Tipo de documento: Tesis de maestría

Escuela de Gobierno. *Maestría en Políticas Públicas*

Análisis de capacidades en ciberseguridad de la Administración Pública Nacional de la República Argentina a partir de un estudio de caso

Autoría: Gómez González, Sofía
Año: 2024

UNIVERSIDAD TORCUATO DI TELLA

ESCUELA DE GOBIERNO

MAESTRÍA EN POLÍTICAS PÚBLICAS

"Análisis de capacidades en ciberseguridad de la Administración Pública Nacional de la República Argentina a partir de un estudio de caso"

Alumna: Sofía Gómez González
Directora: María Patricia Prandini

Mayo de 2024

ÍNDICE

RESUMEN

A través de un estudio de caso, esta investigación tiene como objetivo identificar los factores institucionales que contribuyeron al incidente de ciberseguridad ocurrido en el mes de octubre del año 2021 en Argentina, en el cual se comprometieron datos alojados en el Sistema de Identidad Digital (SID). Mediante entrevistas a expertos de los distintos sectores que conforman el ecosistema de la ciberseguridad, se aborda un análisis de aspectos clave como el capital humano especializado en la órbita de la Administración Pública Nacional, la interoperabilidad entre sistemas de distintas dependencias ministeriales, los recursos tecnológicos disponibles y la gobernanza de la ciberseguridad.

Palabras clave: incidente de ciberseguridad, Administración Pública Nacional, capital humano, interoperabilidad, recursos tecnológicos, gobernanza de la ciberseguridad.

ABSTRACT

Through a case study, this research aims to identify the institutional factors that contributed to the cybersecurity incident that occurred in October 2021 in Argentina, during which data housed in the Digital Identity System (SID) was compromised. By conducting interviews with experts from various sectors within the cybersecurity ecosystem, the study analyzes key aspects such as specialized human capital within the National Public Administration, interoperability between systems across different ministerial departments, available technological resources, and cybersecurity governance.

Keywords: cybersecurity incident, National Public Administration, human capital, interoperability, technological resources, cybersecurity governance.

I. INTRODUCCIÓN:

La irrupción de las Tecnologías de la Información (TIC) ha implicado un cambio de paradigma (Castells, 2009), así como generado una creciente dependencia de los sistemas digitales. Este hecho ha transformado en gran medida el funcionamiento de las sociedades, impactando significativamente en los diferentes campos de la actividad humana y la vida cotidiana.

Evidencia de ello es el constante surgimiento de tecnologías nuevas y emergentes como la inteligencia artificial, la computación en la nube, el Internet de las cosas (IoT), la masificación en el uso de plataformas digitales y el desarrollo de 5G; los cuales han puesto de manifiesto numerosas potencialidades para mejorar la prestación de servicios en pos de elevar la calidad de vida de las personas y agregar valor en las organizaciones.

Estos cambios estructurales también han impactado en las administraciones gubernamentales, impulsando un proceso de transformación digital del Estado, que ha modificado las formas y mecanismos habituales de comunicación dentro de la Administración Pública y en su interacción con la ciudadanía. Al mismo tiempo, se han generado oportunidades para mejorar la eficiencia y eficacia de las políticas, así como para elevar la participación y el acceso de la ciudadanía a las prestaciones estatales.

Sin embargo, la intensificación en el uso de estas tecnologías también ha implicado la exposición de numerosa y valiosa información personal dentro del complejo entorno virtual, lo cual ha sido utilizado como una ventana de oportunidad para el perfeccionamiento de ilícitos en el espacio cibernético (Miró Linares, 2013). Así, se han incrementado los riesgos y amenazas con formas y conductas cada vez más sofisticadas que aprovechan las vulnerabilidades humanas y tecnológicas.

De acuerdo con datos de la Dirección Nacional de Ciberseguridad, en 2022 el Estado Nacional fue el segundo sector más afectado por incidentes de ciberseguridad[1], con un total de 71 ataques reportados por diversas entidades de la Administración Pública Nacional (en adelante, APN). En este contexto, el resguardo de la información bajo control o guarda de los organismos públicos, presenta severos desafíos (CERTar, 2023)

A través del presente trabajo se pretende comprender los factores institucionales que contribuyeron a la ocurrencia de un incidente de ciberseguridad de alto impacto, el cual resultó en el acceso no autorizado a un sistema de alcance nacional, que almacena información personal ciudadana.

Particularmente, se analizará como caso de estudio, el incidente de ciberseguridad ocurrido en octubre de 2021, por el que se vio comprometida información ciudadana resguardada por la Dirección Nacional del Registro Nacional de las Personas (en adelante, RENAPER), organismo descentralizado del Ministerio del Interior de la Nación, y producto del cual se filtraron documentos nacionales de identidad de ciudadanos de la República Argentina.

[1] Se aclara que, al día 15/5/2024, el informe correspondiente a la actividad sobre incidentes registrada en el año 2023 no ha sido publicado.

La relevancia del tema de investigación encuentra justificación en el impacto que tienen los incidentes de ciberseguridad, tanto en la vulneración de derechos fundamentales de los ciudadanos, como en los daños que ocasionan a los organismos y entidades que los sufren, en virtud de la repercusión económica, social y reputacional que traen aparejados.

II. SITUACIÓN PROBLEMÁTICA:

De acuerdo con cifras de la Encuesta Permanente de Hogares del Instituto Nacional de Estadística y Censos (INDEC), durante el cuarto trimestre de 2023 se evidencia que la población con acceso a internet asciende a 89,2%, lo que representa un incremento de casi 10 p.p. respecto del tercer trimestre de 2019, donde el acceso ascendía al 79,9%. Como puede observarse, el acceso a internet se ha incrementado significativamente en los últimos 4 años, y uno de los factores que posiblemente haya contribuido es la irrupción de la pandemia en 2020, la cual obligó a adoptar vertiginosamente el espacio cibernético para realizar actividades cotidianas como estudiar, trabajar e incluso esparcirse.

Consecuentemente, gran parte de las gestiones y trámites que en forma habitual se debían realizar de forma presencial viraron al espacio virtual, lo que significó en muchos casos, ahorros de tiempo y mayor eficiencia para la administración y la ciudadanía. Tal es así que la Plataforma de Trámites a Distancia (TAD), implementada en 2016 mediante Decreto N° 1063 de ese año con el objetivo de que la ciudadanía pueda realizar gestiones ante organismos de la APN, nuclea en la actualidad más de 2500 trámites y de acuerdo con las cifras oficiales -hasta abril de 2023-, 3.772.712 usuarios interactuaron en dicha plataforma para realizar gestiones.

En igual sentido, mediante el Decreto N° 87 del 2 de febrero de 2017 se creó la “Plataforma Digital del Sector Público Nacional”, la cual, según los argumentos que la motivaron, nació con el objetivo de “facilitar la interacción entre las personas y el Estado y unificar la estrategia de servicios y trámites en línea, brindando la posibilidad de realizar trámites a través de las distintas herramientas y servicios insertos en la plataforma, como consultas, solicitud de turnos, credenciales digitales y acceso a información mediante diversos canales”. Así es que se crearon tanto el portal web argentina.gob.ar, como la aplicación “Mi Argentina”, la que en febrero de 2019 contaba con aproximadamente 1.400.000 usuarios, y, tres años y medio después había aumentado casi doce veces la cantidad de personas registradas.

Una paradoja que acompaña la masividad del uso del entorno virtual es que, a mayor desarrollo, mayor es la vulnerabilidad. Ello así, en tanto a medida que una sociedad avanza y mayor es la cantidad de personas y organizaciones públicas y privadas que se conectan a las redes, mayores son los riesgos y desafíos que se presentan en términos de las vulnerabilidades a las que se exponen (Primera Estrategia Nacional de Ciberseguridad de la República Argentina, 2019).

Diversos estudios e informes públicos y privados evidencian que el crecimiento de la actividad en línea -profundizado en los últimos años tanto por factores exógenos al desarrollo tecnológico, particularmente por el aislamiento obligatorio a raíz de la pandemia, como por la rápida evolución de la inteligencia artificial, el internet de las cosas (IoT), blockchain, entre otros- potenciaron nuevas formas de delito y demostraron un crecimiento de la actividad ilegal en el ciberespacio.

Según un reporte de la empresa de seguridad informática Fortinet (Fortinet, 2023), América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022. De acuerdo con el Panorama de Amenazas en América Latina 2021 de la firma Kaspersky Lab, Argentina ocupa el tercer lugar de la región en lo que refiere al crecimiento de los ciberataques que explotan vulnerabilidades en las tecnologías de acceso remoto, con un crecimiento del 90% respecto al año anterior.

De acuerdo con el análisis de Propuesta de Préstamo efectuado por el Banco Interamericano de Desarrollo (BID) en el marco del programa de préstamo "Ciberseguridad para Infraestructuras Críticas de Información (ICI)" AR-L1343, uno de los principales problemas identificados en Argentina es el alto costo de los incidentes de ciberseguridad para el Estado y la ciudadanía. Tal como expresa el organismo:

> (...) el 81,7% de los incidentes procesados durante 2021 fueron de severidad alta o crítica, que tienen un costo 100 veces mayor que los de severidad baja. Países de la región como Uruguay no alcanzan el 2% en esta categoría. Esto se debe a la limitada capacidad del país para gestionar las funciones básicas de la ciberseguridad de las ICI.

En efecto, uno de los incidentes más relevantes y de estado público[2] que aconteció en el ámbito de la APN, tuvo lugar en el mes de octubre de 2021, cuando un usuario de la red social Twitter a través de la cuenta identificada como @aniballeaks, publicó las imágenes de los DNI de cuarenta y cuatro individuos, entre ellos funcionarios y personajes públicos de conocimiento general tales como el jugador argentino de fútbol Lionel Messi y el entonces presidente de la Nación, Alberto Fernández.

Dicha información obtenida ilegalmente, fue sustraída mediante el acceso al Sistema de Identidad Digital (en adelante, SID), una plataforma implementada por el Estado nacional en el año 2018 para validar la identidad a distancia y en tiempo real con la RENAPER, que provee de diversos servicios de validación de datos identitarios y biométricos a aquellas entidades privadas y públicas adheridas mediante convenio.

---

[2] "Preocupación por la venta online de los datos de los argentinos que tiene el Registro Nacional de las Personas", Diario La Nación 13/10/2021.
https://www.lanacion.com.ar/tecnologia/preocupacion-por-la-venta-de-los-datos-de-millones-de-argentinos-que-tiene-el-registro-nacional-de-nid13102021/
"La insoportable inseguridad de nuestros datos", Agencia de Noticias Ciencias de la Comunicación UBA 10/11/2021 https://anccom.sociales.uba.ar/2021/11/10/la-insoportable-inseguridad-del-dato/

Constituido como un repositorio de información ciudadana, el SID se conecta con otros sistemas de gobierno para facilitar transversalmente el confronte de información permitiendo confirmar a quien consulta, la autenticidad y vigencia de documentos nacionales de identidad, así como verificar la identidad por medio de imágenes de huellas digitales o fotografías de rostros.

A través de este sistema, el RENAPER implementó entre 2019 y 2023, 371 servicios de validación de datos y de identidad con organizaciones públicas y privadas, entre las que se encuentran distintos ministerios nacionales y los Poderes Legislativos y Judicial así como por instituciones bancarias y billeteras virtuales (RENAPER, 2023). Con la pandemia, y la acentuada necesidad de verificar la identidad a distancia, se extendió su uso, siendo implementado incluso por universidades para acreditar la identidad de alumnos al momento de evaluarlos (La Nación, 2021).

De acuerdo con un comunicado oficial del RENAPER, publicado el miércoles 13 de octubre de 2021, días después de identificarse el incidente, el organismo expresaba haber formulado una denuncia penal tras detectar que:

> (...) mediante el uso de claves otorgadas a organismos públicos, en este caso el Ministerio de Salud, se filtraron imágenes como pertenecientes a trámites personales realizados en el Renaper. Desde el organismo dependiente del Ministerio del Interior se confirmó que se trató de un uso indebido de usuario o robo de la clave del mismo, y que la base de datos no sufrió vulneración o filtración alguna de datos.

La información sustraída constó de imágenes completas de los documentos nacionales de identidad, exponiendo todos los datos personales de los titulares exhibidos en el frente y reverso del mismo. Entre ellos, se encontraba el número de trámite contenido en el margen inferior frontal de los D.N.I. Este episodio afectó directamente a las personas expuestas, permitiendo conocer datos que facilitan otros delitos como el robo o la suplantación de identidad. Si bien en la cuenta de la red social Twitter se publicaron 44 archivos, diversos medios de prensa[3] publicaron imágenes que evidencian el ofrecimiento de la base completa de documentos nacionales de identidad de la República Argentina. A mayor abundamiento, en el Anexo I se adjunta una captura de dicho ofrecimiento en la *deep web*. En la publicación el oferente de la base de datos anunciaba:

> Vendo todos los datos del documento nacional de identidad de cualquier persona en Argentina. Esto incluye foto, nombres, apellidos, domicilios, número de trámite (esto es muy importante), código de

[3] "Si sos argentino, tus datos personales tal vez se estén vendiendo en la deep web", Portal CriptoNoticias, 20/10/21 https://www.criptonoticias.com/seguridad-bitcoin/sos-argentino-datos-personales-tal-vez-vendiendo-deep-web/#google_vignette
"El robo del siglo: una reveladora entrevista a [S], el enigmático e "indetectable" hacker del Renaper", Diario Rosario 3, 27/10/21
https://www.rosario3.com/tecnologia/El-robo-del-siglo-una-reveladora-entrevista-a-S-el-enigmatico-e-indetectable-hacker-del-Renaper-20211027-0050.html

barras calculado por un algoritmo y todos los datos necesarios para crear un documento de identidad falso.

A través de esta investigación se pretenderá analizar y comprender los factores que dieron lugar a la existencia de un incidente de ciberseguridad por el cual se vio comprometida información ciudadana alojada en el SID.

III. PREGUNTA DE INVESTIGACIÓN Y OBJETIVOS.

Pregunta de investigación:

¿Qué factores institucionales contribuyeron a la ocurrencia del incidente de ciberseguridad que comprometió información ciudadana alojada en el Sistema de Identidad Digital (SID), en octubre de 2021?

Objetivo general:

Describir y analizar los factores institucionales que contribuyeron a la filtración de información ciudadana alojada en el Sistema de Identidad Digital (SID) en el mes de octubre de 2021.

Objetivos específicos:

-Examinar el marco normativo que propicia medidas de seguridad de la información para los organismos de la Administración Pública Nacional hasta el año 2023.

- Analizar los factores que contribuyeron a la filtración de información, desde la percepción de los actores involucrados en el ecosistema de la ciberseguridad.

IV. METODOLOGÍA:

Para abordar esta investigación se utilizó una metodología cualitativa, específicamente se optó por la realización de un estudio de caso. Como señala Stake, esta aproximación ofrece la oportunidad de obtener descripciones detalladas e interpretaciones profundas proporcionadas por diferentes actores involucrados en el caso estudiado (Stake, 1999).

Para desarrollarlo se recopilaron fuentes primarias y secundarias de información. En el ámbito de las fuentes primarias, se ha recurrido a informes y documentos oficiales provenientes de organismos tanto nacionales como internacionales. Además, se ha implementado la estrategia de entrevistas con informantes clave, seleccionados estratégicamente, con el propósito de profundizar en la comprensión de los factores que incidieron en la génesis del incidente objeto de análisis. En cuanto a las fuentes secundarias, se ha llevado a cabo un exhaustivo análisis de la literatura académica,

informes de expertos y otros recursos que proporcionan una perspectiva secundaria pero contextualmente enriquecedora sobre el tema en cuestión, buscando fortalecer la robustez y amplitud del marco de investigación.

De acuerdo con Dexter (1970), las entrevistas en profundidad se engloban dentro del conjunto de entrevistas de investigación, las cuales pueden a su vez, ser clasificadas entre: 1) Entrevista focalizada. 2) Entrevista estandarizada no programada, entrevista no estandarizada 3) Entrevista especializada y a elites. 4) Entrevista biográfica; intensiva; individual abierta semidirectiva; larga; etc. (Valles, 2007 p.26)

De esta clasificación, nos detendremos en la entrevista especializada y a elites, la cual ha sido descripta por Dexter (1970) como:

> una entrevista con cualquier entrevistado (...) a quien de acuerdo con los propósitos del investigador se le da un tratamiento especial, no estandarizado. Por tratamiento especial, no estandarizado quiero decir:
> 1. enfatizando la definición de la situación por el entrevistado,
> 2. animando al entrevistado a estructurar el relato de la situación,
> 3. permitiendo que el entrevistado introduzca en medida considerable (...) sus nociones de lo que considera relevante, en lugar de depender de las nociones del investigador sobre relevancia.

Ahondando en la explicación de este tipo de entrevista, Valles (2007) indica que no se trata de aquellas hechas únicamente a élites de la política, las finanzas o las profesiones de prestigio sino más bien, de un estilo o tratamiento de entrevista que recomienda utilizar un entrevistado "experto" o "bien informado" (en sentido llano).

En resumen, la elección de este caso y la metodología cualitativa aplicada buscan desentrañar los factores que contribuyeron al incidente explorando dimensiones técnicas, normativas y de gestión. A través de entrevistas especializadas y en profundidad, se pretende obtener una comprensión robusta y contextualizada del caso, con el objetivo de responder así la pregunta de investigación: ¿Qué factores institucionales contribuyeron a la ocurrencia del incidente de ciberseguridad que comprometió información ciudadana alojada en el Sistema de Identidad Digital (SID), en octubre de 2021?

A efectos de tener una mirada omnicomprensiva y representativa de los factores que coadyuvaron a la concreción de dicho incidente, se efectuaron entrevistas de tipo semiestructurada a los distintos actores que intervienen en el ecosistema de la ciberseguridad.

Para ello, se identificaron expertos y expertas del sector público (con énfasis en los organismos públicos involucrados en el incidente), así como del sector privado, de la sociedad civil, de un organismo internacional y del sector académico, según se detalla a continuación:

Informante Clave N° 1, empleado del Centro Nacional de Respuestas ante Emergencias Informáticas (CERTar)

Informante Clave N° 2, directiva de la Fundación Vía Libre.

Informante Clave N° 3, responsable del área de Tecnologías de la Información en el Ministerio de Salud de la Nación, al momento del incidente.

Informante Clave N° 4, socio del área de Ciberseguridad y Responsable de la práctica de Cyber Incident Response en la empresa Deloitte, al momento del incidente.

Informante Clave N° 5 - Docente e investigadora en ciberseguridad y seguridad de la información, y directiva del Programa Seguridad en TIC en la Fundación Sadosky.

Informante Clave N° 6 Informante clave N° 6 - Especialista en Ciberseguridad en el Banco Interamericano de Desarrollo (BID).

Informante Clave N° 7 Empleado del Registro Nacional de las Personas (RENAPER) al momento del incidente.

Finalmente, y en virtud de la petición explícita de algunos de los informantes, cabe mencionar que las entrevistas desarrolladas en esta investigación fueron anonimizadas, circunstancia que coadyuva al objetivo preponderante de contar con la visión más honesta y cabal de los hechos y antecedentes bajo análisis.

Preguntas:

- ¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente de ciberseguridad por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?
- ¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?
- ¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?
- ¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?
- ¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?
- ¿Consideras que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?
- ¿Deseas agregar algo que no se haya preguntado?

IV.1 SELECCIÓN DEL CASO.

El incidente de ciberseguridad que ocurrió en octubre de 2021 y comprometió la información ciudadana alojada en el Sistema de Identidad Digital (SID) se destaca como un caso de relevancia significativa. Su difusión pública generó un debate en diversos medios y entre distintos actores sobre la necesidad de elevar las medidas de protección de los activos de información del Estado. Este incidente adquiere una relevancia aún mayor por su coincidencia con el contexto post-pandemia, momento en el cual la APN enfrenta nuevos desafíos debido al trasvase masivo de operaciones, trámites y contactos presenciales hacia el entorno digital.

El caso se seleccionó también por la gravedad de sus implicancias. La información filtrada y comercializada permitía la construcción de perfiles ciudadanos, lo que ponía en riesgo no solo los derechos patrimoniales, sino también aspectos fundamentales como la privacidad y seguridad de las personas.

Una faceta adicionalmente interesante del caso es su impacto en el esquema de interoperabilidad de la información entre organismos públicos. Como se analizará más adelante, este incidente motivó una transformación en el enfoque del RENAPER respecto a la forma en que comparte datos con otras entidades gubernamentales.

V. DESARROLLO

V1. LOS DESAFÍOS DEL CIBERESPACIO

En la actualidad, la información conforma uno de los activos más relevantes que existen, a tal punto que como afirmó el matemático Clive Humby en 2006, los datos son el petróleo del nuevo siglo. Esta aseveración está estrechamente vinculada con el estrepitoso avance del desarrollo tecnológico que, desde el surgimiento de internet en 1958 a esta parte, ha recreado en la virtualidad un nuevo entorno de existencia, el ciberespacio. Es así que el trasvase operacional entre el mundo físico y el ciberespacio ha convertido a las personas, empresas y organismos en usuarios de las cibertecnologías (Arroyo Guardeño, et al. 2020).

En esa lógica, el ciberespacio y su penetración en las distintas esferas de la cotidianeidad, han puesto en el centro del debate el papel que ocupan los datos, quiénes los poseen, qué tipo de uso le dan y cómo se los protege. Estos interrogantes atraviesan de forma transversal a todos los actores sociales y políticos que, interceptados por la extensiva virtualidad, han debido ajustarse de forma vertiginosa a nuevos mecanismos y demandas. Tal como expresan Díaz, M., & Núñez, R (2023), el aumento alarmante de incidentes que amenazan la confidencialidad, integridad y disponibilidad de estos datos ha suscitado la necesidad imperante de alinear el comportamiento de los actores con las exigencias de proteger la información y salvaguardar derechos fundamentales, como la privacidad.

Como puede verse a esta parte, el concepto de datos como recurso esencial para el desarrollo que motoriza la transformación digital, se entiende en la dicotomía entre ser el "combustible" que

impulsa nuestro mundo y, simultáneamente, el elemento que revela nuestra privacidad, ya sea por colaboración consciente o sin consentimiento explícito (Canals Ametller, 2021).

En la esfera pública, la respuesta a estos interrogantes resulta de vital importancia porque el ciberespacio plantea desafíos significativos al Estado democrático de derecho. Canals Ametller (2021) destaca la inestabilidad de las instituciones frente a las peculiaridades del espacio digital y la imperante necesidad de que tanto las libertades públicas como los derechos fundamentales, y a su vez las instituciones que los garantizan, se adapten al ciberespacio y a los riesgos que éste presenta para su ejercicio.

V2. CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA: CLARIFICACIÓN DE CONCEPTOS.

Términos como "ciberseguridad", "seguridad de la información" y “seguridad informática” pueden plantear límites difusos en tanto plantean escenarios conceptuales que poseen interdependencia y similitudes, no obstante es posible determinar algunos de sus alcances (Frati, G. B., & Aguerre, C., 2022).

El área de seguridad informática es aquella encargada de la protección de las infraestructuras tecnológicas y demás activos de información, incluyendo los propios datos, que soportan el conjunto de actividades que lleva adelante una organización. La seguridad informática es una disciplina técnica que contempla las medidas de seguridad aplicadas en el ámbito de la tecnología informática y de telecomunicaciones, ya sea el desarrollo de sistemas de información, los protocolos de comunicación, aplicaciones móviles, las infraestructuras, las bases de datos, la virtualización, las “nubes”, las redes, los dispositivos que incluyen un circuito integrado, etc. De manera genérica, comprende la seguridad del software, del hardware, de las redes y de sus interacciones.

Por su parte, la seguridad de la información puede ser entendida como el conjunto de prácticas destinadas a preservar la integridad, la disponibilidad y la confidencialidad de la información con independencia de su soporte y desde el punto de vista de procesos (Pallero & Heguiabehere, 2022). La visión de la seguridad de la información se integra a las distintas funciones de una organización para incluir las prácticas recomendadas, tanto en los procesos de la organización como en sus servicios. Cabe mencionar que la seguridad de la información se refiere a un proceso y no necesariamente a un producto en sí mismo.

De tal forma, la gestión de la seguridad de la información dentro de una organización incluye el diseño e implementación de planes de prevención desde los distintos procesos (clasificación de la información, gestión de accesos, de vulnerabilidades y amenazas, evaluación de riesgos, etc.) que se relacionan dentro de la organización, así como la gestión de los recursos necesarios para dichas actividades, y la consideración de un análisis de riesgos que permita balancear objetivos de seguridad con recursos disponibles y la exposición a las amenazas con mayor probabilidad de afectar a la

organización (Pallero & Heguiabehere, 2022).

En lo que respecta a la ciberseguridad, si bien aún no se ha arribado a una fórmula de consenso internacional, como concepto ha sido abordado en distintos instrumentos y marcos de organismos ampliamente reconocidos tales como el NIST[4], ISO[5] o UIT[6] los cuales en muchos casos conforman un marco de referencia para la legislación interna de los países.

La UIT, entidad especializada de la ONU para las tecnologías de la información, definió la ciberseguridad en la Recomendación UIT-T X.12052 aprobada mediante Resolución 1813, como el

"(...)conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios **en el ciberentorno** (...)*"* (el resaltado me pertenece).

De acuerdo con la norma ISO/IEC 27100 en el año 2020, la ciberseguridad importa la defensa de protección de las personas, la sociedad, las organizaciones y las naciones frente a los ciberriesgos, teniendo por principal objetivo, reducir los riesgos cibernéticos a un nivel tolerable.

En lo que respecta a la legislación local, a través de la Resolución 1523 de fecha 12 de septiembre de 2019 de la Jefatura de Gabinete de Ministros, se aprobó el Glosario de Términos de Ciberseguridad, definiendo a la ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad -principios comúnmente encuadrados como la triada CID- de la información en el ciberespacio, de acuerdo con los parámetros establecidos en la norma ISO/IEC 27032 del año 2012.

