CENTRO LATAM DIGITAL

Políticas públicas sobre ciberseguridad en América Latina: el caso de Argentina

Gonzalo Bustos Frati y Carolina Aguerre

Diciembre 2021

Centro Latam Digital 2022
Primera edición: Abril de 2022

Para más información sobre las publicaciones y proyectos de Centro Latam Digital, visite nuestro sitio web centrolatam.digital.

Este trabajo se llevó a cabo con una subvención del Centro Internacional de Investigaciones para el Desarrollo (IDRC), Ottawa, Canadá. Las opiniones expresadas en este documento no representan necesariamente las del IDRC o su consejo superior

Diseño de tapa y diagramación:
Elisabet Lunazzi

Índice

Agradecimientos

Esta investigación ha sido posible por el apoyo del Centro Latam Digital del Centro de Investigación y Docencia Económicas (CLD) y del Centro de Tecnología y Sociedad de la Universidad de San Andrés (CETYS-UDESA), de México y Argentina, respectivamente. Asimismo, muchas personas colaboraron para hacer esta investigación posible.
En especial, queremos expresar nuestra gratitud a Judith Mariscal (y todo el equipo del CLD), así como a cada uno de los y las informantes clave que nos permitieron entrevistarlos. Aquí debemos limitarnos a mencionar a la académica Marcela Pallero, pues el resto de las fuentes consultadas, en virtud de que se desempeñan en el ámbito público o privado, optaron por mantener su anonimato. Por lo tanto, se trata de un agradecimiento genérico, pero no por ello menos sentido. Sin sus valiosos y generosos aportes, este informe sería muy distinto.

Prefacio

El objetivo de este informe es evaluar la gobernanza de la ciberseguridad en la Argentina, con foco en el complejo institucional conformado por las políticas públicas elaboradas por el Estado desde 1999 hasta mediados de 2020. El informe es fruto de una investigación realizada entre julio de 2019 y julio de 2020. Ahora bien, desde julio de 2020 hasta la fecha en la que esta publicación concluyó, en diciembre de 2021, han transcurrido ya 18 meses de gestión del gobierno de Alberto Fernández (2019-2023). En tal sentido, los autores del informe hemos considerado pertinente incorporar un breve prefacio que mencione, al menos de forma muy sumaria, las tendencias que parecen estar teniendo lugar en materia de políticas públicas en el campo de interés.

Lo fundamental es que, aunque cuando sigue siendo muy pronto para sacar conclusiones, consideramos que la realidad está confirmando varias de las aseveraciones vertidas en el estudio, y a la vez matizando ciertas expectativas.

Algunos hechos ya habían sido considerados en el informe. Por ejemplo, allí se señala que las nuevas autoridades a cargo de la Dirección Nacional de Ciberseguridad (DNC), la autoridad de aplicación en la materia, cuestionaron la legitimidad de la Estrategia Nacional de Ciberseguridad (ECN), publicada meses antes del inicio de su administración, por considerarla poco representativa de la realidad federal del país. Asimismo, se menciona que se crearon reuniones especializadas en el Consejo Federal de Políticas (CFP), en búsqueda de una mayor federalización de las políticas sobre ciberseguridad, así como de un desarrollo más homogéneo de las capacidades a nivel subnacional. No obstante, no encontramos evidencia de que este espacio haya sido consolidado o sostenido en este periodo. A su vez, es interesante que se haya decidido crear un espacio dentro del CFP en lugar de procurar "federalizar" la composición del Comité Nacional de Ciberseguridad (que creó la ECN de 2019).

En cuanto a los hechos que se produjeron luego de julio de 2020, encontramos evidencia de un cierto fortalecimiento de la capacidad de gestión de la autoridad de aplicación, si bien muy incipiente. El dato fundamental es el relanzamiento del CERT (antes denominado ICIC-CERT, tal es la denominación utilizada en el estudio) bajo bases que parecen procurar la recuperación del sendero institucional de un centro nacional orientado a fortalecer las capacidades estatales para responder a incidentes en el ámbito de la función pública. Esta cuestión nos remite a uno de los hallazgos clave del estudio, que repone los aspectos negativos de los varios cambios de sentido estratégico que se le han impreso al CERT nacional desde la creación (pionera) de su primera versión, el AR-CERT, en 1999.

La DNC también ha dado un paso interesante al poner un mayor foco en los programas de capacitación, donde incluso participaron, como formadores, actores de la sociedad civil. En 2021 se dio capacitación inicial en materia de seguridad de la información a 4.500 empleados públicos del Poder Ejecutivo. Ahora bien, respecto a lo dicho acerca de un CERT creador de capacidades federales, cabe señalar que el foco de los cursos estuvo dirigido a funcionarios del gobierno nacional, antes de los gobiernos provinciales, donde se detectan deficiencias técnicas aun mayores que en el nivel nacional.

Como alternativa a la cuestionada ENC, la única publicación estratégica publicada hasta ahora son los Requisitos Mínimos de Seguridad de la Información para Organismos Públicos, de 2021 (Decisión Administrativa 641/2021).

En síntesis, hasta aquí se confirma la hipótesis acerca de la discontinuidad como norma, antes como excepción, en materia de ciberseguridad. También confirmamos el hecho de que, en términos de diseño institucional preferido, los gobiernos peronistas (2003-2007, 2007-2011, 2011-2015, 2019-2023) han priorizado a la Jefatura de Gabinete como organismo rector de la ciberseguridad. También se confirma que las políticas argentinas en la materia exhiben un enfoque de la gobernanza de la ciberseguridad centrado casi exclusivamente en los gobiernos, un aspecto que se agudiza en el caso del ciberdelito y la ciberdefensa. Al respecto, entonces, cabe matizar las expectativas generadas por las señales iniciales vertidas desde la DNC en torno a la idea de buscar un "diseño conjunto del entorno de seguridad público", como alternativa superadora del enfoque limitado a la concientización ciudadana y el accionar de la justicia para restituir derechos ya vulnerados.

También corresponde matizar la idea de que la pandemia podía llegar a generar un sentido de urgencia en las máximas esferas gubernamentales acerca de la importancia de la ciberseguridad. Ni siquiera la sucesión alarmante de graves incidentes de ciberseguridad en el ámbito gubernamental parece estar generando este sano sentido de una coyuntura crítica. Considerando solo los últimos meses, podemos mencionar al menos tres eventos de gravedad: en septiembre de 2020, fueron filtrados 1,8 gigas de datos de documentos sustraídos a la Dirección Nacional de Migraciones a través de un *ransomware* llamado NetWalker; en julio de 2021, a partir de un spam en el correo de la cartera de Salud, se produjo la filtración de 964 millones de datos sensibles de unos 50 mil ciudadanos argentinos, alojados en las bases de 40 hospitales nacionales y los ministerios de salud de las 24 jurisdicciones del país; y en octubre de 2021 se informó la filtración de la base de datos completa de documentos nacionales de identidad que gestiona el Registro Nacional de las Personas

(RENAPER), es decir, una base de datos de 45 millones de ciudadanos argentinos. La investigación, en proceso, llevó a identificar como potenciales sospechosos a ocho empleados del Ministerio de Salud, con acceso a la base de datos vulnerada. En el mismo periodo, a su vez, fue archivada, sin que se hallaran culpables, la causa judicial iniciada a partir de un grave incidente producido julio de 2019, cuando más de 700 gigabytes de información sensible de los servidores de la Policía Federal Argentina fueron robados tras una maniobra de phishing, y luego difundidos en la Deep Web.

Otro aspecto de interés es que, en materia de ciberdiplomacia, el gobierno ha profundizado su preferencia por la participación en el *Open-Ended Working Group* de la ONU (OEWG). De hecho, personal del Ministerio de Relaciones Exteriores tuvo un rol activo en la elaboración del primer documento de dicho organismo. No obstante, no está claro que este camino haya de ser profundizado en el futuro, en virtud de algunos cambios en el área en la Cancillería. En cuanto al 5G, el presidente Fernández ha dado interesantes muestras de su intención de mantener cierta equidistancia tanto respecto de las soluciones ofrecidas por actores con base en Estados Unidos como por parte de actores con base en China, si bien cuánto se podrá sostener esta estrategia permanece como interrogante.

En materia de ciberdelitos no ha habido cambios de relevancia, lo que confirma que en este ámbito sí existe una cierta consolidación de una política de estado; lo que en los hechos acaba dándole a la propia política de ciberseguridad cierta tónica de una política más centrada en el aspecto punitivo que en el aspecto preventivo.

En materia de ciberdefensa, en tanto, los hechos relevantes nos remiten al inicio de la gestión, por lo que fueron considerados en el estudio. Como se señala allí, la primera decisión institucional de peso de la Subsecretaría de Defensa durante el gobierno de Fernández, en junio de 2020, fue derogar dos decretos clave de la gestión macrista —el que había establecido una nueva Directiva de Política de Defensa Nacional (DPDN) y el que había reformado el decreto reglamentario de la Ley de Defensa— donde se disponía que el uso del instrumento militar sería utilizado ante "agresiones de origen externo", fueran o no estatales.

Junto a este cambio doctrinario, cabe sumar otro de tipo institucional. Durante la gestión de Macri (y en el marco de la organización de la cumbre del G-20, entre otros eventos de la misma envergadura) se había creado una miríada de organismos, la mayoría de los cuales no tendrían aplicación efectiva. El máximo organismo sigue siendo la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa (MINDEF). De ella, siguen dependiendo dos direcciones, si bien han cambiado ligeramente de nombre: la Dirección de Políticas y Seguridad de la Información (antes, Dirección de Diseño de Políticas para la Ciberdefensa), y la Dirección de Protocolos y Asuntos Regulatorios de la Ciberdefensa (antes, Dirección de Asuntos Regulatorios de la Ciberdefensa). A su vez, se creó la oficina de Coordinación de Infraestructura Tecnológica, bajo la supervisión directa de la Subsecretaría.

El informe también alcanza a incluir la mención del acuerdo entre el MINDEF y ARSAT, la empresa satelital nacional, el cual señalaba la intención de retomar un sendero de desarrollo de capacidades endógenas en materia de comunicaciones y disminución de dependencia tecnológica con proveedores externos, el cual había sido abandonado durante la gestión anterior. No se encuentra evidencia de la profundización de esta línea de trabajo, si bien tampoco de su discontinuidad.

Por otro lado, no encontramos evidencia de la continuidad del CSIRT de Defensa, creado durante la gestión anterior, en el marco de los preparativos para alojar la cumbre del G-20.

Por último, y como dato para nada menor, permanece la incertidumbre respecto cómo se definen los roles entre *ciberseguridad* y *ciberdefensa* en relación a la protección de las infraestructuras críticas.

Esperamos que, hechas estas aclaraciones, el informe resulte un valioso y actual aporte a la conversación sobre una temática central para la buena gobernanza del país.

Los autores
Diciembre de 2021

Introducción

El objetivo de este informe es evaluar la gobernanza de la ciberseguridad en la Argentina, con foco en el complejo institucional conformado por las políticas públicas elaboradas por el Estado desde 1999 hasta mediados de 2020.

El estudio forma parte del proyecto CETyS UDESA-Centro Latam Digital, que elaboró un marco analítico original para el análisis de las *políticas públicas relativas a la gobernanza de la ciberseguridad en los países latinoamericanos*.

Dicho marco parte de tres premisas. En primer lugar, una inscripción crítica en la literatura sobre procesos de maduración de capacidades que apela a diversos índices de preparación en ciberseguridad (OEA-Oxford, ITU y Potomac-OEA), a partir de la propuesta de profundizar allí donde ellos no logran (ni buscan) calar: los procesos de formación de preferencias a nivel nacional, y las dinámicas de convergencia o divergencia de estándares en los niveles regional y global. Los procesos de desarrollo de capacidades no son lineales, y quizá no sean el modo más adecuado para conceptualizar y analizar la trayectoria de los organismos públicos, en tanto no permiten problematizar los procesos de formación (y cambio) de preferencias estatales, algo central en una materia como la ciberseguridad, donde no existe un estándar universal sino un "complejo de regímenes". Por tanto, resulta más conveniente indagar en las trayectorias de los *senderos de desarrollo institucional*, atendiendo tanto las distribuciones de preferencias (y sus procesos de formación) como las de capacidades (y sus procesos de creación).

En segundo lugar, se parte de una definición amplia de "gobernanza de la ciberseguridad", donde también aparecen, diferenciadas pero incorporadas al análisis, las políticas sobre delitos informáticos, por un lado, y las políticas sobre ciberdefensa, por el otro. Es decir, *ciberseguridad*, *ciberdelitos* y *ciberdefensa* se abordan como *ámbitos de incumbencia estatal* diferenciados, si bien involucrados en una perspectiva amplia de la *gobernanza de la seguridad*. Esto porque se parte de considerar que el problema de la ciberseguridad como objeto de la política pública se encuentra atravesado por diversas dimensiones que atraviesan el aparato estatal tanto en sus múltiples funciones como en sus diversas jurisdicciones. Tanto técnica como prácticamente, el problema presenta cruces con aspectos de defensa nacional, infraestructura crítica, desarrollo de capacidades (organizativas e individuales), prevención e investigación de ciberdelitos, y relaciones diplomáticas, entre otros asuntos. Por ende, deliberadamente la investigación adopta una perspectiva amplia que permita a su vez identificar continuidades y rupturas en materia de gobernanza de este tema en función de las distintas dimensiones.

En tercer lugar, se propone concebir a los Estados como ecosistemas institucionales complejos (en lugar de actores racionales y homogéneos), a las políticas públicas como instituciones con trayectorias socio-históricas, y a las relaciones entre dichas políticas como dinámicas sistémicas con propiedades emergentes. Como resultado, consideramos que los diversos senderos de desarrollo institucional se ven conformados por múltiples dinámicas asociadas a la complejidad institucional estatal, donde es esperable encontrar, en torno de cada ámbito de incumbencia, arreglos regulatorios y prácticas informales impulsados por múltiples y diversas agencias públicas, entre las que se registran dinámicas de cooperación y competencia por recursos institucionales.

En concreto, para la aplicación del marco al caso de Argentina, el informe propone un análisis integral de las políticas sobre *ciberseguridad* en Argentina. Para lograrlo, recurre a un análisis integrado de las políticas públicas sobre *ciberseguridad*, *delitos informáticos* y *ciberdefensa*, a las que hemos de considerar como un *complejo institucional*, conformado por múltiples arreglos regulatorios y prácticas informales impulsados por múltiples y diversas agencias estatales (por ej. Jefatura de Gabinete, Modernización, Seguridad, Defensa, Justicia, Ministerio Público Fiscal), entre las que se registran dinámicas de cooperación y competencia por recursos institucionales.

En cuanto al periodo analizado, comprende desde 1999 hasta mediados de 2020.

Así definido el encuadre, algunos elementos por destacar, como principales hallazgos del estudio. Por empezar, encontramos que el país todavía se encuentra en sus etapas formativas en la mayoría de las dimensiones a considerar en materia de ciberseguridad; en especial, en materia de protección de las infraestructuras críticas y respuestas a incidentes informáticos.

Desde una perspectiva de mediana duración, las políticas sobre ciberseguridad están caracterizadas a la vez por dinámicas de innovación y dinámicas de discontinuidad. Por ejemplo, Argentina fue pionero en materia de ciberseguridad en tanto tuvo el primer CERT gubernamental de la región en 1999, pero no logró darle continuidad a su sendero de desarrollo y de hecho durante la última década modificó tanto la jerarquía como el objeto del organismo, según la relevancia que se le ha dado al área, o la prioridad que se pretendió asignarle al organismo, respectivamente. Como resultado, puede afirmarse que

Un tercer elemento es que las innovaciones institucionales asociadas a la gobernanza de la ciberseguridad, en especial en los organismos y agencias del Poder Ejecutivo, tienden a identificarse con gestiones de gobierno antes que políticas de Estado que se sostienen y evolucionan en el tiempo. Esta característica es común a varios de los temas de la agenda del gobierno, en

la que la baja institucionalidad (Stein, Tommasi, 2003, 2006) es por otra parte compensada por acuerdos de carácter informal (Acuña, 2013). Ahora bien, se verifican discontinuidades dentro de un mismo periodo presidencial, en gobiernos de diverso signo político.

Otro elemento por destacar es que se halla evidencia de interesantes matices y contrastes en materia de los *senderos de desarrollo institucional* (atendiendo tanto las distribuciones de preferencias como las de capacidades) seguidos en los tres ámbitos de incumbencia estatal relevados. En términos de capacidades, se verifica una mayor continuidad en las políticas y trayectorias institucionales con eje el ámbito de los delitos informáticos o "*ciberdelitos*" que en torno a la *ciberseguridad* y la *ciberdefensa*. A su vez, en términos de preferencias encontramos que a nivel estatal en general (y ya no en cada ámbito de incumbencia), se registra un enfoque de la gobernanza de la ciberseguridad más bien limitado a la tipificación penal de los delitos en el ciberespacio, donde el accionar estatal tiene lugar una vez vulnerados los derechos de los individuos, antes que uno extensivo a la prevención, la resiliencia o la industrialización de los servicios basados en la gestión de la ciberseguridad.

Por otra parte, las políticas analizadas exhiben un enfoque de la gobernanza de la ciberseguridad centrado casi exclusivamente en los gobiernos, y esto se agudiza en el caso del ciberdelito y la ciberdefensa. Es cierto que varios de los organismos analizados han intentado construir redes multisectoriales, pero en los hechos han tenido un carácter declarativo, o más bien informal y con un mandato limitado a un objetivo específico. Con todo, diremos que aquellos intentos de crear redes multisectoriales, junto a esta trayectoria continuada en términos de participación en foros técnicos orientados a la construcción de confianza y buenas prácticas, nos permite complejizar la noción de un esquema gubernamental estricto en materia de gobernanza de la ciberseguridad.

En cuanto a las técnicas de investigación utilizadas en el análisis de caso, se trató de un abordaje multi-metodológico, consistente en trabajo de gabinete, análisis documental, análisis institucional, análisis sociohistórico, y entrevistas semi-estructuradas con informantes clave de los tres ámbitos de la ciberseguridad, la ciberdefensa y los ciberdelitos. Al respecto, cabe señalar que, salvo una excepción proveniente del campo académico, todas las fuentes solicitaron mantener su anonimato.

El estudio se divide en diez secciones. La primera mapea los actores estales en los tres ámbitos de incumbencia, a los cuales se los parte de considerar como parte de un mismo complejo institucional. A su vez, se pone la mirada en las redes multisectoriales esbozadas o proyectadas por dichos actores. La segunda describe y mapea las líneas de tiempo del desarrollo institucional en los tres ámbitos de incumbencia. La tercera parte pone el foco en la normativa nacional. La cuarta, en las definiciones conceptuales clave. La quinta, en las estrategias nacionales. La sexta, en las dinámicas de la cooperación internacional. La séptima, en el análisis de las preferencias institucionales, y la novena, en el análisis de capacidades. Por último, se resumen los hallazgos y se establecen algunos interrogantes, de cara al análisis comparado con otros casos.

El caso de Argentina en los estudios sobre maduración de capacidades

Este apartado repone brevísimamente lo dicho sobre Argentina en los estudios que se proponen medir los índices de preparación en ciberseguridad de los países del sistema internacional (OEA-BID-Oxford, ITU).

Los dos estudios que incluyen datos sobre Argentina (OEA-Oxford e ITU), por su escala global o regional, aportan una mirada inicial, pero sistemática a las políticas sobre ciberseguridad. Se basan en encuestas a funcionarios públicos, por lo que se deben tomar ciertas precauciones extra a la hora de elaborar conclusiones acerca de la evolución de las políticas, en virtud de la medición en cada edición puede responder a diversas valoraciones. Sin embargo, son un punto de partida para la conversación sobre políticas de ciberseguridad en tanto establecen una línea de base común, a nivel multilateral y regional.

