkNet	Refiere a la porción encriptada de Internet, donde interacciones pueden realizase de forma anónima y la información no es accedida por buscadores como Google y Bing. Generalmente asociada a actividades ilícitas, debido a la naturaleza secreta y difícil de rastrear de sus sitios.
Bots	Un programa autónomo que funciona en una red (normalmente Internet) que puede interactuar con otros sistemas siguiendo un determinado patrón o respondiendo ordenes de un comando central.
Brokers	Una persona que compra y vende activos, en este contexto refiere a brokers de datos o vulnerabilidades, donde se compra y vende información al mejor postor y generalmente por fuera de la ley (o al menos en grises difíciles de definir con la legislación actual)
Supply Chain	Es la secuencia de procesos que permite la producción y distribución de bienes y servicios
Botnets	Es una red de computadoras infectadas por software malicioso que controlada por un individuo u organización pueden actuar de forma conjunta para realizar ataques sin que sus dueños estén al tanto.
Ecomerce	Transacciones comerciales que ocurren en el ciberespacio
Hacker	Una persona que utiliza computadoras para obtener un acceso privilegiado a sistemas, siendo el mismo no autorizado por el

Término	Definición
	propietario. Existen hackers de diversos tipos, siendo muy difícil definir sus intenciones, generalmente se clasifican en Black, Gray y White (Negro, Gris y Blanco), siendo el color identificativo de la naturaleza de sus actividades.
TICs	Se utiliza para referirse a las Tecnologías de la Información y Comunicaciones.
Hub	Se conoce como el centro de una red, que permite a los nodos de una red comunicarse entre sí. Puede cumplir diversos roles en la red, pero su rol principal es unir nodos y facilitar o permitir el flujo de información.
0-day	Son vulnerabilidades que aún no han sido detectadas por el fabricante y para los cuales no existe todavía un parche que permita prevenir este vector de ataque. Tienen un gran valor comercial por su capacidad de daño.

Referencias

[1] U. D. o. H. Security, «Cibersecurity Strategy,» US Department of Homeland Security, 2018.

[2] R. Kissel, «Glossary of Key Information Security Terms,» NIST, 2013.

[3] ENISA, «Definition of Cybersecurity - Gaps and overlaps in standardisation,» ENISA, 2015.

[4] Kaspersky, «What is Cyber-Security?,» Kaspersky, [En línea]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 19 09 2018].

[5] E. A. Fischer, «Cybersecurity Issues and Challenges: In Brief,» Congressional Research Service, 2016.

[6] O. Dictionaries, «Oxford Dictionaries,» Oxford , [En línea]. Available: https://en.oxforddictionaries.com/definition/cybersecurity.

[7] T. Moore, «Introducing the Economics of Cybersecurity: Principles and Policy Options,» *Harvard University - National Academy of Sciences.*

[8] Accenture, «CYBER THREATSCAPE REPORT 2018,» Accenture - MIDYEAR CYBERSECURITY RISK REVIEW, 2018.

[9] F. B. S. Deirdre K. Mulligan, «Doctrine for Cybersecurity,» 2011.

[10] U. S. G. A. Office, «Responsibilities, CRITICAL INFRASTRUCTURE PROTECTION - Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity,» 2005.

[11] J. A. Lewis, «Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,» Center for Strategic and International Studies, Washington DC, 2002.

[12] W. M. M. D. Oliver Thonnard, «Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making,» *CSI-KDD,* 2009.

[13] J. R. Lindsay, «Tipping the scales: the attribution problem and the feasibility of deterrance against cyberattack,» *Journal of Cybersecurity,* 2015.

[14] ITU, «List of ITU Member States,» [En línea]. Available: https://www.itu.int/en/ITU-R/terrestrial/fmd/pages/administrations_members.aspx. [Último acceso: 18 02 2019].

[15] ITU, «National Strategies Repository,» ITU, 02 18 2019. [En línea]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/pages/national-strategies-repository.aspx. [Último acceso: 02 18 2019].

[16] K. B. P. d. G. Eric Luijf, «Nineteeen National Cyber Security Strategies,» *International Journal of Critical Infrastructure Protection,* vol. 9, 2013.

[17] M. o. E. A. a. C. -. Estonia, «Cyber Security Strategy,» Ministry of Economic Affairs and Communication, 2014.

[18] New Zealand Goverment, «New Zealand's Cyber Security Strategy,» New Zealand Goverment, 2015.

[19] Federal Ministy of the Interior, «Cyber Security Strategy for Germany,» Federal Ministry of the Interior, 2011.