Por su parte, la Segunda Estrategia Nacional de Ciberseguridad aprobada mediante Resolución N° 44/2023 de la ex Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros, entiende a la ciberseguridad como el conjunto de políticas y acciones orientadas a elevar los niveles de seguridad de las infraestructuras de las TIC, que podrían, según el caso, ser potencialmente vulnerables ante amenazas y/o incidentes, teniendo como principal objetivo, prevenir acciones que afecten a la administración del Estado, a las organizaciones, a los servicios esenciales y, en consecuencia, a las personas.

Dicho esto, podemos afirmar que la seguridad de la información es un ámbito más amplio que abarca todas las medidas para proteger tanto la información como los activos que la respaldan (esto incluye todas las medidas de resguardo físicas, tanto de las personas como de los propios servidores

[4] El Instituto Nacional de Estándares y Tecnología de (NIST, por sus siglas en inglés) es un organismo dependiente del Departamento de Comercio de los Estados Unidos, el cual se dedica al desarrollo de normas, directrices, marcos y mejores prácticas en materia de ciberseguridad.

[5] La Organización Internacional de Normalización (ISO, por sus siglas en inglés) en materia de ciberseguridad ha establecido dos directrices: ISO 27001 y 27002. A través de la primera se establecen los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), mientras que la segunda ofrece directrices para el establecimiento de medidas de seguridad efectivas.

[6] La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

donde se aloja la información, entre otros). En cambio, la ciberseguridad se centra específicamente en proteger esta información en el ciberespacio, sin considerar el entorno físico asociado.

V. 3 SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

El marco de protección de datos personales que en Argentina descansa en la Ley N° 25.326, consagra a través de su artículo 9° el principio de seguridad de los datos. Según este precepto, los responsables del tratamiento de datos personales deben implementar medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de dichos datos. En congruencia con esto, la Agencia de Acceso a la Información Pública, en su calidad de Autoridad de Aplicación de la mencionada ley, ha emitido la Resolución N° 47/2018, la cual ofrece pautas específicas para administrar, planificar, controlar y mejorar la seguridad en el procesamiento de datos personales. Esta resolución fomenta la adopción de medidas que anticipen los posibles riesgos a los que podría estar expuesta la información, al tiempo que promueve la transparencia en las acciones emprendidas para proteger los datos personales.

Por su parte, y como se verá en profundidad en el apartado V.8 Análisis Normativo, la Resolución N° 641/2021 establece una política de seguridad de activos de información la cual instaura una serie de pautas y requisitos mínimos de seguridad de la información con que deben contar los organismos de la APN. Algo interesante de este marco normativo, es que parte del supuesto de que todos los agentes públicos tienen la obligación de manejar y utilizar los datos de manera segura y responsable, tanto dentro como fuera del entorno institucional. Asimismo, subraya la necesidad de proteger los datos, ya sea que estén en formato físico o digital, durante su tratamiento, almacenamiento o transmisión.

Esta intersección entre las políticas de seguridad de la información y la protección de datos personales refleja la importancia de salvaguardar la privacidad de los mismos en tanto activos críticos de una organización. Asimismo, este enfoque conjunto se ve respaldado por normas técnicas como ISO 27002:2022, que define la evaluación de impacto en la privacidad como un componente integral de la gestión de riesgos de una organización.

Tal como explican Pallero y Heguiabehere, la gestión del riesgo y de la seguridad de la información se fundamenta tanto en la identificación de los procesos, el software, el hardware y las actividades de las personas, como en la identificación y clasificación misma del dato o la información. En este sentido, la gestión de la seguridad de la información, desde el análisis del riesgo, la gestión de las tecnologías y la protección de datos, son áreas y funciones de trabajo que las organizaciones deberían ver en su conjunto. Por lo tanto, en la implementación de servicios a través de sistemas de información o aplicaciones que involucren el tratamiento de datos personales, se vuelve esencial la consideración tanto de los aspectos tecnológicos como a los relacionados con la seguridad, protección y la privacidad de la información (Pallero & Heguiabehere, 2022).

V.4 CIBERDELITOS Y PANDEMIA

Para prevenir actos que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, el derecho penal se ha enfocado en tipificar estos delitos y establecer mecanismos para su identificación. A nivel internacional, el Convenio de Budapest sobre la Ciberdelincuencia se creó con el objetivo de proteger derechos fundamentales como la protección de datos y la privacidad en el ciberespacio, instando a los países signatarios a incorporar delitos como el acceso deliberado e ilegítimo a sistemas informáticos.

En el ámbito local, la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)[7], ha definido a la ciberdelincuencia como un fenómeno criminal que abarca tanto los ataques a los sistemas informáticos -por ejemplo, casos de accesos ilegítimos o de destrucción de información- como aquellos supuestos en los que se utilizan esos sistemas como medio para cometer otros delitos -como los fraudes a través de internet- (UFECI, 2021).

La tipificación de delitos informáticos en nuestro ordenamiento jurídico se encuentra receptada en el Código Penal a partir del año 2008, con la sanción de la Ley N° 26.388 (promulgada de hecho el 24 de junio de 2008). Esta norma tiene relevancia en la introducción de modificaciones al delito de daño en dos aspectos fundamentales: por un lado, introdujo el daño a bienes intangibles -previo a la reforma sólo se consideraba el daño de bienes tangibles-, tales como el borrado de software o de datos contenidos en un ordenador, y a su vez, incluyó como delito en particular la distribución de programas destinados a causar daños -i.e. virus informáticos- (Palazzi, 2016).

No obstante ello, doctrinarios como Palazzi (2016) afirman que la Ley N° 26.388 no introdujo una reforma omnicomprensiva del Código Penal en tanto muchos de los nuevos delitos que requieren una respuesta, a veces de fondo y otras en términos procesales, no tuvieron una clara recepción en el ordenamiento jurídico. Una de esas faltas tiene que ver con el delito de robo de identidad. Tal como explica el doctrinario, si bien la jurisprudencia exhibe que esta figura termina siendo configurada dentro de tipos penales como la estafa o defraudación, las cuales no permiten dar solución acorde a prácticas cada vez más sofisticadas y de mayor alcance como el robo de identidad y claves en forma masiva.

¿La pandemia contribuyó a la existencia de una mayor cantidad de delitos? Tal como se expresó al principio de este trabajo, el desplazamiento de actividades típicamente presenciales a la virtualidad, evidenció un crecimiento de usuarios en línea. Una revisión de la literatura -aún en proceso de crecimiento considerando lo reciente del suceso histórico que implicó la pandemia- muestra cierta divergencia en relación al impacto que tuvo este fenómeno.

[7] Esta Unidad, creada en 2015 mediante resolución P.G.N. n° 3743/20151 en el ámbito del Ministerio Público Fiscal, posee facultades para investigar ciberdelitos y tiene entre sus objetivos fortalecer la política criminal contra el cibercrimen, intensificar las tareas para su abordaje de modo articulado y atender a sus especificidades.

El estudio de Hawdon, Parti y Dearden (2020) titulado *"Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment",* consistió en recolectar información antes y después del COVID (noviembre de 2019 y abril de 2020) con la expectativa de medir niveles de cibervictimización en función de haber experimentado o no, algunos de los siete delitos indagados[8]. De acuerdo con los resultados del estudio, no se evidenciaron diferencias estadísticamente significativas antes y después en ninguno de los delitos y más aún, el delito de robo de datos mostró una mayor tasa de victimización antes de la pandemia.

Otras investigaciones sobre el impacto del COVID-19 en la cibercriminalidad como la abordada por Miró Linares (2021), exhibe que en dicho periodo ha existido un desplazamiento en las oportunidades de delito al ciberespacio fruto del mayor tiempo y más actividades realizadas en internet. A través del relevamiento de distintas mediciones efectuadas por empresas y organismos públicos[9], el autor concluye en: (i) la existencia de un aumento de ciertos ciberdelitos (ii) el desplazamiento dentro del ciberespacio hacia ciertas formas delictuales -como el phishing para suplantación de identidad- (iii) una aceleración y exageración de tendencias preexistentes.

En el ámbito local, los datos provistos por la UFECI muestran que en el periodo comprendido durante los doce meses anteriores a la pandemia -04/2019 al 03/2020-, se recibieron un total de 2.581 denuncias-. Sin embargo, al analizar los doce meses posteriores -04/2020 al 03/2021- en esa cifra se incrementó en más de un 460%, ascendiendo a 14.583 de reportes recibidos.

Estas cifras parecen condecirse con las exhibidas en otros Estados. Ejemplo de ello lo conforman las estadísticas del Internet Crime Complaint Center del Federal Bureau of Investigation (FBI) de los Estados Unidos donde al observar la evolución 2016-2020[10] de los casos presentados ante esa oficina, puede notarse que hasta el 2019 el crecimiento era bajo (en promedio un 13%). Sin embargo, entre el 2019 y el 2020, los casos recibidos ascendieron más de un 40%. Estas cifras muestran que gran parte de los delitos que crecieron -sea por desplazamiento de otras formas delictuales o por la oportunidad de otros nuevos a raíz en el trasvase a la virtualidad- tienen que ver con fraudes y estafas, muchos de ellos asociados al phishing.

V. 5 ALCANCES Y DELIMITACIÓN DE LA INVESTIGACIÓN

El caso de filtración de información objeto de estudio en esta investigación puede ser

[8] Las encuestas se realizaron entre el 24 y 30 de noviembre de 2019 y luego, entre el 14 y 17 de abril. Participaron 1109 encuestados en el primer año y 1021 en 2020. Antes y después del COVID19, se les consultó si fueron víctimas de: (1) pérdida de dinero por estafas informáticas, (2) suplantación de identidad para apertura de cuentas; (3) presencia de transacciones bancarias desconocidas; (4) recepción de notificaciones de una empresa u organización de que su información privada, como nombre, seguridad social tarjeta de crédito o contraseña, ha sido robada o publicada públicamente, (5) comentarios hirientes, fotos o vídeos hirientes sobre ti publicados en Internet; (6) comentarios o insinuaciones sexuales no deseados; (7) virus informático que afectó al funcionamiento de dispositivos como computadora.

[9] Dentro del estudio se consideran distintas fuentes de información como informes de transparencia de Google, informes de empresas reconocidas en el sector como Kaspersky y Mimecast y también datos provistos por el Centro Nacional de Denuncias de Fraude y Delitos Cibernéticos del Reino Unido y la Oficina Europea de Policía, entre otros.

[10] De acuerdo con cifras del organismo en relación al número de casos presentados ante esa oficina: durante el año 2016 ascendió a 298.728, en el año 2017 a 301.580, en el año 2018 a 351.937, en el año 2019 a 467.361 y, ya para el año 2020, los casos ascendieron a 791.790.

analizado desde perspectivas diferentes pero al fin complementarias, como lo es el enfoque punitivo, o la óptica de los principios generales relativos a la protección y tutela de los datos personales en el marco de la referida Ley N° 25.326 de Protección de Datos Personales; representando cada una de ellas, distintas caras de un mismo hecho. Sin embargo, esta investigación busca comprender los factores que contribuyeron a la ocurrencia del incidente bajo estudio, desde la perspectiva de la ciberseguridad que, como objeto de política pública, se encuentra atravesada por diversas dimensiones del aparato estatal (Frati, G. B., & Aguerre, C., 2022).

V. 6 ECOSISTEMA DE LA CIBERSEGURIDAD

De acuerdo con la OEA, la definición de un modelo de gobernanza de ciberseguridad adecuado para un país inicia con la identificación de los actores que conforman el ecosistema de dicho Estado y su correspondiente clasificación. Una vez identificadas las partes interesadas, debe definirse cuál es la función que desempeña cada uno de estos actores en el ecosistema de ciberseguridad, sus responsabilidades particulares y sus expectativas (OEA, 2023). Como puede verse, la formulación de una política pública en ciberseguridad no sólo involucra al sector público. El sector privado, dueño de la mayor cantidad de infraestructura crítica asociada al ciberespacio, representa un actor crítico en este tipo de políticas.

A su vez, la academia y la sociedad civil son sectores esenciales en tanto conforman un entorno crucial para el florecimiento de la cultura e industria de la tecnología y la innovación, a través del desarrollo de conocimientos e investigación. Los organismos internacionales, por su parte, constituyen un canal de influencia en la formulación de políticas, consenso internacional y cooperación financiera. Ejemplo de esto es el contrato de préstamo BID 5735/OC-AR[11] mencionado precedentemente y celebrado entre la República Argentina y el BID para el financiamiento del "Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI)".

Muestra de la importancia de incluir diversas voces en la formulación de políticas públicas en ciberseguridad se evidencia en el proceso consultivo llevado a cabo durante la aprobación de la Segunda Estrategia Nacional de Ciberseguridad. En este proceso, representantes de todos los sectores del ecosistema realizaron aportes y sugerencias, muchas de las cuales fueron incorporadas en el texto final de lo que hoy conforma el documento estratégico más importante de Argentina en materia de ciberseguridad.

[11] Aprobación del Contrato de Préstamo efectuada mediante Decreto N° 284/2023: https://www.boletinoficial.gob.ar/detalleAviso/primera/287208/20230529

V7. ANÁLISIS NORMATIVO

Para analizar el conjunto de normas que propicia medidas de seguridad de la información para los organismos de la Administración Pública Nacional, se ha examinado el marco teórico y se han recogido los principales hallazgos del estudio efectuado por el Dr. Carlos Galán (2022) en su "Análisis del marco jurídico y de gobernanza de la ciberseguridad para la protección de las Infraestructuras Críticas en Argentina". Esta elección obedece a que, a través de su investigación, el autor ofrece un exhaustivo análisis de las normas que regulan la seguridad de la información en el ámbito de la APN, presentando una valoración sistematizada de cada una de ellas. A su vez, justifica su relevancia en este ámbito el hecho de que dicho análisis haya sido una de las piezas fundamentales para la aprobación de una inversión de US$30 millones por el BID en el marco del programa más relevante de financiamiento en materia de ciberseguridad en la APN. Por ello, a través del presente trabajo se buscará revisar y ponderar críticamente las valoraciones efectuadas por el autor, así como examinar la evolución de las mismas desde la fecha en que se presentó dicho informe -junio de 2022-, hasta el mes de diciembre de 2023.

Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)

El Programa Nacional ICIC fue creado mediante **Resolución N° 580/2011** del Jefe de Gabinete de Ministros con el objetivo central de elaborar un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del país.

En su artículo 3° la norma enuncia dieciocho objetivos específicos vinculados principalmente al desarrollo normativo de la ciberseguridad y la protección de infraestructuras críticas de información; el fortalecimiento de la investigación en esta materia; la articulación con todos los sectores del ecosistema de la ciberseguridad para la protección de dichas infraestructuras; el fortalecimiento de la gestión de incidentes de seguridad y de vulnerabilidades; y la incorporación de nuevas herramientas y la asistencia a organismos públicos, incluyendo la coordinación de actividades; la realización de ciberejercicios y la promoción de la concientización sobre los riesgos que acarrea el uso de medios digitales.

En junio de 2015, el gobierno nacional creó la Subsecretaría de Protección de Infraestructuras Críticas de Información y Seguridad en el ámbito de la Secretaría de Gabinete de Jefatura de Gabinete de Ministros, transfiriendo el Programa Nacional ICIC a la órbita de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad. Un reporte efectuado por la OEA y la empresa Trend Micro en 2015, reconoció el avance que tuvo el país a partir de la creación del Programa Nacional de ICIC, pero observó como principales problemas (i) que la integración de las organizaciones del sector público y privado a este marco de control establecido por el ICIC era voluntario y no obligatorio, por lo que su evolución no ha sido tan ágil como se esperaba (ii) una falta de conciencia en torno a la ciberseguridad y (iii) la existencia de financiamiento insuficiente (OEA y

Trend Micro, 2015).

Las críticas que ha formulado Galán (2022) en relación a esta norma son primordialmente vinculadas a la operativización de los preceptos que en ella se enuncian. En primer lugar, señala la falta de evidencia sobre la evolución de los objetivos del Plan Nacional de ICIC en acciones posteriores. Al igual que la valoración efectuada por la OEA y Trend Micro, cuestiona el programa indicando que la adhesión al mismo es opcional, lo que dificulta una protección homogénea de las infraestructuras críticas de información y pone en riesgo la seguridad nacional. Finalmente, destaca que estas funciones asignadas, no abarcan completamente la implementación de los objetivos del plan mencionado, lo que indica una posible falta de coherencia entre la normativa y su aplicación práctica.

El diagnóstico realizado por el autor parece acertado: no se registran avances concretos del Programa Nacional ICIC, y tampoco se han declarado como tal, infraestructuras críticas nacionales. Luego, en lo que atañe a la cuestión más formal, analizando los objetivos establecidos en el Programa Nacional ICIC, y la evolución normativa posterior[12], se puede observar que los mismos fueron reemplazados por las funciones y competencias asignadas a la Subsecretaría de Tecnologías de Información, a la Dirección Nacional de Ciberseguridad, la Dirección de Seguridad en Redes y Sistemas Informáticos y el Equipo Nacional de Respuesta ante Emergencias Informáticas (CERTar).

Una última reflexión sobre esta norma, es que, considerando que tanto sustancial como formalmente el Programa Nacional ICIC ha evidenciado un desuso y virtual desaparición por la absorción de sus objetivos en otras áreas y programas, sería adecuado propiciar su derogación, al mismo tiempo que avanzar en la creación de metodologías específicas para identificar y declarar como tales a las ICI, propendiendo a elevar su protección mediante medidas de seguridad acordes.

Requisitos Mínimos de Seguridad de la Información para organismos del Sector Público.

Los Requisitos Mínimos fueron aprobados mediante **Decisión Administrativa N° 641/2021** y representan la sucesión y jerarquización de una serie de políticas modelo de Seguridad de la Información que fueron dictadas oportunamente por la Oficina Nacional de Tecnologías de la Información (ONTI) mediante normas de menor jerarquía (Disposiciones N° 6/2005, N° 3/2013, 3/2014, 1/2015). El alcance de esta norma se encuentra limitado a las entidades y jurisdicciones de la Administración Nacional (conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social), así como sus proveedores (en todo lo relacionado con las tareas que realicen y conforme la normativa o contrato que los vincule).

De acuerdo con los artículos 3° y 4° de la Decisión Administrativa N° 641/21, los organismos y jurisdicciones debieron aprobar sus respectivos Planes de Seguridad en el plazo máximo de noventa (90) días desde su entrada en vigencia, y en el mismo plazo, remitirlos a la Dirección Nacional de

[12] Decreto N° 50/2019 (texto actualizados), la Decisión Administrativa N° 1865/2020, Decisión Administrativa N° 641/2021 y la Disposición N° 1/2021 de la Dirección Nacional de Ciberseguridad.

Ciberseguridad para su aprobación.

Otros puntos destacables de esta pieza normativa son que: (i) obliga a las jurisdicciones y entidades alcanzadas, a la designación de un punto de contacto responsable de las funciones relativas a la seguridad de los sistemas de información y (ii) establece aspectos procedimentales en relación a la comunicación de incidentes de ciberseguridad, indicando que los mismos deben ser notificados a la Dirección Nacional de Ciberseguridad, dentro de las cuarenta y ocho (48) horas de tomado conocimiento de que efectivamente ocurrió o su potencial ocurrencia.

Carlos Galán (2022) cuestiona algunos aspectos de la Decisión Administrativa 641/2021. En primer lugar, entiende que su alcance es limitado, argumentando que debería abarcar también a otras jurisdicciones como a las empresas estatales y entidades donde el Estado tenga participación mayoritaria. Además, señala la falta de un Esquema de Evaluación y Certificación de la Ciberseguridad, similar al modelo implementado en otros países y regiones como España y la Unión Europea, entendiendo que sin el mismo se dificulta la efectividad de las medidas de seguridad propuestas. También expresa preocupación por la falta de evidencia sobre el cumplimiento de las disposiciones de la norma, incluyendo la aprobación de los Planes de Seguridad, la designación de puntos de contacto, la adopción de medidas preventivas y la presentación de reportes de incidentes de seguridad tal como se establece. Según el autor, esta falta de transparencia y seguimiento pone en duda su efectividad y aplicación real.

Observando arreglos normativos adoptados en otros países de la región, el plazo de cuarenta y ocho (48) horas que establece la norma para reportar incidentes parece excesivo. Recientemente, en abril de 2024, Chile aprobó la Ley Marco de Ciberseguridad N° 21.663, donde estipula que los organismos afectados por incidentes tienen el deber de emitir una alerta temprana sobre la ocurrencia del evento dentro del plazo máximo de tres (3) horas contado desde que se tiene conocimiento del mismo, y dentro de las setenta y dos horas (72), una actualización de la información del incidente. Considerando que la detección temprana de un incidente es vital para evitar la propagación de los daños que pueden causar, Argentina podría mejorar sus niveles de resiliencia al establecer la obligación de reportar los incidentes en plazos menores a los vigentes.

Respecto a la falta de evidencia sobre el nivel de cumplimiento que Galán (2022) enuncia, cabría resaltar que a través del sitio institucional de la Dirección Nacional de Ciberseguridad, luce un recuadro que enuncia la cantidad de planes de seguridad de la información aprobados por dicha entidad, así como la cantidad de puntos focales de ciberseguridad designados[13].

Algo que el autor no menciona específicamente, y posiblemente constituya una dificultad ostensible en términos de implementación, es la imposibilidad de sancionar a los organismos y

[13] Accediendo al sitio institucional https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad, se observa un recuadro que al día 5/5/2024 indicaba lo siguiente: "Se informa que en el marco de la Decisión Administrativa 641/2021 se registraron -hasta el 31 de diciembre del 2022- 67 planes de seguridad de la información, y un total de 89 Puntos Focales de Ciberseguridad."

entidades alcanzadas que no cumplan con las exigencias allí estipuladas, tanto en lo que refiere a la aprobación de planes de seguridad, designación de puntos de contacto e incluso en lo atinente al deber de reporte de incidentes. De lo estipulado en el artículo 11 de la norma bajo análisis - donde se prevé que la aludida Dirección Nacional es la encargada de verificar su cumplimiento, sin perjuicio de las competencias asignadas a la Sindicatura General de la Nación (SIGEN)- cabe considerar que no se clarifica cuál es el procedimiento para operativizar ese tipo de sanciones, y, amén de los procesos de auditoría interna de cada organismo alcanzado, la Dirección Nacional de Ciberseguridad no posee herramientas de fiscalización y sanción sobre los organismos alcanzados. Arreglos institucionales como el recientemente instaurado en Chile, promueven la creación de una Agencia Nacional de Ciberseguridad con facultades para controlar y sancionar el incumplimiento de los deberes y responsabilidades de aquellas entidades y organismos alcanzados dentro su órbita, estableciendo un procedimiento administrativo sancionador (Art. 42) y explicitando la responsabilidad administrativa de los jefes superiores de los organismos en la implementación de medidas para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a lo establecido en la aludida Ley Marco de Ciberseguridad.

Finalmente, podría considerarse que, pese a que la aludida Decisión Administrativa prevé en su artículo 8° la revisión y actualización periódica de los Requisitos Mínimos, desde el año 2021 -fecha en que se dictaron- no se observa que dicha manda normativa haya sido cumplida.

Creación del Comité Nacional de Ciberseguridad

En el año 2017, tiene lugar la creación de un Comité integrado por diversas carteras ministeriales con competencia en la materia, con el objetivo de desarrollar una Estrategia Nacional de Ciberseguridad. De los fundamentos esbozados en el **Decreto N° 577/2017**, se observa la intención gubernamental de establecer previsiones en materia de protección del ciberespacio, a efectos de implementar en forma coherente y estructurada acciones de prevención, detección, respuesta, defensa y recuperación frente a las amenazas cibernéticas, conjuntamente con el desarrollo de un marco normativo acorde.

En esa lógica, se entabla en la órbita del entonces Ministerio de Modernización un cuerpo deliberativo integrado por representantes de ese Ministerio, y los Ministerios de Defensa y Seguridad para desarrollar la referida Estrategia Nacional y el plan de acción necesario para la implementación de sus objetivos, asignándole también facultades para convocar a otros organismos a que participen en la implementación de medidas en el marco de dicho plan de acción. Entre las facultades que se le asignan al Comité, también se encuentran las de impulsar el dictado de un marco normativo en materia de ciberseguridad y fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.

En el año 2019, al modificarse la estructura orgánica administrativa y eliminarse el Ministerio de Modernización de la Nación, el Comité Nacional pasa a la órbita de la Jefatura de Gabinete de

Ministros que, como continuadora de dicho Ministerio, absorbió las competencias en materia de ciberseguridad. Asimismo, mediante **Decreto N° 480/2019** se amplían los organismos que integran el cuerpo deliberativo, sumando al Ministerio de Relaciones Exteriores y Culto (Cancillería), la Secretaría de Asuntos Estratégicos y al Ministerio de Justicia y Derechos Humanos.

Galán (2022) advierte que tratándose de un Comité con las importantes funciones que se señalan en la norma, su composición luce bastante exigua, máxime considerando que una Estrategia Nacional de Ciberseguridad, que nace como respuesta a la problemática de los riesgos del ciberespacio y que resulta de aplicación a toda la nación (sector público, sector privado, profesionales y ciudadanos), debe contemplar el impacto de la materialización de tales riesgos en todos los sectores concernidos, incluyendo también la Economía, Ciencia, Cultura, Educación, Interior, Salud, entre otros.

Sobre esto se puede señalar que en la ya referida Ley Marco de Ciberseguridad de Chile, el Comité Interministerial sobre Ciberseguridad que se crea, incluye además de las áreas ministeriales incluidas en la normativa local, a las dependencias con competencias en materia de Telecomunicaciones, Hacienda e Inteligencia. Continuando con la apreciación del autor y observando la composición adoptada en el país vecino, parece razonable advertir que la ampliación en la integración del Comité Nacional incluyendo áreas críticas y con gran incidencia en la materia, como las telecomunicaciones (ENACOM), la inteligencia (AFI), las políticas de interior (Ministerio del Interior) y el Ministerio de Salud, significaría reconocer la vital importancia que ocupan estas dependencias en pos de los propósitos que la Estrategia Nacional y su plan de acción deben promover y también coadyuvaría a conocer y jerarquizar los desafíos que estos sectores críticos de la Administración Pública atraviesan.