La premisa, como se dijo, es complementar esta conversación profundizando allí donde ellos, precisamente por su escala, no logran calar: los procesos de formación de preferencias a nivel nacional, y las dinámicas de convergencia o divergencia a nivel regional y global. Para ello, luego pondremos el foco en la respuesta a incidentes y la protección de las infraestructuras críticas (IICC).

En cuanto al informe de la ITU (se consideran las ediciones 2017 y 2018), su objetivo es mensurar el nivel de "compromiso" de los gobiernos con la ciberseguridad. Para ello se consideran 25 indicadores en cinco dimensiones: legal, técnica, organizacional, construcción de capacidades y cooperación. Se pondera cada dimensión con un puntaje (a partir de las respuestas binarias solicitadas a los funcionarios de cada país), y se elabora un promedio general que permite ubicar a los países en tres grupos: "iniciando", "madurando" y "liderando". A su vez, entre ambas ediciones se produjeron modificaciones en la metodología, como la reducción de 153 a 50 preguntas.

Así las cosas, en la edición 2017 Argentina figuraba en el grupo intermedio, con capacidades en desarrollo. En el mismo grupo se encontraban otros países latinoamericanos, como Brasil, Chile, Colombia, Costa Rica, Ecuador, Panamá, Paraguay, Uruguay y Venezuela, si bien con amplias diferencias en su puntaje general. Con un puntaje de 0.482, Argentina figuraba en el puesto 62 a nivel global (de 163 países analizados), y en el sexto lugar a nivel regional, por debajo de Brasil, Colombia,

México y Uruguay, cerca de Panamá y Ecuador, y por encima del resto de los países latinoamericanos. En la edición 2018, en tanto, el puntaje de Argentina descendió a 0.407, lo que ubicó al país en la posición 97 a nivel global, y al noveno puesto a nivel regional, por debajo de países con menor desarrollo relativo, como Paraguay y Cuba. De nuevo, la metodología de encuesta a funcionarios cierta profundas limitaciones en términos de trazabilidad de la evolución de cada caso. Entre ambas ediciones, a su vez, cambió el gobierno en Argentina, lo que puede explicar parte del cambio en el auto-diagnóstico.

Ocurre algo similar con el informe de la OEA, desarrollado de forma conjunta con el Banco Interamericano de Desarrollo (BID) y el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford. Sin embargo, a diferencia del informe elaborado por la ITU, el informe de la OEA propone un abordaje más cualitativo, a partir del desarrollo de perfiles nacionales de los países de la región. Denominado "Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones", identifica cinco etapas de madurez: inicial, formativa, consolidada, estratégica y dinámica. Se consideran cinco dimensiones: política y estrategia de ciberseguridad; cultura cibernética y sociedad; educación, capacitación y habilidades; marcos legales y regulatorios; y estándares, organizaciones y tecnologías.

En materia de puntaje, Argentina se posiciona, en general, entre la etapa formativa y consolidada, aunque en algunos aspectos se lo ha definido en una etapa estratégica: identificación de incidentes, y marcos legales de privacidad. Lo segundo parece más justificado, en tanto Argentina fue uno de los primeros países en incorporar una ley integral de protección de datos, ser reconocido como adecuada al estándar europeo, y en adherir al Convenio 108 de tratamiento automatizado de datos. Asimismo, en 2018, su autoridad de aplicación presentó un proyecto de ley para la reforma del régimen, hoy sin vigencia legislativa.

1. Mapeo de los actores estatales

En la Figura 1 se mapean los actores estatales de interés en torno a los tres ámbitos de aplicación: *ciberseguridad*, *ciberdelitos* y *ciberdefensa*. El criterio para la inclusión de los actores fue buscar un equilibrio entre la solución ideal (incluir a todos los actores formalmente creados con un interés en la materia) y un diagnóstico realista (limitarse a los actores realmente involucrados).

No se consideran todos los organismos formalmente creados mediante normativa nacional, sino los efectivamente constituidos, aunque sean de conformación reciente (como el Centro de Ciberdefensa o la reunión especializada del COFEFUP)[1], o no se hayan mantenido operativos en el tiempo. Por ejemplo, se incluye al Comité de Ciberseguridad, que operó durante el periodo 2016-2018, pero no al Comité Consultivo de Ciberdefensa, que se creó en 2018 pero cuya implementación permanece pendiente. Tampoco se incluye a la Oficina Nacional de Tecnologías de Información (ONTI), que tuvo un rol clave en la primera década del siglo, pero que desde 2015 ha sido relevada por organismos especializados, como la DNC.

Por otro lado, se incluye a la Dirección Operacional de Inteligencia sobre Ciberseguridad (DOIC). Si se trata de sus misiones y funciones, esta tiene implicancias en los tres ámbitos de incumbencia. No obstante, sus prácticas no están claras, y en tanto se trata de un órgano de inteligencia, la información de su comportamiento resulta en general reservada.[2]

Solo se consideran organismos de los niveles nacional, federal o regional. Por ejemplo, no se considera el BA-CSIRT de la Ciudad Autónoma de Buenos Aires.

Se consignan a su vez qué actores forman parte de más de un ámbito de incumbencia (por ejemplo, ciberseguridad y ciberdelitos).

En cuanto a lo relativo a cada ámbito de aplicación, encontramos tres organismos dedicados directa o indirectamente al campo de la *ciberseguridad*: la Dirección Nacional de Ciberseguridad (DNC), máximo organismo dedicado a la cuestión, del cual a su vez depende el Grupo de Trabajo ICIC-CERT (sin embargo, por la mayor trayectoria institucional del segundo, y su función más específica, se los incluye de forma diferenciada). Asimismo, se considera a la Agencia de Acceso a la Información Pública, encargada de velar por la aplicación de la ley de protección de datos personales y, por tanto, indirectamente involucrada en la gobernanza de la ciberseguridad.

En materia de *ciberdefensa*, el máximo organismo es la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares del MINDEF.

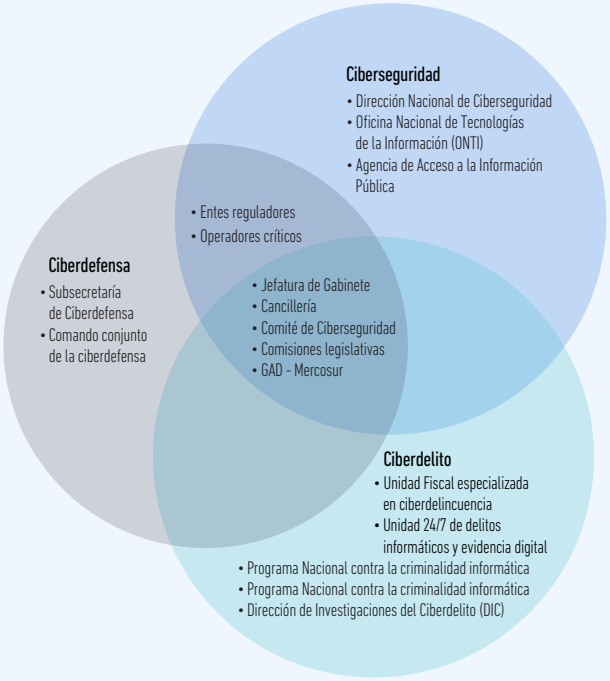
1. Creado y constituido a fines de 2019, el Centro Nacional de Ciber. defensa, dependiente de la Subsecretaría de Ciberdefensa, es el espacio donde se articulan los diversos actores militares involucrados en la ciberdefensa: el Centro de Respuesta ante Emergencias Informáticas del Ministerio de Defensa (CSIRT De Defensa), el Centro Inteligente de Operaciones de Seguridad (Isoc) del Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas y el Laboratorio de Análisis Cibernético (CyberLab),

2. Conformada en 2015 con la reforma del sistema de inteligencia que supuso la creación la Agencia Federal de Inteligencia (AFI), la DOIC tiene dos direcciones: una de Inteligencia Informática, encomendada a "actividades relativas a riesgos o conflictos vinculados o derivados del uso de tecnologías de información y la comunicación, que afecten la defensa nacional o la seguridad interior"; y otra sobre Delitos Informáticos, destinada específicamente a "actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades".

De ella, ahora dependen dos direcciones, la Dirección de Políticas y Seguridad de la Información (antes, Dirección de Diseño de Políticas para la Ciberdefensa), y la Dirección de Protocolos y Asuntos Regulatorios de la Ciberdefensa (antes, Dirección de Asuntos Regulatorios de la Ciberdefensa). Asimismo, bajo la supervisión directa de la Subsecretaría se encuentra la oficina de Coordinación de Infraestructura Tecnológica. A su vez, cabe mencionar el Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas (el cual, a su vez, centralizaría la operación de los Centros de Operaciones de Seguridad -iSOC- remotos de cada una de las Fuerzas Armadas).[3]

Cabe mencionar que durante la gestión de Macri (y en el marco de la organización de la cumbre del G-20, entre otros eventos de la misma envergadura) se había creado una miríada de organismos que tendrían aplicación efectiva limitada o nula. Estos eran: el Centro Nacional de Defensa (CND), el Centro de Respuesta ante Emergencias Informáticas del Ministerio de Defensa (CSIRT de Defensa), el Centro Inteligente de Operaciones de Seguridad (ISOC), y el Laboratorio de Análisis Cibernético (CYBERLAB). Este último sí tuvo aplicación efectiva, pero merece una nota aclaratoria. Se proyectó en la Política de Ciberdefensa de 2019 como "Think Tank de la Ciberdefensa" y "punto de confluencia de los diferentes sectores con interés concurrente en la actividad" (es decir, agencias estatales, entes reguladores de servicios esenciales, actores del sector privado que producen bienes de interés para la Defensa Nacional, la academia, y organizaciones no gubernamentales). No obstante, en los hechos su trabajo se ha limitado más bien al trabajo forense, a la vez que ha servido para el fortalecimiento de diálogo entre las fuerzas armadas, el Cibercomando y el personal del Ministerio, en tanto brinda asistencia técnica a dichos organismos.[4] No encontramos evidencia de su sostenimiento en el tiempo, tras el cambio de gestión.

Figura 1. Actores estatales involucrados en las políticas de ciberseguridad en Argentina



Fuente: elaboración propia

Por último, en materia de *ciberdelitos* encontramos diversos actores, dependientes de tres organismos diferentes: el Ministerio de Justicia y Derechos Humanos (Programa Nacional contra la Criminalidad Informática y Unidad 24/7 de Delitos Informáticos y Evidencia Digital), el Ministerio Público Fiscal (Unidad Fiscal Especializada en Ciberdelincuencia, y el Ministerio de Seguridad (Dirección de Investigaciones del Ciberdelito). Ahora bien, la clave está en los actores que pertenecen a más de un ámbito de incumbencia. Por empezar, ¿qué actores forman parte de los tres ámbitos? Incluimos aquí, a nivel nacional, a la Jefatura de Gabinete, el Ministerio de Relaciones Exteriores, el Comité de Ciberseguridad (cuya continuidad es una incógnita) y las comisiones legislativas de las dos cámaras del Poder Legislativo.[5]

Cabe señalar que se menciona a la Cancillería, de un modo general, porque todavía Argentina no cuenta con una agencia de al menos cuarto orden administrativo que lidie con la agenda digital en materia de

3. Ver sitio web (último acceso diciembre 2021).

4. Una fuente consultada (que prefirió mantener el anonimato) señala un ejemplo de esta colaboración en torno al CyberLab: en el marco de los preparativos del G20, se desarrolló una "wiki" interna de inteligencia (con una biblioteca de malware y un clipping de noticias asociadas a incidentes) elaborada mediante Web Intelligence a partir de un equipo integrado por técnicos de la Subsecretaría y de tres agencias de inteligencia: la Dirección Operacional de Inteligencia sobre Ciberseguridad de la Agencia Federal de Inteligencia (DOIC-AFI), la Dirección Nacional de Inteligencia Estratégica Militar (DINIEM), y la Dirección Nacional de Inteligencia Criminal (DINIC-RI), dependiente del Ministerio de Seguridad. Esto, según la fuente consultada, era luego presentado al CYBERLAB como insumo para hacer estudios forenses.

5. Se menciona a la Jefatura de Gabinete (JDG) como un organismo diferenciado de la DNC, que depende de aquella. Es evidente que no son el mismo actor, pero un modo de visualizar cuán relevante es esta diferenciación es atender a los momentos donde la JDG deliberadamente estableció pautas con impacto en la materia. Por ejemplo, la Estrategia Nacional de Ciberseguridad originalmente iba a ser publicada como Decreto, no como resolución, lo que le garantizaría mayor rango normativo. Sin embargo, a último minuto la JDG intervino para bajarle el rango.

política exterior, es decir, lo que abordamos en la Sección 6 como "ciberdiplomacia". Desde enero de 2020 cuenta con un organismo especializado: la Oficina de Ciberseguridad, Ciberdelito y Asuntos Digitales (OCCAD), dependiente de la Dirección de Seguridad Humana, Innovación y Asuntos Tecnológicos Internacionales.[6]

La mención de las "comisiones legislativas" también supone una forma genérica, que conviene aclarar. En especial, porque el "giro" a ciertas comisiones es un hecho más político que técnico, si bien dentro de ciertos márgenes de lo apropiado. En tal sentido, las comisiones que tienen un mandato institucional específico son: a nivel bicameral, la Bicameral Permanente de Promoción y Seguimiento de la Comunicación Audiovisual, las Tecnologías de las Telecomunicaciones y la Digitalización, y la Bicameral Permanente de Fiscalización de los Organismos de Inteligencia; por el Senado, Sistemas, Medios de Comunicación y Libertad de Expresión, y Justicia y Asuntos Penales; y por la Cámara de Diputados, Comunicación, Medios y Sistemas, y Legislación Penal. Esto en lo formal, pues en ambas cámaras las comisiones con mayor trayectoria han sido las asociadas al ciberdelito (por ej. leyes de delitos informáticos, grooming y ratificación del Convenio de Budapest). En el último tiempo, no obstante, esto ha comenzado a modificarse, en virtud de un mayor activismo en sendas comisiones asociadas a la comunicación y los sistemas informáticos (en especial, a partir de un debate en torno a las responsabilidades de los intermediarios de Internet).

A nivel federal, se identifica al Comisión de Infraestructura Tecnológica y Ciberseguridad del COFEFUP, creada en julio de 2020, por lo que se trata de la última incorporación a este conjunto, y no está claro qué función cumplirá. Por lo pronto, desde la DNC se han dado recientes señales de que podría ser un canal para la creación de una nueva Estrategia Nacional.[7]

Por último, a nivel regional, identificamos al Grupo Agenda Digital (GAD) del MERCOSUR. Creado en 2017 casi en espejo con el GAD de la Alianza Pacífico, el GAD del MERCOSUR ha desarrollado una agenda continua, asentada primero en un Plan de Acción 2018-2020, y ahora en el Plan de Acción 2020-2022.

Si bien se optó por dejarlo fuera, aquí también se podría considerar el Sub-Grupo de Trabajo n°1 del MERCOSUR, de Comunicaciones (SGT1), creado en los inicios bloque, y que a mediados de 2019 incorporó las funciones de la (novedosa, pero nunca constituida) Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica (RAPRISIT).

Asimismo, y como puede verse, se identificaron varios puentes entre *ciberseguridad* y los otros dos ámbitos, pero no así entre ciberdelitos y ciberdefensa, aparte del compartido, al menos formalmente, en el Comité de Ciberseguridad.

Entre *ciberseguridad* y *ciberdelito*, se consignan el mencionado ICIC-CERT y el CERT del Ministerio de Seguridad.[8] Nos interesa más la dinámica entre ciberdefensa y ciberseguridad, donde se registran varios puentes, en virtud de la cooperación necesaria para la protección de las IICC. Aquí encontramos, además del CSIRT de Defensa, a los entes reguladores de diversos servicios críticos, entre los que se destaca el Ente Nacional de Comunicaciones (ENACOM), así como a los operadores de dichos recursos críticos. Volveremos sobre este asunto cuando abordemos las preferencias institucionales, en la sección 7, cuando examinemos el diseño institucional planteado por la Estrategia Nacional de Ciberdefensa de 2019 y la Política de Ciberdefensa de 2019.

En cuanto a ARSAT, se trata de una empresa estatal de comunicaciones creada en 2007, cuyo rol estratégico ha variado según las preferencias gubernamentales. Comenzó como empresa de bandera orientada al

6. La OCCAD ha continuado el trabajo de la Dirección de Innovación y Asuntos Tecnológicos Internacionales (DIATI), que había sido creada en 2018, aunque con la difícil tarea de coordinar un mandato sobre la agenda digital como sobre la agenda energética. La OCCAD tiene un orden administrativo informal, debido a las limitaciones que supone la estructura orgánica del ministerio (semejante a un sexto orden), pero a pesar de su baja jerarquía, presenta mayor identidad temática que la DIATI, a la vez que concentra personal con valiosas capacidades sociotécnicas que participan en múltiples foros internacionales con incidencia en la ciberdiplomacia: ICANN; el GGE, pero también (y sobre todo) el GTCA; las negociaciones, también en la ONU, respecto a la resolución de Rusia relativa al ciberdelito. Además, corresponde a la Oficina de Ciberseguridad, Ciberdelito y Asuntos Digitales la participación de Cancillería en el Comité de Ciberseguridad. Fuera de su órbita, no obstante, se encuentra nada menos que las negociaciones en el Grupo de Trabajo sobre Comercio Electrónico en la OMC, y el Grupo Agenda Digital (GAD) del MERCOSUR.

7. Como se dijo, el COFEFUP es el organismo representativo de la voluntad federal en materia de gestión pública, y si bien existe desde 1992, ha tenido un rol muy cambiante a lo largo del tiempo, tanto en funciones como en gravitación institucional. Se trata de un órgano federal de carácter consultivo integrado por autoridades de las áreas de gestión e innovación públicas de los gobiernos nacional, provinciales y la Ciudad Autónoma de Buenos Aires. Su finalidad es colaborar en la planificación, coordinación, asesoramiento e implementación de los aspectos de las políticas de la función pública.