[20] Ministerio de Tecnologías de la Información y las Comunicaciones - Colombia, «AGENDA ESTRATÉGICA DE INNOVACIÓN: CIBERSEGURIDAD,» Ministerio de Tecnologías de la Información y las Comunicaciones, Bogota, 2014.

[21] Presidential Decree of Ukraine, «CYBER SECURITY SRTATEGY OF UKRAINE,» Administration of the President of Ukraine , 2016.

[22] Gobierno de Mexico, «Estrategia Nacional de Cibersecuridad,» Gobierno de Mexico, Mexico , 2017.

[23] M. o. T. M. A. a. C. -. R. o. Turkey, «National Cyber Security Strategy,» Ministry of Transport Maritime Affairs and Communications - Republic of Turkey, 2016.

[24] Central Intelligence Agency (CIA), «The Wold Factbook,» Central Intelligence Agency (CIA), [En línea]. Available: https://www.cia.gov/library/publications/the-world-factbook/rankorder/rankorderguide.html. [Último acceso: 03 09 2018].

[25] Wikipedia, «Escalas numéricas larga y corta,» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Escalas_num%C3%A9ricas_larga_y_corta. [Último acceso: 21 02 2019].

[26] M. P. d. B. L. B. P. F. N. M. Geoff Smith, «Cibersecurity policy making at a turning point,» OECD, 2012.

[27] Infobae, «El gobierno creo un comite para elaborar una estrategia de ciberseguridad,» *Infobae,* 31 07 2017.

[28] Presidencia de la Nación Argentina, «Creación del Comité de Ciberseguridad,» Boletín oficial, Ciudad de Buenos Aires, 2017.

[29] Casa Rosada - Presidencia de la Nacion Argentina, «Objetivos de Gobierno,» [En línea]. Available: https://www.casarosada.gob.ar/objetivosdegobierno/. [Último acceso: 25 09 2018].

[30] PODER EJECUTIVO NACIONAL (P.E.N.), *Decreto 996 / 2018 - AGENDA DIGITAL ARGENTINA,* Ciudad de Buenos Aires: Boletin Oficial, 2018.

[31] Presidencia de La Nacion Argentina, «Gobierno Digital | Argentina.gob.ar,» [En línea]. Available: https://www.argentina.gob.ar/gobiernodigital. [Último acceso: 27 08 2018].

[32] Ministerio de Justicia y Derechos Humanos, *LEY DE MINISTERIOS - Ley 22.520 - TEXTO ORDENADO POR DECRETO 438/92,* Buenos Aires: Boletin Oficial, 2015.

[33] Wikipedia, «Ministerio de Modernizacion (Argentina),» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Ministerio_de_Modernizaci%C3%B3n_(Argentina). [Último acceso: 27 08 2018].

[34] Wikipedia, «Ministerio de Seguridad (Argentina),» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Ministerio_de_Seguridad_(Argentina). [Último acceso: 27 08 2018].

[35] Agencia Federal de Investigaciones, «Agencia Federal de Investigaciones - Seccion: Que Hacemos,» AFI, [En línea]. Available: http://afi.gob.ar/#idSeccionQueHacemos. [Último acceso: 27 08 2018].

[36] I. B. Israel, Interviewee, *GT sobre Políticas Digitales y Ciberespacio - CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES.* [Entrevista]. 5 Julio 2018.

[37] N. A. Sales, «REGULATING CYBER-SECURITY,» *Northwestern University School of Law,* vol. 107, nº 4, 2013.

[38] D. D. Clark, «The Landscape of Cyber-security,» 2015.

[39] IC3, «Internet Crime Report,» IC3, 2017.

[40] Commonwealth of Australia, Department of the Prime Minister and Cabinet, «Australia's Cyber Security Strategy,» Australian Goverment, 2016.

[41] Goverment of Canada, «National Cyber Security Strategy,» Goverment of Canada, 2018.

[42] Gobierno de Chile, «National Cybersecurity Policy,» Gobierno de Chile, 2017.

[43] R. Anderson, «Why Information Secuirity is Hard - An Economic Perspective,» *University of Cambridge Computer Laboratory,* 2001.

[44] I. L. D. D. S. W. M. T. J. H. L. Zachary A collier, «Cybersecurity Standards: Managing Risk and Creating Resilience,» IEEE Computer Society, 2014.

[45] E. G. S. L. P. M. Eric Johnson, «Security trough Information Risk Management,» IEEE Security and Privacy, 2008.

[46] O. d. l. E. A. (OEA), «TENDENCIAS DE SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE,» Organizacion de los Estados Americanos (OEA), 2014.

[47] A. Catalano, «Raúl Martínez, secretario de País Digital: "Nos tenemos que poner los pantalones largos en ciberseguridad",» *IProfesional,* 01 06 2018.