Finalmente, entendiendo que el Comité Nacional encarna el nivel estratégico más relevante del marco institucional adoptado, cabría cuestionar la conveniencia de elevar su jerarquía para que el mismo dependiera estructuralmente de la Presidencia de la Nación.

Estrategia Nacional de Ciberseguridad

A través de la **Resolución N° 829** de fecha 24 de mayo de 2019, se aprobó la implementación de la primera Estrategia Nacional de Ciberseguridad de la República Argentina. De acuerdo con los fundamentos que motivan la medida, el documento nace como fruto de la labor del Comité Nacional de Ciberseguridad en consulta con diversos actores de los sectores privado y académico, los cuales de forma coordinada prestaron conformidad a su aprobación, con el fin de elaborar un documento preliminar que refleje el desarrollo tecnológico y la realidad geopolítica de nuestro país.

Dicha Resolución, además de aprobar este documento cimentado sobre cinco (5) principios rectores y ocho (8) objetivos[14], mediante el artículo 3° invitó a las Provincias y Ciudad Autónoma de

[14] **Los cinco principios rectores receptados en el documento constan de:** 1) Respeto por los derechos y libertades individuales, 2) Liderazgo, Construcción de capacidades y fortalecimiento federal, 3) Integración internacional, 4) Cultura

Buenos Aires para que adhieran a la aludida Estrategia Nacional. Además, a través de uno de sus artículos creó, en la órbita del Comité de Ciberseguridad, una Unidad Ejecutiva a fin de coordinar el funcionamiento y brindar asistencia administrativa a dicho cuerpo.

Galán (2022) formula una serie de observaciones frente a la Resolución bajo análisis. En primer lugar, cuestiona el nivel jurídico del documento, argumentando que el tipo de norma posee un rango normativo inferior al requerido para una política de tal envergadura. Concretamente aduce que "(...)por la importancia de esta norma, que viene a aprobar el instrumento político-estratégico más importante de la nación Argentina en materia de ciberseguridad pública, evidencia que el instrumento jurídico elegido posee un rango menor del deseable". Asimismo, señala que la redacción del artículo 3° sugiere que su observancia no es obligatoria para las provincias y la Ciudad Autónoma de Buenos Aires, lo que podría suponer una grave merma de la esperanza de penetración de la Estrategia en la Argentina. Seguidamente, critica la regulación de la Unidad Ejecutiva del Comité de Ciberseguridad, sugiriendo que su creación debería haber sido dispuesta mediante un instrumento normativo de mayor jerarquía para asegurar su adecuada implementación.

Por último, y más específicamente vinculado al texto de la Estrategia en sí, sugiere que los 8 objetivos fijados deberían haber sido ordenados de acuerdo al grado de relevancia de los mismos, priorizando algunos como la protección de los sistemas del sector público y las infraestructuras críticas de información (enumerados en el orden 8 y 6), sobre otros objetivos considerados instrumentales de los anteriores.

En el año 2022, el aludido Comité dió curso a una revisión de la Estrategia Nacional. A raíz de ello, en enero de 2023 se dictó la Resolución N° 1/2023 de la entonces Secretaría de Innovación Pública, a partir de la cual inició un proceso de consulta pública respecto del documento de la Segunda Estrategia Nacional de Ciberseguridad de Argentina. A través del Informe resultante de la consulta pública, se observa que distintos actores del ecosistema participaron emitiendo sus consideraciones y sugerencias al texto mediante dieciocho (18) aportes, distribuidos entre: tres (3) propuestas provenientes del Sector Público, cuatro (4) del Sector Privado, siete (7) de la sociedad civil, una (1) del sector académico, dos (2) de organismos y entidades internacionales y una (1) de la comunidad técnica (Secretaría de Innovación Pública, 2023).

Posteriormente a su aprobación por parte del Comité de Ciberseguridad, el 1° de septiembre finalmente se aprueba el texto de la Segunda Estrategia Nacional de Ciberseguridad mediante la **Resolución N° 44/2023** de la entonces Secretaría de Innovación Pública.

Además de resolver la entrada en vigencia de la nueva Estrategia, esta norma es relevante por otras dos cuestiones: (i) en primer término, crea una Unidad de Gestión y Cooperación en

---

de ciberseguridad y responsabilidad compartida y 5) Fortalecimiento del desarrollo socioeconómico. **A su vez, se establecen los siguientes ocho objetivos:** 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 y 8) Protección de las Infraestructuras Críticas Nacionales de Información.

Ciberseguridad en la órbita de la Subsecretaría de Tecnologías de la Información y (ii) además, modifica las funciones de la Unidad Ejecutiva del Comité de Ciberseguridad y estipula que la misma pasará a depender de la Unidad de Gestión y Cooperación creada.

Del análisis de la Segunda Estrategia, se observa que en este nuevo texto se conservan los principios presentes en la primera Estrategia pero también, se incluyen dos nuevos principios rectores: (i) la Seguridad en el ciberespacio para personas en situación de vulnerabilidad o históricamente discriminadas y (ii) Perspectiva de género y derechos humanos en el desarrollo de todas las actividades orientadas a la concreción de los objetivos de la estrategia y su plan de acción. Algo destacable es que estos principios fueron receptados a partir de las sugerencias y aportes recibidas por el organismo en el marco del proceso de consulta pública. Ello así, en tanto se observa que el documento puesto a consideración no receptaba estos principios, y del análisis de los aportes que hicieron los distintos sectores del ecosistema, se observa el señalamiento acerca de la conveniencia de incorporarlos.

En relación a la observación que hiciera Galán (2022) referente a la conveniencia de ordenar los objetivos en función de la principalidad y relevancia, este punto se observa resuelto en la Segunda Estrategia, en tanto se puede percibir una estructuración distinta de los mismos, estableciendo en primer término objetivos como el fortalecimiento del sistema institucional, la protección de las ICI nacionales, así como la protección y recuperación de los sistemas de información del Sector Público; seguido de otros de mayor accesoriedad como el desarrollo del marco normativo[15].

En lo que atañe al alcance y su observancia por parte de las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires, cabe poner de resalto dos cuestiones. En primer término, el documento bajo análisis se sitúa como un marco estratégico donde se estipulan directrices generales que buscan marcar un posicionamiento nacional en torno a la evolución del desarrollo tecnológico y la realidad geopolítica de nuestro país, circunstancia que explica el hecho de situarlo como un marco referencial al cual adherirse, máxime considerando que el poder de definir cuestiones atinentes a la seguridad nacional no ha sido delegado por las provincias al Gobierno federal, y por tanto -tal como lo prescribe el artículo 121 de la Constitución Nacional- las mismas lo conservan.

En segundo lugar, algo que Galán (2022) no menciona específicamente pero quizás tenga una mayor relevancia en términos de la participación de las instancias locales a la concreción de los propósitos que se consagran en la Estrategia Nacional vigente, es que a la fecha no se ha elaborado el Plan de Acción necesario para implementarla, tal como lo prescribe el inciso d) del artículo 1° del Decreto N° 577/2017 y sus modificatorios, al detallar las tareas del Comité de Ciberseguridad.

[15] **El orden asignado a los objetivos en la Segunda Estrategia Nacional es el siguiente:** 1) Fortalecimiento del sistema institucional para el abordaje de la problemática de la ciberseguridad a nivel federal 2) Protección de las Infraestructuras Críticas Nacionales, 3) Protección y recuperación de los sistemas de información del Sector Público, 4) Fortalecimiento de capacidades de prevención, detección y respuesta, 5) Concientización, Capacitación, Educación y promoción para la formación de especialistas en ciberseguridad, 6) Desarrollo del marco normativo, 7) Cooperación Internacional y 8) Fomento de la industria de la ciberseguridad.

Finalmente, una crítica que el autor efectúa reiteradamente, tiene que ver con la jerarquía de la norma adoptada tanto para aprobar el texto de la Estrategia, como para crear la Unidad Ejecutiva. Esta observación que Galán (2022) formula para el caso de la primera Estrategia aprobada en 2019, mantiene validez en lo que respecta al texto de la Segunda Estrategia porque el instrumento jurídico utilizado se trata en igual sentido de una Resolución, tipo normativo de menor nivel en relación a otros existentes en la esfera del Poder Ejecutivo nacional como las Decisiones Normativas o Decretos.

Infraestructuras Críticas (IC) e Infraestructuras Críticas de Información (ICI): definición y clasificación.

En septiembre de 2019, a través de la **Resolución N° 1523/2019** de la Ex Secretaría de Gobierno de Modernización se aprobó un documento que contiene la definiciones tanto de las IC como de las ICI, al mismo tiempo que se identifican una serie de criterios para identificarlas y se listan los sectores críticos identificados (tales como Energía, Tecnologías de Información y Comunicaciones, Transportes, entre otros).

Entre los criterios de identificación surgen el impacto en la vida humana, impacto económico, en el medio ambiente, en el ejercicio de los derechos humanos y de las libertades individuales, y en lo que atañe al presente trabajo, uno de los criterios consiste en el impacto detectado en el ejercicio de las funciones del Estado, "cuando debido a la afectación de un sistema informático, se afecte de manera sustancial el normal desempeño de los órganos de los poderes Ejecutivo, Legislativo o Judicial".

Al respecto, se definen como IC a aquellas infraestructuras 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. En cambio, las ICI se definen como aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las IC.

Esta norma aprueba además, en su Anexo II, un Glosario de Términos de Ciberseguridad, donde consta la definición de ciberseguridad adoptada por la República Argentina, la cual fuera explicada en el acápite V2 del presente trabajo.

Carlos Galán (2022) presenta una serie de críticas específicas a la Resolución bajo análisis. En primer lugar, y al igual que en el examen de otras normas, sugiere que el instrumento normativo utilizado podría haber tenido un rango más alto, dada la importancia de los criterios de identificación de las IC, las ICI y los sectores afectados, sugiriendo que la misma podría haberse dictado mediante Decreto.

A su vez, el autor señala que la norma carece de una falta de delimitación de los umbrales para determinar aquellas situaciones en que se puede considerar que han generado un impacto significativo y por tanto son críticas, lo que dificulta la aplicación efectiva de la normativa.

Además, destaca la ausencia de evidencia sobre qué instalaciones o dependencias se han identificado como infraestructuras críticas.

Por último, pone de resalto que en la Resolución N° 1523/2019, no se identifica a las entidades responsables de controlar situaciones de emergencia, como ciberataques. Agrega que:

> (...)en la Directiva Europea NIS y en las legislaciones que la transponen a los diferentes ordenamientos jurídicos nacionales, por ejemplo, se definen y determinan las llamadas Autoridades Competentes (en general, tantas como sectores implicados, que cubrirán los sectores determinados y que supervisarán la aplicación de la Directiva a escala nacional) y los CSIRT de referencia (uno o varios, que cumplan los requisitos establecidos en la Directiva, que cubran al menos los sectores que figuran la norma y los tipos de servicios digitales que se señalan, que serán responsables de la gestión de incidentes y riesgos de conformidad con un procedimiento claramente definido.)

En lo que atañe a la falta de delimitación de los umbrales para la determinación de la criticidad de los incidentes cabe destacar que, en el año 2023, a través de la **Disposición N° 3/2023** de la Dirección Nacional de Ciberseguridad, se dictó la "Guía de Notificación y Gestión de Incidentes de Ciberseguridad", en virtud de la cual se establecen criterios para determinar el niveles de criticidad e impacto de los distintos tipos de incidente que pueden afectar a una organización en el ámbito de la Administración Pública Nacional, tal como se identifica en el Anexo II del presente trabajo.

Tal como se desprende del documento aprueba la referida Disposición N° 3/2023, la Guía de Notificación y Gestión de Incidentes de Ciberseguridad se diseñó en base a diversas guías y documentos internacionales relacionados con mejores prácticas de ciberseguridad[16], con el propósito de lograr que el personal técnico de los organismos estatales responda de forma rápida, ordenada y eficaz contra aquellos incidentes de ciberseguridad que pudieran afectarlos, para preservar sus activos de información.

Respecto de la crítica consistente en la ausencia de instalaciones y/o dependencias identificadas y declaradas como infraestructuras críticas, la normativa evidencia que Argentina no ha evolucionado sustancialmente en este aspecto. De la revisión del ordenamiento jurídico, únicamente se observa que en el año 2020, a través de Resolución N° 36/2020 de la Ex Secretaría de Innovación Pública, se declaró al Sistema de Gestión Documental Electrónica (GDE) como Infraestructura Crítica de Información del Estado. Para hacerlo, la ex Secretaría fundó la decisión en la existencia de un alto grado de dependencia de los sistemas informáticos en el normal y adecuado funcionamiento de la Administración Pública Nacional; sosteniendo que el avance tecnológico ha alcanzado la gestión de los organismos públicos, haciendo de los sistemas informáticos un elemento esencial para el

[16] Concretamente se mencionan: Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés); Organización Internacional de Estandarización (ISO); Unión Internacional de Telecomunicaciones (ITU); Guía de Mejores Prácticas para la Gestión de Incidentes de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

desempeño eficiente de toda organización, contribuyendo a alcanzar altos estándares en materia de eficiencia y transparencia en la gestión pública.

Del análisis de la Resolución N° 1523/2019, surge que si bien la norma hace un aporte considerable al proporcionar una definición de IC e ICI, y entablar un criterio marco basado en el impacto y sus dimensiones de análisis en pos de identificar los sectores críticos, se observa una carencia operativa vinculada a: (i) la inexistencia de un método para desglosar los mismos en subsectores (ii) las dificultades para identificar las infraestructuras dentro de cada subsector, así como evaluar su interdependencia y determinar su importancia relativa. Esta falta de detalle dificulta llevar a cabo un análisis completo y fundamentado de la criticidad de las infraestructuras. En este punto, cabría destacar que conforme lo estipulado en el artículo 2° inciso e) del Decreto N° 577 de fecha 28 de julio de 2017, una de las tareas encomendadas al Comité de Ciberseguridad es la de "fijar los lineamientos y criterios para la identificación y protección de las infraestructuras críticas nacionales", por lo que podrían adoptarse estrategias y metodologías en la órbita de este cuerpo deliberativo que aporten claridad a los puntos detallados.

Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR)

La existencia del CERT.ar que se materializa en 2021, a través de la Disposición N° 1/2021 de la Dirección Nacional de Ciberseguridad, encuentra antecedentes en otros grupos de trabajo establecidos previamente con similares propósitos. El primero de ellos, se remonta al año 1999, cuando se creaba en el ámbito de la entonces Subsecretaría de Tecnologías Informáticas, la Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina - ArCERT. Entre las facultades encomendadas a este equipo se destacan las de "Coordinar, colaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito de la Administración Pública Nacional" y "Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos de la Administración Pública Nacional."

Más adelante, mediante la Disposición N° 2/2013 de la Oficina Nacional de Tecnologías de Información, se crearon diversos Grupos de Trabajo como el ICIC-GAP (Grupo de Acción Preventiva), ICIC-GICI (Grupo de Infraestructuras Críticas de Información), ICIC-INTERNET SANO, y particularmente el grupo "ICIC - CERT" (Computer Emergency Response Team) el cual poseía entre otras, la responsabilidad de administrar y centralizar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional.

Es en este contexto que, en el año 2021, a través de la aludida Disposición N° 1/2021, se crea bajo la órbita de la referida Dirección Nacional de Ciberseguridad, el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR, del inglés Computer Emergency Response Team), con el objetivo de coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del sector público nacional definidas en el inciso

a) del artículo 8° de la Ley de Administración Financiera N° 24.156 y sus modificatorios y a las Infraestructuras Críticas de Información, declaradas como tales.

Este Centro Nacional que encarna la faceta táctica del entramado institucional argentino (Galán, 2022), se erige con responsabilidades que abarcan desde el asesoramiento técnico ante incidentes informáticos hasta la coordinación de acciones con otros programas y equipos de respuesta a nivel nacional. Además de contribuir al fortalecimiento de la capacidad de prevención y recuperación ante incidentes de seguridad, el CERT.ar colabora con equipos similares de otros países y mantiene registros estadísticos a nivel nacional. También juega un papel crucial en la promoción de la formación de capacidades para la gestión de incidentes y en la colaboración con gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en materia de seguridad informática.

Analizando las observaciones que formula Galán a la Disposición N° 1/2021, por un lado, enfatiza en el bajo rango normativo por el cual se propició su creación. En lo que respecta a este punto, parece positivo el señalamiento considerando la importancia de las funciones encomendadas al CERTar. Al revisar otras experiencias en la región, se observa por ejemplo que a través del artículo 73 de la Ley N° 18.362 se ha creado en Uruguay el CERTuy, así como mediante el artículo 1° del Decreto Ejecutivo No. 709/2011 se ha instituido el CSIRT Panamá, y en forma más reciente, a través del artículo 24 de la Ley Marco de Ciberseguridad de Chile antes mencionada, se crea el CSIRT Nacional de dicho Estado. En todos los casos, se trata de normas de mayor jerarquía que una mera Disposición emitida por una dependencia con jerarquía de Dirección Nacional.

Tal como refiere la OEA, las consideraciones sobre el marco legal a la hora definir la creación del Equipo de Respuestas ante Incidentes (CSIRT/CERT) son relevantes. Tanto el marco legal elegido como el institucional adoptado, pueden resultar condicionantes en aspectos centrales como la financiación que estos equipos reciban, la infraestructura que se le asigne y los recursos humanos con que cuenten (OEA, 2016).

Por otro lado, Galán (2022) destaca negativamente el acotado ámbito de actuación del CERT, en función de los organismos y jurisdicciones alcanzadas bajo su margen de actuación, es decir, aquellos contemplados en el inciso a) del artículo 8° de la Ley de Administración Financiera N° 24.156 y sus modificatorios y a las Infraestructuras Críticas de Información, declaradas como tales. El autor entiende que los organismos alcanzados podrían incluir asimismo a las entidades y jurisdicciones comprendidas en el inciso b) de dicha Ley [17]. En lo que respecta a agrandar el espectro de organismos y entidades alcanzadas por el CERTar, resultaría congruente con los objetivos de "Ampliar y mejorar las capacidades de detección, monitoreo y respuesta ante ciberataques dirigidos

[17] **De acuerdo con el artículo 8° de la Ley de Administración Financiera N° 24.156, en el inciso a)** se encuentran comprendidos la Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social; **en el inciso b)** a las Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

contra objetivos críticos nacionales" y "Ampliar, acelerar y mejorar las capacidades de detección y respuesta ante eventos de fugas de información que perjudiquen la privacidad de los ciudadanos y/o organizaciones", establecidos en la Segunda Estrategia Nacional de Ciberseguridad, máxime considerando que algunas de las Empresas y Sociedad del Estado, como ARSAT S.A, administran y centralizan grandes volúmenes de datos que se producen y/o recolectan en organismos de la APN.

V8. CASO DE ESTUDIO: FILTRACIÓN DE INFORMACIÓN DEL SID EN OCTUBRE DE 2021

El 9 de octubre de 2021, tras tomar conocimiento de que un usuario de la red social Twitter a través de la cuenta identificada como @aniballeaks, había publicado la imagen completa del documento nacional de identidad de varias personas, el equipo de seguridad informática del RENAPER llevó a cabo una investigación interna preliminar con el objetivo de identificar las causas de esa filtración y detener posibles flujos de datos desde la institución hacia agentes externos.

De acuerdo con declaraciones proporcionadas por RENAPER, tras la finalización de dicha investigación, el organismo pudo concluir que no había existido un ingreso no autorizado por parte de terceros dentro de sus sistemas (comúnmente denominado "hackeo"), ni tampoco fueron comprometidos usuarios y contraseñas con acceso a los sistemas. Asimismo, no detectó consumos de información por fuera de los parámetros habituales de los organismos que utilizan los servicios de datos del RENAPER a través del SID, servicios que están limitados a proporcionar una porción de datos básicos contenidos en el DNI -lo que no incluye por ejemplo, datos biométricos como huellas dactilares-, y que a su vez, representaría una parte acotada de la información ciudadana resguardada en dicho repositorio.

No obstante ello, a raíz de dicha investigación RENAPER explicó haber identificado consumos legítimos a través de un canal securitizado mediante credenciales otorgadas al Ministerio de Salud de la Nación, que coincidían en tiempo y características con la información filtrada.

El Sistema Integrado de Información Sanitaria Argentina (SISA) operado por el Ministerio de Salud se nutre de información de distintas fuentes, entre ellas, de algunos datos específicos del DNI que son otorgados a través del SID. Así, ante un requerimiento de algún organismo, hospital, clínica o centro de salud, el Ministerio de Salud de la Nación, como administrador del SISA, requiere la información a través del servicio de datos securitizados por VPN[18] que le brinda el RENAPER y, una vez que cuenta con el dato, lo reenvía a quien lo esté solicitando a través de su red de servicios. De acuerdo con el RENAPER "(...) Este sistema administra su propio sistema de validación el cual aporta

[18]Una red privada virtual (RPV) más comúnmente identificada por su sigla en inglés como VPN (virtual private network), es una tecnología de redes de computadoras que facilita la extensión segura de una red de área local (LAN) a través de una red pública o no controlada, como Internet. Esta tecnología permite que un dispositivo conectado a la red envíe y reciba datos a través de redes compartidas o públicas, operando como si estuviera en una red privada, con todas las funcionalidades, niveles de seguridad y políticas de gestión que caracterizan a una red privada.

datos a 50 grandes dominios propios y, de forma directa o indirecta, a toda la red de centros de salud del país (50.000 usuarios aproximadamente).”

Como explica el informante clave de RENAPER, en el Ministerio de Salud se había constituido una red federal compuesta por entidades de salud provinciales y municipales, como hospitales o clínicas de relevancia en distintas jurisdicciones del país, a las cuales se les asignaba un dominio específico dentro de la red, a partir del cual cada unidad podía autogestionar la asignación de usuarios y contraseñas institucionales que se otorgaban.

Como puede observarse, desde la postura del organismo, producto de una evaluación interna pudieron descartar la existencia de un “hackeo” o la obtención ilegítima de claves de usuarios para ingresar al SID y obtener así la información filtrada. Sin embargo, sí fue constatado que la información filtrada, había sido consultada y obtenida a través de consumos legítimos a través del SISA, en el marco de los servicios prestados al Ministerio de Salud.

V8.1 RENAPER y la interoperabilidad del SID con otros sistemas

En 2016, a través del Decreto N° 434/2016 se crea el “Plan de Modernización del Estado” el cual se erige sobre cinco ejes principales. Uno de ellos, transversal a todos, es la creación de la “Estrategia País Digital”. Esta Estrategia tiene entre sus principales objetivos, la interoperabilidad e integración de los sistemas de gestión entre las distintas jurisdicciones de gobierno, favoreciendo el intercambio y transparencia de la información.

A partir de dicho Plan de Modernización, se dicta el mismo año, el Decreto N° 1273/2016 a través del cual se obliga a las entidades y jurisdicciones del Estado Nacional, a intercambiar la información pública que produzcan, obtengan, obre en su poder o se encuentre bajo su control, con cualquier otro organismo público que así se lo solicite. Asimismo, a través del Decreto N° 891/2017 de “Buenas Prácticas en Materia de Simplificación”, se establece que el Gobierno Nacional debe fomentar la interoperabilidad entre las administraciones públicas provinciales, y de la Ciudad Autónoma de Buenos Aires, generando un intercambio y colaboración mutua, “a fin de implementar todas las herramientas tecnológicas existentes, permitiendo de este modo acercar a los ciudadanos herramientas eficaces para su interacción con la Administración.”

Es en este marco, que el 13 de julio de 2018, los ministros del Interior y Modernización presentan la implementación del SID, en función de las prerrogativas que, por medio del Decreto Nº 1501 del año 2009, se le dieron al RENAPER para utilizar tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros, como así también en la emisión del Documento Nacional de Identidad. En lo que respecta a la implementación del SID, el RENAPER establece un Convenio Modelo para operativizar el confronte de datos con las entidades y jurisdicciones que lo soliciten, el cual tiene algunas particularidades.

En primer lugar, el intercambio de información se enmarca en los actos de cesión de información previstos en el artículo 11 de la Ley N° 25.326 de Protección de Datos Personales,

precepto que habilita la cesión de datos personales siempre que (i) se acredite el interés legítimo tanto del cedente como del cesionario en lo que respecta a la transferencia de los datos en cuestión, (ii) el deber de informar al titular de los datos sobre la cesión y (iii) la prestación de consentimiento por parte del titular de los datos. Sin embargo, cabe aclarar que la norma aludida prevé una excepción en lo que respecta a la prestación de consentimiento por parte de los titulares de la información, cuando la cesión de datos personales "se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias".

Luego, la información que se interopera entre el RENAPER y los organismos solicitantes se organiza en distintos tipos de servicios que éstos últimos pueden adquirir, según se detalla a continuación:

Tipo de servicio	Información que debe proveer la entidad o jurisdicción que solicita el confronte de datos	Información que devuelve el RENAPER
Autenticación y vigencia del D.N.I.	.Número de D.N.I. .Indicación del sexo del titular	Los datos del D.N.I. vigente de la persona consultada y como dato adicional, la fecha de fallecimiento, en caso de que el Registro Civil correspondiente lo haya registrado.
Verificación de identidad por medio de fotografías de rostros	.Fotografía de frente .Número de D.N.I. .Indicación del sexo del titular	Puntaje en una escala de cero a cien, en función la similitud encontrada con los registros fotográficos de su base de datos.
Datos básicos del D.N.I.	.Número de D.N.I. .Indicación del sexo del titular .Número de trámite del D.N.I	.Nombres, apellidos y fecha de nacimiento del titular. .Fecha de creación, vencimiento y letra/s del ejemplar del D.N.I. .Número de CUIL (si está disponible), .Dirección, nacionalidad y país de nacimiento del titular
Validación múltiple	.Imagen del frente y dorso del D.N.I. .Fotografía de frente del titular	.Puntaje en una escala de cero a cien en función de la similitud encontrada en la comparación de rostros. .Porcentaje de validación de acuerdo al chequeo del frente y dorso del D.N.I.