8. A su vez, cabe señalar que desde la actual gestión de la DNC se planteó la posibilidad de celebrar un "convenio de cooperación tripartito" con el Ministerio de Justicia y compañías del sector privado, como las proveedoras de servicio, para el diseño de entornos seguros que permitan pasar de un enfoque reactivo a uno preventivo. A su vez, el nombramiento de Gustavo Saín como Director Nacional de Ciberseguridad en 2019 permite suponer que se profundizarán los vínculos entre las comunidades de ciberseguridad y ciberdelitos, pues Sain forma parte de ambas redes; de hecho, es Coordinador Académico del Programa en Ciberseguridad y Delitos Informáticos de la Facultad de Ciencias Sociales de la UBA desde 2018. Ver Télam, 5/7/20. Disponible en: https://www.telam.com.ar/notas/202007/485583-gobierno-analiza-empresas-privadas-estrategias-ciberseguridad-preventiva.html#.XxRqYb6hU1Q.twitter

logro de la autonomía tecnológica, en general, y satelital, en particular, y fue reconvertida en 2016 a un rol más discreto de proveedora estatal en materia de infraestructura para la conectividad. Desde diciembre de 2019, se ha recuperado su objetivo original, si bien este proceso recién está en marcha. En esta línea, en julio de 2020, el MINDEF y ARSAT firmaron un acuerdo marco orientado al uso de capacidad y servicios satelitales, la red de fibra óptica y el Centro Nacional de Datos.[9] A su vez, su participación en el ámbito de la *ciberseguridad* es clave, no solo porque mantiene la infraestructura digital del ICIC-CERT, sino porque también dependen de ARSAT los contratos de su personal.[10]

2. Líneas de tiempo de las trayectorias institucionales

El Estado argentino se ha digitalizado de forma muy prometedora en 20 años, pero sin una política de ciberseguridad que protegiera a los activos que generó dicha transformación. Argentina fue pionero en gobierno electrónico, protección de datos y ciberseguridad en la región, pero en la última década, fruto de múltiples motivos, ha presentado una cierta involución. La cuestión no es si Argentina tiene o no capacidades medias, sino que se tenía (y se tiene todavía) potencial para tener capacidades altas. Sin embargo, falta sentido de urgencia en la dirigencia, y compresión del problema. A veces quienes están a cargo no saben lo que es un CERT y asumen que es una cuestión que se resuelve comprando equipamiento técnico. Y hay fragmentación porque los organismos públicos compiten entre sí como empresas, y todos los gobiernos tienden a empezar nuevamente desde cero proyectos o programas que podrían continuarse con leves o medianas modificaciones.

(Entrevista a ex – empleado con antigüedad en el área de ciberseguridad)

En este apartado abordaremos la evolución histórica de las trayectorias institucionales en los tres ámbitos bajo consideración. Las tres líneas de tiempo consideran: i) creación (y modificación) de organismos públicos; ii) normativas generales y específicas; y iii) instrumentos de cooperación (tanto internacionales como público-privados).

La línea de tiempo para el caso de la *ciberseguridad* (ver Figura 2) deja en evidencia que ya hace más de dos décadas que Argentina ha incursionado en el campo, si bien durante la última década la pauta ha sido la discontinuidad. La mayoría de los hitos considerados, por otra parte, tuvieron lugar de forma concentrada durante ciertos periodos: 1997-1999, 2003-2005, 2011-2014, y 2016-2019.

El primer periodo tuvo lugar hacia finales del segundo gobierno de Carlos Menem (1995-1999) y está marcado por la creación del AR-CERT en 1999. Sin embargo, las primeras acciones específicas a nivel del Poder Ejecutivo en materia de ciberseguridad datan de 1998. En la Jefatura de Gabinete se había creado una Oficina de Coordinación e Integración Tecnológica, que desde 1996 se abocó a coordinar la primera agenda nacional en gobierno electrónico, centrada en la firma digital. Sobre la base de dicho trabajo, el mismo equipo se abocó luego a coordinar los eventos preparatorios para la adaptación de la administración pública al denominado "Y2K". Asimismo, en 1998, dicha Oficina identificó a la seguridad informática como nuevo asunto prioritario. La metodología adoptada en los tres casos fue la misma, según retrata una fuente consultada que participó en dicho proceso: la organización de un gran evento temático anual servía para instalar el tema en la agenda y recabar las demandas de las partes interesadas, lo que luego era seguido de una serie de políticas, junto a la identificación de un nuevo tema estratégico asociado a la transformación digital.

En tal sentido, podemos decir que el comienzo de la trayectoria institucional de Argentina en ciberseguridad refleja un caso de *spillover* funcional, derivado de la adaptación de la administración pública a la modernización estatal, por entonces conceptualizada como "gobierno electrónico".[11]

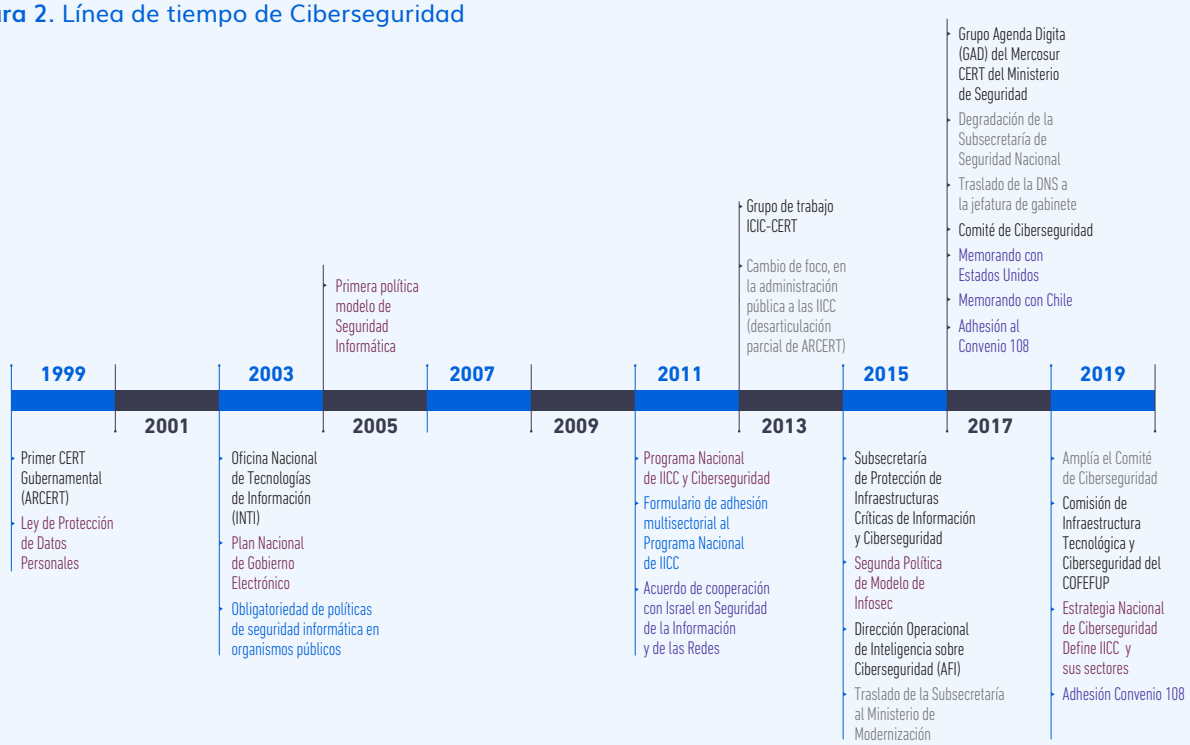
Puede decirse que este rico primer periodo inicial se cierra con el gobierno de Fernando De la Rúa (1999-2001). Como suele recordarse, este este gobierno vetó parcialmente la ley integral de protección de datos, para eliminar el carácter independiente de la autoridad de aplicación. Menos sabido es que también desmanteló el trabajo del AR-CERT, que luego sería reactivado durante el gobierno de Néstor Kirchner.

9. Ver Télam 27/7/20. Disponible en: https://www.telam.com.ar/notas/202007/495165-defensa-y-arsat-firmaron-convenio-de-cooperacion-en-areas-de-conectividad-y-ciberseguridad.html (último acceso 8/8/20).

10. Este esquema fue implementado durante el mandato de Macri y no fue revertido. Algunas fuentes criticaron esta situación, por constituir un recurso poco transparente, que deja en evidencia la baja prioridad asignada a la institucionalización en materia de ciberseguridad.

11. A su vez, motorizaron este primer sentido de urgencia sendos incidentes informáticos sufridos en 1998 por la Corte Suprema de Justicia y en 1999 por las Fuerzas Armadas. En ambos casos, se trató de episodios de defacement del sitio web, obra de un grupo llamado X-Team. Esto suscitó que la Corte le solicitara al gobierno, mediante una acordada, que incorporara la figura de los delitos informáticos. Ahora bien, el gobierno de De la Rúa procesó esta experiencia menos mediante la tipificación penal de los ciberdelitos que mediante la creación del AR-CERT (Resolución 1/99), y su reglamento operativo (Disposición 1/99). Ver Página12, 8/5/2002, disponible en: https://www.pagina12.com.ar/diario/sociedad/3-4891-2002-05-08.html, y La Nación, 15/4/2002, disponible en: https://www.lanacion.com.ar/sociedad/los-mensajes-que-dejo-el-x-team-nid388791/

Figura 2. Línea de tiempo de Ciberseguridad



Fuente: elaboración propia

La presidencia de Kirchner coincidió con los tumultuosos años de la Cumbre Mundial de la Sociedad de la Información (WSIS, en inglés), 2003-2005. En materia de políticas se registraron algunos hechos destacables, como la creación de la ONTI en 2003, la obligatoriedad de contar con políticas de seguridad informática en organismos públicos en 2004, y el Plan de Gobierno Electrónico y la primera Política Modelo de Seguridad Informática, ambos hechos en 2005. La ONTI recuperó la línea de trabajo de la Oficina de Coordinación e Integración Tecnológica de los años 90, y hasta 2015 serviría como organismo multipropósito para la transformación digital de los organismos públicos, incluyendo desde procesos de estandarización, hasta la protección de la infraestructura crítica. Desde el año 2000 hasta 2008, a su vez, se mantuvo de forma ininterrumpida la participación del AR-CERT en el FIRST, mediante la participación presencial en sus eventos de al menos dos técnicos por año. Asimismo, durante este periodo el AR-CERT adoptó cierto carácter de CERT coordinador nacional, en tanto brindó asistencia técnica en las provincias, así como para la apertura del CERT de Banelco (especializado en el sector financiero) y el CERT de la Universidad Nacional de La Plata (CERT-UNLP), y patrocinó al Sistema Nacional de Gestión de Incidentes Telemáticos de Venezuela (VEN-CERT) para que se incorporara a la red FIRST.

Los alcances y límites de las políticas sobre ciberseguridad durante el periodo 2011-2014 son más difíciles de caracterizar. Por un lado, se dieron avances importantes: en 2011 se creó el Programa Nacional de Infraestructuras Críticas, en 2013 se creó el Grupo de Trabajo ICIC-CERT (que heredó el trabajo del AR-CERT), y en 2014 se publicó la segunda Política Modelo de Seguridad Informática, mientras que a nivel MERCOSUR se creó la RAPRISIT en 2014. También se comenzó a participar en la red multisectorial *Global Forum on Cyber Expertise*.

Sin embargo, no se trató de hechos coordinados a partir de una estrategia, sino de eventos aislados, que en algunos casos obturaron el proceso de maduración institucional desplegado en la última década. Así, algunas fuentes han planteado que el ICIC-CERT, a pesar de suponer un cambio de foco hacia las IICC, no logró consolidar una visión unificada acerca de estas: "Los criterios de clasificación no eran claros y la adhesión voluntaria al Programa era problemática: no debería haber sido optativo para aquellas infraestructuras que realmente eran críticas", señala una fuente que participó en el proceso.

Al mismo tiempo, tampoco se logró profundizar ni sostener las capacidades sociotécnicas desarrolladas por el AR-CERT desde 1999, centradas más bien en elaborar respuestas a incidentes informáticos en la administración pública. Esto no solo en virtud de un proceso de reformulación de preferencias institucional inacabado, sino también, según la misma fuente, como resultado de "una merma en el personal técnico, reemplazado en su mayoría por personal administrativo en el CERT, que se limitaba a ingresar incidentes con un aporte mínimo de valor a quienes requerían asistencia especializada".

Finalmente, el RAPRISIT del MERCOSUR nunca sería constituido en los hechos.[12]

Del incluso más contradictorio periodo 2015-2019 destacamos cuatro elementos: i) cierto desarrollo institucional de relevancia, a partir de la creación de la Dirección Nacional de Ciberseguridad (DNC) y el Grupo Agenda Digital (GAD) del MERCOSUR, y cierto desarrollo doctrinario (en especial en la última etapa del gobierno), mediante la publicación de una Estrategia Nacional de Ciberseguridad (ENC) y algunas definiciones conceptuales estratégicas; ii) las diversas modificaciones a los organismos ya creados, sea para modificar su objeto, su jerarquía o su dependencia funcional (con la migración temporal desde Jefatura de Gabinete al ministerio de Modernización); iiii) el desarrollo de capacidades institucionales sobre ciberseguridad en el Ministerio de Seguridad, primero, y Defensa después, complejizando el escenario de construcción de capacidades materiales, técnicas y de coordinación para la DNC; y iv) una profusa actividad en materia de ciberdiplomacia, si bien como tomador de normas, mediante la firma de memorandos de cooperación en ciberseguridad con Chile y Estados Unidos, ambos transversales a los tres ámbitos de aplicación.[13] A su vez, durante este periodo tuvieron lugar las cumbres del G20 y los Juegos Olímpicos de la Juventud (JJOOJ), además de la OMC y la ITU.

Finalmente, podríamos considerar como un nuevo periodo el iniciado con la actual gestión de Fernández, marcado en términos contextuales por la pandemia del Covid-19. En tal sentido, se consigna un hito en esta etapa: la mencionada constitución de la Comisión de Infraestructura Tecnológica y Ciberseguridad del COFEFUP.

La línea de tiempo para el caso de la *ciberdefensa* (ver Figura 3) es menos densa, pero pone en evidencia algunos elementos interesantes, como una continuidad de las políticas de cooperación tecnológica con Israel. Precisamente con el Memorando de Entendimiento de 2010 damos inicio a la línea de tiempo, si bien dicho instrumento, a diferencia del celebrado en 2018, refería a la cooperación tecnológica en sentido amplio y no estrictamente a la ciberdefensa.

El proceso de desarrollo de capacidades institucionales comienza en 2015, con la creación de la Dirección General de Ciberdefensa, por entonces dependiente de la Unidad Ministro del MINDEF, es decir, bajo control directo del titular (civil) de la cartera. No obstante, ya en 2014 se habían incorporado, por primera vez, lineamientos en relación con el dominio ciberespacial en la Directiva de Política de Defensa Nacional (DPDN):

> La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la 'guerra real' y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes (DPDN, 2014).

El mayor desarrollo de capacidades en el ámbito del MINDEF, no obstante, tuvo lugar desde 2018, en el contexto de la preparación del G20, durante el gobierno de Macri. Más allá de la solución llave en mano que supuso la adquisición del SIEM Q-Radar en términos de capacidades defensivas, los informantes consultados también destacaron que este proceso supuso acelerar el desarrollo de capacidades de coordinación entre el MINDEF, el Ciber-Comando del Estado Mayor Conjunto, y las tres fuerzas (Ejército, Fuerza Aérea y Armada). No se registra evidencia de un avance en materia de capacidades ofensivas.

Por otra parte, cabe destacar que aquí encontramos cierta continuidad entre gobiernos de diverso signo político, en virtud de la firma en 2018 de un nuevo acuerdo con Israel, para el desarrollo de capacidades en protección de las IICC a través de un núcleo CIRT. No todo en ciberdiplomacia fue continuidad, sin embargo: mediante el ya aludido memorando de entendimiento de 2017, se profundizó el vínculo con Estados Unidos, mientras que los gobiernos predecesores plantearon una relación más crítica, en sintonía con las potencias emergentes como China y Rusia.

También se produjeron cambios de dependencia e incluso de objeto en los organismos de *ciberdefensa*, aunque no en la misma magnitud que lo ocurrido en materia de *ciberseguridad*, y con un mayor sentido estratégico. En concreto, la Subsecretaría de Ciberdefensa pasó de depender de la Secretaría de Ciencia, Tecnología y Producción para la Defensa, a la de Estrategia y Asuntos Militares. Finalmente, en 2019, se publicó la primera Política de Ciberdefensa, que creó diversos organismos en el seno del Ministerio de Defensa, no todos operativos.

Durante el mandato de Macri también se publicó una nueva DPDN (2018) con más definiciones estratégicas sobre la defensa en el ciberespacio (el prefijo "ciber"

12. Una de las fuentes consultadas, especialista en seguridad informática que ha liderado un programa nacional de desarrollo de capacidades digitales, sostiene que la creación del ICIC-CERT, y su foco en las IICC, planteó un desafío para la nueva autoridad de aplicación: cómo aprovechar el acervo institucional y el conocimiento socio-técnico en materia de respuesta a incidentes en la administración pública nacional, acumulado desde 1999. Hasta el momento, "este desafío no ha sido resuelto por ninguno de los gobiernos", concluye. Otra fuente, también especializada en seguridad informática y que ocupó cargos jerárquicos, coincide con dicha apreciación, y agrega que desde 2011-2013 ha habido "una involución" en la materia.

13. En 2017, en el marco de los preparativos para la cumbre del G20, Argentina firmó un memorando con Estados Unidos para establecer un grupo de trabajo para la cooperación en materia de seguridad cibernética, el cual resulta transversal a los tres ámbitos de incumbencia. Ver Joint Statement on U.S.-Argentina Partnership on Cyber Policy, disponible en: https://www.state.gov/joint-statement-on-u-s-argentina-partnership-on-cyber-policy/

Figura 3. Línea de tiempo de Ciberdefensa

Fuente: elaboración propia

es mencionado 25 veces), y se reformó el decreto reglamentario de la Ley de Defensa. Esta última reforma supuso la revisión de la noción de que un ataque externo que justifica la intervención del instrumento militar debe ser realizado por actores estatales.

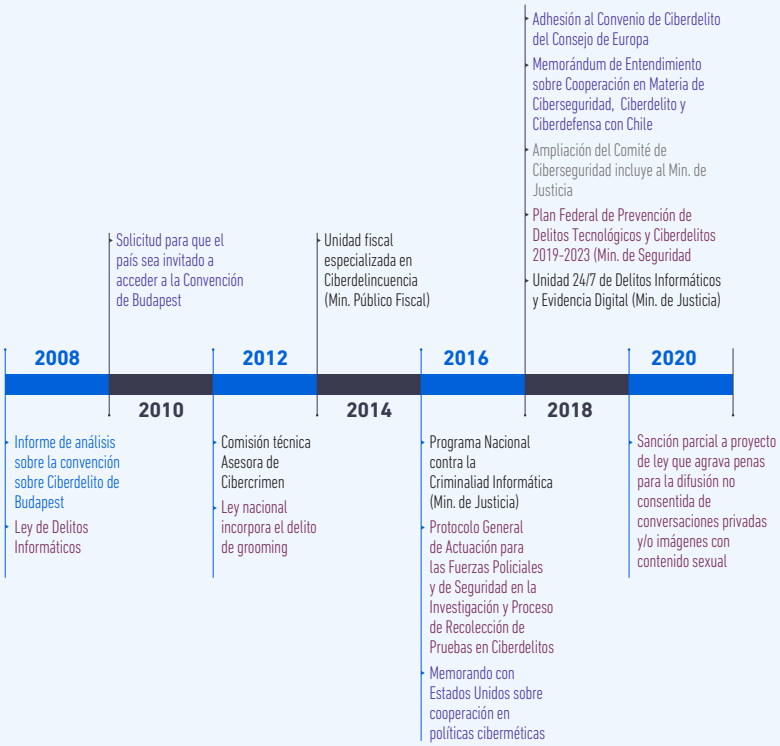
Las políticas consideradas durante lo que va del gobierno de Alberto Fernández son, justamente, la derogación de los decretos reformadores de 2018, restituyendo los decretos reglamentarios de 2006 y 2007, y la derogación de la DPDN2018, por lo que hoy rige la DPDN2014.

La línea de tiempo para el ámbito del *ciberdelito* (ver Figura 4) evidencia tres elementos de interés. En primer lugar, una relativa continuidad, en general, y en especial en materia de ciberdiplomacia, en virtud del alineamiento con el Consejo de Europa y su Convención de Budapest: ley de delitos informáticos en 2008, solicitud para ser invitado como firmante no europeo en 2010, adhesión en 2018, y ampliación del Comité de Ciberseguridad para incluir al Ministerio de Justicia en 2019 (en línea, según sus propios considerandos, con lo planteado por el Consejo de Europa en la materia). En segundo lugar, resaltamos la apelación a leyes nacionales como instrumentos con impacto sistémico en el ecosistema digital. Y, por último, el desarrollo de capacidades institucionales en tres ministerios diferentes: el ministerio de Justicia, el Ministerio Público Fiscal, y el Ministerio de Seguridad.