*Elaboración propia en base a información proveniente del Convenio Modelo aprobado como Anexo de la Disposición N° 4133/2018.

De acuerdo con el servicio acordado, el intercambio de información se genera mediante la utilización de servicios web con tecnología SOAP o API REST[19], y cada consulta o transacción que se

[19] Las API o "interfaz de programación de aplicaciones" son mecanismos que permiten a dos software (más precisamente, dos componentes de software), comunicarse entre sí mediante un conjunto de definiciones y protocolos.

realiza en el marco de estos servicios, se almacena en una base de datos registrando la IP[20] de quién realiza la consulta, la fecha, la hora, el número único de transacciones y el resultado de la misma.

De acuerdo con el informante clave de RENAPER, estos servicios se prestaban con una gran diferencia dependiendo si la entidad solicitante era de carácter público o privada. En el caso de las entidades privadas como bancos o medios de pago, el RENAPER no entregaba datos, sólo los recibía. El proceso de validación de identidad en una aplicación proveniente de una entidad bancaria, habitualmente requiere que el usuario declare información personal y en muchos casos solicita datos biométricos (por ejemplo, tomarse una foto). A partir de esta información recolectada del usuario, la entidad privada remite los datos al RENAPER, quien efectúa una respuesta respecto si se condicen o no con los albergados por el SID, pero en ningún caso las entidades privadas acceden a información alojada en el sistema (tal como la fotografía del D.N.I).

De acuerdo con el informante clave de RENAPER, en el caso de los organismos públicos, hasta el incidente ocurrido en octubre de 2021, el proceso era distinto en tanto se permitía el acceso directo de otros organismos públicos al SID facilitando información que en el caso de empresas u organismos privados no era posible obtener. Tal como expresó, el objetivo de implementar las API fue facilitar ese proceso de interoperabilidad con los organismos públicos que antes era muy complicado y permitía que se entregue información.

V8.2 El Sistema Integrado de Información Sanitaria Argentino (SISA)

En 2014, mediante la Resolución N° 1048 del Ministerio de Salud de la Nación, se estableció la creación del Sistema de Información de Salud (SISA). Este sistema tuvo como objetivo principal integrar y poner a disposición la información necesaria para atender las demandas tanto del Ministerio de Salud de la Nación como de los ministerios provinciales en lo que respecta a la gestión de la información de sus programas y servicios para la comunidad.

El SISA se encarga de gestionar los datos relacionados con establecimientos, profesionales, programas, insumos y prestaciones para la comunidad. El sistema alberga un módulo dedicado a los registros federales de establecimientos y profesionales de la salud, administrados por los ministerios provinciales y supervisados desde el nivel central. Dentro del SISA, existe también el "padrón de ciudadanos", compuesto por las personas que reciben prestaciones en el ámbito sanitario, permitiendo verificar la existencia de un ciudadano y sus transacciones registradas en los diferentes programas gestionados desde el sistema. Toda esta información se visualiza en la "ficha del ciudadano", un repositorio único e individual con acceso restringido que centraliza las prestaciones y servicios de salud de cada individuo.

[20] De acuerdo con NIC Argentina, las direcciones IP (o, simplemente, IPs) son identificadores numéricos únicos asignados a todo lo que está conectado a Internet, desde servidores web hasta smartphones, cámaras, computadoras e impresoras. Pueden clasificarse en dinámicas y estáticas (fijas), o en públicas y privadas, entre otras.

Para verificar la identidad de las personas registradas en el padrón de ciudadanos, utilizado por todos los distintos registros nominalizados del SISA, este sistema interopera información con el SID del RENAPER. Mediante esta articulación se posibilita la identificación de los ciudadanos en el SISA y su condición de vivo/fallecido, siempre que cuenten con el DNI emitido. Hasta la ocurrencia del incidente bajo estudio, el Ministerio de Salud podía acceder al repositorio de información del SID, no obstante desde entonces el proceso de identificación consta de los siguientes pasos:

1. SISA consulta a RENAPER (SID) por número de documento y sexo de la persona que requiere identificar.
2. RENAPER envía respuesta. Si encuentra una persona que coincida con el número de documento y sexo enviado, devuelve el conjunto de datos correspondiente al ciudadano. Si no encuentra una persona que coincida con el número de documento enviado, devuelve una respuesta informando que no encontró a la persona.
3. SISA procesa la respuesta y a partir de ella, crea o actualiza la Ficha del ciudadano y le otorga un estado que puede ser "Identificado por RENAPER" o "No identificado por RENAPER." En este último caso, el proceso de creación de la Ficha avanza sin recuperar datos de RENAPER.

V9 ANÁLISIS DE FACTORES INSTITUCIONALES

V9.1 CAPITAL HUMANO

Escasez de personal especializado:

La escasez de personal especializado en ciberseguridad emerge como un desafío significativo en la respuesta a incidentes de seguridad cibernética. Según las entrevistas realizadas, esta carencia se evidencia en la falta de una estructura formal con responsabilidades claras y definidas en materia de ciberseguridad en muchos organismos.

De acuerdo con el reporte "Cybersecurity WorkForce Study" en su edición 2023, existe una escasez mundial de casi 4 millones de trabajadores calificados en ciberseguridad. Si bien se detectó durante dicho año un crecimiento de la mano de obra en esta especialidad del 8,7%, siguió aumentando la diferencia entre el número de trabajadores necesarios y disponibles, con un incremento interanual del 12,6% (ISC2, 2023).

Esta situación, si bien global, se presenta de manera exacerbada en América Latina y el Caribe, generando fuertes presiones en las organizaciones tanto públicas como privadas con el subsiguiente impacto en la ciberseguridad de los países de la región, que, según Fortinet, sufrió 137 mil millones de intentos de ciberataques de enero a junio de 2022, un aumento del 50% en comparación con el mismo período del año pasado -con 91 mil millones- (Fortinet, 2022).

La APN no está ajena a las problemáticas que imperan en el orden global. De acuerdo con estimaciones del BID, mientras que las buenas prácticas internacionales muestran que las agencias públicas más maduras en ciberseguridad tienden a ocupar aproximadamente entre 5% y 10% de su personal de Tecnologías de la Información (TI) en el área de ciberseguridad, en la APN Argentina solo organizaciones maduras como la Administración Federal de Ingresos Públicos (AFIP) o la Empresa Argentina de Soluciones Satelitales (ARSAT), cumplen con esta relación (BID, 2023).

En lo que respecta a la paridad de género, al igual que otras ramas de las carreras CTIM (Ciencia, Tecnología, Ingeniería y Matemáticas), el campo de la ciberseguridad también evidencia una baja participación de mujeres, representando apenas el 25% de la fuerza laboral (ISC2, 2023).

Como refería el informante clave N° 7 de RENAPER, "(...) el contexto de recursos humanos en informática de estos últimos años fue muy difícil en el país en general, en todos los sectores, desde las grandes empresas, las pymes hasta el sector público. Creció mucho el trabajo freelance para el exterior, en un marco de brecha cambiaria, con una Argentina muy barata en dólares, eso agudizó la situación". Asimismo, asevera que "(...) hay algunos recursos humanos que quedan en el Estado que son de primer nivel, pero hay una falencia de densidad de volumen".

Esta percepción se observa congruente con la visión de gran parte de los entrevistados, los cuales han hecho foco reiteradamente en las dificultades que atraviesan los organismos públicos en términos de composición de equipos técnicos especializados. Si bien algunos equipos de TI cuentan con personas capacitadas, la mayoría de los organismos, entre ellos el RENAPER y el Ministerio de Salud de la Nación, enfrentaban dificultades para encontrar y retener talento en el campo de la ciberseguridad. De acuerdo con la percepción de los informantes clave, esta situación se vió agravada por la ausencia de escalas salariales específicas y condiciones laborales adecuadas para el personal de ciberseguridad, lo que limitaba la capacidad de contratación y retención de profesionales.

Evidencia esta dificultad lo expresado por el informante clave N° 4 por cuanto afirma que "(...) los organismos muchas veces no tienen a quién recurrir dentro del gobierno, porque no hay muchos recursos más que enviar una guía u ofrecer un mail, o sea no hay ayuda técnica, entonces (...) generalmente recurren a empresas, por ejemplo en el caso de este incidente llamaron a Deloitte."

Preparación y capacitación del personal:

La preparación y capacitación del personal constituyen aspectos críticos en la gestión efectiva de la ciberseguridad. Sin embargo, según las opiniones recogidas en las entrevistas, existe una falta generalizada de preparación y conciencia de ciberseguridad dentro de los organismos afectados. En lo que refiere a las políticas de capacitación de los agentes públicos, de acuerdo con información del BID, el sector público de Argentina presenta un estancamiento de la capacidad de formación de profesionales especialistas en materia de ciberseguridad, pese a la gran demanda de formación de los funcionarios en estas temáticas (BID, 2023).

Aunque se reconoce la existencia de algunas áreas con un nivel de preparación relativamente alto, como las entidades financieras, la mayoría de los organismos carecen de capacitación adecuada para enfrentar incidentes de ciberseguridad. Al respecto, de acuerdo con la percepción de la informante clave N° 5 "(...) salvo ANSES, el Banco Central, AFIP y probablemente algún otro organismo robusto, en general los recursos humanos de los organismos no están preparados para responder ante incidentes"

Se destaca la necesidad de implementar programas de capacitación efectivos, que incluyan simulacros de ataques y sensibilización sobre las prácticas de seguridad, para mejorar la preparación del personal ante posibles incidentes. Tal como refiere el informante clave N° 1, "la capacitación que existe es la más barata, rápida y también, menos efectiva. Hay capacitaciones efectivas que se podrían hacer, por ejemplo armar un simulacro efectivo de ataque, pero no se hace nunca eso."

Otra de las deficiencias que se observa es en relación a la falta de perfiles especializados, como refiere el informante clave del CERT.ar, se confunde al personal de las áreas de IT con las de ciberseguridad, y, dentro de los organismos ocurre que a los perfiles que en la práctica se encargaban de tareas vinculadas a ciberseguridad, cuando desde el CERT.ar se le consultaba qué tareas tenían a cargo contestaban "arreglar computadoras, instalar impresoras, actualizar software, eso es lo más que hago de ciberseguridad".

De acuerdo con el informante clave N° 4, del sector privado, en base al modelo FIRST[21], hay distintas capacidades tanto preventivas como proactivas, con que un equipo debe contar. Dentro de las preventivas se encuentran las acciones formativas y de capacitación.

Organización de las áreas de TI:

La organización de las áreas de Tecnologías de la Información (TI) también juega un papel crucial en la gestión de la ciberseguridad. Según las entrevistas, muchos organismos carecen de una estructura formal y clara en materia de ciberseguridad, lo que dificulta la implementación de medidas efectivas. Como expresa el informante clave N° 6 del BID, la estructura organizativa de las administraciones públicas de toda la región, y Argentina no escapa de dicha realidad, no contempla la ciberseguridad como un área sustantiva.

La falta de un área específica de ciberseguridad tanto en el RENAPER como en el Ministerio de Salud, así como la ausencia de una dirección dedicada a este tema, es un aspecto relevante a considerar, en tanto contribuyó a la falta de documentación de procesos, así como la carencia de planificación de acciones de mantenimiento proactivo (informante clave N° 3).

Otro aspecto que se resalta en la entrevista a la informante clave del sector académico, es el

[21] La red FIRST se presenta a través de su sitio web como un foro mundial de equipos de seguridad y respuesta a incidentes, la cual tiene por objetivo mejorar la cooperación entre los equipos de seguridad en el manejo de los principales incidentes de ciberseguridad. A tales fines, ha publicado el "Marco de servicios del equipo de intervención en caso de incidentes de seguridad de productos (EIISP)" donde se detallan distintas esferas de servicio entre las que se encuentra la esfera de servicio N° 6 sobre Formación y capacitación.

atinente a los intereses controvertidos que tienen las áreas de TI y las de ciberseguridad, en función de los objetivos disímiles que pueden presentarse a raíz de los propósitos que cada especialidad persigue dentro de la organización. De acuerdo con la informante clave N° 5 del sector académico, el problema está en que se pone a la seguridad de la información dentro de lo que conforma el área de sistemas, cuando en realidad tienen objetivos diferentes y por ello la recomendación de que se sitúen en áreas separadas. Tal como se explica, el área que desarrolla un servicio (sistemas/TI) tiene como objetivo que el mismo se entregue de acuerdo a los requerimientos de la organización en cuanto a funcionamiento y tiempos. Por el contrario, en el caso del área de seguridad, el objetivo primordial es contribuir a garantizar la integridad, la disponibilidad y confidencialidad de la información, es decir, que el desarrollo sea seguro independientemente de cuándo tenga que salir y de la funcionalidad que se pretenda. En palabras de la informante clave: "(...) la recomendación es, precisamente, que las áreas de seguridad no dependan de sistemas, porque cuando vos tenés que sacar un producto, un servicio o dar el visto bueno, si seguridad está dependiendo del sistema, como que no tiene peso. Por eso siempre se habla de que sean independientes."

V9.2 INTEROPERABILIDAD:

Una de las preguntas que se efectuaron a los entrevistados consistió en averiguar si la interoperabilidad puede considerarse un factor de riesgo en términos de la seguridad de la información.

Tal como se abordó en el acápite anterior, al analizar las particularidades del caso de estudio, surge que hasta la ocurrencia de la filtración de datos bajo análisis, el RENAPER ofrecía servicios diferenciados dependiendo si el "cliente" se trataba de un organismo público o uno privado. Lo cierto es que al reconocer las vulnerabilidades ante las que se vieron expuestos los sistemas de información luego de la filtración de DNIs, el RENAPER adopta nuevas medidas de seguridad en lo que refiere al intercambio de información. Desde entonces, se inhabilita el acceso irrestricto de otros organismos públicos al sistema, emparentando el servicio al que se ofrece a las entidades privadas como bancos o medios de pago, en virtud de los cuales el organismo recibía un input de datos y a partir de ellos devolvía una confirmación de la identidad de la persona consultada.

La cuestión de la interoperabilidad de los sistemas, -y en lo que respecta al caso de estudio, del SID-, ha sido objeto de debate entre los entrevistados, quienes ofrecen perspectivas divergentes sobre su impacto en la seguridad de la información. Algunos de ellos, indican que la interoperabilidad puede ampliar la superficie de ataque y aumentar el riesgo de incidentes de ciberseguridad, especialmente si no se implementan medidas adecuadas de protección.

En la visión de algunos de los informantes clave como el N° 6, se argumenta que la interoperabilidad es necesaria y beneficiosa en tanto evita la réplica infinita de bases de datos, mejorando finalmente el factor de exposición de riesgos. Dicho de otra forma, si el SID no interopera la información que almacena, todos los demás organismos deberían conformar sus propias bases de

datos lo cual finalmente contribuye a incrementar el factor de riesgo. En palabras del informante N° 6 "(...)una interoperabilidad ordenada, con medidas adecuadas, no sólo creo que no aumenta el riesgo, yo creo que hasta a lo mejor lo reduce."

Algunos de los informantes clave del sector público (tanto el proveniente del CERT.ar como del Ministerio de Salud), mencionaron el caso de Estonia como ejemplo de éxito en materia de interoperabilidad, en virtud del desarrollo e implementación de la herramienta X-Road[22] para conectar servicios de distintos organismos de manera segura. De acuerdo con su percepción, este caso de éxito ilustra cómo la interoperabilidad bien implementada puede facilitar el intercambio de información entre organismos gubernamentales, optimizando la prestación de servicios sin comprometer la seguridad de los datos.

Algo que no puede soslayarse es que en el caso del Ministerio de Salud, la pandemia representó un antes y un después. Tal como expresa la informante clave N° 3, hasta ese momento la digitalización era muy escasa y al irrumpir este fenómeno inusitado, el organismo no sólo debió transitar un rápido recorrido hacia la digitalización sino que empezó a generar mucha cantidad de nuevos datos consideradamente valiosos en el mercado negro. De acuerdo con la informante, "(...)por suerte estaba todo preparado, había sistema de información, porque podría habernos pasado que no hubiera sistema software desarrollado para eso.". En este aspecto, parece referirse a que la digitalización se pudo efectuar sobre las bases que el SISA ya había cimentado.

V9.3 RECURSOS TECNOLÓGICOS:

De acuerdo con un reporte del BID, la Administración Pública Nacional presenta una baja productividad en la gestión de incidentes cibernéticos. Según explica el organismo, cuando las capacidades de detección, prevención y respuesta son limitadas y los incidentes se detectan una vez que ya han iniciado la producción de daño, este tiende a aumentar mientras continúan sin solucionarse.

En relación al diagnóstico, dicho reporte asegura que lo descripto se debe principalmente a que: (i) no es posible monitorear, en tiempo real, ataques y amenaza a las ICI, actividad que en otros contextos se realiza a través de un Centro de Operaciones de Ciberseguridad del Gobierno (G-SOC); (ii) la plataforma tecnológica con que cuenta el CERT.ar sólo permite el registro de incidentes y el seguimiento de los mismos, sin contar con capacidades para la prevención y gestión de su respuesta; y (iii) los mecanismos de intercambio de información relativa a ataques e incidentes de ciberseguridad no ofrecen la confidencialidad y seguridad requerida por los actores para colaborar oportunamente, dificultando la capacidad de prevención y respuesta ante dichos ataques.

[22] X-Road es un software de código abierto que permite a instituciones y organizaciones intercambiar información a través de Internet, desarrollado por el Instituto nórdico para Soluciones de Interoperabilidad (NIIS), una asociación fundada conjuntamente por Finlandia y Estonia. Este sistema, implantado a nivel estatal en la administración pública de Estonia constituye una capa de integración distribuida entre sistemas de información, que proporciona un modo estandarizado y seguro de desplegar y utilizar servicios.

Para comprender en qué medida las capacidades tecnológicas pudieron influir en este incidente, se consultó a los informantes si consideraban que los recursos tecnológicos eran los adecuados para enfrentar incidentes de ciberseguridad, y también si la existencia de un G-SOC podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido. A continuación se recopilan los principales hallazgos.

Infraestructura tecnológica:

Salvo la informante clave N° 5, quien indicó no conocer con precisión la situación de los organismos involucrados, todos consideraron que la infraestructura tecnológica no era la adecuada. No obstante ello, resulta interesante que todos los informantes coinciden en que la tecnología per se, no fue el factor más crítico ni determinante en la concreción del incidente. Reflejo de esto es lo que expresa el entrevistado del BID, cuando afirma que el mayor problema no radica en los recursos tecnológicos, ya que estos se pueden adquirir eventualmente, "(...) la parte más difícil de implementar está relacionada con el capital humano y los procesos. Aunque la tecnología es fundamental y puede tomar medidas finales para prevenir incidentes, no resulta el factor más crítico".

El informante clave del sector privado expresa una visión crítica sobre la falta de herramientas tecnológicas suficientes en la APN para prevenir y detectar incidentes de ciberseguridad, mencionando entre otras la ausencia de soluciones como las soluciones DDR (de detección y respuesta de incidentes), la inexistencia de factores múltiples de autenticación, y la carencia de tecnología SIEM[23] (Security Information and Event Management). Asimismo, destaca que estas herramientas son comunes en el sector privado pero prácticamente inexistentes en la APN, lo que sugiere una brecha significativa en la infraestructura tecnológica entre ambos sectores.

Además, se plantea como complejidad agregada, el hecho de que la falta de herramientas tecnológicas adecuadas se combina con recursos humanos poco capacitados, generando un desafío adicional en materia de ciberseguridad. Esta percepción resulta congruente con lo que prevé el estándar de la ISO 27002:2022, en donde se afirma que el nivel de seguridad que solo puede lograrse mediante medidas tecnológicas es limitado y debe estar respaldado por actividades de gestión y procesos organizativos apropiados.

En lo que atañe a la infraestructura tecnológica del RENAPER, el informante clave N° 7, aporta que "(...) cuando se masificó el uso del SID, se abrieron más posibilidades de vulnerabilidades. En ese marco, hacía falta una actualización tecnológica".

Actualización y mantenimiento de software

La cuestión de la actualización y mantenimiento de las soluciones de software en la APN ha sido objeto de análisis entre los entrevistados. Varios de los informantes clave indicaron como factor

[23] La gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten las operaciones del negocio.

crítico la existencia de licencias vencidas en la APN, circunstancia que limita la capacidad para mantener actualizados los sistemas y aplicaciones. Esta situación la atribuyen principalmente a restricciones presupuestarias y a la dependencia de proveedores externos que imponen planes de mantenimiento y actualización costosos. A modo de ejemplo, el informante N° 1 expone el caso de la adquisición de firewall[24] -solución de software que promueve una primera línea de defensa en seguridad de la red-, en virtud de la cual se necesita de actualizaciones constantes que deben ir adquiriendose posteriormente. De acuerdo con el entrevistado, no existe una amplia gama de proveedores de este tipo de software enlatados, con lo cual resulta inevitable afrontar los precios de un mercado poco competitivo. A su vez, estas soluciones requieren de un mantenimiento que debe sostenerse en el tiempo para que el producto tenga las funcionalidades más actualizadas.

De acuerdo con el informante N° 5, tener sistemas operativos y todo tipo de aplicaciones actualizadas es una de las prioridades de la ciberseguridad. Es por ello que depender de licencias muy costosas y diversificadas, cuando no se dispone de recursos y una gobernanza adecuada expone una debilidad de la APN, motivo por el cual esas decisiones deberían ser evaluadas a niveles estratégicos, en el corto, mediano y largo plazo. Al momento de analizar la gobernanza como factor, se abordará las dificultades que se observan en el sostenimiento de políticas y decisiones a lo largo del tiempo.

Centro de Operaciones de Ciberseguridad Gubernamental:

De acuerdo con el informante clave N° 1 del CERT.ar, los SOC tienen un trabajo de detección y respuesta, no de prevención. Entonces, de haber contado con uno, probablemente se podría haber detectado la filtración en forma más certera y con mejor calidad de información, permitiendo actuar más rápido y eficazmente. No obstante ello, en términos de prevención, un solo GSOC a nivel nacional no iba a ser útil.

Por su parte, la informante clave N° 5 aduce que, dado que el GSOC es básicamente tecnología para centralizar eventos, se necesita estabilidad y permanencia de determinados parámetros atinentes a las organizaciones que producen la información que se pretende relevar. Por ejemplo, la identificación de los organismos, de los agentes que están autorizados a acceder a distintos niveles de información, entre otros aspectos. En este sentido, la informante pareciera hacer referencia a que en la idiosincrasia de Argentina, donde regularmente hay cambios de estructura y personal incluso en áreas técnicas como las de IT, la utilidad de un SOC gubernamental podría verse obstruida por estos factores.

En lo que aporta el informante clave N° 6, desde el punto de vista de detección y respuesta, las fugas de información son procesos que toman mucho tiempo en producirse, por lo que de haber

[24] Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico entrante y saliente de red y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad (Cisco, s.f.) . El término proviene del concepto de paredes físicas que actúan como barreras para ralentizar la propagación del fuego hasta que los servicios de emergencia pueden extinguirlo. En comparación, los firewalls de seguridad de red sirven para la administración del tráfico web y normalmente están destinados a ralentizar la propagación de las amenazas web (Kaspersky, s.f.)

tenido un GSOC, se podría haber relevado información valiosa que contribuya a reducir su impacto. Tal como lo expresó dicho informante, si bien el GSOC no hubiera evitado la filtración, sí podría haber reducido el impacto y mejorado la respuesta frente al incidente.

V9.4 GOBERNANZA DE LA CIBERSEGURIDAD

La literatura sobre gobernanza de ciberseguridad se encuentra aún en una etapa prematura (Kuerbis y Badiei, 2017). En el ámbito de los estudios de la seguridad, aquellos que han explorado la gobernanza de la ciberseguridad se han centrado de manera principal en las instituciones y acuerdos público-privados desarrollados por diversos países para reestructurar las responsabilidades de ciberseguridad. Más específicamente, la literatura ha buscado comprender cuál es el rol y la estructura de los organismos públicos encargados de la ciberseguridad y cómo estos establecen acuerdos de colaboración con el sector privado, los organismos y redes internacionales (Del-Real, 2022).

Uno de los objetivos de este trabajo ha sido examinar la normativa existente, buscando entender si la misma resulta adecuada para establecer las reglas y mecanismos que promuevan condiciones eficaces de seguridad de la información en la APN, considerando los derechos fundamentales que pueden verse comprometidos en el ciberespacio. Para ello, a lo largo de este trabajo se analizaron críticamente distintas piezas normativas que encuadran el marco jurídico de la ciberseguridad.

Siguiendo el lineamiento de Galán (2022), la gobernanza de la ciberseguridad se compone tanto del marco normativo como del institucional. En esta instancia, y para comprender más acabadamente en qué medida este factor contribuyó o no a la ocurrencia del incidente, resulta interesante complementar ese análisis a través de la percepción de los informantes clave.

Marco institucional

De acuerdo con Galán (2022), en lo que respecta al marco institucional, este debe desarrollarse en tres niveles: (i) estratégico, (ii) ejecutivo y (iii) táctico. El primer nivel se enfoca en la creación de un órgano estratégico ubicado directamente bajo las instancias ejecutivas más altas del país (tales como la Jefatura de Gabinete). El nivel ejecutivo implica la creación de un órgano encargado de implementar las directrices del nivel estratégico. Sus funciones abarcan asesoramiento, apoyo y orientación técnica, participación en grupos y eventos de confianza, servicios de apoyo, colaboración con la industria, apoyo a la política y la regulación, y seguridad en nuevas tecnologías, entre otros aspectos. En lo que respecta al nivel táctico, este consiste en la constitución de Equipos de Respuesta a Incidentes de Seguridad Cibernética o Equipo de Respuesta ante Emergencias Informáticas (CSIRT o CERT, por sus siglas en inglés) que pueden existir en varios sectores o niveles de administración pública.

Centralización del nivel ejecutivo

Una de las cuestiones que afloraron en las entrevistas es la falta de una instancia centralizadora de la ciberseguridad en el nivel ejecutivo. Quien ocupa ese rol en el esquema vigente al momento del incidente y en la actualidad, es la Dirección Nacional de Ciberseguridad, dependencia que de acuerdo con la Decisión Administrativa N° 1865 del 14 de octubre de 2020 y modificatorios, tiene a su cargo el diseño de políticas de ciberseguridad, la elaboración de planes, programas y proyectos con perspectiva federal en materia de ciberseguridad, colaborar en la ejecución de decisiones que se adopten en el marco del Comité de Ciberseguridad y proponer proyectos de normas, entre otros.

De acuerdo con la informante clave N° 3 del Ministerio de Salud, es necesario centralizar "en algún ente que tenga también facilidad en las compras públicas y la decisión rápida de invertir y tener equipos especializados en estos temas que no son fáciles de armar para un organismo". En el mismo sentido, el informante clave N° 7 de RENAPER aduce que la existencia de un área que centralice los procesos de adquisición de bienes y servicios en materia de seguridad informática hubiese sido muy útil. Una cuestión que resalta este informante clave es la utilidad de una agencia que no sólo audite la existencia de medidas de seguridad de la información sino que adopte medidas proactivas tendientes a garantizarlas.

Congruentemente, la informante clave N° 2 se refiere a la falta de una autoridad de seguridad de la información con "los más altos estándares técnicos y la más alta calidad en materia de acceso a tecnologías".

Desde la perspectiva del sector privado, el informante N° 4 agrega que si bien percibe necesario que cada organismo cuente con un equipo de ciberseguridad que trabaje en sus capacidades de ciberseguridad generales, en una instancia jerárquica superior debe existir un equipo que lleve adelante acciones proactivas, y que se constituya como "una línea roja a la que los organismo puedan llamar". En su visión, ese modelo funciona muy bien en el sector privado y en palabras del entrevistado "eso se debe a que el organismo que está más arriba vé todo el bosque, no sólo el árbol". Por el contrario, la entidad afectada por un incidente de ciberseguridad, además de encontrarse en un momento de mucha presión, únicamente cuenta con la información que observa a través de la situación que transita. Ahí es precisamente donde contar con un nivel superior donde se reúnan expertos con capacidad técnica y conocimiento de las prácticas y procedimientos necesarios puede conformar una herramientas vital en la asistencia del resto de los organismos.

Políticas de ciberseguridad ¿falta normativa o implementación?

Una cuestión a considerar es si existe una carencia de instrumentos jurídicos que sienten las bases adecuadas sobre las cuales se han de cimentar las decisiones y políticas en materia de seguridad que corresponde a cada organismo debe adoptar. Por otro lado, si la implementación de las políticas que se formalizan normativamente encuentra un correlato con los objetivos que en ellas se trazan.

Del análisis de las entrevistas surge que si bien la normativa es perfectible[25], el mayor problema que se observa es en su etapa de implementación. El informante clave N° 7 de RENAPER, se refiere a la existencia de un gran listado de normas que en general se inspiran en lo que otros países están haciendo en la materia, por lo que aduce entender que el problema se encuentra en el enforcement.

El informante clave N° 4 del sector privado, agrega que en su ejercicio profesional se ha encontrado con entidades públicas nacionales que expresan tener que cumplir con varios requisitos de seguridad pero no cuentan con los recursos humanos, tecnológicos ni presupuestarios para hacerlo. Desde su percepción, esto expone un nivel de madurez muy bajo de las organizaciones.

En esa lógica, también se observa una asimetría significativa entre distintos organismos de la APN en cuanto a capacidades en materia de ciberseguridad. Algunos de los entrevistados se refieren a entidades que gozan de condiciones de seguridad notoriamente mayores respecto al resto, como el Banco Central, la AFIP, PAMI o ARSAT. Es notorio que en ningún caso se mencionan como destacados, organismos pertenecientes a la Administración Central, sino que siempre se trata de entidades descentralizadas.

Otro de los desafíos que se señalan tiene que ver con el tiempo que demora la implementación. En el caso de la informante clave N° 3 del Ministerio de Salud, expresa que efectuar consecuentemente un plan de inversión y ejecutarlo, con los tiempos que existen administrativamente por normativa "(...) tarda mínimo dos años y en dos años, es tanto el avance tecnológico que pueden implementar los hackers que siempre vas a estar atrasado".

Resulta interesante al respecto, la apreciación del informante clave N° 6 del BID cuando se refiere al hecho de que la implementación de medidas para aumentar la capacidad en materia de ciberseguridad en una organización, requiere una "gestión del cambio" algo que suele tomar tiempo. Desde su visión, "(...) eso significa que si hoy me pongo con todo a trabajar en mejorar la capacidad en ciberseguridad de mi organización, con suerte voy a poder ver algún tipo de cambio dentro de un año y medio.".

Según el informante clave N° 6, en la implementación subyace un problema de origen que tiene que ver con la falta de diagnóstico de necesidades. Es decir, con la construcción de evidencia en base a métricas e indicadores que permitan entender las capacidades que tiene una organización, y las debilidades en las que debe trabajar. Desde su percepción, esto se evidencia regularmente cuando ocurre un incidente, porque es en ese momento que la ciberseguridad escala en la agenda pública y las organizaciones ven como prioridad "hacer algo". El problema en muchos casos, es que no se cuenta con un sólido diagnóstico previo que permita guiar adecuadamente el impulso que acontece en ese tipo de oportunidades.

[25] Al respecto, el informante clave N° 1 aduce que se debería actualizar la Decisión Administrativa N° 641/2021 y la informante clave N° 2 expresa observar en la normativa la inexistencia de protocolos claros de seguridad, una definición dentro de esos protocolos de quién y qué accesos tiene, un elemento que deje marcadas las manos de quien entra y quien usa los datos.

Asimismo, entre los argumentos más reiterados por los informantes para explicar las dificultades de implementación de las políticas existentes, se menciona consistentemente la falta de posicionamiento de la ciberseguridad dentro de la agenda política.

VI. CONCLUSIONES:

Capital humano:

La escasez de perfiles profesionales técnicos en ciberseguridad se manifestó como un desafío crítico en la APN. Tratándose de empleos principalmente remotos, las condiciones salariales poco competitivas del sector público en un contexto de disparidad cambiaria -donde el sector privado ofrecía remuneraciones en divisa extranjera- plantearon un escenario desafiante para la captación de talentos en los organismos públicos. En este aspecto, RENAPER y el Ministerio de Salud no estuvieron ajenos a este escenario adverso, producto del cual los equipos de TI no disponían de la cantidad de recursos necesarios para afrontar el desafío que se planteó, en el contexto de la pandemia y la masificación de datos sanitarios que emergieron. El segundo aspecto del problema atinente al capital humano se vinculó a la preparación y capacitación de los agentes públicos. Aunque algunos organismos descentralizados como la AFIP y ARSAT se encontraban mejor preparados, en el ámbito de la Administración Central las debilidades eran ostensibles. La carencia de un programa formativo para los perfiles técnicos y la inexistencia de programas de concientización generalizados en un contexto donde la pandemia acrecentó exponencialmente las vulnerabilidades, resultaron factores determinantes. En tercer y menor orden de incidencia, en la organización de las áreas de TI de los organismos de la APN se observa que la seguridad de la información quedaba relegada a otros intereses más relevantes en el contexto crítico de la pandemia, como por ejemplo el desarrollo de las aplicaciones Cuidar y Mi Argentina para facilitar el otorgamiento de permisos de circulación, y asignación de turnos de vacunas.

Algunas estrategias para mitigar los efectos de esta debilidad institucional podrían consistir en:

- Establecer una formación básica y obligatoria dirigida a todos los agentes públicos que se desempeñen en la APN, que contribuya a establecer niveles aceptables de concientización en materia de seguridad de la información.
- Para los puestos de profesionales técnicos que desempeñan en las áreas de TI de los distintos organismos de la APN, y particularmente, de los agentes que componen el CERT.ar, sería pertinente efectuar un plan formativo basado en el modelo de FIRST, que contemple formación técnica, en comunicaciones, en procesos, y en el uso de herramientas. La adquisición de una plataforma de simulación de ataques cibernéticos como la prevista en el marco del Programa de Ciberseguridad para ICI, permitiría desarrollar habilidades concretas tendientes a elevar la capacidad de prevención, detección y gestión de los incidentes.

- Para abordar la escasez de personal especializado, se podría establecer un programa de formación profesional para jóvenes en colaboración con universidades técnicas. Este programa permitiría que la APN se convierta en un semillero de profesionales altamente capacitados, ofreciéndoles la oportunidad de insertarse en empleos donde enfrentar problemáticas y desafíos de alto impacto público. La retención es quizás el mayor desafío. Para ello, debería considerarse el establecimiento de escalas salariales diferenciadas para perfiles técnicos de ciberseguridad y estimular la permanencia a través del financiamiento de programas certificados altamente valorados en el mercado de trabajo de la ciberseguridad.

Gobernanza:

En orden de prelación, el segundo factor institucional con más peso para explicar la ocurrencia del incidente se vincula a las deficiencias en la gobernanza de la ciberseguridad en Argentina: (i) la ciberseguridad no es un tema prioritario en la agenda política, aunque suele escalar cuando existen incidencias significativas como la que se analizó en este caso. A diferencia de países como Chile, donde se ha desarrollado una estrategia a mediano y largo plazo que coadyuvó a jerarquizarla normativa e institucionalmente, en Argentina no se observa un plan de estas características (ii) existe una disparidad de capacidades muy relevante entre organismos de la APN. En el caso de algunos descentralizados, donde las áreas de TI cuentan con mayores recursos, se le da una importancia mayor a la ciberseguridad. No obstante, en organismos de la Administración Central como el Ministerio de Salud, la debilidad en este campo es considerable, (iii) si bien el marco normativo es perfectible -jerarquizando y actualizando normas relevantes como la Decisión Administrativa N° 641/2021-, no es un obstáculo al crecimiento en capacidades de la APN. El mayor déficit está dado por la falta de implementación de las normas existentes y la carencia de mecanismos que las operativicen.

Algunas tácticas para contrarrestar los impactos de esta debilidad institucional podrían incluir:

- Si bien Argentina es uno de los países pioneros en la región al haber dictado una Segunda Estrategia Nacional de Ciberseguridad, no cuenta con un plan de acción que permita operativizar los objetivos en ella enunciados. El desarrollo de este plan de acción, que se encuentra encomendado al Comité de Ciberseguridad por Decreto N° 577/17, puede convertirse en el puntapié de una estrategia a corto y mediano plazo. Partiendo de un diagnóstico para establecer la línea de base, este plan es una herramienta útil para medir la evolución de actividades y objetivos concretos a lo largo del tiempo. La participación de los múltiples actores que componen el ecosistema de la ciberseguridad, será trascendental para dar representatividad y sostenibilidad al desarrollo del plan.
- Evidenciadas las debilidades que genera la fragmentación del nivel ejecutivo de la ciberseguridad, en términos de capacidad de enforcement y asignación de recursos, fortalecer

la gobernanza requiere de adoptar un modelo de gestión centralizado. Para ello, sería necesaria la creación de una Agencia Nacional de Ciberseguridad como organismo descentralizado de la Administración Central, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, con dependencia funcional de Presidencia de la Nación, que disponga de facultades para regular, fiscalizar y sancionar los incumplimientos normativos. Este organismo debiera asimismo, contar con facultades para establecer las infraestructuras críticas nacionales, con la suficiente autoridad para dotarlas de funciones y obligaciones básicas de protección.

Interoperabilidad:

El crecimiento de la digitalización en la pandemia, y el trasvase al ciberespacio de muchos datos que existían y se administraban de forma manual, resultaron factores con significancia en lo ocurrido, circunstancia que asimismo se evidencia en el importante aumento de los ciberdelitos durante 2020 y 2021, respecto del 2019. Del análisis se advierte que la pandemia exacerbó debilidades preexistentes de la APN en materia de seguridad de la información, y en un contexto de urgencia la carencia de procesos y análisis de riesgos en las organizaciones, expusieron vulnerabilidades que fueron hábilmente explotadas por ciberdelincuentes. Sin embargo, el hecho de que la información filtrada se haya obtenido explotando vulnerabilidades en datos que se intercambiaban entre el RENAPER y el Ministerio de Salud, no explica que la interoperabilidad sea un factor que, per se, haya contribuido a la ocurrencia del incidente.

- En este sentido, sería fundamental fortalecer la interoperabilidad mediante la securitización adicional de las VPN, asegurando que el intercambio de información sea más robusto. Esto se podría lograr mediante herramientas como el filtrado de tráfico y la monitorización de las direcciones que utilizan la VPN, así como la detección de fugas de DNS, y empleando algoritmos de cifrado seguros para garantizar la protección de los datos (INCIBE, 2020).

Tecnología:

A partir del análisis de las entrevistas efectuadas en el marco de esta investigación, surge que la tecnología de los organismos involucrados, y de forma más general en la APN, no era la adecuada para prevenir este incidente a través de una detección temprana. Esto se ratifica con el diagnóstico que efectúa el BID en el marco del Programa de Ciberseguridad para ICI que se menciona en reiteradas ocasiones. Ahora bien, estas deficiencias no parecieran ser las más trascendentes para explicar la ocurrencia del incidente estudiado. No obstante ello, vale aclarar que, un año después del incidente, RENAPER efectúa una licitación para la “Provisión de Hardware de Red y Seguridad Informática” por la suma de $640.613.138,96, y entre los bienes y servicios a adquirir se observan distintas soluciones de ciberseguridad como Firewalls, Autenticación de Usuarios y Protección de Ataques

Distribuidos de Denegación de Servicio (DDoS), buscando así elevar la capacidad tecnológica del organismo.

El análisis de este último factor resulta particularmente interesante porque reafirma el hecho de que la construcción de capacidades en ciberseguridad requiere de mucho más que la compra de soluciones tecnológicas, y que, las personas somos finalmente el último y más importante eslabón de análisis en la cadena de prevención, detección y respuesta de incidentes.

VII. REFERENCIAS

- Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). Ciberseguridad. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas. Recuperado de https://elibro.net/es/ereader/utdt/172144?page=12.
- Banco Interamericano de Desarrollo (BID). (2023). Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI). Recuperado de: https://www.iadb.org/es/whats-our-impact/AR-L1343
- Banco Interamericano de Desarrollo (BID). (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Recuperado de https://publications.iadb.org/en/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
- Brizio, A., Campbell, M., & Gomez, S. Tecnologías emergentes y políticas públicas, TIC en Argentina: crecimiento, accesos, usos y políticas públicas. En M. Sánchez Malcolm (Comp.), Jefatura de Gabinete de Ministros. Secretaría de Innovación Pública (2023, 1ra ed.).
- Canals Amettler, D. (Dir.) (2021). Ciberseguridad: un nuevo reto para el Estado y los gobiernos locales. Madrid: Wolters Kluwer España. Recuperado de https://elibro.net/es/ereader/utdt/181960?page=130.
- Castells, M. (2009). Comunicación y poder. Alianza Editorial.
- Del-Real, C. (2022). Panorama institucional de la gobernanza de la seguridad en España. Revista de Estudios Jurídicos y Criminológicos, (6), 15-51. https://doi.org/10.25267/REJUCRIM.2022.i6.03
- Dexter, Lewis A. (1970) Elite and specialized interviewing. Evanston, US: Northwestern University, 1000. Print.
- Díaz, M., & Núñez, R., con la colaboración de Núñez, G. (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. CEPAL. https://www.cepal.org/es/publicaciones/49086-ciberataques-la-logistica-la-infraestructura-critica-america-latina-caribe
- Fortinet. (2022). 2022 Cybersecurity Skills Gap - Global Research Report. Recuperado de https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf
- Frati, G. B., & Aguerre, C. (2022). Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos. Centro Latam Digital.
- Galán, C. (2022). Análisis del marco jurídico y de gobernanza de la ciberseguridad para la protección de las Infraestructuras Críticas en Argentina. Banco Interamericano de Desarrollo (BID). Recuperado de: https://www.iadb.org/es/whats-our-impact/AR-L1343
- González Hernández, I. (2023). Protección de datos y seguridad de la información. Revista Canaria De Administración Pública, (1), 285-311. https://doi.org/10.36151/RCAP.2023.9

- Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID19: the Initial Results from a Natural Experiment. American Journal of Criminal Justice, 45(4), 546-562.
- Huissoud, J. M., & Gauchon, P. (2013). Las 100 palabras de la geopolítica. Akal.
- INCIBE. (2020). Recomendaciones de seguridad en el empleo de redes VPN. Recuperado de https://www.incibe.es/empresas/blog/recomendaciones-seguridad-el-empleo-redes-vpn
- International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection (ISO/CEI 27002:2022). Recuperado de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-3:v2:en
- ISC2 Cybersecurity Workforce Study (2023). How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. Recuperado de: https://cybergovernancealliance.org/wp-content/uploads/2024/01/ISC2_Cybersecurity_Workforce_Study_2023-1.pdf
- Kuerbis, B., & Badiei, F. (2022). Mapping the cybersecurity institutional landscape. Digital Policy, Regulation and Governance. https://doi.org/10.1108/DPRG-05-2017-0024
- Latin America and Caribbean Cyber Competence Centre. (2023). Evolution of Cybersecurity Latin America and the Caribbean: Secure Horizons in the Digital Ecosystem. Recuperado de https://www.lac4.eu/
- Mason, A. G. (2002). Cisco Secure Virtual Private Network. Cisco Press.
- Miró Linares, F. (2013). Delincuencia asociada al uso de las TICs. Universitat Oberta de Catalunya.
- Miró Linares, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. IDP. Revista de Internet Derecho y Política, 32.
- Olivares Rojas, D., & Arriagada Alvarado, V. Ciberseguridad y género: La perspectiva de género en las políticas de ciberseguridad en América Latina y el Caribe. Centro de Estudios en Derecho Informático, Facultad de Derecho de la Universidad de Chile.
- Organización de los Estados Americanos (OEA) y Trend Micro. (2015). Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. Recuperado de https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf
- Organización de los Estados Americanos (OEA). (2016). Buenas prácticas para establecer un CSIRT nacional. Recuperado de: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

- Organización de los Estados Americanos (OEA). (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. Recuperado de https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf
- Organización de los Estados Americanos (OEA). (2023). Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones: Panorama Nacional de Ciberseguridad de la República Argentina 2023. Recuperado de https://www.argentina.gob.ar/noticias/se-desarrollo-la-jornada-optimicemos-la-ciberseguridad-junto-la-oea-y-aws
- Palazzi, P. A. (2016). Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388. (3ª ed., actualizada y ampliada). Buenos Aires: Abeledo Perrot.
- Pallero, M., & Heguiabehere, J. M. (2023). Seguridad de la información y ciberseguridad. Fundación Sadosky.
- Principios Actualizados sobre la Privacidad y la Protección de Datos Personales adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA en 2021.
- Romero, D. (2019). El arte de la ingeniería social. Universidad Piloto de Colombia.
- Santana Soriano, E., & Baez Vizcaíno, K. (2022). Ciberespacio y Cibermundo: delimitaciones conceptuales desde el materialismo sistémico. Ciencia y Sociedad, 47(1), 45-57.
- Stake, R. E. (1999). Investigación con estudios de casos. Ediciones Morata.
- Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2021). Informe de gestión durante la pandemia. Recuperado de https://www.mpf.gob.ar/ufeci/files/2021/09/UFECI_informe-pandemia.pdf
- Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2023). Informe de gestión 2023. Recuperado de https://www.fiscales.gob.ar/wp-content/uploads/2023/12/UFECI_informe-de-Gestion_23_15-12.pdf
- Unión Internacional de Telecomunicaciones (UIT). (2008). Recomendación UIT-T X.1205 Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad.
- Unión Internacional de Telecomunicaciones. (2021). Índice Mundial de Ciberseguridad 2020. Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-s.pdf
- Valles, M. S. (2007). Entrevistas cualitativas. España: Centro de Investigaciones Sociológicas.
- Verizon. (2024). Data Breach Investigations Report 2023. Recuperado de https://verizon.com/dbir

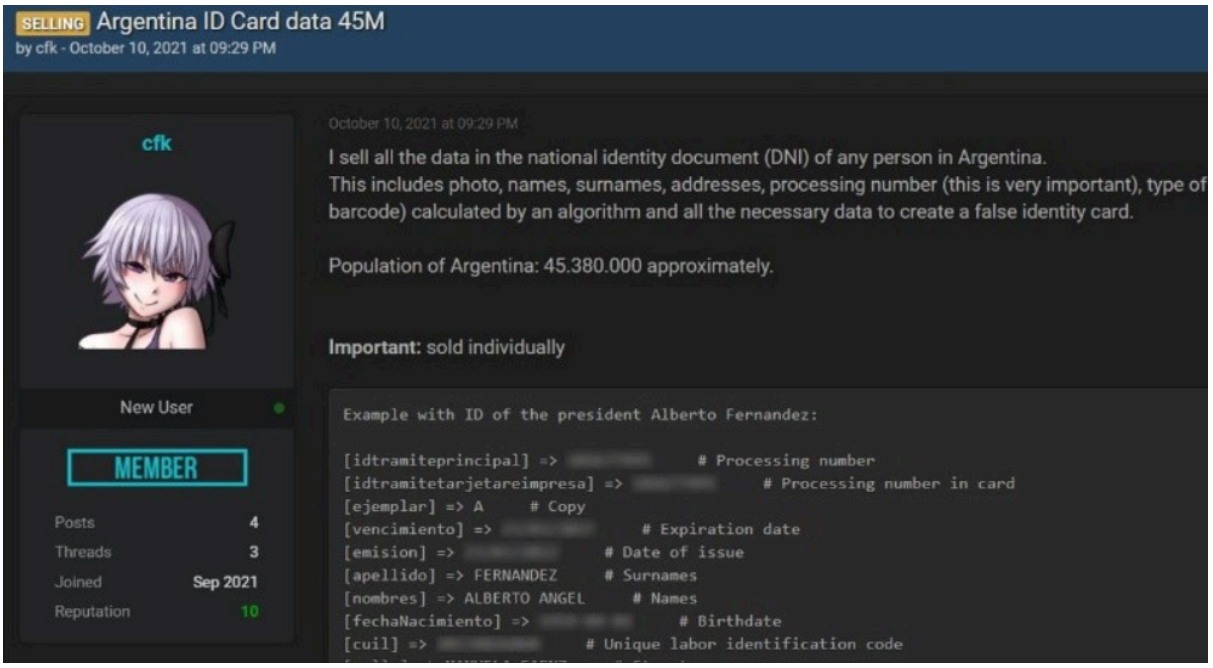
BIBLIOGRAFÍA

- Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (n.d.). CERTUY. Recuperado de https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/certuy#:~:text=El%20Centro%20Nacional%20de%20Respuesta,a%20los%20incidentes%20de%20seguridad
- Arthur, C. (2013). Tech giants give user data to the US government under PRISM: Top internet firms comply with demand for access, but deny complicity in NSA spying. The Guardian. Recuperado de https://www.theguardian.com/technology/2013/aug/23/tech-giants-data
- Banco Interamericano de Desarrollo (BID). (n.d.). Recuperado de https://www.iadb.org/es/whats-our-impact/AR-L1343
- CERT Panamá. (2015). Decreto Ejecutivo no 709. Recuperado de https://cert.pa/wp-content/uploads/2015/09/Decreto-Ejecutivo-no-709.pdf
- Digital Planet. (2021). Digital intelligence index. Recuperado de https://sites.tufts.edu/digitalplanet/files/2021/03/digital-intelligence-index.pdf
- Fortinet. (2023). FortiGuard Labs reports destructive wiper malware increases over 50 percent. Recuperado de https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent
- Gobierno de Argentina. (n.d.). Código de buenas prácticas para el desarrollo de software público. Recuperado de https://www.argentina.gob.ar/onti/codigo-de-buenas-practicas-para-el-desarrollo-de-software-publico
- Gobierno de Argentina. (2023). La app Mi Argentina fue premiada como la mejor solución en transformación digital de. Recuperado de https://www.argentina.gob.ar/noticias/la-app-mi-argentina-fue-premiada-como-la-mejor-solucion-en-transformacion-digital-de#:~:text=La%20herramienta%20tiene%20m%C3%A1s%20de,a%20cargo%20de%20Juan%20Manzur
- Gobierno de Argentina. (2023). Optimicemos la ciberseguridad: CMM Argentina 2023 - Reporte. Recuperado de https://www.argentina.gob.ar/sites/default/files/2023/04/optimicemos_la_ciberseguridad_cmm_argentina_2023_reporte.pdf
- Gobierno de Argentina. (2023). Se presentó la licencia nacional de conducir digital. Recuperado de https://www.argentina.gob.ar/noticias/se-presento-la-licencia-nacional-de-conducir-digital
- Gobierno de Argentina. (n.d.). Trámites a distancia (TAD). Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/tramites-distancia-tad
- Instituto Nacional de Estadística y Censos (INDEC). (2023). Encuesta permanente de hogares - Informes de prensa. Recuperado de https://www.indec.gob.ar/uploads/informesdeprensa/mautic_05_20A36AF16B31.pdf
- Instituto Nacional de Estadística y Censos (INDEC). (2023). Encuesta permanente de hogares - Informes de prensa. Recuperado de https://www.indec.gob.ar/uploads/informesdeprensa/mautic_05_24F87CFE2258.pdf

- Kaspersky. (n.d.). Firewall. Recuperado de https://latam.kaspersky.com/resource-center/definitions/firewall
- Microsoft. (2023). Ciberseguridad es el principal desafío de las pymes argentinas. Recuperado de https://news.microsoft.com/es-xl/ciberseguridad-es-el-principal-desafio-de-las-pymes-argentinas/
- Microsoft. (n.d.). ¿Qué es SIEM? Recuperado de https://www.microsoft.com/es-ar/security/business/security-101/what-is-siem
- Ministerio de Economía de la Nación Argentina. (n.d.). Pliego de condiciones para la contratación pública. Recuperado de https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhz7gUib6RTsgNzvtKrpgdvcYdt1Qw1CI/X0LtPpaGtFTSAybHaA0YFVMgdWjcPPuVxN2Jgzut5%7CfxD2MTPV9tDtzcorCXGImrcMXMuZbVxRjU7M3VTfwiLrzm/PTW9W8OyFBmYJoPMLkUqlA4TcnO8in5Ob/h7PeqlwsypgiQnuj9RpAgj7KOhZ
- Ministerio del Interior, RENAPER. (2023). Informe de gestión RENAPER 2019-2023. Recuperado de https://www.argentina.gob.ar/sites/default/files/2023/03/informe_gestion_renaper_2019-2023.pdf
- Ministerio del Interior. (n.d.). Sistema de Identidad Digital (SID). Recuperado de https://www.argentina.gob.ar/sid/adherir
- Ministerio de Salud de la Nación Argentina. (n.d.). Sistema Integrado de Información Sanitaria Argentina (SISA). Recuperado de https://sisa.msal.gov.ar/sisa/
- Molina, A., & Ortiz, M. (2023). Impacto de la digitalización en la administración pública argentina. Revista de Administración Pública, 54(3). Recuperado de https://www.redalyc.org/journal/870/87070563004/html/
- Presidencia de la Nación Argentina. (n.d.). Se presentó el nuevo sistema de identidad digital para realizar trámites. Recuperado de https://www.casarosada.gob.ar/gobierno-informa/43153-se-presento-el-nuevo-sistema-de-identidad-digital-para-realizar-tramites
- Ria. (2018). Introduction to X-Road. Recuperado de https://web.archive.org/web/20180425050611/https://www.ria.ee/en/introduction-to-xroad-part1.html
- Secretaría de Innovación Pública (2023). Se aprobó la segunda Estrategia Nacional de Ciberseguridad. Recuperado de https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad
- Secretaría de Innovación Pública. (2023). Finalizó la consulta pública sobre la “Segunda Estrategia Nacional de Ciberseguridad”. Argentina.gob.ar. https://www.argentina.gob.ar/noticias/finalizo-la-consulta-publica-sobre-la-segunda-estrategia-nacional-de-ciberseguridad

ANEXOS

ANEXO I - Captura de la puesta en venta de la base de datos completa de documentos nacionales de identidad de la República Argentina.