En síntesis, en los tres ámbitos de aplicación se están desarrollando políticas orientadas a fortalecer sus capacidades institucionales, aunque de un modo dispar, sin una coordinación integral salvo ciertas coyunturas críticas (en general producidas por factores internacionales), y sin una continuidad en el tiempo, en particular, tras los respectivos cambios de gobierno. No obstante, se registra cierta continuidad en materia de ciberdelitos, lo que puede explicarse por la combinación de la memoria institucional de las organizaciones asociadas al poder judicial, menos condicionada por la lógica de la alternancia política, por un lado, y porque existe un claro *stakeholder* internacional formador de normas sobre *ciberdelito* con cierto nivel de consenso a nivel internacional, el Consejo de Europa, por el otro. Donde la trayectoria institucional en ciberdelitos se asemeja más a *ciberseguridad* y *ciberdefensa*, en cambio, es en sus dificultades en términos de coordinación estratégica e integración multisectorial, en particular, a la hora de lograr una capilaridad a nivel federal. Actualmente se encuentra impulsando un proceso de federalización, pero todavía en etapa inicial: solo cinco de las 24 jurisdicciones del país cuentan con fiscalías especializadas en ciberdelitos (Ciudad Autónoma de Buenos Aires, Chubut, Salta, Chaco y Córdoba).

Por último, cabe resaltar que, de los tres ámbitos, el de la *ciberseguridad* ha sido el más difícil de demarcar. Las idas y vueltas de Modernización a Jefatura de Gabinete durante el mandato de Macri dan prueba de ello. No obstante, no se trata de una tendencia exclusiva de dicho gobierno. La co-existencia entre tres tipos de definiciones de "infraestructura crítica" y las dificultades para definir los roles entre ciberseguridad y ciberdefensa se mantienen hasta el día de hoy, aunque la incertidumbre se resuelva de hecho a partir del mayor desarrollo relativo de capacidades en la cartera de Defensa.

Figura 4. Línea de tiempo de Ciberdelitos



Fuente: elaboración propia

3. Normativa nacional

En este apartado se mapea la normativa existente en materia de ciberseguridad, ciberdefensa y ciberdelito (ver Tabla 1). No obstante, para ser breves, solo se menciona la normativa, consignando si corresponde a específicamente al ámbito de aplicación (por ejemplo, ciberseguridad) o más bien de una norma vinculada a la gobernanza de las partes interesadas, y por tanto, con impacto indirecto sobre la cuestión. Como vemos, Argentina cuenta con normativa específica exclusivamente para el caso de *ciberdelitos*, donde el desarrollo institucional es mayor y su inicio ha sido previo en el tiempo. En materia de *ciberseguridad*, la normativa está limitada a un conjunto de normas de relevancia, aunque no específicas (entre las que se destaca la ley de Protección de Datos Personales), y a documentos oficiales con definiciones que establecen una dirección común para las múltiples partes interesadas (entre las que se destaca la definición de Infraestructuras Críticas). Esto último también ocurre para el caso de la Ciberdefensa, pero aquí se cuenta con la Directiva Nacional de Defensa, la cual establece la misión institucional del Sistema de Defensa en el ciberespacio.

Tabla 1. Normativa sobre Ciberseguridad, Ciberdefensa y Ciberdelitos

Comunidad / Normativa	Normativa específica	Normativa vinculada a la gobernanza de las partes interesadas
Ciberseguridad	• Definición de Infraestructuras Críticas de Información, sectores alcanzados y glosario de términos de ciberseguridad (Resolución SGM N° 1523/2019) • Estrategia Nacional de Ciberseguridad (Resolución 829/2019) • Creación del Comité de Ciberseguridad (Decreto N° 577/2017) • Política Modelo de Seguridad de la Información (Disposición ONTI N° 1/2015) • Creación del ICIC-CERT (Disposición ONTI N° 2/2013) • Formulario mediante el cual se le permite a las múltiples partes interesadas adherir al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad: Disposición ONTI N° 3/2011 • Obligatoriedad para los organismos públicos nacionales de contar con una Política de Seguridad de la Información, de asignar responsabilidades en Seguridad y de tener un Comité de Seguridad (Decisión Administrativa N° 669/2004) • Creación del AR-CERT (Resolución 81/99) • Reglamento de operación del ARCERT (Disposición 1/99).	• Agenda Digital Argentina (Decreto 996/2018) • Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Ley 27483) • Nueva Doctrina de Inteligencia Nacional • (Decreto 1311/2015) • Ley de Inteligencia Nacional (Ley 27.126) • Relevamiento de Equipamientos Tecnológicos, Redes de Comunicaciones y Datos y Estructuras de Funcionamiento en Centro de Procesamiento de Datos (DA 252/2016) • Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica del MERCOSUR (RAPRISIT) (Decisiones CMC 17/14 y 09/19) • Principios generales relativos a la protección de datos personales (Decreto Reglamentario N° 1558/2001) • Ley de Firma Digital (Ley 25.506) y Reglamentación de la ley de Firma Digital (Decreto N° 2628/2002) • Ley de Protección de Datos Personales (Ley 25.326)
Ciberdefensa	• Política Nacional de Ciberdefensa (Resolución 1380/2019)	• Convenio entre el MINDEF y ARSAT (2020) • Ley de Defensa Nacional (Ley 23.554) • Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas (Decreto 1691/2006) • Decreto reglamentario de la Ley de Defensa Nacional (Decreto 727/2006)
Ciberdelito	• Ley de Delitos Informáticos (Ley 26.388) • Ley de Grooming (Ley 26.904, noviembre de 2013) • Adhesión al Convenio de Ciberdelito del Consejo de Europa, con cinco reservas (Ley 27.411)	• "Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas" (Resolución 144/2020) [14]

Fuente: elaboración propia.

4. Definiciones conceptuales clave

¿Cómo se define al "ciberespacio", la "ciberseguridad", la "ciberdefensa" y los "ciberdelitos" en Argentina? Se consignan las definiciones conceptuales de cada ámbito de incumbencia de los organismos públicos (ver Tabla 2).

14. Además, se encuentra en consideración un proyecto de ley con sanción del Senado mediante el cual se agravan las penas para quienes difundan sin consentimiento imágenes o conversaciones privadas con contenido sexual. Disponible en https://www.telam.com.ar/notas/202007/493689-senado-aprueba-agravar-penas-quienes-difundan-conversaciones-privadas-desnudos-sin-permiso.html (último acceso 8/8/20)

Tabla 2. Definiciones conceptuales de los tres ámbitos de incumbencia

Concepto / Definición	Definición
Ciberespacio	"Nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones, tiene entre otras, como características esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución" (*Estrategia Nacional de Ciberseguridad, 2018*).[15]
Ciberseguridad	Las "previsiones nacionales en materia de protección del Ciberespacio. Su finalidad es brindar un contexto seguro para su aprovechamiento por parte de las personas y organizaciones públicas y privadas, desarrollando de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, juntamente con el desarrollo de un marco normativo acorde" (*Estrategia Nacional de Ciberseguridad, 2018*).
Ciberdefensa	"Las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia. (*Política Nacional de Ciberdefensa, 2019*).
Ciberdelitos	Delitos realizados por a través de las tecnologías de la información y comunicación (TIC's) en el ciberespacio. Asimismo, debe entenderse como "Delitos Tecnológicos" aquellos delitos cuya planificación, organización, ejecución o resultado se encuentra expuesta en el ciberespacio o en elementos tecnológicos que pueden ayudar tanto en la investigación de delitos tradicionales como en ciberdelitos (*Plan 2019-2023 de Ministerio de Seguridad)*.
Ciberdiplomacia	"La diplomacia puesta al servicio de la cooperación y creación de normas para el ciberespacio" (*Glosario de Términos de Ciberseguridad, Secretaría de Gobierno de Modernización*).[16]

Fuente: elaboración propia en base a documentos oficiales.

5. Estrategias nacionales

¿Existen estrategias nacionales que propongan un enfoque sistémico de la ciberseguridad, la ciberdefensa y el combate al ciberdelito o rigen abordajes particulares según la agencia estatal interesada?

Tanto en materia de *ciberseguridad* como de *ciberdefensa* y de *ciberdelitos* existen instrumentos que sirven de guías rectoras para el accionar de las múltiples partes interesadas, en particular desde y dentro del ecosistema institucional estatal. No obstante, su aplicación efectiva es limitada, sobre todo en el caso de ciberseguridad. En los tres casos, a su vez, se trata de instrumentos recientes, impulsados durante gobiernos de signo político diverso, por lo que su continuidad en el tiempo permanece como una incógnita.

Ciberseguridad

La Estrategia Nacional de Ciberseguridad (ENC), publicada en 2019, establece "los principios esenciales y los objetivos centrales de la República Argentina en torno a su proyecto para la protección del ciberespacio", orientándose al desarrollo de "adecuadas capacidades de prevención, detección, análisis, investigación, recuperación, defensa y respuesta", en particular en lo referido a las infraestructuras críticas de información (Resolución 829/2019). A su vez, también desde 2019, el país cuenta con un Glosario de términos relativos a la protección de la infraestructura crítica.

Los "principios rectores" de la ENC son cinco: (i) Respeto por los Derechos y Libertades Individuales; (ii) Liderazgo, Construcción de Capacidades y Fortalecimiento Federal; (iii) Integración Internacional; (iv) Cultura de Ciberseguridad y Responsabilidad Compartida; y (v) Fortalecimiento del Desarrollo Socioeconómico.[17] Sobre

15. En este punto, encontramos una clara semejanza con la definición del ciberespacio utilizada por España en su Estrategia Nacional de Ciberseguridad. En efecto, dos informantes consultados señalaron que el INCIBE de España representa un referente global para la Argentina (Maurer y Morgus, 2013a: 9).

16. Es decir, se basa en lo planteado a nivel conceptual por el investigador y diplomático norteamericano Shaun Riordan (2019).

17. En materia de ciberdiplomacia, cabe señalar que, a partir de una perspectiva crítica del "uso militar creciente del Ciberespacio", la ECN plantea una cierta base doctrinaria para el accionar gubernamental: "la República Argentina promoverá en todos los foros en los que participe el uso pacífico del Ciberespacio y apoyará toda iniciativa que tenga por fin la instauración de valores como la Justicia, el respeto al Derecho Internacional, el equilibrio y la disminución

dichas bases define ocho objetivos centrales y delinea diversos planes de acción para su consecución. Estos objetivos son:

1. Concientización del uso seguro del Ciberespacio
2. Capacitación y educación en el uso seguro del Ciberespacio
3. Desarrollo del marco normativo
4. Fortalecimiento de capacidades de prevención, detección y respuesta
5. Protección y recuperación de los sistemas de información del Sector Público
6. Fomento de la industria de la ciberseguridad
7. Cooperación Internacional
8. Protección de las Infraestructuras Críticas Nacionales de Información

En cuanto a las condiciones en que la ENC fue producida, cabe señalar que fue publicada hacia el final del mandato del gobierno de Macri (lo que lógicamente habría de dificultar su sostenimiento en el tiempo, considerando la falta de políticas de Estado ya señalada). Se introdujo a partir de un Resolución de la Secretaría de Gobierno de Modernización, dependiente por entonces de la Jefatura de Gabinete de Ministros. Es decir, no se trató de una estrategia emanada de una ley, sancionada tras el debate en el Poder Legislativo, con la participación de múltiples partes interesadas. En lugar de ello, fue creada a partir de la labor del Comité de Ciberseguridad, constituido en julio de 2017. En cuanto al nivel de representatividad multisectorial de dicho comité, es más bien limitado. Inicialmente estuvo integrado por la mencionada Secretaría de Gobierno de Modernización (a cargo de la presidencia), y por los ministerios de Seguridad y de Defensa; luego fue ampliado para incluir a los ministerios de Relaciones Exteriores y Culto, y de Justicia, junto a la Secretaría de Asuntos estratégicos de Jefatura de Gabinete. O sea, su conformación es eminentemente estatal y, en rigor, estrictamente gubernamentalista. Con todo, se trató del principal intento de elaborar una mesa de coordinación estratégica con los actores estatales de los tres ámbitos de incumbencia, si bien con nivel de consulta muy limitado en materia de actores de la sociedad civil. De cualquier modo, la Estrategia se presentó como el resultado de un proceso multisectorial, centrado en dicho Comité de Ciberseguridad. En efecto, la resolución que crea la ENC sostiene que "los integrantes del Comité de Ciberseguridad, en consulta con diversos actores de los sectores privado y académico, han trabajado de forma coordinada y han prestado conformidad a la aprobación de la Estrategia Nacional de Ciberseguridad, con el fin de elaborar un documento preliminar que refleje el desarrollo tecnológico y la realidad geopolítica de nuestro país".

A nivel local, contó con la asistencia de la Facultad de Ingeniería de la Universidad de La Plata. A nivel global, se consultó al *Forum of Incident Response and Security Teams* (FIRST), el *National Institute of Stantards and Technology* (NIST), a los gobiernos de Costa Rica, España e Israel, y compañías dedicadas a la seguridad de sistemas informáticos industriales.

Como se dijo ya, existían algunos antecedentes de peso para la ECN, elaborados durante los gobiernos kirchneristas: la Política Modelo de Ciberseguridad de 2005, y su actualización y ampliación a partir de la Nueva Política de Seguridad de la Información Modelo, de 2014. La ENC, no obstante, no los considera entre sus referencias. Esto es una constante en Argentina: la ausencia de políticas de Estado que trasciendan a los gobiernos. A su vez, como se dijo, también desde el actual gobierno de Alberto Fernández (2019-2023) se ha cuestionado a la estrategia elaborada durante el gobierno macrista por considerarla "porteño-centrista", y se ha planteado la necesidad de una nueva Estrategia de carácter federal.

Así, en lugar de buscar los antecedentes necesarios para una memoria institucional en el propio historial nacional, la Estrategia Nacional se asienta fundamentalmente sobre la labor de organizaciones internacionales. Así, y como podrá verse en la Figura 7 y el apartado 1.5, el Decreto N° 577/2017 que creó el Comité de Ciberseguridad con el objeto de elaborar una Estrategia Nacional inscribe sus antecedentes en el accionar de la OEA y en la ITU. Respecto a la OEA, identifica como antecedente la Estrategia Interamericana Integral de Seguridad Cibernética, creada mediante la Resolución AG/RES 2004 (XXXIV-O/04). Respecto a la ITU, se identifica con la iniciativa denominada Agenda sobre Ciberseguridad Global (GCA) y la iniciativa IMPACT.

Ciberdefensa

La Política Nacional de Ciberdefensa también fue publicada en 2019 (PNC19), a meses de concluir el mandato de Macri (de hecho, una semana antes de la derrota electoral ante Fernández). Considerando el historial de la Argentina ante cambios de signo político, resulta difícil decir a ciencia cierta si esta política será continuada. Por lo pronto, la derogación de los decretos asociados a la reforma del sistema de Defensa de 2018 no incluyó a la PNC de 2019. En tal sentido, este documento sienta las bases conceptuales, doctrinales e institucionales de la política de ciberdefensa en el país, si bien todavía no se han aplicado varios de sus elementos, a la vez que permanece cierta incertidumbre respecto al ámbito de aplicación respecto al área de Ciberseguridad.

La PNC19 fue publicada mediante una resolución del Ministerio de Defensa (Resolución 1380/2019). Su

de la brecha digital entre las naciones, impulsando el diálogo y la cooperación. El Ciberespacio debe constituirse en un dominio en el que impere la paz, sustrayéndolo de posibles conflictos armados".

punto de partida es establecer una nueva definición de ciberdefensa mediante una caracterización donde se menciona a las principales partes interesadas en la materia: el ministerio de Defensa, el Estado Mayor Conjunto y las Fuerzas Armadas (Ejército, Armada y Fuerza Aérea). Esto es central porque es precisamente la coordinación y la construcción de confianza entre dichas agencias lo que se presenta, de acuerdo con el diálogo con los informantes clave y el análisis de la evidencia empírica, así como del análisis de la larga duración en la Argentina, como el principal desafío en el país. Esto no solo por la aprehensión entre las distintas fuerzas, sino también, y sobre todo, por las dificultades vinculadas a la convivencia entre civiles y militares en un país donde la conducción civil de las fuerzas armadas, construida de forma ardua pero sostenida desde la restauración democrática en 1983, es una de las principales políticas de Estado.

Un segundo aspecto saliente de la definición es el alcance de la misión de la ciberdefensa, que se orienta a la protección de la infraestructura crítica, pero mediante una enumeración de categorías que conviene desglosar. En tal sentido, la ciberdefensa argentina se define como las acciones y capacidades desarrolladas por las tres partes ya consignadas para "anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar":

- al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional;
- a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa;
- a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa;
- o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia.

En tercer lugar, de un modo algo confuso, la PC establece seis misiones para el MINDEF en el ciberespacio, cuatro "líneas de acción", tres ejes de políticas y dos planes operativos. Las misiones del MINDEF en el ciberespacio son:

a. Anticipar y prevenir ataques en el ciberespacio.
b. Disminuir vulnerabilidades y aumentar la resiliencia de los sistemas y redes TICs de las Fuerzas Armadas, Estado Mayor Conjunto y Ministerio de Defensa.
c. Detectar amenazas y gestionar riesgos de ciberataques, y recuperación de los sistemas e infraestructura crítica de interés para la Defensa Nacional.
d. Adoptar las acciones contra potenciales adversarios o agentes hostiles que afecten la integridad y disponibilidad de las redes y sistemas de la Defensa.
e. Contribuir a potenciar la base tecnológica e industrial nacional de ciberseguridad en trabajo conjunto con el Ministerio de Relaciones Exteriores y del Ministerio de Producción.
f. Impulsar programas de capacitación para superar brecha entre los recursos humanos disponibles y los demandados.

Para poner en práctica estos objetivos, la PC establece cuatro Líneas de Acción:

i. Creación del Centro Nacional de Ciberdefensa (CNC). Por cierto, además de crear al CNC en tanto espacio donde articular a los diversos actores militares involucrados en la ciberdefensa (constituido en diciembre de 2019), introdujo al Comité Consultivo de Ciberdefensa (con cierto carácter multisectorial, si bien todavía no constituido).
ii. Proteger la disponibilidad del ciberespacio como espacio soberano
iii. Reingeniería de las redes de las Fuerzas Armadas, del Estado Mayor Conjunto y del Ministerio de Defensa
iv. Convergencia de las capacidades de las FFAA

A su vez, se establecen tres políticas para el desarrollo de dichas líneas de acción:

a. Políticas regulatorias
b. Políticas de desarrollo de capacidades para la interacción en el ciberespacio
c. Políticas de concientización y capacitación

En conjunto, estos lineamientos se disponen a través de dos planes:

1. Plan Nacional de Infraestructuras críticas de la Defensa Nacional
2. Plan de Adecuación de las organizaciones militares

El Plan Nacional de Infraestructuras críticas de la Defensa Nacional cuenta con cierto nivel de detalle en la PC2019, si bien permanece la incertidumbre respecto cómo se definen los roles entre *ciberseguridad* y *ciberdefensa*. Un dato sintomático de este fenómeno es que la PC2019 menciona en 16 oportunidades a la palabra "ciberseguridad".