ANEXO II- Tabla de clasificación de criticidad según tipo de incidente.

A través del Anexo I de la Disposición N° 3 de fecha 4 de julio de 2023 de la Subsecretaría de Tecnologías de la Información, se aprobó la Guía de Notificación y Gestión de Incidentes de Ciberseguridad. En el punto 5.1.1 se detallan los criterios para establecer la criticidad de los mismos, estableciendo que la determinación estará dada por el tipo de incidente en cuestión y el nivel de criticidad que cada organismo le otorgue al activo de información afectado. Seguidamente la mencionada Guía aporta la siguiente tabla orientativa de nivel de criticidad según tipo de incidente:

Nivel	Clasificación	Tipo
Crítico	Otros	Amenaza persistente avanzada - APT
Alto	Contenido dañino	Malware
		Ransomware
		Command & Control
	Disponibilidad	Sabotaje
		Interrupciones
		Denegación de servicio (DoS/dDoS).
	Contenido abusivo	Abuso sexual infantil, contenido sexual.
	Intrusión	Robo
		Explotación de vulnerabilidades
		Ataque de fuerza bruta
		Ataque desconocido
		Compromiso de equipo/sistema
	Compromiso a la información	Acceso no autorizado a la información
		Modificación no autorizada de la información
		Pérdida de datos
	Indicio de fraude	Phishing
	Contenido dañino	Botnet

Medio	Intrusión	Compromiso de cuenta
	Contenido abusivo	Manifestación de odio
	Obtención de información	Ingeniería social
	Disponibilidad	Configuración errónea
	Indicio de fraude	Uso no autorizado de los recursos
		Derechos de autor
		Suplantación
	Activo vulnerable	Sistema vulnerable
		Publicación de servicios vulnerables
		Revelación de información
Bajo	Contenido abusivo	SPAM
	Obtención de información	Escaneo de redes / análisis de tráfico
	Otros	Sectores no críticos

ANEXO III- Transcripción de entrevistas a informantes clave.

Informante clave N° 1 - Empleado del Centro Nacional de Respuestas ante Emergencias Informáticas (CERTar).

¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?
Nosotros éramos un país que no estaba acostumbrado ni al teletrabajo, era medio mala palabra en ese momento, y en especial en el sector estatal. Teníamos formas de trabajar de manera remota que no eran estandarizadas, cada organismo dependía de directivas del responsable de sistemas de IT.

La pandemia fue un factor relevante porque sacó a toda la gente de una superficie de ataque chica, como eran las oficinas, y las expuso a una superficie de ataque muy grande, que eran todas las casas, más todos los dispositivos no securizados que uno tenía en la casa.
Otro factor relevante es que tampoco había una estandarización en lo que era la relación con proveedores en ese momento, cualquier proveedor externo hacía lo que quería y no tenía que rendir cuentas internamente dentro del organismo, por ejemplo para mostrar que los software pasaban exámenes de código. No se hacían ninguno de los tipos de examen que se realizan habitualmente sobre código propio o externo y que exigen muchas de las certificaciones internacionales, como puede ser la ISO 27000.
Después se suma que a la gente de IT, la toman como gente que se tiene que ocupar de ciberseguridad, cuando se tratan de dos roles diferentes. En muchos organismos como Ministerio de Salud y otros, a la persona encargada de ciberseguridad cuando le preguntabas qué tareas tenía a cargo te decía “arreglar computadoras, instalar impresoras, actualizar software, eso es lo más que hago de ciberseguridad”.

¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?
No, por desgracia no. En general no hay gente que esté del todo preparada en los organismos, sacando los financieros o que manejan caja propia como AFIP o ANSES. En esos hay un mejor nivel, tampoco quiero decir que sea un nivel excelente, pero mejor.
En lo que respecta a capacitación, la que existe es la más barata, rápida y también, menos efectiva. Hay capacitaciones efectivas que se podrían hacer, por ejemplo armar un simulacro efectivo de ataque, pero no se hace nunca eso. Quizás porque requiere una logística que no se dispone en los organismos, imagínate que si querés hacer por ahí una simulación real, real, tenés que frenar toda la operatoria, recuperar todo, ver si levantaste todo, etc.

¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?
No, por desgracia existen muchas licencias vencidas y la mayor parte de los equipos están obsoletos. Esto pasa en todos los organismos. Pero es por un tema de costos, tener el equipo actualizado sale muchos miles de dólares y un país como Argentina que no los tiene, lo hace más difícil. Sumado que las soluciones de software como firewall, no es algo que compras y es tuyo. Estás bastante preso de tres, cuatro empresas que te ofrecen software enlatados, y se ocupan de parchearlo constantemente, entonces te cobran el mantenimiento porque te están

dando todo el tiempo actualizaciones.

¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?
Depende mucho de cómo esté implementada. Y ahí es donde entrarían políticas a nivel nacional. Yo ahí sigo pensando lo mismo. Necesitas una agencia a nivel nacional que sea la que regule, la que regule todo lo que es la coordinación a nivel seguridad, porque es un cross. Lo que sucede es que cada organismo termina haciendo lo que quiere o puede, y se multiplican las posibilidades de error. Por ejemplo, el Gobierno de la Ciudad ciudad con RENAPER se maneja de una manera, pero las provincias con RENAPER se pueden manejar totalmente diferente, no hay nadie que diga algo específico. Sumado a eso, cuando cambia la gestión, cambian las autoridades y nadie se acuerda de lo que pasó porque en muchos casos cambian las personas y la información se va con ellas.
En Estonia desarrollaron una herramienta que se llama X- Road, que sirve justamente para conectar servicios de distintos organismos en forma segura y en forma orquestada de manera razonable. Esa es una herramienta que está testeada, homologada, y ya implementada en otros países con mucho volumen de trabajo. Pero para hacer algo así se necesita decisión política.

¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?
En general los SOC lo que tienen es un trabajo de detección, no de prevención. Entonces sí, creo que de tenerlo lo hubiéramos detectado por ahí de una manera más certera y con mejor calidad de información. Por ahí hubiéramos actuado más rápido en cuanto empezaban a salir algunas alertas tempranas. Pero un GSOC solo a nivel nacional no iba a ser útil en términos de prevención.

¿Consideras que el marco jurídico existente proporciona una base sólida para garantizar la protección de la información que tutela la APN?
El marco jurídico que tenemos no soporta bien todas las todas las necesidades actuales. Es algo muy común que la tecnología vaya a una velocidad, y el avance legal vaya a un tercio de esa velocidad. La última ley de tipificación de delitos informáticos es del 2008 y está basada en la que son delitos físicos. En el caso de la ley de datos personales, ya tiene sus años. Desconozco detalles porque no soy especialista pero sé que hay proyectos de actualización.
También creo que se debería actualizar la Resolución 641, porque fue redactada en base a la ISO ya desactualizada siendo que hay versiones posteriores. Otra de las cosas que se deberían actualizar es la obligatoriedad de los organismos de reportar al CERT, también clarificar en la normativa cuáles son las responsabilidades del CERT y mismo contemplar normativamente la coordinación con otros CERTs a nivel provincial por ejemplo.

Hay un montón de cosas que están es que si no bajan con una ley, con una obligación, no me parece que vayan a avanzar de ninguna manera. En la nueva ley de ciberseguridad de Chile, se establece que tenes que reportar en las primeras 3 hs el incidente, y durante los siete días posteriores el organismo afectado tiene que explicar en un reporte de qué manera lo está

resolviendo y se resolvió, si no lo hacen hay una sanción monetaria y es muy cara. Nosotros tenemos 72 hs de plazo, y no hay una obligación después para el reporte final.

¿Consideras que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?

Yo creo que una entidad superior debería establecer una gestión del riesgo correcta, definiendo el valor de los bienes de los organismos, ya sean datos, servicios, equipos, todo lo que consideren que tiene un valor. También a nivel nacional alguien tiene que encargarse de coordinar y capacitar en el caso de que necesite al organismo. Pero cada organismo después tiene que ocuparse de armar sus propias políticas. Se baja una política general a nivel nacional, donde se fija la estrategia del Estado y esta política de ciberseguridad de cada organismo es la que acompaña ese objetivo.
Por ejemplo, si como Estado se pretende hacer crecer las exportaciones de gas natural, lo que tengo que definir primeramente es una infraestructura crítica, que sea todo el gasoducto y todo lo que esté relacionado con la cadena de producción. Entonces, a partir de que yo defino esa infraestructura crítica, interactúo con los organismos asociados y les digo qué objetivos tienen que cumplir en base a esa estrategia nacional.

¿Desea agregar algo que no se haya preguntado?

Para mí ciberseguridad es trabajo mancomunado. No se pueden tener objetivos o dependencias aisladas o equipos de trabajo aislados, siempre tienen que estar en comunicación. Esto es una red, mientras más aceitada esté la red, mejor va a funcionar.

Informante clave N° 2 - Directiva de la Fundación Vía Libre

¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?
En el caso de Renaper específicamente, la pandemia no es un elemento diferenciador, como sí podría serlo en otros trámites que se digitalizaron o en otras bases de datos que sí crecieron a raíz de la pandemia.
A mí me parece que hay una cuestión estructural del Estado argentino que trasciende al RENAPER, pero del cual el organismo no es ajeno, que tiene que ver con un vacío absoluto de políticas de seguridad de la información. Existen algunas resoluciones y documentos burocráticos que dicen que hay que tener un responsable de seguridad en cada ministerio, y cosas por el estilo, pero más allá de eso, hay un vacío de política pública de seguridad de la información, y el RENAPER es un ejemplo más en ese vacío. Creo que falta de convicción política de que esto es una necesidad del Estado y junto con ella, la sabida falta de presupuesto que trae aparejada.

Un factor institucional relevante y particular del RENAPER creo tiene que ver con las consultas, parecen casi una canilla abierta a cualquier organismo del sector público y privado que vaya a buscar información y eso me parece un problema de protocolo no menor.

Esto que te digo lo evidencia no solo este incidente, si no uno que estuvimos siguiendo de

cerca y que está documentado en la justicia. Es el caso del acceso a los datos biométricos que tuvo el Gobierno de la Ciudad Autónoma de Buenos Aires a raíz de la utilización del sistema de reconocimiento facial. Cuando se investigó qué estaba pasando con el sistema de reconocimiento facial, se detectó que el Ministerio de Seguridad del Gobierno de la Ciudad, había accedido a nueve o diez millones de datos biométricos de personas del RENAPER, incluso personas relevantes de la vida pública. Fue bastante escandaloso y tuvo que ver con que el RENAPER, no ponía ni tenía un control sobre qué datos biométricos se estaba llevando el Ministerio de Seguridad de la Ciudad.

¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?

No quiero cargar las tintas sobre el personal, en particular considerando la situación en la que está el personal del Estado, no sólo en la que está atravesando en este momento, sino históricamente. Desde hace muchos años, está instalada esta idea de que hay que achicar el Estado y que hay que reducir los costos, reducir los salarios y demás. Y me parece que hay áreas sensibles, sobre todo las áreas que administran datos personales de la ciudadanía, en las que debería invertirse más, no menos.

¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?

Me parece que en general el Estado responde a esta lógica de falta una política, falta inversión en recursos humanos, faltan protocolos y por supuesto, faltan también inversión en seguridad de la información. A ver, Argentina no tiene, como tienen otros países, una oficina especializada que se dedica a esto y que baje una línea. Argentina además tiene la característica de que cada organismo hace lo que puede con lo que tiene. No hay una política integral de seguridad de la información.

Por ejemplo, en Alemania o Francia, existen oficinas dedicadas a eso, que son las que marcan la línea de cómo se tiene que proteger la información al resto de las oficinas. Uno no puede esperar que el ministerio de Salud por ejemplo tenga su política de seguridad, que el ministerio de infraestructura tenga la suya, tiene que haber un ente especializado que baje política y eso tiene que ser profesionalizado, con presupuesto y capacidad de inversión, y tiene que marcar la línea política de la seguridad de la información para todo el Estado. Eso en Argentina no sólo no lo tenemos, sino que ni siquiera está en el radar como una necesidad.

¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?

Hasta donde se supo, esta filtración tuvo que ver con la interoperabilidad con el Ministerio de Salud, había usuarios en ese Ministerio que tenían acceso y a partir de ahí se produjo. Asumiendo que fue así, esto deja en evidencia que los procesos de interoperabilidad generan una serie de riesgos importantes, aunque es claro que siendo RENAPER el organismo encargado de validar identidad, la interoperabilidad parece ser necesaria. Lo que está faltando, son protocolos claros de seguridad, una definición dentro de esos protocolos de quién y qué accesos tiene, un elemento que deje marcadas las manos de quien entra y quien usa los datos.

También que los funcionarios sean responsables de esos datos que usan. Creo que hay una grieta de seguridad y que se basa en problemas técnicos, estructurales e institucionales.

¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?
Definitivamente hace falta que exista una autoridad de seguridad de la información. Esa autoridad de seguridad de la información tiene que tener los más altos estándares técnicos, la más alta calidad en materia de acceso a tecnologías. Tiene que estar en la cresta de la ola, digamos, porque los ataques y este tipo de cosas son materia corriente hoy en día. Pero además tiene que tener cierta autoridad para cuestionar las decisiones en materia informática que pueda tomar un ministerio, por ejemplo, que cada decisión en materia informática tenga estándares mínimos de seguridad.

Y hay otro elemento que es importante, y es que la seguridad tiene que ser vista desde el punto de vista preventivo, estratégico, de construcción de capacidades, y no debe ser pensada desde el punto de vista policial. Muchas veces está esta lógica de confundir la ciberseguridad con el ciberdelito, con el cibercrimen, cuando son dos cosas que tienen que estar necesariamente separadas, porque la ciberseguridad es todo un protocolo preventivo, de construcción de capacidades, de diálogo con la comunidad. Una oficina de ciberseguridad tiene que estar preparada para recibir inputs de la comunidad, por ejemplo, para recibir denuncias de vulnerabilidades. Si se mezcla la ciberseguridad con el cibercrimen, cuando alguien reporta vulnerabilidades a esa oficina de ciberseguridad, termina siendo denunciado o corre el riesgo de una investigación penal, esto desincentiva el reporte de vulnerabilidades.

¿Consideras que el marco jurídico existente proporciona una base sólida para garantizar la protección de la información que tutela la APN?

Yo creo que necesitamos actualizar la Ley de Protección de Datos Personales en tres esferas. Uno de los elementos que es indispensable, es la obligación de notificación a los afectados que no existe hoy en nuestra normativa. Porque si se filtra información esencial como el DNI y el número de trámite, que sirve como validador de distintos servicios está comprometido, el Estado tiene que informarte para permitirte tener la potestad de tomar cartas en el asunto.

Además, la ley vigente tiene una cláusula que establece que las bases de datos tienen que tener un mínimo de seguridad de la información. Esa definición es un tanto vaga, porque no establece ningún marco claro de cuáles son esos mínimos de seguridad de la información. Bueno, eso debería ser mucho más detallado.

Por otra parte, también tenes que tener una autoridad de aplicación con la espalda suficiente para ordenar el cumplimiento de la ley, hacer auditoría sobre organismos públicos. Hoy la Agencia de Protección de Datos no tiene el poder para ordenar a un ministro cómo tiene que ser su política de seguridad, porque depende del organigrama de Jefatura de Gabinete y no tiene autoridad realmente sobre el resto del organigrama del estado.

¿Consideras que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?

No me lo había puesto a pensar a eso, pero mientras hacías la pregunta me vino a la mente algo que me parece que es importante. El organismo que fue atacado o que perdió una base de datos, muchas veces tiene que dar respuesta punitiva por los hechos y a veces puede tener ver con que hay negligencias internas. Entonces, si es el propio organismo el encargado de responder al incidente, muy probablemente, digo, no estoy diciendo que esto sea el caso de RENAPER, pero muy probablemente haya una tendencia a minimizar el incidente o a ocultarlo porque puede que quien está reportando el incidente o quien tiene que atender el incidente puede que sea el responsable mismo.

Muchas veces un incidente de este tipo puede costarte el puesto, o puede dejar en evidencia una gestión negligente del trabajo. Entonces me parece que ahí hace falta una autoridad que se ocupe del relevamiento del real alcance del incidente, de un reporte responsable del incidente, y de una atención responsable que incluya hacer cargo de las responsabilidades pertinentes a quienes corresponda.

¿Desea agregar algo que no se haya preguntado?

Quizás agregar que el RENAPER tiene un rol clave, junto con la ANSES, construye bases de datos que se solapan en muchas cosas fundamentales de toda la población argentina. Desde Vía Libre estamos elaborando un informe que saldrá pronto donde abordamos la historia de la existencia del RENAPER la doctrina que hay detrás de la existencia del organismo, las responsabilidades que tiene, y ponemos algunas cosas en discusión, como la existencia de un DNI, la posibilidad de poner datos, de capturar datos biométricos de manera permanente de todas las personas.

Informante clave N° 3 - Responsable del área de Tecnologías de la Información en el Ministerio de Salud de la Nación, al momento del incidente.

¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?

Un factor importante es que no está concientizado en la agenda política el tema de la ciberseguridad. Yo creo que existe un gap entre el riesgo existente, que crece año a año, mes a mes, por el desarrollo de los hackers, de cómo hackear grandes bases de datos, y el Estado que tiene otros tiempos, tiene otra agenda política y otra agenda institucional.
En el caso de Salud la pandemia fue un antes y un después, porque hasta ese momento la digitalización era muy escasa. Cuando llegó, no quedó otra, ahí había que digitalizar sí o sí; por suerte estaba todo preparado, había sistema de información, porque podría habernos pasado que no hubiera sistema software desarrollado para eso.
¿Y ahí qué empezó a suceder? Comenzó a haber mayor cantidad de información sanitaria que antes no había, y es una información que vale un montón de dinero en el mercado negro.

Otro tema son los planes de ciberseguridad a nivel institucional, no recuerdo la fecha exacta, pero había una normativa en la que la Dirección de Ciberseguridad que planteaba unas directrices para todos los organismos públicos, eso fue en el 2021 también, plena pandemia. Era un buen dispositivo para que cada uno de los organismos públicos vaya generando el suyo y empezando a invertir en eso. Lo que pasa es que ahí está el tema de los tiempos. Hasta que

un organismo público arma el plan de ciberseguridad, hace un plan de inversión y lo ejecuta, con los tiempos que existen administrativamente por normativa en el Estado, eso tarda mínimo dos años. Y en dos años, es tanto el avance tecnológico que pueden implementar los hackers que siempre vas a estar atrasado.

Y también hay una cosa más, como bien dice la normativa, la Dirección de Ciberseguridad plantea las directrices, pero no tenía gobernanza en cada uno de los Ministerios. Para que eso ocurriera tenía que haber otro mecanismo institucional o quizás concentrar la ciberseguridad en algún ente que tenga también facilidad en las compras públicas y la decisión rápida de invertir y tener equipos especializados en estos temas que no son fáciles de armar para un organismo.

El RENAPER me acuerdo salió a hablar sobre ese incidente, el Ministerio de salud no dijo nada públicamente. Está todo bien documentado en el expediente judicial, pero no es como dijo RENAPER que la filtración fue por Salud. Hay mucha historia que por ahí no salió de las noticias, pero no el tema no empezó en 2021, venía de antes también con otros incidentes que salieron a la luz. Pero ese fue muy visto, me acuerdo que salió una nota creo en el Cronista y se ve que habían sacado foto de un informe que elaboramos para el expediente judicial, porque en la nota mezclaron todo pusieron todo al revés, como ellos les convenía para decir, o sea, que había el súper agujero en salud, cuando no era así. Me di cuenta que porque usaban las mismas palabras y los mismos párrafos del informe.

¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?

No había ni hay un área que sea de ciberseguridad en Salud que documentara procesos, planificara acciones proactivas o hiciera mantenimiento proactivo. Una Dirección de Ciberseguridad casi no tiene que hacer nada tecnológico, es más hacer documentación de procesos y procedimientos, controles y sobre todo tener fondos para hacer test vulnerabilidad, contratar empresas o especialistas que te hagan esos test. Había gente especializada dentro del equipo que por una cuestión hasta una motivación individual podía estar al tanto de qué tecnología usar, pero no había algo formal. Lo que hacía esa gente era intercambiar con equipos más preparados como ARSAT, ahí hay un montón de potencial.

En el mundo en que vivimos actualmente, que todo es volátil, incierto, caótico, la tecnología irrumpe, nunca van a estar los equipos preparados para tener todas las competencias y habilidades maduras para enfrentar un ciberataque. Pero si hubiera una política de Estado que marcara una hoja de ruta concreta, los equipos se arman. El Estado tiene esa potencia de decir, tengo que capacitar a determinado grupo de personas en tal tema. Pero mientras no esté como priorizado en una agenda política y pública, no sucede.

¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?

Creo que no. Toda esa información viaja por VPN, viste, es una de las cuestiones hasta ahora más seguras. Pero hay proyectos tecnológicos que hubiesen ayudado a mejorar la ciberseguridad y no los está usando el Estado nacional. Hay otras formas también de ponerles capas a la seguridad, proyectos como el que utiliza el gobierno de Estonia. También hay

software de inteligencia artificial que te permite identificar y tener alertas de dónde están queriendo entrar, pero el ejecutivo nacional no avanza en este tipo de cosas.

Creo que ARSAT es una buena institución en quiere basarse. Cuando tenes la información alojada ahí, como organismo estás cubierto casi en el 99 % por temas de seguridad, porque la infraestructura de ARSAT está cubierta, pero no todos los organismos tienen la información en el centro.

¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?

Yo creo que no tiene relación la interoperabilidad con la ciberseguridad, sino la cantidad de datos y el valor de los datos sanitarios. Cuanto más datos tengas, en donde los tengas, o de personas, uno de los riesgos son los ciberataques, pero no la interoperabilidad. No, para mí no cambia la perspectiva.

¿Consideras que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?

Eso está normado. Cada organismo se tiene que hacer responsable. O sea, cada organismo se hace responsable. Hay siempre cuando hay vpn, intercambio información, hay acuerdos, términos, condiciones, digamos que eso está hasta por la ley administrativa, digamos. De los ministerios, de cómo es la organización de eso.

¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?

Existe un Centro en la Dirección de Ciberseguridad, el CERT. Ahí ellos hacen monitoreo de todos los organismos públicos. De hecho, un montón de veces ellos nos han llamado para avisarnos que nos querían hackear, porque están haciendo todo el tiempo monitoreo de las infraestructuras críticas, pero que formalmente no están en ningún lugar definidas. Si bien formalmente existe esa área, debería tener mayor inversión, cantidad de personal. Pero están dadas las condiciones formales para que tome este trabajo.

También un tema importante para mí es que hay que hacer una definición de cuáles son las infraestructuras críticas en el gobierno nacional y a partir de ahí darle más, fortalecer esas instancias. Digamos que si ves la normativa de las funciones y responsabilidades que tienen en la Dirección de Ciberseguridad, está resguardar y revisar cuál es la infraestructura crítica, algo que llevaba en su momento Jefatura de Gabinete, pero eso no ocurrió.

¿Consideras que el marco jurídico existente proporcionaba una base sólida para garantizar la protección de la información que tutela la APN?

Yo creo que hay un montón de normativas, pero me parece que la justicia no sabe cómo gestionar estos temas. No soy abogada, pero no sé si es que faltan las leyes, o falta que la justicia tenga gente formada para encarar estos temas. Porque en mi experiencia, me pareció

que en el juzgado a los delitos de ciberseguridad no los veían desde una perspectiva tecnológica. Los que lleven las causas deberían ser abogados formados en ciberseguridad y tienen que saber algo de tecnología. No podés resolver temas si no sabes algo de lo tecnológico.

A la brecha la veo más en el Poder Judicial que en el Ejecutivo, porque cuando se establecen acuerdos con otro organismo para compartir información, se firman documentos para estar resguardados. A los empleados también les hacíamos firmar acuerdos de confidencialidad, y un montón de cosas como para estar cubiertos de las responsabilidades y las obligaciones de cada uno. El tema es que después, si pasa algo, la justicia me parece que no sabe cómo investigar, cómo manejar estos temas. Tendría que ponerme a investigar, pero no conocí ningún caso de cualquier organismo que haya ido a la justicia y que la justicia lo haya resuelto.