Lo que sí se define, al menos formalmente, son los actores intervinientes en la protección de infraestructuras críticas cibernéticas: el Comité de Ciberseguridad, la Secretaría de Gobierno de Modernización (luego sustituida por la Jefatura de Gabinete), entes reguladores, operadores críticos y el MINDEF.

También se dispone que el CSIRT del MINDEF, entre otras funciones, actúa: i) como la "puerta de enlace para la recepción de datos de incidentes o conductas cibernéticas anómalas desde otros CERT's nacionales y extranjeros y desde fuentes abiertas", de modo tal que permita "enriquecer la toma de decisión ante un ciberataque"; y ii) en la captura de información sobre amenazas cibernéticas a objetivos estratégicos IICC de la Defensa. Para efectuar dicha captura procesa la información recibida desde los sensores y demás hardware específicos de las redes TO instaladas en los puntos acordados con los Entes Reguladores de los servicios esenciales y objetivos estratégicos de las IICC de interés para la Defensa Nacional. Luego puede poner a disposición de dichos Entes Reguladores o organismos

correspondientes, de acuerdo con el ordenamiento jurídico vigente, los datos necesarios para la construcción de "la imagen situacional oportuna del ciberespacio". En cuanto al Plan de Adecuación de las organizaciones militares, en cambio, no ha sido detallado en la PC2019, y solo ha sido proyectado.

Ciberdelitos

En materia de ciberdelito, finalmente, el país no cuenta con una estrategia nacional que facilite la coordinación estratégica entre múltiples actores como Justicia, el Ministerio Público Fiscal y el Ministerio de Seguridad. Este último, para lo competente a su accionar específico, sí cuenta con un Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2019 - 2023), a la vez que cuenta con un Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos, ambos instrumentos fueron aprobados durante la gestión de Macri. Asimismo, cuenta con un Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas, aprobado durante el gobierno actual de Alberto Fernández, y muy cuestionado por las organizaciones de la sociedad civil. Por otra parte, el alineamiento del país con las preferencias definidas en la ciberdiplomacia del Consejo de Europa a través de su Convención de Budapest sobre Ciberdelito establece pautas doctrinarias de peso que marcarán una dependencia de sendero institucional.

6. Diplomacia normativa

Entendemos por "ciberdiplomacia" a la "diplomacia puesta al servicio de la cooperación y creación de normas para el ciberespacio" (Riordan, 2019). Otra definición valiosa es aportada por André Barrinha y Thomas Renard (2017): "la diplomacia en el dominio ciberespacial o, en otras palabras, el uso de recursos diplomáticos y la performance de funciones diplomáticas para asegurar intereses nacionales relativos al ciberespacio" (2017).

En materia de cooperación internacional, ha habido cierta continuidad en las preferencias, a pesar de las diferentes aproximaciones a las negociaciones con las principales potencias, en especial hacia Estados Unidos y China. Esto, sin que exista un organismo en la Cancillería encargada de velar por coordinar una agenda integral en el campo de las políticas digitales. Desde inicios del siglo, así como un organismo como la ONTI tuvo un rol multi-propósito en el ámbito de la Jefatura de Gabinete, en la Cancillería fue ejercido por la Dirección de Asuntos Digitales (cuyo rango y ámbito de dependencia se vio modificado múltiples veces desde su creación hasta ser sucedida por la DIATI en 2018, y por la Oficina de Ciberseguridad, Ciberdelito y Asuntos Digitales (OCCAD), en 2020.

En *ciberseguridad*, en la agenda externa de Argentina encontramos a la OEA, la OTAN, la ITU, y el GGE de la ONU; y a nivel bilateral, Estados Unidos, Israel y Chile, mediante acuerdos formales, y España y Costa Rica, a través de su influencia en términos de ciberdiplomacia, así como organismos técnicos como el NIST el FIRST. En *ciberdefensa*, se observa una trayectoria consolidada de asociación con Israel, mientras que en *ciberdelitos* se registra un consenso en torno al alineamiento con la OEA y el Consejo de Europa; esto último se extiende a otros estándares sobre protección de datos definidos por las autoridades europeas (con incidencia indirecta en la gobernanza de la ciberseguridad).

A continuación, se analizan los alineamientos internacionales según el ámbito de aplicación (ciberseguridad, ciberdefensa y ciberdelitos), pues existen tanto semejanzas como diferencias en materia de alianzas e instrumentos preferidos de cooperación internacional. Luego, se analiza el comportamiento de Argentina en relación con sus interlocutores externos: acuerdos bilaterales, agenda regional y organización de cumbres internacionales.

Según ámbito de aplicación

En las materias de *ciberdelitos* y *ciberseguridad*, los actores internacionales clave han sido la OEA y el Consejo de Europea. Su influencia, de un modo u otro, se registra en prácticamente todos los gobiernos comprendidos entre 1999 y 2020, en especial desde 2013. Ya sea a partir de su Resolución AG/RES 2004, o por el accionar en torno al Comité Interamericano contra el Terrorismo (CICTE-OEA), la OEA ha sido tomada como referencia para instituciones tanto sobre ciberdelito como sobre seguridad de la información.

Por ejemplo, al CICTE-OEA se lo menciona como principal antecedente en la creación del ICIC-CERT en agosto de 2013. A la Resolución AG/RES 2004 se la menciona en la creación del Comité de Ciberseguridad y del CERT del Ministerio de Seguridad en 2017. En ambos casos, los gobiernos respondían a signos políticos diferentes.[18]

Respecto al Consejo de Europa, si bien la ratificación del Convenio de Budapest se produjo en el año 2017 (durante el gobierno de Macri), la primera misiva de un gobierno argentino al Consejo de Europa manifestando el deseo de ser país invitado data de 2010, durante el segundo mandato presidencial de Cristina Fernández de Kirchner.

18. Cabe señalar que una fuente consultada, especialista en seguridad informática que ha participado en procesos de consulta multisectorial impulsados por los gobiernos argentinos y ha ocupado un cargo nacional relacionado, considera "problemático" desde un punto de vista académico el hecho de que la resolución que creó al ICIC-CERT en agosto de 2013 haya inscripto la decisión en línea con la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" del CICTE-OEA. Coincidimos en su apreciación, sobre todo considerando que habían pasado dos meses desde la primera

En *ciberseguridad* (ver Tabla 3), cabe mencionar acuerdos de cooperación bilaterales, tanto con gobiernos como organizaciones técnicas. Entre los primeros cabe mencionar a Israel, Estados Unidos, España y Costa Rica, mientras que entre los actores no estatales se incluye al FIRST y el NIST.

En *ciberdefensa* (ver Tabla 4) se destacan los acuerdos con Israel, que se tradujeron en la adquisición del SIEM Q-Radar, comercializado por la empresa mixta israelí *Rafael Advanced Systems*. Además, el país participa desde 2019 en dos plataformas de inteligencia contra amenazas: *Malware Information Sharing Platform* (MISP), basada en Luxemburgo, y *Trusted Automated Exchange of Intelligence Information* (TAXII), centrada en EEUU.

filtración de datos sobre el programa PRISM, a la vez que el proceso de cooperación regional se encontraba orientado hacia la búsqueda de autonomía, vía la creación de organismos como la Unión de Naciones Suramericanas (UNASUR). De hecho, a nivel MERCOSUR, el RAPRISIT sería creado poco después, 2014, como órgano destinado a la seguridad cibernética en el bloque, precisamente bajo lineamientos autonomistas. Por otra parte, en julio de 2013, un mes antes de la creación del ICIC-CERT, se había aprobado la Decisión CMC del MERCOSUR sobre el Rechazo al Espionaje por parte de los Estados Unidos sobre los Países de la Región, mientras que la UNASUR, casi al mismo tiempo, había dado a conocer la Declaración de Paramaribo, también en línea autonomista (Bustos, 2016). Sin embargo, otra fuente consultada, con un rol en el ámbito diplomático, considera que el acercamiento a la OEA tiene más de pragmatismo que de ideología: "la OEA tiene más capacidades, pero sobre todo tiene mejor implementados sus programas de capacitación. Lo inteligente es aprovechar todas estas oportunidades, sin dejar de avanzar en nuestras propias definiciones".

Tabla 3. Ciberdiplomacia y ciberseguridad

MERCOSUR / Región	ONU	OEA	Consejo de Europa	Otros
• Creación de la Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica del MERCOSUR (RAPRISIT), en 2014. A mediados de 2019, las facultades del RAPRISIT fueron trasladadas al Sub Grupo de Trabajo 1 del Grupo Mercado Común del bloque (Comunicaciones) • En 2009 se patrocinó al Sistema Nacional de Gestión de Incidentes Telemáticos de Venezuela (VEN-CERT) para que se incorporara a la red FIRST.	• Creación del Comité de Ciberseguridad en 2017 se referencia en Agenda sobre Ciberseguridad Global (GCA) de la ITU • Creación del CSIRT del Ministerio de Seguridad en Agenda GCA. • OCCAD de Cancillería participa de forma creciente en el Grupo de Trabajo Abierto de la ONU, conformado en 2019 (GTCA). A su vez, pondera la Resolución AGNU 70/237, que consolida trabajo del GGE	• Creación del ICIC-CERT en 2013 se referencia en el CICTE-OEA y la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" de 2012. • Creación del Comité de Ciberseguridad en 2017 se referencia en la Estrategia Interamericana Integral de Seguridad Cibernética de la OEA (Resolución AG/RES 2004) • Creación del CSIRT del Ministerio de Seguridad en 2017 se referencia en Resolución AG/RES 2004 de la OEA	• Suscriptor del Convenio 108 de Tratamiento Automatizado de Datos de Carácter Personal (2018) • Adhesión al Convenio de Ciberdelito del Consejo de Europa (2017)	• Participación en ICANN (vía OCCAD de Cancillería) • Acuerdo con Israel en materia de Telecomunicaciones, Servicios Postales y Seguridad de la Información y de las Redes (2011). • Declaración Conjunta con Estados Unidos sobre Políticas Cibernéticas (2017). • Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad, Ciberdelito y Ciberdefensa con Chile (2018) • Participación en iniciativa conjunta Canadá, Gran Bretaña, Nueva Zelanda, Australia y Países Bajos para promover la participación de mujeres en procesos negociadores de acuerdos sobre ciberseguridad (vía OCCAD) • Participación en red FIRST desde el año 2000 y en la red Global Forum on Cyber Expertise desde 2011. • Definición de "ciberespacio" en Estrategia Nacional de Ciberseguridad (2018) inspirada en definición española.

Fuente: elaboración propia

Tabla 4. Ciberdiplomacia y ciberdefensa

MERCOSUR / Región	Vínculos bilaterales	G20	Otros mecanismos de cooperación
• Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad, Ciberdelito y Ciberdefensa con Chile (2018) • Entre 2016 y 2019, el ciber-comando del Estado Mayor Conjunto organizó dos congresos de ciberdefensa donde participaron Colombia, Brasil, México, Chile, Portugal y España.	• Memorando de Entendimiento respecto a la Cooperación Industrial y Tecnológica en Defensa con Israel (2010) • Acuerdo con Israel para armar núcleo CIRT (2018).	• Influencia clave del G20 en formación de preferencias y desarrollo de capacidades en ciberdefensa durante preparación de la Cumbre en Argentina.	• Participación en redes de intercambio MISP (basada en Luxemburgo) y TAXII (centrada en Estados Unidos). • OCCAD de Cancillería participa de forma creciente en el Grupo de Trabajo Abierto de la ONU, conformado en 2019 (GTCA). A su vez, pondera la Resolución AGNU 70/237, que consolida trabajo del GGE.

Fuente: elaboración propia

Tabla 5. Ciberdiplomacia y ciberdelitos

MERCOSUR / Región	Consejo de Europa	Instrumentos de cooperación internacional
• Participa en Subgrupo de trabajo informal de fiscales de delitos informáticos del MERCOSUR • Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad, Ciberdelito y Ciberdefensa con Chile (2018)	• Debate legislativo para sanción de la Ley de delitos informáticos se referencia en Convención de Budapest (2008) • Informe de Análisis sobre la "Convención sobre Ciberdelito de Budapest", publicado el 19/6/2008. • Creación de Comisión Técnica Asesora de Ciberdelito se referencia en Convención de Budapest (2011) • En 2011 (gobierno Fernández de Kirchner) solicita ser invitado a acceder a la Convención de Budapest. • Ampliación del Comité de Seguridad se referencia en Convención de Budapest (2019) • Adhesión al Convenio de Ciberdelito del Consejo de Europa (2017) • El país integra el Bureau del Consejo de Europa entre 2018 y 2020. • Desde 2016 a 2019, se celebraron talleres de formación para 2016 más de 850 operadores judiciales de todo el país, impulsados por el Ministerio de Justicia con apoyo internacional del Consejo de Europa y la OEA.	• Participa de la Asociación Iberoamericana de Fiscales Públicos, que cuenta con una red de fiscales electrónicos. • Participa en Interpol • Participa en red del G7

Fuente: elaboración propia

Además, el país participó del Grupo de Expertos Gubernamentales (GGE) en Ciberseguridad de Naciones Unidas en una oportunidad, en la edición 2012-2013. De hecho, entre los fundamentos
de la creación del RAPRISIT en el Mercosur en 2014 figura el GGE de la ONU, por lo que cabe pensar en la influencia de dicha experiencia para Argentina.[19]

Por otra parte, el ciber-comando del Estado Mayor Conjunto organizó dos congresos de ciberdefensa, en los cuales participaron Colombia, Brasil, México, Chile, Portugal y España.

La exploración de alternativas en clave regional, como las que podría ofrecer el Consejo Suramericano de Defensa asociado a la UNASUR, parecen haber quedado en el camino con la salida del país del bloque, en 2018.

Asimismo, Argentina participa en diversos foros donde se producen instancias de networking, construcción de capacidades y ciertos procesos informales de convergencia de preferencias: la Asociación Iberoamericana de Fiscales Públicos, que cuenta con una red de fiscales electrónicos; la red Interpol; la red del G7; y el Subgrupo de trabajo de Justicia del MERCOSUR, a partir de un agenciamiento por ahora informal entre fiscales de delitos informáticos del bloque. La participación en la red de Interpol se traduce, al igual que en el caso de la Convención de Budapest, en un instrumento disponible para contar con mayores capacidades en procesos de investigaciones judiciales. De hecho, uno de los informantes consultados, quien ocupa un rol clave en el sistema judicial nacional, consideró que contar con la red de Interpol es fundamental para realizar investigaciones que involucran países no suscriptores de la Convención de Budapest. De hecho, la misma fuente sostuvo que de no contar con dicho instrumento de cooperación se presentarían serias dificultades a la hora de abordar investigaciones que involucran a países como Rusia, en tanto país no suscriptor del acuerdo europeo, pero sí integrante de la red Interpol, y uno de los países a los que deben acudir de forma creciente a la hora de investigar ciberdelitos. En tal sentido, la fuente sostuvo que la membresía limitada de la Convención de Budapest presenta sus desafíos, y que ante la complejidad de contar con una normativa que exija la localización de datos en servidores locales, su preferencia sería celebrar acuerdos de cooperación en ciberdelitos con ciertos países específicos, como sería el caso de China y Rusia.

19. El contexto de la decisión del bloque estaba marcado por las controversias en la región a raíz de diversos episodios asociados a la autonomía tecnológica, suscitadas en especial, pero no exclusivamente, a partir de las develaciones de Snowden (Bustos, 2016).

Acuerdos bilaterales y foros multilaterales

Argentina tiene acuerdos de cooperación bilateral para el desarrollo de capacidades y construcción de confianza en ciberseguridad con Israel (tres acuerdos), Estados Unidos (un acuerdo) y Chile (un acuerdo).

De los tres, el vínculo formal que mayor profundidad ha desarrollado en los hechos es el celebrado con Israel. Si bien el vínculo estratégico en materia de cooperación tecnológica se profundizó durante el mandato de Macri (2015-2019), hasta materializarse en la adopción de una solución "llave en mano" mediante la adquisición de un SIEM (*Security Information and Event Management*), se trata de un alineamiento con bastante grado de consenso en las principales fuerzas políticas. El primer instrumento bilateral con Israel específico a la materia de interés data de 2010, durante el primer mandato de Fernández de Kirchner, y abordó la cuestión de la cooperación en defensa. El siguiente fue celebrado poco después, en 2011, y estableció disposiciones relativas a la seguridad de la información y de las redes.[20]

El Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad, Ciberdelito y Ciberdefensa con Chile (2018) no se ha traducido, hasta el momento, en iniciativas concretas para la creación de capacidades.[21] En cuanto al celebrado con Estados Unidos en 2017, estuvo sobre todo orientado a los preparativos para que el país fuera sede de las cumbres del G20, la OMC y la ITU.

En cuanto a la participación en organismos multilaterales, en especial en el marco de la ONU, en diversas cuestiones relativas a la gobernanza digital Argentina ha sostenido su histórica posición de país defensor del multilateralismo. En los hechos, esto se tradujo en una activa participación en la ITU (desde Jefatura de Gabinete),[22] y de forma más reciente, en el *Open-Ended Working Group* de la ONU (OEWG, GTCA en castellano), conformado a finales de 2018 a instancias de Rusia.

Esto último resulta interesante de cara a lo que viene en la gobernanza global de la ciberseguridad. Argentina ha participado en el Grupo de Expertos Gubernamentales (GGE) en el año 2012-2013. A nivel subregional, no obstante, el rol de participar en dicho espacio durante el resto de las ocasiones ha correspondido a Brasil, y en segunda instancia, a Uruguay. La profundización del trabajo de Argentina en el GTCA plantea interrogantes respecto a si las tensiones geopolíticas entre sendos grupos pueden trasladarse al seno del proceso de integración.[23]

Finalmente, otro asunto abordado en la arena multilateral es la cuestión del ciberdelito, y la posibilidad de elaborar un acuerdo que supere a la Convención de Budapest, o al menos la complemente mediante un instrumento global (esta última es la lectura más difundida entre las fuentes consultadas). En este punto, la posición de Argentina en este aspecto es compleja. Como se señaló en el apartado anterior, el país es suscriptor del acuerdo de Budapest, pero eso no se traduce en un desinterés por avanzar en acuerdos multilaterales, o incluso bilaterales con países como Rusia o China. En esto han coincidido fuentes provenientes del ciberdelito y de la ciberdiplomacia. Por tanto, es esperable que el país profundice una estrategia que combine la participación en el Consejo de Europa y a la vez participe de un proceso negociador de un acuerdo multilateral en la materia.[24]

---

20. Ver el Memorando de Entendimiento entre sendos ministerios de Defensa en materia de Cooperación Industrial y Tecnológica en Defensa, de diciembre de 2010; y el acuerdo entre ambos gobiernos sobre Cooperación en materia de Telecomunicaciones, Servicios Postales y Seguridad de la Información y de las Redes, del 4 de abril de 2011.

21. Acompañó, sin embargo, un acuerdo bilateral que estableció las disposiciones respecto a las instalaciones informáticas y el flujo transfronterizo de datos para un acuerdo firmado por Argentina. El acuerdo comercial dispone que cada Parte permitirá la transferencia transfronteriza de información por medios electrónicos, cuando esta actividad sea para la realización de la actividad comercial de una persona de una parte. En materia de instalaciones informáticas, a diferencia de los acuerdos Chile-Uruguay o Chile-Brasil, el texto solo señala un norte, pero no establece pautas vinculantes. En concreto, dispone que las partes "reconocen la importancia de no exigir a una persona de la otra Parte usar o ubicar las instalaciones informáticas en el territorio de esa Parte, como condición para la realización de negocios en ese territorio". Asimismo, sostiene que las partes se comprometen a intercambiar buenas prácticas, experiencias y marcos regulatorios vigentes respecto a la localización de servidores (Bustos, Rivero, Palazzi, en prensa).