¿Desea agregar algo que no se haya preguntado?

No, creo que tocamos todos los temas. Espero que te sirva.

Informante clave N° 4 - Socio del área de de Ciberseguridad y Responsable de la práctica de Cyber Incident Response en la empresa Deloitte, al momento del incidente.

¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?

A nivel institucional, el primer factor es que el RENAPER no tenía un responsable de ciberseguridad. La estructura del RENAPER, si uno la ve en el momento del incidente, había un área de tecnología con un responsable de IT, como un gerente de sistemas, pero no había nadie responsable de ciberseguridad. Ese es el primer punto. O sea, al no haber nadie responsable, se hacían todas las tareas relacionadas con ciberseguridad, pero no había nadie responsable a cargo.

Como segundo punto, al no tener a alguien responsable, todas las tareas que hay que hacer de ciberseguridad para proteger la información de los clientes, que obviamente estaba en el RENAPER, digamos, se iban haciendo, pero con la visión de IT, no con la visión de ciberseguridad. Entonces se priorizaba la rapidez, la disponibilidad de información, las integraciones, las velocidades. La visión de ciberseguridad es distinta.

Entonces, no había una estructura formal con responsabilidades claras, definidas. Segundo, no había una estructura de gente. Al no haber un equipo de ciberseguridad, tampoco se trabajaban en tareas de prevención y seguridad de los sistemas, no se le prestaba tanta atención de alguna manera. Sé que después del incidente pusieron un responsable de ciberseguridad.

Y el otro factor por el cual creo que el incidente llegó a suceder, es que no había medidas técnicas para detectarlo. No tenían herramientas de tecnología o de ciberseguridad para detectar, se enteraban cuando la información se publicaba en un foro, lo levantaba alguien del

mercado y le avisaba al RENAPER. Recién ahí recién es donde se empieza a investigar el incidente, pero el incidente venía de varios meses atrás.

La pandemia de alguna manera ayudó, potenció el tema porque los distintos organismos empezaron a consultar al RENAPER. Entonces, lo que hizo RENAPER fue desarrollar lo que llama una API. Una API es como un web services, que permitía a organismos conectarse a través de esa API y poniendo el número de documento, te traía la data. Formalmente se firmaban acuerdos con organismos y una vez celebrado RENAPER le armaba lo que sería una especie de VPN. A partir de ahí, el organismo justificaba cuantos usuarios necesitaba y el RENAPER los habilitaba. Algunos usuarios tenían permiso para acceder a cierto tipo de información, no a todo el conjunto de datos. Con ese usuario, la persona se conectaba vía web al sistema, colocaba el número de DNI y si era masculino o femenino; si el usuario y clave estaba configurado correctamente, del otro lado, RENAPER le traía la información de una persona. Es decir, yo no podía traerme toda la información, era uno a uno los DNI. Si lo ves desde el punto de vista de seguridad, está muy bien el modelo. El tema es que del lado de RENAPER no había ningún monitoreo o control.
No sé si me explico qué es lo que sucedió en el incidente. Cuando se investigó lo que había pasado, alguien desde las credenciales que tenía el Ministerio de Salud, a través de ese túnel VPN, armó un script, es un programa que se conectaba al web services, poniendo el número de documento, no sé, por ejemplo DNI 20.000.001 F (femenino), 20.000.002 M (masculino) y así sucesivamente. ¿Y entonces qué hacía el sistema? Le iba devolviendo los datos de todos, básicamente. ¿Se entiende? Cuando se investigó el incidente se vió eso, millones de consultas secuenciales y por la velocidad de las consultas, está claro que un script.
No sé cómo se habrán adquirido esas credenciales, una hipótesis que se barajaba era que alguien había hackeado el Ministerio de Salud y desde ahí se hizo la conexión. Que alguien haya entrado al Ministerio de salud revisó, revisó, llegó a una máquina y se llevaron toda la data. Esa es la hipótesis que más sonaba, de alguna manera. Porque justamente cuando se analizó, el usuario con el que se hacía la consulta, también era un usuario que hacía consultas en su trabajo del día a día. Vos veías el patrón de ataque a todas las consultas secuenciales, pero también venía que la persona consultaba, digamos, se usaba para hacer consultas generales.

La pandemia pudo haber influido, sí, influyó. Porque antes esa información estaba cerrada en el RENAPER y muy pocos organismos tenían esos acuerdos. Con la pandemia,empezó también todo el proceso de validación digital. Por ejemplo muchos bancos empezaron a ofrecer onboarding digital, ese onboarding termina en algún caso validando contra datos de RENAPER.

¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?
No, para nada. No estaban y tampoco lo están. Es un gran problema que tenemos los argentinos, porque pensá que en esa filtración se llevaron los datos de los 40 y pico millones de personas. Yo lo divido: hay recursos humanos para la gestión y para la preparación para proteger a una organización, después tenés recursos humanos para detectar un posible incidente, y tenés recursos humanos para gestionar un posible ciber incidente. Hoy el RENAPER tiene gente que está trabajando en proteger más la información, en eso mejoró pero en lo que es detección de intentos de intrusión y gestión, no.

Sintetizando, no. No había suficientes recursos humanos ni estaban capacitados.

¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?
La respuesta es no. Y todas las veces me tocó trabajar. En lo que es herramientas tecnológicas o tecnología, siempre el sector público está mucho más abajo de lo que es el sector privado, incluso por ahí en los organismos más "top", como sería AFIP o PAMI, que son los que por ahí tienen más recursos económicos, siempre están más abajo que el sector privado.
En lo que es herramientas de tecnología de ciberseguridad, yo lo separo. Existen herramientas que te permiten prevenir, por ejemplo, tener un muy buen firewall con capacidad para bloquear ataques.

Adquirir este tipo de software tiene todos los temas evidentemente de licitaciones, procesos, etc, lo que hace que se demoren los organismos tanto en comprarlo como en actualizarlo.

Después, otra tecnología que ayuda mucho es la parte de lo que son las soluciones DDR, detección, response, que básicamente, es un agente que vos pones en los distintos servidores que detecta si alguien cuando entra intenta hacer algo fuera de lo común. Son soluciones muy buenas pero yo no conozco a nadie de la Administración Pública que las tenga, probablemente porque son costosas.

Otro punto es el multifactor de autenticación, para acceder en forma remota. Muchos de los incidentes que han sucedido en el Estado, se originan comprometiendo usuarios y password en accesos remotos a sistemas. Hoy el doble sector de autenticación es clave. Hay organismos que los tienen implementados, sí, pero depende mucho de la persona de IT o ciber, que usualmente busca alguna solución open source.

Y después, una de las claves para detectar es hacer monitoreo. Podes hacer de todo para protegerte, pero cuando hay un incidente, la clave es que cuanto más rápido lo detectes, mejor. Para la detección, usualmente una de las herramientas que se utilizan es un SIEM. Lo que hace un SIEM es básicamente juntar logs y eventos y te los correlaciona, pero es un tipo de tecnología que prácticamente no existe en la Administración Pública Nacional.

Creo que es un combo complejo, porque por un lado está el organismo que no tiene las herramientas tecnológicas suficientes para prevenir ni para detectar, y después por otro, los recursos humanos están poco capacitados, con lo cual es un panorama difícil.

¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?
Totalmente. El primer proyecto que hicimos con RENAPER fue hace más o menos unos 20 años, nos contrataron en su momento para hacer una evaluación, y en ese momento el organismo tenía la ventaja de que los datos que guardaba, estaban todos cerrados, no había forma de sacarlos. Entonces vos ibas, pedías tu DNI o tu pasaporte, pero la información estaba cerrada. Durante todo ese tiempo que sucediera así, no hubo ningún incidente de fuga de información. Con la interoperabilidad y los acuerdos que se empezaron a hacer más personas pudieron acceder a la información, esto facilitó ese incidente y otros.
Con el diario del lunes, te diría que se podían haber implementado medidas antes del incidente pero que después obviamente se implementaron. Por ejemplo, este sistema (el SID) después implementó un control que no te permitía hacer consultas secuenciales. De la misma

forma se generaron sistemas para alertar las búsquedas de DNIs que ellos llamaban “VIP” por ejemplo el del presidente porque no es común que ciertos tipos de documentos se tengan que consultar. Estos casos de uso se armaron y se implementaron después del incidente.

¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?
Yo creo fervientemente que sí. El tema es que ahí depende ya no solo de los organismos sino del país. Argentina fue pionera en crear el Arcert, pero ese equipo tuvo su ciclo. Yo siempre planteo que nunca hubo un plan estratégico. Hoy la Argentina debería tener un *government* SOC, pero te lo subo un nivel más. Para mí la Argentina debería tener lo que sería como un centro coordinador de equipo de respuesta ante incidentes en general. Abajo puede haber un centro común de monitoreo gubernamental, pero tengo que decir que para mí el GSOC también es una moda. En el mundo cyber cada equis tiempo tenés modas.

Por eso yo lo que veo como estratégico en Argentina o cualquier país, es tener un centro de coordinación de respuestas de incidentes a nivel gubernamental. En base al modelo FIRST, hay distintas capacidades que vos que podés tener, tanto preventivas como proactivas. Dentro de las preventivas tenes capacitaciones, explicar, ayudar, dar cursos, herramientas, conseguir licenciamiento (para eso podes hablar con distintas empresas y entablar acuerdos).

Y después está la parte más proactiva, cuando ocurre el incidente. Los organismos muchas veces no tienen a quién recurrir dentro del gobierno, porque no hay muchos recursos más que enviar una guía u ofrecer un mail, o sea no hay ayuda técnica. Entonces los organismos generalmente recurren a empresas, por ejemplo en el caso de este incidente llamaron a Deloitte. Entonces lo que deberían tener es, en la parte proactiva, sí, un equipo técnico que vaya ayudando en cada incidente. Después, obviamente, este equipo podría ayudar al sector privado.

¿Consideras que el marco jurídico existente proporciona una base sólida para garantizar la protección de la información que tutela la APN?
No soy abogado, no estoy en ese mundo pero sé que las entidades públicas tiene que cumplir ciertas cuestiones. Desde la Dirección de Ciberseguridad habían salido unas resoluciones o declaraciones, no sé cómo es el nombre técnico exactamente, que recomendaban u obligaban ahí no sé la diferencia, a toda entidad pública a tener su área de seguridad. Pero la realidad es que las entidades estatales después no la llegan a cumplir.
No la llegan a cumplir no porque no quieran, sino porque a veces me ha pasado la inversa, estar por ahí en alguna entidad pública, y que me digan “mirá, tengo que cumplir con todo esto, no tengo recursos, no tengo gente, no tengo equipo, no tengo tecnología” y quizás quedan expuestos ante chequeos, con un nivel de madurez muy bajo. Ahí la responsabilidad es de cada organismo, pero mi sensación es que los que están más arriba sean más conscientes de esto, o como pasa en otros lugares, que sean responsables. Si, hay un incidente en una compañía privada, en muchos casos he visto que al CISO lo echan, ¿se entiende? En el Estado jamás lo vi, nunca.
Apunto a que por lo menos la línea está, o las políticas están, pero no se cumplen. No sé cómo son los mecanismos para que se cumplan, pero a los organismos les cuesta después

cumplirlos.

¿Considera que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?
Mira, te cuento que pasa en el sector privado, que quizás sirve para pensar o ponerlo como ejemplo. Nosotros, éramos un equipo de Incident Response con 15 personas,que hacíamos actividades preventivas, digamos, respuestas, investigaciones, todo, todo ese proceso, 15 personas dedicadas a eso. Y después teníamos muchos clientes que eran de distintas empresas. Si lo llevamos al Estado, era como que imagínate, damos algo supra nosotros y después están las distintas entidades estatales por debajo y las empresas del Estado.

En el sector privado existe lo que se llama el servicio de retainer. Más allá de hacer tareas proactivas, como empresa podes contratar este servicio que incluye tener a disposición un grupo, a nosotros, para tener el teléfono rojo y llamarlo 7/24. Entonces muchas empresas decían, bueno, yo hago mi procedimiento, pero tengo el contrato retainer para que si me pasa algo a la 1:30 a.m., levanto el teléfono, y viene en 40 minutos hay un equipo acá que está trabajando con nosotros.

Yendo a tu pregunta, lo ideal es que cada organismo tenga un equipo de ciberseguridad que trabaje en sus capacidades de ciberseguridad generales, y que más arriba haya un equipo de acciones proactivas, que sea como esta línea roja a la que los organismo puedan llamar. Ese modelo funciona muy bien en el sector privado. Y esto tiene la ventaja de que el que está más arriba vé todo el bosque, no sólo el árbol. La entidad afectada sólo ve lo que le pasa, en cambio cuando vas arriba te pueden decir si justo el que te atacó es la misma banda que atacó a otro. Entonces por ahí se saben las técnicas, prácticas y procedimientos y hay más herramientas para ayudar.

La tendencia mundial en algunos otros países es que los Equipos de Respuesta ante Incidentes tiene actividades proactivas. Dentro de las actividades proactivas, existe el famoso GSOC, un centro de monitoreo que sirve también para organismos más chiquititos que no tienen capacidad para implementar un SIEM, y entonces pueden contratar el GSOc para que los logs los mande ahí. Entonces se conforma un equipo arriba, más grande con las atribuciones para que, si pasa algo, rápidamente cuente con los recursos para reaccionar.

¿Desea agregar algo que no se haya preguntado?

Creo que en síntesis al sector público le cuesta mucho más que al sector privado mantener esos niveles que conversábamos, el legal, el tecnológico y el humano. La tecnología le cuesta más comprarla y mantenerla. También el tema de cumplir con las regulaciones. Y en la parte humana contratar gente, capacitarla, retenerla, cuesta mucho en ciberseguridad y particularmente en lo que sería team response.

Como lo veo yo, viene costando más, y creo que en los próximos años va a costar más todavía. Entonces, si el Estado no hace algo, me refiero a crear este centro, o invertir en recursos para que eso pase, la tendencia va a ser a que cada vez va a haber más incidentes en

el sector público, más que en el privado.

Informante clave N° 5 - Docente e investigadora en ciberseguridad y seguridad de la información, directiva del Programa Seguridad en TIC en la Fundación Sadosky

¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?

Sí, claramente la pandemia fue un factor relevante en todo el mundo y en Argentina también. ¿Después, qué factores institucionales? Yo creo que la falta de un equipo de respuesta incidente sólido es un factor muy relevante porque es la parte operativa siempre.

En términos de gestión tenemos una gobernanza, dirección o como le quieran llamar, una parte de gestión que es, digamos, cómo implementar. Después en términos de ciberseguridad hay un componente muy determinante que es la operación. Nosotros en Argentina tenemos unas normas preciosas, un montón de documentos y políticas, instrucciones, instructivos, pero no tenemos operación, no vamos a ir a ningún lado. Y lo digo en términos de seguridad de la información y ciberseguridad.

Si tenemos solo operación tampoco sirve, porque lamentablemente si no tenés una instrucción, un mandato o la posibilidad de interacción y coordinación a nivel de gestión, tampoco funciona. En una organización, tenés una cabeza, un objetivo, no hay mucho más problema; en cambio la administración pública, la necesidad de una gestión coordinada, tiene muchísimo más peso. Entonces necesitamos operación, operación desde un área específica como ciberseguridad, pero además operación en los distintos organismos públicos.

Necesitamos capa de gestión y adicionalmente, un mandato que permita llevar adelante ciertas acciones, ese mandato se lleva a cabo en los países a través de leyes o decretos. En principio Latinoamérica empieza por decretos, porque los Ejecutivos se dan cuenta de que esto es necesario y en general la regulación se da a través de Decretos. Justo estoy colaborando con una consultora internacional ahora que está haciendo un análisis de la ciberseguridad en América Latina y el Caribe y veo un montón de historias parecidas.

La evolución del tema generalmente presiona a los países para regular a través de una Ley. A mí en un principio me parecía que una Ley era súper importante, pero hoy se podría decir que tener una Ley sin tener bases operativas y de gestión medianamente sólidas, tampoco nos va a servir. Porque de cara al público en general, al sancionar una ley es como que “ya está”, y eso sería un riesgo aún peor. La ley es un mandato, pero necesitas mucho antes tener esto, operación y gestión y coordinación. Al abarcar tantos temas la ciberseguridad, me parece que dentro de las administraciones públicas, cómo se coordina es clave.

Entonces como factores determinantes institucionales, me parece que está el tema de la operación en términos de seguridad informática y de seguridad de la información. Vos tenés todo lo que es seguridad informática, que si bien no hay una frontera específica, siempre es como el Computer Security, todo lo que tiene que ver con el software, el hardware, las redes, la infraestructura. Y después tenés la seguridad de la información, que es la información independientemente del soporte, involucra la revisión de todos los procesos en cómo se

gestiona la información. Pero bueno, en ese contexto tenés la seguridad informática y tenés la gestión que es un poco más amplia, que es la seguridad de la información, pero van juntos.

Y después, bueno, tenés gobernanza. Al momento de dictar la Resolución 641/21, no haber asignado a un responsable también tiene mucho peso. Si vos no asignas responsabilidades tu alcance es muy limitado. ¿A quién se asignaron esas funciones? A las áreas de sistemas. Y la verdad es que eso no es una buena práctica. La normativa debería haber creado un cargo en cada área como responsable, pero hacerlo implica erogaciones y esto muchas veces es un impedimento. En ese contexto también institucional, no tener un responsable es de alguna forma no reconocer institucionalmente que el tema amerita un cargo. ¿Se entiende? Si no tenés ni siquiera un responsable, se diluye mucho todo lo que es gestión. Resumiendo, me parece que más allá de que nosotros tenemos una tradición de dictar normas para regular algunos aspectos de la ciberseguridad, nunca hubo responsabilidades claras asignadas en la materia.

¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?
Salvo ANSES, el Banco Central, AFIP y probablemente algún otro organismo robusto, así como algunas pocas provincias que en sus administraciones públicas provinciales hay gente capacitada y procesos con un grado de madurez aceptable, digamos, en general los recursos humanos de los organismos no están preparados para responder ante incidentes.

Sé que se hizo un pedido de acceso a la información pública por el incidente y una de las cosas que contestaron desde el RENAPER es que el acceso fue con credenciales válidas, entonces no se lo consideraba un incidente. No sé si es una tomada de pelo o una negligencia del que lo contestó. Se deberían controlar todos los accesos que se hacen a RENAPER, y (no sé si hoy sigue igual), pero en su momento el organismo bajo acuerdo, delegaba responsabilidades de seguridad en los organismos que le solicitaban información. No es una práctica delegar este tipo de cosas, hay que tener cierta debida diligencia. En términos de lo que hoy se llama ataque a la cadena de suministros, eso es impensable. Imaginate si una empresa dice: “ Ah, no, yo era muy segura, el que era inseguro era mi proveedor”. No existe esa respuesta y esa responsabilidad no podría haber sido delegada por contrato.

Creo que el problema está en que se pone a la seguridad de la información dentro de lo que es el área de sistemas, cuando en realidad tienen objetivos diferentes. La recomendación de que estén en áreas separadas, es porque hay oposición de intereses. El que desarrolla en general desarrolla, quiere que el sistema funcione, y si tiene una fecha de entrega, va a tratar de cumplir con los requerimientos del cliente en cuanto a funcionamiento y los tiempos. En el caso de seguridad, el objetivo primordial es garantizar la integridad, la disponibilidad y confidencialidad de la información. Entonces los intereses a veces son opuestos porque a la seguridad le interesa que sea seguro, independientemente cuando tenga que salir. La recomendación es, precisamente, que las áreas de seguridad no dependan de sistemas, porque cuando vos tenés que sacar un producto, un servicio o dar el visto bueno, si seguridad está dependiendo del sistema, como que no tiene peso. Por eso siempre se habla de que sean independientes.

¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?
La verdad es que no tengo datos del organismo, puedo darte un comentario general de ese

tema. La seguridad requiere inversión, no se puede hacer seguridad sin inversión en personas y sin inversión en tecnología. Las licencias por software, hardware salen mucha plata, y el Estado debería hacer elecciones óptimas, en términos de funcionalidad, pero también económica. Esto requiere bastante coordinación. Yo creo que hay software que debería coordinarse para que sea software libre, pero en general ya depende más de tecnología que de ciberseguridad.

Hoy tener sistemas operativos actualizados, y tener todo tipo de aplicaciones actualizadas, de las cientos de actividades que tiene la ciberseguridad, creo que es uno de los tres primeros. Entonces, si vos dependes de licencias muy costosas y muy diversificadas, y no podés actualizar sistemas o aplicaciones, o cualquier tipo de aplicación crítica, estás teniendo una debilidad. Entonces, esas decisiones deberían ser evaluadas a niveles estratégicos, en el corto, en el mediano y en el largo plazo. Porque finalmente tenemos cierta antigüedad, cierta historia para tomar algunas decisiones.

¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?

Depende de la implementación. Hoy hay formas de desarrollar sistemas que puedan ser interoperables y seguros. Seguros siempre bajo un nivel de riesgo aceptable, no hay seguridad 100 %, lo aclaro.

Mal incorporada la interoperabilidad, amplía la superficie de ataque. Pero la interoperabilidad y la seguridad, además de darse en el contexto de las tecnologías, también tiene que darse en el contexto de los procesos y de la cultura de la organización, concientizando sobre riesgos como el phishing que sigue siendo la puerta de entrada al ransomware más grande o chico.

¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?

Yo creo que en nuestra idiosincrasia en particular, un SOC centralizado no lo veo eficiente. En países chicos o en ambientes chicos, sí. Además de ser un país grande, tampoco tenemos una organización ministerial estática, fijate que de 22 ministerios ahora pasamos a 9, y mañana quizás sean 15.

Porque el SOC es una operación, es centralización de eventos, tecnología básicamente. Entonces para vos analizar un montón de eventos, necesitas que el sistema entienda todo lo que les llega rápidamente. Cuando cambias los sistemas, o la identificación de los organismos y de las personas que acceden, esas transiciones necesitan una adaptación que me parece que, digamos, termina siendo un shock. Vos la tecnología la necesitas para la respuesta a incidentes, pero lo que necesitas muchísimo más es tener gente que entienda de qué se trata un incidente y tener concientizado desde el Ministro hasta la persona que hace las tareas de mantenimiento, de lo que es un incidente. Eso es muchísimo más importante.

Claro que para eso tenés que tener procesos, también divulgación de la información, en un sentido que permita que sea accesible y entendible por todos. También tenés que tener

procesos que sean prácticos, no se trata de escribir documentos y publicarlos, se trata de que puedan llevarse a la práctica.

Creo que la clave está en que se entienda la gravedad de un incidente, porque realmente puede dejar al organismo sin que funcione. En las áreas de tecnología tienen que saber que ese incidente puede dejar sin servicio toda una estructura. El SOC podría venir después, pero hoy creo que falta generar más concientización en los recursos humanos sobre la importancia que tiene la información y que eso se traduzca en una mejora de procesos. En nuestro nivel de desarrollo, de madurez, todavía nos falta entender cuál es el problema.

Además, si tuvieras todo un sistema interconectado e interoperable, probablemente sí serviría un SOC, porque todos los eventos que se producen en ese sistema se pueden analizar y probablemente se pueda hacer un tratamiento, y una respuesta técnica más apropiada. Pero en nuestro contexto actual, hace falta un montón de actividades no técnicas o de desarrollo de tecnología "inside" en cada uno de los organismos primero, para después conectarlos, agregarlos.

¿Consideras que el marco jurídico existente proporciona una base sólida para garantizar la protección de la información que tutela la APN?

Sí, yo creo que sí.

Si uno piensa en una ley, y en qué debería abarcar una ley, esto tiene que ver básicamente con la protección de las infraestructuras críticas o de los servicios esenciales. Y después hablar de la ciudadanía. Entonces ahí te queda la Administración Pública como una de las infraestructuras críticas, y la ciudadanía ahí como todo otro tema que tenés que tratar. La administración pública es infraestructura, redes y servicios que hay que dar al ciudadano, pero por otro lado está la persona en su familia.

Para dotar a todo ese sistema de talento, hay que hacer fuente de hincapié en la educación. En tener planes de formación, no solamente de carreras, sino de oficios. No necesitamos todos ingenieros en seguridad, necesitamos gente que desarrolle seguros, que haga test de inclusión, carrera, formación práctica, técnica, teórica, gente que entiendan en estándares, etc.

Por otro lado, necesitas industria. Los frameworks de análisis de ciberseguridad como el de NIST o el de Oxford que usan el BID y OEA para medir el nivel de madurez de los países abordan estas cuestiones (formación de talento, industria) desde la perspectiva de alentar un mercado común. Estos marcos no están hechos bajo el eslogan de proteger a la ciudadanía, sino de promover un mercado, partiendo de la idea de que sin ciberseguridad se desalienta el mercado. Ese es un fundamento que en Argentina no se escucha ni se promueve, quizás porque no se ve o no se entiende. Porque finalmente la ciberseguridad importa en términos de que representa pérdida de plata, pérdida de recursos. Entonces me parece que también está ahí por el lado jurídico de cómo se va a dar el enfoque.

¿Considera que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?

Esto no es una novedad, no hay mucho que inventar. Si se derrumba una columna en un organismo, va a ser responsabilidad del funcionario que estaba a cargo y de todo lo que tuvo que haber hecho antes para que no pase. Si se roban una silla, va a ser hacer responsabilidad de que tenía a cargo la silla. Bueno, en esto es lo mismo.

Riesgos, seguridad e incidentes, son tres formas de ver el mismo problema. El análisis de riesgo, la gestión de los controles de seguridad y la respuesta al incidente. Para vos tener una respuesta a incidentes aceptable, tuviste que haber hecho seguridad de la información, es decir, controles, análisis, con todas las medidas que supone.