22. Si bien no se vincula directamente a la cuestión de la ciberseguridad, la adopción o no del Régimen de Telecomunicaciones adoptado por la ITU en 2012, en la Cumbre Mundial de Telecomunicaciones de Dubai, en su momento solía ser considerado como una variable proxy de las preferencias institucionales en relación con la gobernanza digital (Aguerre y Galperin, 2015). En tal sentido, Argentina ha sido identificado como un país con una política exterior en relación con el ciberespacio "potencialmente oscilante" (Maurer y Morgus, 2014), en tanto presentaría a la vez elementos del "intergubernamentalismo" y del "multisectorialismo".

23. Una fuente consultada al respecto, proveniente del ámbito diplomático, precisa los términos de lo que consideramos una preferencia institucional emergente en el campo de la ciberdiplomacia: "El GGE establece una línea de base, pero el GTCA es el horizonte. Argentina tiene que definir qué constituye al uso de fuerza en el ciberespacio. Eso tiene que ser producto de una discusión abierta, inclusiva, transparente y multisectorial. Plantear así el escenario no supone una posición extrema, que supondría desconocer los logros del GGE. En tal sentido, reconocemos la importancia de la Resolución AGNU 70/237, que consolida el trabajo del GGE, y le da carácter multilateral mediante un acuerdo consensuado. Asimismo, tiene sus riegos, porque sabemos qué tan inclusivo es el GTCA, pero no qué tan productivo resulte. Siempre hay que hacer ese tipo de balances".

24. Cabe señalar que la resolución propuesta por Rusia ante la ONU, denominada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", fue puesta en consideración por la Asamblea General en diciembre de 2019. En dicha votación, la Argentina se abstuvo, al igual que varios países de la región de América Latina. Las fuentes consultadas sostienen que dicha posición se planteó como una solución de equilibrio, considerando que se espera para 2021 la publicación de un informe relativo a cómo mejorar el acuerdo de Budapest y hacerlo un instru-

MERCOSUR: entre el GAD y los SGT

A nivel MERCOSUR, como se adelantó en la Sección 2, se destaca el rol del Grupo Agenda Digital (GAD), creado en 2017.

Históricamente en el bloque, la agenda asociada al "gobierno electrónico", como se les daba a llamar a inicios de siglo, había sido abordada por el Sub-Grupo de Trabajo 1 del Mercosur, dedicado a Comunicaciones (SGT-1), mientras que la agenda asociada al "comercio electrónico" había sido abordada por el SGT-13, de Comercio Electrónico.

El GAD del MERCOSUR se creó en sintonía con el GAD creado por la Alianza del Pacífico un año antes. Tiene mayor jerarquía que cualquier SGT, y asesora de forma directa al Grupo Mercado Común. A pesar de su corta historia, ha servido para establecer una línea de base para la agenda digital del MERCOSUR.

Si bien es demasiado pronto para ver los alcances del proceso, se puede decir que la agenda de seguridad cibernética se presenta como uno de los *drivers* de la cooperación efectiva, más acá de los 13 objetivos formalmente delineados en 2017 para el GAD. En 2019, precisamente a instancias de Argentina, circuló entre los países parte un primer "cuestionario sobre seguridad cibernética", elaborado por personal del ICIC-CERT en conjunto con la Dirección Nacional del MERCOSUR (encargada de coordinar el trabajo del GAD). En su última reunión, en mayo de 2020, incluso se proyectó un "Acuerdo de Cooperación en materia de Seguridad Cibernética en el MERCOSUR", y se facultó a Brasil para que elabore "los antecedentes tanto del cuestionario", como del propio "borrador de acuerdo de Seguridad Cibernética". No obstante, hasta el momento Brasil no ha presentado la documentación, a la vez que no está muy claro si ha de ceñirse a lo identificado en el cuestionario promovido por Argentina un año antes.

Además del GAD, cabe mencionar al RAPRISIT, creada en 2014 en el MERCOSUR para proponer políticas e iniciativas comunes en el área de la seguridad cibernética y la privacidad, y facultada para crear instancias de expertos para la discusión de aspectos técnicos relacionados con su mandato.

Esto supone retrotraernos por un momento al periodo 2011-2014 (ver Sección 2.1.). Consideramos que durante estos años se produjo una suerte de coyuntura crítica que sirvió para movilizar a las dirigencias políticas de los países de la región, en general, y del MERCOSUR, en particular, en torno a cierta agenda de desarrollo de capacidades conjuntas en seguridad cibernética, sobre la base de la búsqueda de la "autonomía tecnológica" (Bustos, 2016). En rigor, el proyecto de infraestructura asociado a este objetivo figuraba desde 2011 entre las iniciativas del Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN) –esquema que sucedió a IIRSA–, pero nunca había sido puesto en práctica. De todos modos, el *momentum* solo se tradujo en documentos y declaraciones, porque pronto se produjeron cambios de signo político en los países que lideraban la iniciativa (Brasil, en 2014, y Argentina, en 2015). El RAPRISIT nunca tuvo carácter operativo.

Finalmente, a mediados de 2019, bajo mandato de Macri, el RAPRISIT pasó a la órbita del SGT 1. Es posible que esto contribuya a su dinamización, pero lo más lógico habría sido fortalecer al (GAD).[25]

Finalmente, cabe decir algo sobre el "Acuerdo en Principio" entre la UE y el MERCOSUR, en tanto, establece disposiciones en materia de protección a la privacidad y flujos de datos personales. Mediante el actual Art. 54 (de alineamiento con el GATS), la EU reafirma sus reglas de flujos de datos, a la vez que permite adoptar medidas de amparo de datos personales (art. 54.1.f. ii) siempre que su aplicación no sea discriminatoria o que no sea una barrera disfrazada al comercio (Bustos, Rivero, Palazzi, 2020).

La ciberdiplomacia del G20 como factor aglutinante durante la gestión de Macri

Uno de los aspectos más destacados de las políticas sobre ciberseguridad recientes en Argentina es el impacto que tuvo la realización de la cumbre del G20 en noviembre de 2018. Todos los informantes consultados que tuvieron alguna participación en el gobierno de Macri (2015-2019), en los tres ámbitos de aplicación, coinciden en señalar que fue un vector imprescindible para generar un sentido de urgencia en el gobierno, favorecer la definición de preferencias institucionales homogéneas, generar una instancia de articulación entre las diversas partes interesadas y dejar en evidencia la necesidad de impulsar un proceso acelerado de desarrollo de capacidades. Asimismo, un informante crítico de dicho gobierno reconoce que, precisamente por su alineamiento con factores externos, la gestión de Macri logró cierto nivel de coordinación, no logrado por administraciones previas.

Un informante clave del campo de la ciberdefensa, quien tuvo un rol jerárquico en materia de inteligencia de amenazas, sostuvo que el G20 fue fundamental para obtener los recursos necesarios para el desarrollo de capacidades defensivas:

mento más universal, por lo que se consideró oportuno esperar a dicha publicación, antes de avanzar con la alternativa multilateral.

25. Cabe mencionar que, de acuerdo con las fuentes consultadas asociadas al ámbito del ciberdelito, de forma reciente se ha impulsado la generación de un subgrupo de trabajo de fiscales de delitos informáticos. Los actores nacionales de Argentina involucrados con la investigación de ciberdelitos participan regularmente de este espacio, que ha funcionado como un entorno para el intercambio de experiencias y de desarrollo de vínculos entre los fiscales especializados.

> El G20 fue una bendición. Lo usamos como catalizador. Si no, nunca habrían aceptado gastar tanto. Y fue un éxito. Todavía la Argentina no está preparada para comprender lo que logramos en el G20.

Un informante clave del campo del ciberdelito, quien tiene un rol de conducción en uno de los organismos públicos centrales de la materia, consideró que el evento fue clave para lograr un espacio de articulación entre los diversos actores involucrados:

> En Argentina cuesta encontrar una coordinación de actores en una mesa común. El G20 y los JJOO de la Juventud generaron esa mesa común. Cuando dejás algo afuera de esa mesa corrés el riesgo de vulnerar derechos.

Un informante clave del campo de la ciberseguridad, en tanto, quien tuvo un rol central en el desarrollo de la Estrategia Nacional, indicó que el sentido de urgencia generado por la cumbre también sirvió para dejar en evidencia el talento local:

> El G20 demostró un gran grado de cohesión. Es cierto que contamos con gran soporte del *vendor*. El comentario del mundo tecnológico fue 'no pensamos que Argentina iba a aprender tan rápido'. La implementación de QRADAR se dio en tiempo récord. Se encontraron bugs que los *vendors* no conocían, lo que también habla del talento que hay acá.

Los informantes consultados sostienen que algo similar ocurrió cuando se realizaron los Juegos Olímpicos de la Juventud, tan solo un mes antes del G20, en octubre de 2018. "El Comité Olímpico venía arrastrando una historia de ciber-incidentes. Había escenarios de riesgo. Y terminó siendo el primer juego sin incidentes de la historia", sostuvo una fuente involucrada en ciberseguridad y ciberdefensa.

Diremos entonces que el rol de anfitrión de estas cumbres sirvió como coyuntura crítica, la cual favoreció la creación de un sentido de urgencia favorable al desarrollo de preferencias homogéneas en el gobierno, orientadas al logro de mayores capacidades defensivas, de coordinación estratégica, y de cooperación internacional. Sin embargo, del mismo modo que ocurrido en el caso de la coyuntura crítica generada a nivel regional entre 2011 y 2014, el impacto no sería duradero. En ambos casos, el vector aglutinante fue un factor externo y la agenda fue eminentemente reactiva.

7. Preferencias institucionales

Siguiendo la definición minimalista de Orfeo Fioretos (2001), partimos de definir a las "preferencias institucionales" como "la posición que el gobierno de un país promoverá" en el nivel internacional (2001: 225) ante la existencia de una diversidad de opciones de política exterior en un asunto determinado. Ahora bien, en lo relativo a la gobernanza del ciberespacio, en general, y en lo ateniente a las políticas sobre ciberseguridad, en particular, diremos que las "preferencias institucionales" que nos interesan son las posiciones que los estados promueven en el nivel internacional en términos de ciberdiplomacia, y los diseños institucionales de sus políticas nacionales relativas a la ciberseguridad.[26]

Las políticas públicas sobre ciberseguridad en Argentina tienden a identificarse con gestiones de gobierno más que a seguir una definición de política de Estado. A su vez, la existencia de preferencias divergentes sobre diseño institucional en materia de políticas digitales responde a debates de larga duración. Los gobiernos peronistas (2003-2007, 2007-2011, 2011-2015), incluyendo al de Alberto Fernández (2019-2023), han priorizado a la Jefatura de Gabinete (JGM) como organismo rector en materia de ciberseguridad. El gobierno de Macri (2015-2019), en cambio, mientras pudo contar con los recursos presupuestarios suficientes, procuró darle el liderazgo a un Ministerio de Modernización.

Esto se inscribe en un proceso socio-histórico de larga duración, marcado por la tensión entre el enfoque de la "modernización" vis a vis el enfoque de la "autonomía" (Powers y Jablonsky, 2015; Bustos, 2016). A fuerza de simplificar, diremos que una línea histórica ha apelado más bien a la búsqueda de la "autonomía" vis a vis actores centrales como Gran Bretaña, Estados Unidos o la Unión Europea, (1945-1955, 1973-1974, 1983-1985, 2003-2015). A nivel global esto se materializó en una mayor participación en foros multilaterales como la UNESCO o la ITU, o foros regionales o sub-regionales (como la UNASUR o el MERCOSUR, en la última década), mientras que a nivel local se centró en agencias asociadas a autoridades de aplicación en el ámbito de la comunicación audiovisual, o la Jefatura de Gabinete. La otra línea, en cambio, ha apelado a la búsqueda de la "modernización" (1976-1983, 1985-2001), para lo cual ha seguido una estrategia de acomodación en el nivel internacional, procurando que el alineamiento con Estados Unidos no se tradujera en la pérdida de ventajas institucionales en el vínculo con la Unión Europea, mientras que a nivel nacional ha impulsado programas de modernización estatal centrados, fundamentalmente, en el ministerio de Modernización.[27]

26. Ver el marco teórico en Anexo 1, que contiene al marco analítico para el análisis empírico y comparado de los países latinoamericanos e(Krasner, 1982; Robert Keohane y Joseph Nye, 1989; Rosenau, 1992; Stoker, 1998; Pierson and Skocpol, 2002; Acharya, 2004; Drezner, 2007; Goldsmith y Wu, 2006; Abbott y Snidal, 2008; Lessig, 2009, Sassen, 2010; Diebert y Rohzinski, 2011; Nye, 2014; Canabarro y Borne, 2012; Canabarro, 2014; Maurer y Morgus, 2014; Aguerre, 2015; Aguerre y Galperin, 2015; Abbot, Green y Keohane, 2016; Finnemore y Hollis, 2016; Kerry, 2016; Barrinha y Renard, 2017; Hurel y Lobato, 2018; Dunn Cavelty, 2018; Riordan, 2019).

27. Para un análisis de la evolución de los conceptos de "autonomía en la política exterior" y de "autonomía tecnológica" en la región, y

Esto va más allá de la cuestión bajo análisis. Por ejemplo, desde junio de 2016 a junio de 2020, se modificó la denominación el Consejo Federal de la Función Pública (COFEFUP), creado en 1992, por la de Consejo Federal de Modernización. En 2020, la gestión de Fernández retomó su nombre originario.

Dicho esto, hasta el día de hecho existe cierta indefinición respecto al rol a desempeñar por el ICIC-CERT en el ecosistema digital nacional, lo que cual impacta sistémicamente sobre todas las demás preferencias institucionales a formular por parte de las autoridades. Como se dijo, esto no puede asociarse a un solo gobierno, sino que es más bien una tendencia general que se ha mantenido durante la última década. Un informante clave que estuvo vinculada al área lo describe así:

> "Todavía no definimos para qué está el ICIC-CERT: ¿es la protección de las IICC, o de la administración pública nacional y federal, o es la coordinación como CERT central a nivel nacional, o es ser un poco de todo, hasta lograr delegar algunas de estas funciones? Si es efectivamente la protección de las IICC, como está planteado desde 2011, entonces necesitás desarrollar capacidades técnicas, cosa que en la última década no ha ocurrido. Si no querés ser el CERT nacional que asista a las provincias, de acuerdo, pero la salida de este rol no debe ser acelerada, porque por ahora no hay mejor alternativa. Y si vas a ser el CERT nacional, coordinador, promotor de capacidades y de un entorno seguro público-privado, entonces hay que empezar a coordinar una multiplicidad de temas y actores, cosa que por ahora no ocurre. Lo que está claro es lo que no debe hacerse: limitarse a funcionar como el área de seguridad o como un equipo de respuesta a incidentes de un organismo en particular".

A continuación, se abordan las preferencias institucionales mediante una distinción analítica entre protección de las IICC y respuestas a incidentes informáticos, una diferenciación que en el caso de la Argentina se muestra particularmente pertinente, precisamente en virtud de lo recién dicho.

Protección de las IICC

El mecanismo de protección de las infraestructuras críticas (IICC) sigue un enfoque gubernamental, pero se sitúa a la vez en el ámbito de la *ciberseguridad*, donde adopta un perfil específicamente civil, y (desde 2019) en el de la *ciberdefensa*, donde está sujeto a un esquema de cooperación civil-militar bajo mando civil. En general, no obstante, se evidencia una participación casi exclusiva de actores estatales durante el proceso de desarrollo de la normativa relativa a la protección de las infraestructuras críticas.

Ahora bien, encontramos que los diseños institucionales que definen los roles, los ámbitos de incumbencia y las responsabilidades de los actores estatales, así como los canales de articulación entre ellas, se basan en caracterizaciones de las IICC que dan lugar a ciertas ambigüedades. Por empezar, la autoridad varía dependiendo de la definición de "infraestructura crítica", por lo que no puede decirse que existe una clara estructura institucional con capacidades de coordinación estratégica en lo relativo a la protección de las IICC. La Tabla 6 permite ver las múltiples definiciones asociadas a las IICC con las que se opera.

Como señaló Marcela Pallero, especialista en políticas de ciberseguridad, al ser consultada para este informe, "la distinción entre infraestructura crítica e infraestructura crítica de información es propia de países que están recién iniciando la discusión sobre ciberseguridad, en tanto no contempla como normal un escenario de sistemas ciber-físicos integrados". A su vez, encontramos criterios de clasificación muy amplios en el caso de ciberseguridad, y algo más específicos en el caso de ciberdefensa.

Además, esta inconclusa gobernanza por diseño entre la Dirección Nacional de Ciberseguridad y la Subsecretaría de Ciberdefensa se inscribe en una raigambre socio-histórica compleja, construida en la larga duración, donde la participación de las fuerzas armadas en asuntos de seguridad interior se mantiene estrictamente limitada a la asistencia logística, y el uso del instrumento militar se utiliza en caso de agresión externa estatal. Esto, como parte de los consensos que hicieron posible la vuelta al régimen democrático en los 80, y permitieron consolidarlo en los 90.

Ahora bien, en términos de preferencias institucionales en un sistema político que parece estar recobrando su histórica dinámica bipardista (si bien menos sobre partidos que sobre frentes electorales), esto se tradujo en que los gobiernos de signo peronista han tendido a fortalecer el rol de la Jefatura de Gabinete vis a vis Defensa en materia de Protección de las IICC; mientras que el gobierno de Macri fortaleció las capacidades de Seguridad y de Defensa.

Así, en 2018, Macri planteó una reforma del sistema de Defensa Nacional, que supuso la revisión de la noción de que un ataque externo debía ser realizado por actores estatales. Esto generó una controversia donde la oposición (peronista) se manifestó de forma crítica, en tanto podía interpretarse como una erosión de la distinción entre los ámbitos de aplicación de la defensa y la seguridad, comprometiendo el consenso democrático en torno a la dedicación del instrumento militar a las amenazas estaduales externas, y su no intervención en asuntos domésticos y de índole política.

sus efectos sobre los procesos de cooperación regional, ver Bustos (2016).

Tabla 6. Definiciones estratégicas sobre IICC

Concepto	Definición
Infraestructuras Críticas (IICC)	Las Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. (*Estrategia Nacional de Ciberseguridad, Anexo I, 2018*).
Infraestructura Crítica de la Información	Las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como lainformación asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas. (*Estrategia Nacional de Ciberseguridad, Anexo I, 2018*).
Infraestructuras Críticas Cibernéticas de la Defensa Nacional	Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto en la capacidad operacional del Instrumento Militar en el ciberespacio y/o en la prestación de los servicios esenciales así como la producción de bienes de interés para la Defensa. (*Política Nacional de Ciberdefensa, 2019*).
Infraestructura Cibernética	Las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y/o Tecnologías de Operación (TO). (*Política Nacional de Ciberdefensa, 2019*).
Criterios de clasificación de la ICN	• Criterio para clasificar la ICN: Impacto en la vida humana; Impacto económico; Impacto en el medio ambiente; Impacto en el ejercicio de los derechos humanos y de las libertades individuales; Impacto público o social; Impacto en el ejercicio de las funciones del estado; Impacto en la soberanía nacional; Impacto en mantenimiento de la integridad territorial nacional (*Estrategia Nacional de Ciberseguridad, Anexo I, 2018*). Clasificación de la ICN: • Energía; Tecnologías de Información y Comunicaciones; Transportes; Hídrico; Salud; Alimentación; Finanzas; Nuclear; Químico; Espacio; Estado (*Estrategia Nacional de Ciberseguridad, Anexo I, 2018*). • Criterio y clasificación de la Infraestructura Crítica de la Defensa Nacional: a) Infraestructura crítica del sistema de defensa b) Infraestructura de interés para la defensa Nacional i. Infraestructuras TO soporte de servicios esenciales: energética y nuclear. ii. Infraestructuras TO soporte de procesos industriales, de fabricación de bienes sensibles: Explosivos, moderadores de fisión en reactores nucleares, con capacidad de producir daños masivos al medio ambiente. (*Política Nacional de Ciberdefensa, 2019*).

Fuente: elaboración propia.

No obstante, cabe señalar que, a pesar de dejar sin efecto la DPDN de 2018 y derogar el decreto reglamentario de la ley de Defensa del mismo año, hasta ahora el gobierno de Fernández no ha dado señales claras en lo relativo a la protección de las IICC.[28]

Respecto a la relación entre autoridades, entes reguladores y operadores críticos, también encontramos un desarrollo inicial en términos de diseño institucional. El Objetivo 5 de la ENC19, "Protección y recuperación de los sistemas de información del Sector Público", instruye al Comité de Ciberseguridad a generar un mecanismo consultivo con los responsables de seguridad informática de los Entes Reguladores y el sector privado, así como los organismos de la Administración Pública de los niveles nacional, provincial y municipal "en los cuales se hayan identificado sistemas de información críticos".

La PNC19 va un poco más lejos en este segundo punto. Si bien el documento resulta algo complejo por la multiplicidad de instituciones que crea para coordinar la labor de las tres fuerzas, el Comando Mayor Conjunto, y el propio MINDEF, la directiva de ciberdefensa ofrece algunos más elementos en este sentido. Por empezar, los "operadores críticos" son mencionado 11 veces, versus 1 en la ENC. De la PNC nos interesa resaltar en particular lo dispuesto en torno a los "Actores intervinientes en la protección de infraestructuras críticas cibernéticas". Aquí incluye cinco partes interesadas: "entes reguladores", "operadores críticos", el Comité de Ciberseguridad, al Ministerio de Modernización (por entonces, el ámbito en el que se encontraba el ICIC-CERT, hoy JGM) y al MINDEF.

En la letra, como se ve en la figura 10, la actual definición de sectores comprendidos como infraestructura crítica es muy amplia. En los hechos, no obstante, no contempla a los actores de la capa lógica (como es el ccTLD y NIC.AR) ni de contenidos, sino que se concentra en las capas físicas. Tampoco a sectores de la esfera pública, tales como medios de comunicación y redes sociales. A pesar de esto último, la DNC ha dado señales recientes en torno a un mayor involucramiento

28. Esta indefinición respecto a esta gobernanza conjunta entre la DNC y el MINDEF se verifica incluso entre los propios consultados en el marco de esta investigación. Por ejemplo, una sostiene que la participación de las Fuerzas Armadas en la materia debe limitarse estrictamente a la protección de su propia infraestructura crítica, mientras que otra afirma "No está mala que haya un CERT en Defensa (como tampoco está mal que haya uno en el Ministerio de Seguridad). El tema es que los dos, el CSIRT del MINDEF y el ICIC-CERT, puedan articular la mirada militar y la mirada de la prevención y la resiliencia. Va a haber choques en lo fino, pero si hay choques en lo grueso, como ocurre hoy, es porque no hay acuerdo".

en materia de combate a la desinformación, si bien de forma limitada a la elaboración de recomendaciones a la ciudadanía.[29]

Por otra parte, no se encuentra normativa que exija residencia/localización de datos/operaciones para prestadores de servicios asociados a la infraestructura crítica. Sin embargo, hay ciertas señales de que se va en esta dirección, en virtud de las señales en torno al logro de la "soberanía tecnológica", y a partir de los intentos de consolidar capacidades en infraestructura, incluyendo el despliegue de servicios en la nube, dentro de la operadora estatal ARSAT.

Finalmente, en el ámbito de *ciberdefensa* el país participa en redes de intercambio MISP (basada en Luxemburgo) y TAXII (centrada en Estados Unidos). El ICIC-CERT de Ciberseguridad participa en la red FIRST. A su vez, en preparación de la Estrategia Nacional de Ciberseguridad, consultó al FIRST, el NIST, y a los gobiernos de Estados Unidos, Costa Rica, España, Israel y Chile.

Respuestas a Incidentes

El mecanismo de respuestas a incidentes sigue un enfoque gubernamental, específicamente civil, y se encuentra situado institucionalmente en el ámbito de la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete Ministerial.

Este diseño también se exhibe en el BA-CSIRT del gobierno de la Ciudad Autónoma de Buenos Aires, que además sigue un patrón de colaboradores institucionales similares a los que impulsaron al ICIC originalmente, lo que señala la influencia del Estado nacional en la materia —sobre todo cuando se considera que durante 2015-2019 el gobierno nacional y el de la Ciudad de Buenos Aires tuvieron el mismo signo político.

Adicionalmente, las fuerzas de seguridad tienen su propio CERT dentro de la órbita del ministerio de seguridad, manejando los incidentes de su cartera en forma separada. De esta manera, el ICIC-CERT tiene incumbencia nacional tanto para organismos estatales nacionales y provinciales, así como para empresas e individuos, pero a su vez tiene competencia interna por parte de las entidades gubernamentales, como los casos señalados del Ministerio de Seguridad, o el CSIRT del MINDEF, que operan sus centros de incidentes en forma independiente. Los CSIRTs que funcionan en el ámbito productivo-privado (BANELCO, YPF) o universitario (Universidad Nacional de La Plata) brindan respuestas a sus propias organizaciones, densificando la red de contactos nacionales que trabajan en estos centros con sus particulares características.

El objetivo 5 de la ENC de 2019 proyectó establecer una dinámica de transferencia de información fidedigna entre las diversas agencias estatales y las industrias críticas con liderazgo estatal. Si bien no se puede afirmar categóricamente que existe una política explícita en materia de intercambio de inteligencia/información entre los gobiernos y los sectores de la industria y demás operadores de redes informáticas en el país, el hecho que cuatro de los seis CSIRTs más salientes del país sean miembros del foro FIRST es una muestra que hay una búsqueda más colaborativa entre sectores para enfrentar el problema aun cuando esto no emerge de los aspectos normativos de los CSIRTs gubernamentales, sino en el marco de las buenas prácticas.

En cuanto al gobierno de Alberto Fernández, es demasiado pronto para caracterizar al proceso, pero cabe mencionar que desde el nuevo titular de la DNC se ha planteado como "eje de gestión" el "diseño del entorno de seguridad público juntamente con los sectores privados", como alternativa superadora del enfoque limitado a la concientización ciudadana y el accionar de la justicia para restituir derechos ya vulnerados.[30]

Al mismo tiempo, se ha asociado el desarrollo de una nueva estrategia nacional a la búsqueda de mayor federalización a través de la Comisión de Infraestructura Tecnológica y Ciberseguridad del COFEFUP.

8. Capacidades

A pesar del optimismo planteado por los estudios sobre maduración de capacidades de la OEA y la ITU, puede afirmarse que la Argentina todavía se encuentra en sus etapas formativas en la mayoría de las dimensiones a considerar en materia de ciberseguridad; en especial, en materia de protección de las infraestructuras críticas. Esta sección sintetiza los hallazgos en relación con las capacidades desarrolladas en materia de ciberseguridad, con especial atención a las políticas orientadas a desarrollar capacidades de coordinación estratégica e

29. Ver el Twitter de Gustavo Sain, actual titular de la DNC: https://twitter.com/grsain/status/1285924622895067139?s=09

30. "A veces el rol de los estados se limita a la organización de campañas de concientización o recomendaciones en términos de seguridad informática para que los usuarios o los ciudadanos puedan protegerse frente a eventuales incidentes de tipo informático, o delitos informáticos, como se los conoce habitualmente. Y eso es correcto y está bien. (...) Pero ¿por qué no dar un paso más allá en este paradigma? Que la intervención de los estados o lo gobiernos (no) se dé únicamente cuando el delito ya ha sido consumado, es decir, a partir de la restitución de ese derecho, a partir de la intervención de la justicia. (...) El diseño del entorno de seguridad público juntamente con los sectores privados, es un eje de nuestra gestión, que queremos incentivar. Podemos empezar a pensar a discutir y hablar el trabajo conjunto en el diseño de las condiciones de seguridad informática con el sector privado". Exposición de Saín en el 100° Congreso Iberoamericano de Seguridad de la Información (SEGURINFO), organizado por la Asociación Argentina de Usuarios de la Informática y las Comunicaciones (USUARIA) y el Programa de Ciberseguridad de la OEA, 4 de julio de 2020. Disponible en https://www.youtube.com/watch?v=t3dTXvNud98

integración multisectorial en lo relativo a respuesta a incidentes y protección de las IICC.

Respuestas a incidentes informáticos

Desde 1999 el Estado argentino comenzó su desarrollo de capacidades en ciberseguridad, mediante la creación del AR-CERT. Su reglamento operativo de ese mismo año introdujo definiciones en materia de "Coordinación de Emergencias en Redes Teleinformáticas" que, por entonces, pocos países con un grado de desarrollo semejante a Argentina podían exhibir. Así, la trayectoria técnica e institucional desarrollada desde el cambio de siglo ha permitido generar una línea de base en tanto registro central de incidentes con foco en la seguridad informática de la administración pública nacional.

Sin embargo, como también se adelantó, el proceso estuvo marcado por la discontinuidad. En este caso, esa discontinuidad tomó la forma de una reformulación inconclusa, todavía hoy en búsqueda de su forma equilibrada.

En 2013, el CERT nacional fue relanzado sobre nuevas bases, con el foco en la protección de las IICC, a partir de la creación del ICIC-CERT. No obstante, a pesar de sus años como un registro de incidentes cibernéticos de la infraestructura interna del Estado nacional, el ICIC-CERT no se ha desplegado en todo su potencial, sobre todo en lo ateniente a la coordinación con otras entidades públicas y privadas. Tiene como misión centralizar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional, pero por ahora de forma limitada a las agencias adheridas al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad de 2011. Esta falta de capilaridad, visibilidad y capacidad de acción actual del CERT nacional representa un problema en términos de desarrollo de capacidades en esta materia.

A su vez, no hay evidencia de que la DNC cuente con una estructura de recursos acorde a su mandato institucional (velar por la ciberseguridad a nivel nacional y federal), ni que tenga capacidad de coordinación e integración intersectorial de las múltiples partes interesadas. Ahora que parece definitivamente asentada en el ámbito de Jefatura de Gabinete, la DNC podría estar dando pasos en este sentido, pero es muy pronto para decirlo.

Por otra parte, se constata un creciente canal de contacto entre el sector público y las organizaciones del sector privado (oportunamente identificadas como actores clave para la ciberseguridad nacional), existan o no mecanismos formales de coordinación o de intercambio de información. En parte esto se estaría generando por una suerte de comunidad epistémica en tanto actores que son nucleados en espacios internacionales de intercambios de experiencia y contactos como el foro FIRST, y también porque los especialistas en estas áreas suelen tener un conocimiento personal entre muchas de estas personas.

A su vez, el hecho que cuatro de los seis CSIRTs más salientes del país sean miembros del foro FIRST es una muestra que hay una búsqueda más colaborativa entre sectores para enfrentar el problema, aun cuando esto no emerge de los aspectos normativos de los CSIRTs gubernamentales, sino más bien en el marco de las buenas prácticas. En efecto, de los 539 CSIRTs integrados a la red FIRST, cuatro están localizados en Argentina: el ICIC-CERT, el CSIRT de Banelco, el CSIRT de YPF y el CSIRT de la Ciudad Autónoma de Buenos Aires (BA-CSIRT).

A nivel gubernamental, además del ICIC-CERT de la DNC operan el CSIRT del Ministerio de Seguridad y el CSIRT del MINDEF. El CSIRT del MINDEF, creado en 2019, se presenta como la "puerta de enlace" para otros CERT's nacionales y extranjeros y desde fuentes abiertas. El Q-RADAR gestionado por la Subsecretaría de Ciberdefensa centraliza la información de sensores remotos y otros CERTS nacionales en lo ateniente a "infraestructura crítica para la Defensa".

No se encuentra evidencia de que los objetivos relativos a las respuestas a incidentes informáticos en la ECN y la PNC se actualicen de forma regular, ni de que se haya implementado un sistema de alerta temprana disponible para su utilización por los CERTs sectoriales. Las fuentes consultadas en el ámbito de ciberdefensa (y con un cargo jerárquico durante el gobierno de Macri) consideran que el Q-RADAR del MINDEF puede cumplir esa función, pero en lo ateniente a la protección de Infraestructura Crítica de la Defensa, con las mencionadas dificultades a la hora de delimitar el ámbito de aplicación en cada caso a nivel institucional.

En términos de resiliencia hay una percepción de que existe un déficit en esta materia. El concepto apunta a minimizar el daño y retomar las operaciones en el menor tiempo posible. La OTAN es mencionado como fuente para implementar esta estrategia.

No hay mecanismos de investigación orientados a identificar y analizar las tendencias de incidentes de ciberseguridad de preocupación nacional. Si bien no existe una política formal o sostenida de desarrollo de mecanismos para poner a prueba la resiliencia de la nación ante los incidentes informáticos y las crisis de ciberseguridad, en el nivel nacional se han realizado diversos ejercicios técnicos desde la creación del Programa Nacional de Infraestructuras Críticas y Ciberseguridad. Asimismo, en Ciberdefensa se realizaron diversos escenarios como preparativo para ser sedes de la cumbre del G20, entre otros eventos de peso.

Protección de las IICC

La existencia de una normativa nacional específica para la protección de las IICC está formal e inicialmente contemplada en el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2011), y en la ENC (2019) y la PNC (2019). Sin embargo, como se expuso, la multiplicidad de acepciones y los criterios de clasificación amplios e imprecisos se traduce en dificultades para definir roles y responsabilidades, delimitar ámbitos de incumbencia, y asignar recursos, lo que obstaculiza los procesos de desarrollo de capacidades.
Encontramos organismos de control y coordinación para coordinar acciones de protección y IICC de la Información tanto en la Jefatura de Gabinete como en el MINDEF.
En la medida que la Internet de los Objetos (IoT) es transversal a distintos sectores, y en que la distinción entre "infraestructura crítica" e "infraestructura crítica de información" se hace más impensable, las IICC de la nación "tradicionales" que se ven afectadas por problemas de seguridad recaen sobre la competencia de la DNC. Sin embargo, se adolece de mecanismos más claros de ejecución y coordinación en el área de *ciberseguridad*, y como si fuera poco, desde 2019 se introdujo al MINDEF en la cuestión.
De acuerdo con varios informantes clave, los mecanismos de cooperación y coordinación entre actores estatales afectados por la protección de la IICC de Información en este contexto socio-técnico crítico, marcado por la integración de los sistemas cíber-físicos, no se encuentra debidamente instaurado en la práctica.
Con todo, el ICIC-CERT parece estar dando pasos en dirección a una mayor capacidad institucional de coordinación estratégica, en tanto ahora depende de una Dirección Nacional en el ámbito de Jefatura de Gabinete. De la misma dirección depende a su vez la presidencia del Comité de Ciberseguridad, que (bajo otra administración), si bien el gobierno actual no lo ha reactivado ni ha dado señales de que quiera hacerlo.
Sin embargo, por ahora la Subsecretaría de Ciberdefensa cuenta con mayores recursos para desarrollar capacidades defensivas, a la vez que presenta una mayor continuidad en su trayectoria institucional que la DNC. Si bien no supone el desarrollo de capacidades técnicas endógenas, a nivel técnico, el SIEM Q-RADAR supone una solución integral que permite generar mapas de riesgos de forma automatizada, centralizar la información de sensores remotos y los CERTS de las fuerzas armadas, y generar nuevas evaluaciones de riesgo a partir de técnicas de *machine learning*.
En este sentido, puede decirse que se realizan evaluaciones de la gravedad de incidentes relacionados con activos de las IICC de interés para la Defensa; no así de que la planeación de la respuesta futura se basa en dicha evaluación.
Lo que es más importante, como ya se señaló, es que el diseño institucional de la relación entre la Subsecretaría de Ciberdefensa y la Dirección Nacional de Ciberseguridad no está claro.
No se encuentra evidencia de que se realice de forma regular una auditoría de los activos de la IICC, ni en MINDEF ni en JGM, ni de que la lista de prioridades de los activos se reevalúe regularmente para adaptarse a los cambios en el entorno de amenazas. Tampoco de que, si existe un registro de activos de la ICN, este cuente con la identificación y el mapeo de dependencias intersectoriales que aborden la continuidad de las operaciones y los mecanismos de recuperación de desastres; o de que existan mecanismos de coordinación intersectorial y transversal de partes interesadas para abordar interdependencias críticas, así como mecanismos entre el sector público y privado para la divulgación periódica de vulnerabilidades de la ICN de Información.
En materia de mecanismos de investigación orientados a identificar y analizar los principales riesgos de ciberseguridad de preocupación nacional, así como de mecanismos de intercambio de información fidedigna entre los organismos públicos, existen antecedentes aislados, pero no políticas sostenidas. El principal antecedente a nivel regional tuvo lugar en 2014, en el seno del MERCOSUR, cuando se creó la RAPRISIT, destinada a proponer políticas e iniciativas comunes en el área de la seguridad cibernética y la privacidad, y facultada para crear instancias de expertos para la discusión de aspectos técnicos relacionados con su mandato. Sin embargo, nunca se logró darle operatividad, y en 2019 fue absorbida por el SGT 1.
En términos de resiliencia hay una percepción de que existe un déficit en esta materia. El concepto apunta a minimizar el daño y retomar las operaciones en el menor tiempo posible. La OTAN es mencionado como referente para implementar esta estrategia. No hay mecanismos de investigación orientados a identificar y analizar las tendencias de incidentes de ciberseguridad de preocupación nacional.

Conclusiones

La evidencia señala que las políticas sobre ciberseguridad en Argentina están caracterizadas a la vez por dinámicas de innovación y de discontinuidad. En efecto, si hubiera que sintetizar en una frase el caso argentino, podríamos hablar de una trayectoria institucional pionera marcada por la discontinuidad en sus políticas. Como resultado, a pesar de contar con un CERT desde 1999, el país todavía se encuentra en sus etapas formativas en la mayoría de las dimensiones a considerar en materia de ciberseguridad; en especial, en materia de

protección de las infraestructuras críticas y respuestas a incidentes informáticos.

La baja institucionalidad es común a varios de los temas de la agenda del gobierno y no una circunstancia excepcional en materia de ciberseguridad. Si bien la discontinuidad de las políticas es un fenómeno multi-causal, un factor clave es que las innovaciones institucionales relativas a la gobernanza de la ciberseguridad tienden a identificarse con gestiones de gobierno antes que políticas de Estado que se sostienen y evolucionan en el tiempo. Ahora bien, se verifican discontinuidades dentro de un mismo periodo presidencial, una tendencia que se verifica en gobiernos de diverso signo político.

Otro elemento por destacar es que se halla evidencia de interesantes matices y contrastes en materia de los *senderos de desarrollo institucional* (atendiendo tanto las distribuciones de preferencias como las de capacidades) seguidos en los tres ámbitos de incumbencia estatal relevados.