Este combo de seguridad de la información viene con un combo al mismo tiempo de protección de datos personales; que en mi criterio personal en Argentina pareciera que son planetas que no se tocan, cuando en realidad las recomendaciones internacionales hace tiempo que lo dan como algo natural. La OCDE lo dijo en 2014, por ejemplo, que los equipos de respuesta a incidentes a nivel nacional deben asistir en los incidentes de protección de datos personales. Quiero decir, es el mismo hecho que Datos Personales lo ve con una perspectiva, seguridad con otra perspectiva, y en el campo de los delitos se lo ve con otra perspectiva. Pero es el mismo hecho. Entonces, la coordinación entre agencias debería ser mucho más aceitada, ante un hecho el funcionario debería ir a la Agencia de Protección de Datos y a la Dirección Nacional de Ciberseguridad para informar, y a la oficina que lleve la investigación del delito y denunciarlo. Es un tema en gran medida de coordinación, porque con los recursos existentes podés hacer un montón.

¿Desea agregar algo que no se haya preguntado?

No, creo que ya fui aclarando todos los puntos. Gracias.

Informante clave N° 6 - Especialista en Ciberseguridad en el Banco Interamericano de Desarrollo (BID)

¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente de ciberseguridad por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?

Yo creo que el tema de las capacidades en ciberseguridad es un esfuerzo que es muy transversal. Todos sabemos que requiere de personas, requiere de procesos, requiere técnicas, pero lo más importante es que implementar medidas para aumentar la capacidad en materia de ciberseguridad en la organización, requiere mucha gestión del cambio y toma mucho tiempo. Eso significa que si hoy yo me pongo con todo a trabajar en mejorar la capacidad en ciberseguridad de mi organización, con suerte voy a poder ver algún tipo de cambio dentro de un año y medio.

Habitualmente, en casi todos los países de la región ocurre que las organizaciones no tienen esas capacidades desarrolladas, ni el equipo humano para trabajar en ciberseguridad, ni los procesos de gestión de riesgo, de prevención de fraudes, de detección de incidentes, están desplegados. La tecnología yo creo que quizás no es el mayor de los problemas, pero si querés también es un factor que falta.

La pandemia lo que hizo es acelerar la transformación digital, yo desde los años 90´ no había visto una transformación tan grande en tan poco tiempo. Ese cambio, acompañado de que los procesos y las capacidades de ciberseguridad no estaban desplegadas, generó un conflicto que se puede resumir en: si tengo que esperar a tener capacidades en ciberseguridad para poder hacer esta transformación digital, la voy a poder hacer dentro de dos años; en la toma de decisión se optó por tomar los riesgos.

Me parece que el proceso más importante desde el punto de ciberseguridad es el proceso de riesgo. Si tengo ese proceso, a la hora de hacer un cambio, yo puedo conocer qué nivel de riesgo voy a tener y qué nivel de riesgo estoy dispuesto a aceptar. Muchas veces por compliance existe, pero infelizmente suele ser el proceso más defectuoso, quizás porque es muy subjetivo.

En la toma de decisión a veces es ¿Nos transformamos digitalmente y seguimos funcionando sabiendo que no tenemos las capacidades suficientes en ciberseguridad, o no nos transformamos y no podemos ofrecer los servicios? Me parece que lo que ocurrió en ese incidente, por la fecha en la que ocurre, por el contexto en el que ocurre, está muy asociado a eso.

¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?
La estructura organizativa de las administraciones públicas de toda la región, y por lo que yo he visto en el caso Argentina coincide también, no contempla la ciberseguridad como un área sustantiva. Claramente las áreas de tecnología existen y lo que es infraestructura ahí mismo. Sin embargo, la ciberseguridad como estructura no aparece.

Tampoco existe desde la perspectiva del servicio civil un grado profesional de funcionario público, que para acceder a él se tiene que tener estas habilidades, que también tenga determinadas escalas salariales. Lo que sí existe es una cantidad de gente con muchísima voluntad y ganas de trabajar que se pone el tema al hombro y de forma ad hoc llevan adelante la ciberseguridad, pero más allá de las capacidades individuales, es un tema estructural.

En Argentina, hay resoluciones que indican que debe existir una persona como punto de contacto de ciberseguridad en los organismos, pero muchas veces no están los recursos, no son adecuados o los perfiles no son los correctos. Si pensás esta situación comparada con NICE, que es el National Initiative for Cybersecurity Education de EE.UU, ellos ya definieron, mandaron a un laboratorio definir todos los perfiles, los roles que tienen que tener, las habilidades necesarias. Veo un gap muy grande todavía en los países.

¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?
Yo creo que los recursos tecnológicos como infraestructura, como tecnología pura, no es el mayor problema. En general los recursos tecnológicos como infraestructura, como de vuelta, licencias, software, eso se adquiere, se precisa dinero nada más comprarlos, no lo veo como el factor más crítico. Me parece que la otra parte, la parte de capital humano y de procesos es la más difícil de implementar.

Las tecnologías son efectivas, si el firewall no bloquea, si el EDR (Endpoint Detection and Response) no bloquea, se produce el incidente. Pero si el sistema no bloqueó pero tiró una

alerta, la otra parte es analizar si tengo gente con tiempo para que pueda leer esa alerta, si alguien alguien que sepa leerla, si la leyó y la entendió, etc.

Me parece que la tecnología, si bien es fundamental y es la que va a tomar la acción final para impedir un incidente, no creo que sea el factor más grave, más crítico.

¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?
Siempre que se aumenta la superficie de exposición, aumenta el nivel de riesgo. Pero una vez que se aumenta la superficie de exposición, existen medidas de mitigación del riesgo, controles que lo pueden reducir al mismo nivel que estaba antes de interoperar, o incluso mejorar.

Tener una política interoperabilidad, un marco y medidas estándar de ciberseguridad, siempre van a mejorar la interoperabilidad. Ahora, la interoperabilidad requiere de confianza. Todos los actores que están interoperando tienen que confiar que la otra parte está produciendo información, no solamente de calidad y precisa, sino también protegiéndome con las medidas de seguridad que corresponden.

Creo que algo que mejora mucho es que evita la réplica infinita de bases de datos. Una interoperabilidad bien implementada, con todas las cosas que precisa su política, su marco, gente capacitada, plataformas y su tecnología, con niveles de ciberseguridad adecuados, mejora finalmente el factor de exposición.

Por ejemplo, RENAPER tiene la información sobre DNIs ¿qué pasa si RENAPER no interopera? Va a existir un organismo A, B, C almacenando esa información, haciendo la superficie de exposición mucho más grande y sin ningún tipo de control respecto a la situación. Entonces una interoperabilidad ordenada, con medidas adecuadas, no sólo creo que no aumenta el riesgo, yo creo que hasta a lo mejor lo reduce.

¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?

Bueno, yo creo que sí. Acá estamos hablando de la parte del proceso ya de detección y respuesta. Obviamente que la parte de protección de políticas de desarrollo de software seguro, evaluación de software, análisis, vulnerabilidad, eso podría haber prevenido. Desde el punto de vista de detección y respuesta, las fugas de información son procesos que toman mucho tiempo en producirse. Entonces, si en el momento que la fuga comienza porque está ocurriendo el problema, lo detecto rápido y corto, se puede reducir mucho el impacto. ¿Lo hubiera evitado un SOC? Posiblemente no lo hubiera evitado, pero hubiera reducido el impacto sin duda, y hubiera tenido una respuesta de mejor calidad.

¿Consideras que el marco jurídico existente proporciona una base sólida para garantizar la protección de la información que tutela la APN?

No, no es suficiente. Y de hecho, para hacer la operación de crédito hicimos un diagnóstico con un especialista que es abogado, él sí es abogado e ingeniero, y , no me acuerdo de memoria, pero él marcó una serie de puntos muy concretos, en relación a que tenía que ser mejorado para hacer adecuado el marco jurídico.

¿Considera que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?

Sí, bueno, de hecho tocaste un punto que es el gran tema de hoy día. Hoy Chile promulgó la ley que crea la Agencia de Ciberseguridad. Es un tema super discutido, el de los enfoques centralizados. Yo creo que ahí puede haber una discusión respecto a la parte regulatoria, si la regulación tiene que estar centralizada, la definición de política, la definición de estándar tiene que estar centralizada o se debería regular sectorialmente. La parte que creo que no puede entrar en discusión es la parte de gestión de incidentes. Fijate que el concepto de CERT o CSIRT se invita para gestionar incidentes, para coordinar las respuestas en sí.

El responsable final es la organización afectada, pero no hay duda de que tiene que haber una organización o una entidad centralizada que maneje y coordine todo desde el punto de vista regulatorio.

Hay una tendencia a centralizar el conocimiento y distribuir el enforcement, por ejemplo, se define centralizadamente la política de ciberseguridad, pero a la hora de hacer un ajuste o tomar una definición para el sector salud y hacer el enforcement, va la gente de salud.

Resumiendo, yo creo que la discusión más filosófica sobre centralizado o descentralizado, se separa en dos grandes funciones. Las funciones regulatorias, de supervisión, de fiscalización, etc. donde sí puede haber algún tipo de lugar de discusión si centralizado o descentralizado. Por fuera de eso, la parte de gestión de incidentes, tiene que haber una organización centralizada.

Creo que el nivel de responsabilidades y el nivel de atribución que tiene que tener esta organización centralizada requiere un ajuste del marco normativo y que no se puede hacer por resolución.

¿Desea agregar algo que no se haya preguntado?

Yo creo que volvería a la primera pregunta.

Un incidente es un momento reactivo muy bueno para ayudar a la toma de decisiones que favorezcan el desarrollo de capacidades de ciberseguridad. El fuego está prendido, todo el mundo está dispuesto a agarrar un balde y apagar.

Creo que el desafío está cuando no hay fuego, ahí donde tener, métricas, indicadores de performance, saber qué capacidad real tiene una organización, es fundamental.

Porque si mañana hay otra pandemia o hay algún otro cambio que dice hay que digitalizar todo de golpe, si yo no sé si tengo o no las capacidades, la toma de decisiones se va a hacer

desconociendo los riesgos. Yo creo que la mayor parte de la toma de decisión durante la pandemia se hizo sin evaluar siquiera.

Trabajar donde no hay fuego es lo que lleva más esfuerzo, y cómo motivar eso es el gran desafío. Incluso si tengo que capacidad tengo que conocerla, por eso lo importante de las métricas, indicadores y demás.

Informante clave N° 7 - Empleado del Registro Nacional de las Personas (RENAPER) al momento del incidente.

1) **¿Qué factores institucionales consideras que contribuyeron a la ocurrencia del incidente de ciberseguridad por el cual se vió comprometida información ciudadana en el Sistema de Identidad Digital (SID) en octubre de 2021? ¿Consideras a la pandemia como un factor relevante?**

   En primer lugar, se ve un crecimiento exponencial de las situaciones vinculadas con seguridad informática en organismos públicos y en organismos privados. Hasta organismos de vanguardia en términos de protección de la información, e incluso servicios de seguridad de países desarrollados han tenido algún incidente.

   La pandemia ayudó, porque en forma repentina y bastante masiva, se volcó al mundo virtual una cantidad de público sin tanto conocimiento. Esto generó gran cantidad de oportunidades para delinquir, para el fraude. Creo que sí hubo impacto y no solo en Argentina, sino a nivel global, vinculado con mayor tráfico, mayores oportunidades, negocios más grandes para los que están buscando de alguna manera tener algún crédito a partir de un delito de ese tipo, etc.

   Hay distintos factores, está el tema de la protección de datos, la parte más dura tecnológica (hardware y software que ayudan a resguardarse), y después tenés la parte de la cultura, de las prácticas. Las cuestiones de las prácticas tienen por lo menos dos cuestiones: una es la parte del diseño y el despliegue de las políticas, y la otra parte es la implementación. La implementación viene de la mano del cambio cultural, algo que en el Estado tiene sus dificultades.

   A eso se le suma la cuestión interinstitucional porque hacia dentro del Estado hay organismos distintos, que si bien forman parte del mismo Estado Nacional, tienen distintas conducciones y sus propias políticas. Pero además tienes los gobiernos subnacionales, las jurisdicciones provinciales y las jurisdicciones municipales. Todo eso genera eventualmente un gran entramado súper complejo, que tiene distintos tiempos, que institucionalmente es bastante heterogéneo y que no necesariamente están reguladas por el mismo poder de enforcement. La normativa que regula dentro del Estado Nacional, no regula un municipio o una provincia.

   Después, la forma en que se estructuran los servicios de datos. El sistema que se adaptó allá por el 2017-2018, fue un sistema que es lo que se conoce como Sistema de Identificación Digital (SID) que brinda servicios de datos a través de APIs que se interconectan con cientos de organismos públicos, privados, nacionales, provinciales y municipales, del poder ejecutivo, del poder judicial, o de los poderes judiciales y de los poderes legislativos. Nadie que no sea alguien del ecosistema de Identificación y Documentación de personas argentinas tiene un

acceso a la base de datos del RENAPER. Es decir, todos los que trabajan en registros civiles, o estén en un consulado en algún lugar del mundo argentino, por ejemplo tienen. Es una cantidad, está acotado ahí.

Dicho sea de paso, en la época del incidente se decía que los hackers habían accedido a la base de datos del RENAPER, y la habían bajado. Bajar la base de datos del RENAPER, no digo que sea imposible, pero es muy complicado.

Esa base cubre muchas cosas, no es solo el nombre, apellido, documento, la foto y el número de trámite, la información que hay en el DNI. También están las partidas de nacimiento, las relaciones interpersonales, familiares, huellas digitales, datos de contacto, trámites que hicieron dónde y cuándo los hicieron, etc. La base de datos es muy grande y al menos por ahora no hay antecedentes de que alguna vez haya sido hackeada.

RENAPER fue el segundo organismo de toda la Administración Pública Nacional que en 2021 diseñó, aprobó e implementó una política propia de protección de datos personales. Creo que el único que tenía una antes era la ANSES.

¿Cómo se otorgan los servicios de datos? A través de APIs, canales securitizados, con una VPN, con certificados, y con todos los mecanismos de seguridad o los esquemas de seguridad que habitualmente se utilizan para este tipo de cosas y que son del mundo más de la tecnología y de la informática. Para poder dar un servicio de datos se firma un convenio, y para firmar el convenio se pide una cantidad de requisitos, y dentro de esos requisitos está obviamente lo que tiene que ver con seguridad informática y protección de datos personales. Eso es dinámico.

Había distintos servicios de datos desarrollados históricamente y con una gran diferencia. El sector privado solamente tenía acceso a un servicio que en lugar de entregar datos por parte del RENAPER, solamente los recibía. Por ejemplo un banco, vos haces el proceso de validación de identidad con la app del banco, te sacas una selfie, pones tus datos, el RENAPER recibe esos datos y contesta sí es o no la persona, pero no salen datos de la Base de Datos del Renaper hacia los organismos privados.

En el caso de los organismos públicos es distinto. Hay un DNU de interoperabilidad en el sector público, que de alguna manera exige que en forma gratuita los organismos públicos compartan la información. Digamos que para hacer un Estado Nacional más eficiente necesitas interoperar. Las APIs vinieron a facilitar ese proceso de interoperabilidad que antes era muy complicado. En esa interoperabilidad que había con los organismos públicos, los servicios disponibles de RENAPER entregaban la información.

En el Ministerio de Salud, que a su vez habían armado un hub que tenía aproximadamente 52 grandes dominios (grandes dominios podían ser provincias enteras o algunas grandes instituciones), después esas provincias en esa red federal, tenían usuarios institucionales como puede ser un hospital, para que cuando necesitara alguna institución pública médica en algún rincón del país, poder validar la identidad. Como en el caso de los ministerios había cientos de usuarios institucionales, a los bancos, la lotería, educación, etc. Para darle potencia en escala, el esquema que se armó fue el de APIs, que permitía escalar mucho más que a través del otorgamiento de usuarios.

Para desarrollar la identidad digital, necesitas masividad. Y para lograr masividad, se armó este esquema de APIs en el que RENAPER brinda el servicio pero la red, estructura, responsabilidad, claves, y todo lo que sería la administración de tu infraestructura lo hace cada organismo, no RENAPER. Gráficamente sería como llegar hasta la puerta del organismo, hasta el IP del servidor, lo demás corre por el organismo con que se firma convenio. Considerando también que, en el caso de los organismos públicos nacionales se supone que debe haber cumplimiento de la normativa de Jefatura de Gabinete.

La red de Salud era muy grande, y con la pandemia explotó porque pasó a usarse para distintas cosas vinculadas a servicios remotos de salud, creo que tenía 52000 usuarios. Con muchas transacciones anuales, mensuales y diarias. Del lado de RENAPER ¿qué es lo que había? Estaban las API con los servicios de datos, las VPN, los certificados, todo lo habitual.

También había un monitoreo de flujo de datos. Por ejemplo, si se excedía un determinado flujo, saltaba una alerta y se cortaba. El problema es que al tener un hub tan grande el Ministerio de Salud, el nivel de transacciones habitual también era muy grande.

De alguna manera, el organismo que organiza todo ese sistema (en este caso RENAPER), queda condicionado o vinculado también a cómo gestiona la protección de datos y la seguridad informática cada uno de los organismos con los que se asocia, con los que firma convenio. Entonces ¿qué pasó en este caso? Alguno de los usuarios institucionales del Ministerio de Salud se comprometió, que hasta donde tengo entendido, ni siquiera fue dentro mismo del Ministerio, sino una de las provincias a los que le brindaban servicio.

Cuando se establece una arquitectura de red, como es un hub, se diversifica bastante y depende de cómo es la política de otorgamiento, control, remoción de certificados por parte de cada organismo. En la dinámica de entidades chicas como un hospital provincial, quizás se contrata una empresa, una pyme por ejemplo para asistir en la integración a los servicios. Una cuestión crítica en la práctica de la institucionalidad, es la gestión de los otorgamientos de permisos. Si bien hay políticas de seguridad, el desafío más grande es la implementación.

Obviamente al publicarlo en Twitter fue más fácil cruzarlo, pero nosotros, el RENAPER no llega al usuario final o sea a la IP de la persona que bajó la imagen o que entró la imagen, el RENAPER llega el IP institucional del Ministerio de Salud. Hay que tener en cuenta que para RENAPER, las credenciales habilitadas son las que el organismo le da al Ministerio de Salud, pero después el Ministerio de Salud otorga eventualmente a otros organismos y esos no trazaban, llega un momento que no podés recorrer todo el camino para atrás de los logs para poder llegar al IP final. Eso es lo que después trata de hacer la justicia pero es un trabajo muy difícil.

A partir de este incidente ¿qué se hizo? Bueno, se migró el servicio que se daba a los organismos públicos a uno como el que se daba a las entidades privadas. A partir de ahí se dejaron de entregar datos, para solo recibirlos y validarlos contra la base. Esto permite que ante un eventual evento, no aparezca la foto del DNI, en todo caso sólo la foto que se tomó a sí misma la persona. Además a todos los servicios se les implementó la marca de agua, salvo para algunos organismos como la Cámara Nacional Electoral que por ley deben tener la foto para construir el padrón electoral, o también algunos actores a los que es muy difícil restringir cierto tipo de información, como la justicia, la policía, etc. Para esos, se implementó la marca

de agua.

2) **¿Consideras que los recursos humanos de los organismos afectados estaban preparados para enfrentar incidentes de ciberseguridad?**

Yo creo que el contexto de recursos humanos en informática de estos últimos años fue muy difícil en el país en general, en todos los sectores, desde las grandes empresas, las pymes hasta el sector público.

Creció mucho el trabajo freelance para el exterior, en un marco de brecha cambiaria, con una Argentina muy barata en dólares, eso agudizó la situación.

De todas formas creo que la situación de los años anteriores ya era más complicada para el sector público. Hubo muchas estrategias para hacer manpowering de IT, pero hay que considerar que en los últimos 30 años pasamos de un Estado papel a un Estado digital. Hace 30 años se necesitaba un tipo de perfil de recursos humanos y hoy necesitas otro porque todos los servicios del Estado se entablan de forma virtual. La virtualización del Estado genera que se necesiten otros recursos humanos.

En ese marco creo que hay una restricción complicada, de difícil solución sin alguna política muy específica, como un régimen especial para los informáticos con otras remuneraciones, con otras reglas de juego. Tiene que ser algo en que vos puedas tratar de acercarte a condiciones de mercado, porque si no ocurre que o no los podes contratar, o lo haces pero son personas con tres trabajos.

También podría ser una agencia o una empresa pública que desarrolle para el resto del Estado.

También está la opción de la tercerización, pero tiene un limitante muy claro que para tercerizar vos tenés que comprar. Y para comprar tenés que tener recursos técnicos del mismo rubro para definir qué contratar, cómo controlar lo que se compra, conducirlo. Es muy difícil comprar, tiene que ser transparente, tiene que ser eficiente, tiene que ser eficaz, tenés que comprar lo que corresponde. O sea, es tan difícil como gestionar un proyecto complejo de tecnología.

En ese marco, ¿estaban preparados? Creo que hay algunos recursos humanos que quedan en el Estado que son de primer nivel, pero hay una falencia de densidad de volumen. Es muy difícil conseguir gente, porque es difícil trabajar en el Estado. Además de las cuestiones salariales también está el hecho de que ante situaciones como ésta, incidentes de ciberseguridad, la persona puede terminar siendo parte en una causa judicial, porque al final, son los máximos responsables cuando hay problemas de informática.

3) **¿Los recursos tecnológicos de la APN eran los adecuados para enfrentar las incidencias de ciberseguridad?**

El organismo tenía un esquema más restringido, con acceso cerrado a los funcionarios vinculados al tema identificación de personas y documentación de personas y pasó a un esquema más abierto. Cuando se masificó el uso del SID, se abrieron más posibilidades de

vulnerabilidades. En ese marco, hacía falta una actualización tecnológica, que es lo que encaramos ahora. Hoy en día, los organismos que manejan datos necesitan una inversión permanente en seguridad informática. En este caso no creo que haya sido determinante porque, de hecho, no se trató de un hackeo.

También los usos de inteligencia artificial en las distintas cuestiones informativas, no deja de ser algo bastante nuevo, pero que ofrece cada vez más herramientas, más posibilidades.

De hecho uno de los proyectos que llevamos adelante es el del DNI electrónico, porque Argentina era uno de los pocos países, con desarrollo medianamente avanzado, que no lo tenía. Esta tecnología permite que a través de un certificado de identidad digital embebido en un chip,se genere una validación sin necesidad de exponer, por ejemplo, las fotos. Eso está bastante difundido en el mundo y también está alineado con las mejores prácticas en términos de protección de datos personales.

La tecnología no te deja exento de vulnerabilidades, pero si te pone en un piso más alto. Por eso es que también desde RENAPER se hizo una inversión muy grande en tecnología para ciberseguridad en el marco de un crédito internacional con la CAF.
Toda la tramitación del crédito comenzó en 2021, se pudo hacer la licitación para adquirir equipamiento tecnológico y la mayor parte iba para seguridad informática.

4) ¿Crees que la interoperabilidad de la información entre organismos puede generar mayores riesgos de incidencias?

Sí, el flujo de datos siempre conlleva más riesgos. Es decir, yo tengo un disco rígido encriptado en una caja, en una bóveda, en un banco, y no se me va a perder nada de información. Obviamente si uno empieza a compartir la información o interoperar y siempre va a estar más expuesto a riesgos. Obviamente que hoy hay tecnologías que mitigan muchos riesgos.

Creo que la interoperabilidad es inevitable para tratar de hacer un Estado más eficiente.

Un ejemplo de lo que permite interoperar: desde que se creó, por Ley el DNI es gratis para las personas de bajos recursos. Hasta el año 2021, se le pedía a las personas que acrediten un certificado de pobreza, algo bastante estigmatizante. Desde RENAPER cambiamos eso, se hizo un trabajo con el SINTYS, y en función de determinadas variables económicas se clasificó directamente quieren eran sujeto de percibir el beneficio. Sin interoperabilidad es muy difícil algo así.

El SINTYS mismo sin interoperabilidad no sé cómo funcionaría, creo que la interoperabilidad llegó para quedarse, porque tiene una potencia enorme.

5) ¿Crees que la existencia de un Centro de Operaciones de Ciberseguridad Gubernamental podría haber colaborado en la prevención, detección y mejor respuesta frente al incidente ocurrido?

Sí, sin duda. Es una buena práctica, y eso es indiscutible.

Nosotros recibimos una alerta en el caso de este incidente, pero creo que este área tiene que tener más volumen en términos de orgánica o de estructura institucional, de recursos humanos, presupuesto, etc.

6) **¿Consideras que el marco jurídico existente proporciona una base sólida para garantizar la protección de la información que tutela la APN?**

Para mí, uno de los grandes desafíos que tiene Argentina hace mucho tiempo, es la implementación de las políticas públicas más que parte de su diseño. A nivel diseño creo que a veces ocurre que las normas pueden no estar bien enfocadas desde la perspectiva de la implementación después, por ejemplo por ser muy ambiciosas.

Si uno mira, hay un gran listado de normas, resoluciones, leyes, decretos, disposiciones que en general se inspiran en lo que otros países están haciendo en la materia. No creo que sea un problema normativo, la verdad. Creo que tiene más que ver con un tema de enforcement, de recursos humanos, de formación, si se pretende una política transversal tiene que haber un área dotada de herramientas.

No soy experto en seguridad informática, pero se me ocurre que un área centralizadora por ejemplo de las compras de la APN, ayudaría mucho. Esa agencia con capacidad de gestión, y de enforcement, debería también tener salarios acordes a los perfiles humanos que se requieren. Desde ahí también deberían garantizarse pisos mínimos de seguridad en toda la APN, no sólo auditar sino promoverlo.

7) **¿Considera que la gestión de incidentes de ciberseguridad, como el ocurrido en octubre de 2021, debería ser responsabilidad de los organismos afectados o debería existir una dependencia administrativa a nivel nacional que coordine la respuesta?**
Creo que son las dos cosas. Pero sí creo que debería haber un área transversal mucho más fuerte que garantice lo mínimo. Después eso no quita la responsabilidad que pueda tener cada organismo. Hay cosas que pueden ser transversales y otras más difíciles que no estén deslocalizadas.

8) **¿Desea agregar algo que no se haya preguntado?**

No, creo que se abordó todo.