En términos de capacidades, se verifica una mayor continuidad en las políticas con eje el ámbito de los delitos informáticos o "*ciberdelitos*" que en torno a la *ciberseguridad* y la *ciberdefensa*. A su vez, en términos de preferencias encontramos que a nivel estatal en general (y ya no en cada ámbito de incumbencia), se registra un enfoque de la gobernanza de la ciberseguridad más bien limitado a la tipificación penal de los delitos en el ciberespacio, donde el accionar estatal tiene lugar una vez vulnerados los derechos de los individuos, antes que uno extensivo a la prevención o la resiliencia. Asimismo, no se ha explorado una agenda de políticas de desarrollo asociadas al fomento de la seguridad por diseño como estándar industrial, el desarrollo nacional o federal de capacidades endógenas (como por ejemplo la formación de personal especializado en materia de ciberseguridad), el fomento de la investigación científica en tecnologías de análisis informático y encriptación, el establecimiento de incentivos para la emergencia de start-ups especializadas, el fomento de la industrialización de la seguridad informática de base nacional o el establecimiento de garantías para el ejercicio de actividades propias de la industria de la seguridad informática (como el uso de ingeniería inversa o el desarrollo de tecnologías de uso dual).

Por otra parte, se verifica una mayor discontinuidad en la trayectoria institucional en materia de *ciberseguridad* vis a vis en *ciberdefensa*, si bien el recorrido en relación a la primera se remonta a la creación de ARCERT en 1999, y la de la segunda se limita más bien al último lustro.

Esto puede explicarse porque está menos claro el rol asignado al ICIC-CERT, pues durante la última década este ha ido modificándose no solo en jerarquía sino también en objeto. A su vez, se ha desarrollado una línea de trabajo en torno a la definición conceptual, la institucionalización, y las prioridades para dar continuidad de operaciones de la infraestructura digital. Sin embargo, consideramos que los diseños institucionales que definen los roles, los ámbitos de incumbencia y las responsabilidades de los actores estatales en relación con la protección de las IICC, así como los canales de articulación entre ellos, se basan en caracterizaciones que dan lugar a ambigüedades.

El actor central en *ciberseguridad* es la Dirección Nacional de Ciberseguridad (DNC), un organismo de cuarto orden administrativo, con incumbencia nacional tanto para organismos estatales nacionales y provinciales, así como para empresas e individuos, pero con un equipo técnico reducido, sin recursos acordes a su función. A su vez, si bien cuenta con cierta capacidad formal de coordinación en virtud de la coordinación de la Unidad Ejecutora del Comité de Ciberseguridad y de su pertenencia a la órbita de la Jefatura de Gabinete, tiene cierta competencia interna por parte de las entidades gubernamentales (CERT dentro de la órbita del ministerio de seguridad, y CSIRT del MINDEF, orientado a la IICC para la Defensa). El organismo central en materia de *ciberdefensa* es la Subsecretaría de Ciberdefensa, con mayor jerarquía que la DNC, lo que dificulta la coordinación de iniciativas. En materia de *ciberdelitos*, finalmente, el liderazgo está distribuido entre el Ministerio de Justicia y Derechos Humanos, el Ministerio Público Fiscal y, de forma más reciente, por el Ministerio de Seguridad. Por otro lado, en materia de *ciberdelito* encontramos que han tenido un rol activo los tres poderes del Estado (Ejecutivo, Legislativo, Judicial), mientras que en materia de *ciberseguridad* y *ciberdefensa* este rol se ha limitado al Poder Ejecutivo.

Más allá de estos matices en términos de sendero de desarrollo institucional, un elemento destacable del caso argentino es que sus políticas exhiben un enfoque de la gobernanza de la ciberseguridad centrado casi exclusivamente en los gobiernos, un aspecto que se agudiza en el caso del ciberdelito y la ciberdefensa. Si bien varios de los organismos analizados han intentado construir redes multisectoriales, en los hechos han tenido un carácter declarativo, o más bien informal y con un mandato limitado a un objetivo específico.

A su vez, no se puede afirmar que exista una política en materia de intercambio de inteligencia/información entre los gobiernos y los sectores de la industria y demás operadores de redes informáticas en el país. De hecho, el ICIC-CERT no ha emitido ningún informe anual de incidentes, tal como está facultado a hacer desde 2013. Sin embargo, consideramos que el hecho de que cuatro de los seis CSIRTs más salientes del país sean miembros del foro FIRST es una muestra de que hay una búsqueda más colaborativa entre sectores para enfrentar el problema, aun cuando esto no emerge de los aspectos normativos de los CSIRTs gubernamentales, sino más bien en el marco de las buenas prácticas.

Diremos que aquellos intentos de crear redes multisectoriales, junto a esta trayectoria continuada en términos de participación en foros técnicos orientados a la construcción de confianza y buenas prácticas, nos permite complejizar la noción de un esquema gubernamental estricto en materia de gobernanza de la ciberseguridad.

Sobre esta base, y volviendo a la cuestión de la discontinuidad en las políticas públicas, consideramos que un avance tal vez no se trate tanto de desarrollar nuevos diseños institucionales como de impulsar decididamente procesos de consulta multisectorial abiertos y transparentes que resulten sostenibles en el tiempo, y que construyan la legitimidad necesaria para ser socialmente apropiados por las partes interesadas. En tal sentido, atentos a desarrollar mayores capacidades de coordinación estratégica e integración multisectorial, consideramos que los actores ubicados en la intersección entre los tres ámbitos de incumbencia (ver Figura 2) se presentan como los más indicados para motorizar el proceso, y acompañar a la DNC de la Jefatura de Gabinete en su liderazgo. Estos son: a nivel nacional, el Comité de Ciberseguridad, el Ministerio de Relaciones Exteriores (a través de la OCCAD), y ciertas comisiones legislativas de las dos cámaras del Poder Legislativo. A nivel federal, la Comisión de Infraestructura Tecnológica y Ciberseguridad del COFEFUP. Y a nivel regional, el GAD del MERCOSUR y, complementariamente, al SGT1 (Comunicaciones).

Otro elemento de interés es que los cambios en el signo político de los gobiernos no parecen modificar sustancialmente este esquema, si bien introducen dinámicas que pueden impactar sobre las políticas de ciberseguridad —como en materia de la autoridad de aplicación preferida, el grado de separación preferido entre seguridad interior y defensa, el rol asignado a empresas estatales como ARSAT, o la referencia en los discursos en torno a la autonomía vis a vis los centrados en la modernización.

Destacamos dos cuestiones donde se evidencian diferentes preferencias entre gobiernos de signo político. Por un lado, los gobiernos peronistas (2003-2007, 2007-2011, 2011-2015, 2019-2023)— han priorizado a la Jefatura de Gabinete como organismo rector de la ciberseguridad. El gobierno de Mauricio Macri (2015-2019), en cambio, procuró darle el liderazgo al Ministerio de Modernización. Diremos que estos debates responden a procesos de larga duración, que en Argentina se inscriben en tensiones históricas entre actores sociales con enfoques alternativos del desarrollo intensivo en conocimiento, así como del patrón de inserción internacional (Powers y Jablonski, 2016). Esto hoy se manifiesta en el rol asignado a la Jefatura de Gabinete vis a vis Ministerio de Modernización en la materia.

Una segunda distinción considerable es que los gobiernos peronistas han tendido a mantener una diferenciación más estricta entre *ciberdefensa* y *ciberseguridad*, si bien en tanto extensión de la separación entre seguridad interior y defensa. El gobierno de Macri, en cambio, incrementó las atribuciones y fortaleció las capacidades del Ministerio de Seguridad, primero, y de Defensa, después. Este asunto también se escribe en un debate de larga duración. El acuerdo entre las fuerzas políticas respecto a la no injerencia de las fuerzas armadas en cuestiones de seguridad interior es una de las bases del consenso que permitió el retorno al régimen democrático en los 80; sin embargo, persisten tensiones que, en la lógica bipartidista que rige en la Argentina, se han traducido en lecturas alternativas acerca del rol de las fuerzas armadas en un escenario global marcado por la emergencia del ciberespacio. En tal sentido, la reforma del sistema de Defensa en 2018 por parte de Macri (la cual dispuso que el uso del instrumento militar sería utilizado ante "agresiones de origen externo", fueran o no estatales) supuso un punto de controversia no resuelta, y era esperable que el asunto fuera revisado por un gobierno peronista. De hecho, la primera decisión institucional de peso de la Subsecretaría de Defensa durante el gobierno (peronista) de Alberto Fernández, en junio de 2020, fue precisamente derogar dos decretos clave de la gestión macrista —el que estableció una nueva Directiva de Política de Defensa Nacional (DPDN) y el que reformó el decreto reglamentario de la Ley de Defensa. Ahora bien, qué hará el gobierno de Fernández respecto a la participación de dicha cartera en la protección de las infraestructuras críticas (IICC) está menos claro. Por lo pronto, la Política Nacional de Ciberdefensa de 2019, publicada a semanas de finalizar el mandato de Macri, no ha sido derogada. Aquí cabe la cautela, entonces, puesto que los gobiernos peronistas hayan tendido a mantener una diferenciación más estricta entre *ciberdefensa* y *ciberseguridad* no necesariamente significa que seguirán fortaleciendo el rol de la Jefatura de Gabinete vis a vis Defensa en materia de Protección de las IICC, o al menos que esto sea tan fácil de llevar a la práctica.

Finalmente, en términos de *ciberdiplomacia*, si bien el país carece de una estrategia integral, y se registran ciertas diferencias en materia de influencias externas e instrumentos preferidos de cooperación internacional según el ámbito de incumbencia estatal, puede decirse que existen ciertas tendencias generales que han logrado sostenerse en el tiempo: alineamiento con el NIST, el FIRST, la OTAN, la ITU, la OEA; y a nivel bilateral, con Israel y Chile. La valoración de instituciones regionales ha sido más bien baja, salvo cierta coyuntura crítica (2011-2014, lo que condujo a la creación de la RAPRISIT en el MERCOSUR), y salvo excepciones

recientes, producto del trabajo incipiente en ciberseguridad del Grupo Agenda Digital del MERCOSUR.
En los ámbitos de *ciberdelitos* y *ciberseguridad*, los actores internacionales clave han sido la OEA y el Consejo de Europea, y de forma reciente, el *Open-Ended Working Group* de la ONU (OEWG). A su vez, cabe mencionar una serie de acuerdos de cooperación bilaterales, tanto con gobiernos (Israel, Estados Unidos, Chile) como con organizaciones técnicas (FIRST y NIST). Además, en *ciberdefensa* se destacan los acuerdos con Israel, que se tradujeron en la adquisición del SIEM Q-Radar, y la participación en plataformas de inteligencia contra amenazas (MISP y TAXII). En cuanto a la profundización del trabajo de Argentina en el OEWG de la ONU, plantea un interrogante: ¿Puede generarse una tensión entre los países que prefieran fortalecer el GGE vis a vis aquellos que prefieran fortalecer al OEWG? Si es así, ¿esto puede manifestarse a nivel regional, en especial, en la relación entre Brasil y Argentina?
El análisis de las dinámicas de la ciberdiplomacia también devela que en más de una oportunidad fue un evento externo lo que favoreció la creación de un sentido de urgencia favorable al desarrollo de preferencias homogéneas en distintos gobiernos. Sin embargo, en ninguno de los casos el impacto sería duradero. En 2014, la coyuntura crítica planteó su locus en el nivel sub-regional y se tradujo en la creación de la citada RAPRISIT en el MERCOSUR. En 2018, su locus estuvo en los "clubes" internacionales que organizaron sus cumbres en Argentina: fundamentalmente, la OMC y el G20. Esto deja en evidencia los límites de los procesos de maduración donde el vector aglutinante es un factor externo y la agenda es eminentemente reactiva. Por cierto, en sendos casos se encontraban en el poder gobiernos de signo político opuesto, por lo que no se trata de un problema de una sola fuerza política.
En esta línea, consideramos que puede decirse que la pandemia ha abierto una nueva coyuntura crítica, que marcará la trayectoria del gobierno de Alberto Fernández (2019-2023), así como de quienes lo sucedan. En cuanto a su gestión, solo cabe hacer especulaciones, pero se puede decir que ha dado diversas señales de que pretende modificar varios elementos señalados en este diagnóstico. Por ejemplo, mediante la creación de reuniones especializadas en el Consejo Federal de Políticas, en búsqueda de una mayor federalización de las políticas sobre ciberseguridad así como de un desarrollo más homogéneo de las capacidades a nivel subnacional; o mediante la idea de un "diseño conjunto del entorno de seguridad público", como alternativa superadora del enfoque limitado a la concientización ciudadana y el accionar de la justicia para restituir derechos ya vulnerados; o mediante el acuerdo entre el MINDEF y ARSAT (una señal hacia la recuperación y profundización de un sendero de desarrollo de capacidades endógenas en materia de comunicaciones) y la disminución de dependencia tecnológica con proveedores externos. No obstante, es demasiado pronto para saber si forman parte de un abordaje sistemático, y si finalmente se traducirán en políticas sostenibles y evolutivas sobre ciberseguridad.

Bibliografía utilizada

ABBOTT, Kenneth W., GREEN, Jessica F. y KEOHANE, Robert O. (2016) "Organizational Ecology and Institutional Change in Global Governance", en *International Organization*. Available on CJO 2016 doi:10.1017/S0020818315000338.

ABBOTT, Kenneth W., y SNIDAL, Duncan (2008), "Strengthening International Regulation Through "Transnational New Governance", en *Vanderbilt Journal of Transnational Law*, vol. 42: 501.

ACHARYA, A. (2004), How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism, International Organization, 58(2), 239-275. doi:10.1017/S0020818304582024.

AGUERRE, Carolina (2015). La gobernanza de Internet: Argentina y Brasil en el contexto global. Tesis para optar al título de Doctor en Ciencias Sociales. Facultad de Ciencias Sociales, Universidad de Buenos Aires.

AGUERRE, Carolina y GALPERIN, Hernán (2015), "Internet Policy Formation in Latin America: Understanding the Links Between the National, the Regional, and the Global", report for the Center of Technology and Society (CETYS-UDESA), Internet Policy Observatory and Center for Global Communication Studies. Disponible aquí.

BUSTOS, Gonzalo (2016), Inserción Estratégica Suramericana: alcances y límites de los intereses conjuntos en América del Sur (1985-2015), Eudeba, Buenos Aires.

BUSTOS, RIVERO, PALAZZI (2021), "Economía digital en América Latina: Informe sobre responsabilidad de intermediarios tecnológicos y disposiciones sobre comercio digital en la región", CETYS, BID, ALAI.

BARRINHA, A. y RENARD, T. (2017). "Cyber-diplomacy: the making of an international society in the digital age", Global Affairs, DOI: 10.1080/23340460.2017.1414924

BRADSHAW, Samantha (2015). "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity", Centre for International Governance Innovation and Chatham House, Paper Series 23.

CANABARRO, Diego and BORNE, Thiago, Reflections on the Fog of (Cyber)War (March 1, 2013). NCDG Policy Working Paper No. 13-001, Available at SSRN:

https://ssrn.com/abstract=3155453 or http://dx.doi.org/10.2139/ssrn.3155453

COLEMAN, Katheryn (2013). "Locating norm diplomacy: Venue change in international norm negotiations", en European Journal of International Relations, 19(1), 163–186.

DIEBERT, Donald y ROHZINSKI, Rafal (2011). "Contesting Cyberspace and the Coming Crisis of Authority", en Access Contested, pp.21-41. DOI: 10.7551/mitpress/9780262016780.003.0002

DREZNER, Daniel (2007) "The Global Governance of the Internet: Bringing the State Back In", Political Science Quarterly, Volume 119 Number 3, 2004.

DUNN CAVELTY, Myriam (2018), "Cybersecurity Research Meets Science and Technology Studies", Politics and Governance 2018, Volume 6, Issue 2, Pages 22–30. DOI: 10.17645/pag.v6i2.1385

FINNEMORE, Martha y HOLLIS, Duncan (2016), "Constructing Norms for Global Cybersecurity", en The American Journal of International Law, Vol. 110, No. 3 (July 2016). Disponible aquí.

FIORETOS, Orfeo (2002), "The Domestic Sources of Multilateral Preferences: Varieties of Capitalism in the European Community," in Varieties of Capitalism: The Institutional Foundations of Comparative Advantage, edited by Peter A. Hall and David Soskice. New York: Oxford University Press, 2001: 213-244.

JONG-CHEN, Jing de and O'BRIEN, Bobby (2017) "A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China", in Digital Futures Project, Wilson Center.

GOLDSMITH, Jack y Wu, Tim (2006), Who controls the Internet?, Oxford University Press.

HUREL, L. M. y LOBATO, L. (2018), "Unpacking Cybernorms: Private Companies as Norms Entrepreneurs" (January 22, 2018). GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017.

KIM, Sangbae (2014), "Cyber Security and Middle Power Diplomacy: A Network Perspective", in The Korean Journal of International Studies Vol.12 No. 2 (December 2014), 323-352. http://dx.doi.org/10.14731/kjis.2014.12.12.2.323

KEOHANE, Robert y NYE, Joseph (1989). Power and interdependence. New York: Harper Collins.

KERRY, Cameron (2016), "Bridging the internet-cyber gap: Digital policy lessons for the next administration", Brookings Report. Disponible aquí.

KRASNER, Stephen (1982), "Structural Causes and Regime Consequences: Regimes as Intervening Variables", en International Organization, Vol. 36, No. 2, International Regimes (Spring, 1982), pp. 185-205.

LESSIG, Lawrence. (1999). "The Limits in Open Code: Regulatory Standards and the Future of the Net", 14 Berkeley Tech. L.J. 759.

MORGUS, Robert, Isabel SKIERKA, Mirko HOHMANN, Tim MAURER (2015), "National CSIRTs and Their Role in Computer Security Incident Response", Global Public Policy Institute y New America.

MAURER, Tim y MORGUS, Robert (2014), "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate", CIGI, Internet Governance Papers, Paper N°7.

MAURER, Tim y MORGUS, Robert (2014a), "Compilation of Existing Cybersecurity and Information Security Related Definitions", New America.

NYE, Joseph S. (2014), "The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance", Paper Series, 1. Disponible aquí.

POWERS, S., JABLONSKY, M. (2015) The real cyber war: The Political Economy of Internet Freedom, University of Illinois, Urbana, Chicago, and Springfield.

PISANTY, Alejandro (en prensa). "Regímenes para la ciberseguridad", en Revista de Administración Pública, INAP México.

RIORDAN, Shaun (2019). Cyberdiplomacy: Managing Security and Governance Online. Cambridge: Polity Books.

ROSENAU, James, CZEMPIEL, E. (eds) (1992) Governance Without Government: Order and Change in World Politics. Cambridge University Press, Cambridge, UK.

SASSEN, Saskia (2010). Territorio, autoridad y derechos: De los ensamblajes medievales a los ensamblajes globales. Buenos Aires, Madrid: Katz.

SKOCPOL T, PIERSON P. (2002). "Historical Institutionalism in Contemporary Political Science". In: Katznelson I, Milner HV (editors). Political Science: State of the Discipline. New York: W.W. Norton.

STOKER, Gerry (1998), "Governance as theory: five propositions", en International Social Science Journal, Volume 50, Issue 155, March 1998, Pages 17-28. DOI: https://doi.org/10.1111/1468-2451.00106

THELEN, K. (2018). "Regulating Uber: The Politics of the Platform Economy in Europe and the United States". Perspectives on Politics, American Political Science Association. DOI:10.1017/S1537592718001081

CENTRO
LATAM
DIGITAL

Centro LATAM Digital
Centro de Política Digital para América Latina, A.C.
Ciudad de México, CDMX, México

@LATAMxDigital www.centrolatam.digital