La Agencia Nacional de Ciberseguridad (o por qué la ciberseguridad no es un lujo)

Cristian Bravo Lillo

Ingeniero Civil en Computación por la Universidad de Chile y Ph.D. en Ingeniería y Políticas Públicas por la Carnegie Mellon University, especializado en seguridad usable. Actualmente es director del CSIRT Nacional (Equipo Nacional de Respuesta a Incidentes de Seguridad Informática) de la Agencia Nacional de Ciberseguridad.

crbravo@dcc.uchile.cl

Resumen / La recientemente creada Agencia Nacional de Ciberseguridad es un servicio público técnico con la misión de asesorar al presidente en la materia, colaborar con la protección de intereses nacionales, y coordinar instituciones de ciberseguridad. Su creación fue impulsada por incidentes graves, como la filtración del EMCO en 2022 y los ataques de ransomware a IFX Networks y GTD en 2023, que afectaron a servicios públicos esenciales.

En general, las personas y las organizaciones no se protegen contra riesgos de ciberseguridad pues son abstractos e inciertos; de manera similar, las personas frecuentemente no se protegen contra enfermedades potenciales en el futuro. Al igual que la salud, la ciberseguridad es una responsabilidad personal y del Estado. También de forma similar, el Estado no puede evitar que las personas se dañen a sí mismas (por ejemplo, usando malas claves), pero debe tomar medidas para prevenirlo. Prevenir incidentes es más efectivo que remediarlos.

La Agencia

La Agencia Nacional de Ciberseguridad (ANCI) es un servicio público de naturaleza altamente técnica. Su objeto es asesorar al presidente o presidenta en materias propias de ciberseguridad; colaborar en la protección de los intereses nacionales en el ciberespacio; coordinar el actuar de las instituciones con competencia en materia de ciberseguridad; velar por la protección, promoción y respeto del derecho a la seguridad informática; y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad [1].

Una de las preocupaciones fundamentales de la Agencia es la ocurrencia de incidentes por ciberseguridad en el país. En 2022 y 2023 hubo en Chile casos graves de filtraciones de datos y de ransomware que afectaron al sector público, como la filtración masiva de correos electrónicos del Estado Mayor Conjunto (EMCO) en septiembre de 2022 [2], que obligó a la entonces Ministra de Defensa, Maya Fernández, a volver urgentemente al país para dar explicaciones y contener los efectos políticos de la filtración [3]; los ataques de ransomware sobre IFX Networks [4] y GTD en octubre de 2023 [5], que en el primer caso indisponibilizó el portal de compras públicas durante 9 días [6], y en el segundo caso afectó a más de 80 servicios públicos [7], entre ellos numerosas municipalidades, algunos servicios de salud y al menos dos servicios transversales muy importantes en el sector público: FirmaGob (https://firma.digital.gob.cl/) y DocDigital (https://doc.digital.gob.cl/). En octubre de 2023 el entonces proyecto de ley marco de ciberseguridad (que crea la ANCI) estaba siendo discutido en el Congreso, y los incidentes de ese mes galvanizaron el apoyo de los legisladores al proyecto y generaron un sentido de urgencia que de otra forma no hubiera tenido.

Sumado a lo anterior, el clima en Chile durante los meses que duró la elaboración del proyecto de ley estuvo teñido de una intensa preocupación por la seguridad física, que no hizo sino aumentar durante el gobierno del Presidente Boric. El proyecto de ley fue incluido en una "agenda corta" o agenda priorizada de medidas propuestas para mejorar la seguridad

En 2022 y 2023 hubo en Chile casos graves de filtraciones de datos y de ransomware que afectaron al sector público [incluyendo] el portal de compras públicas, numerosas municipalidades, algunos servicios de salud y dos servicios transversales muy importantes: FirmaGob y DocDigital.

en el país [8]. Esto sin duda benefició el avance del proyecto, que en otras condiciones no habría tenido el espacio legislativo necesario. Los proyectos que tienen una componente fuerte de tecnología rara vez tienen ese espacio legislativo. Todo esto probablemente contribuyó a que el proyecto de ley fuera aprobado y promulgado en tiempo récord. El primer proyecto de ley fue presentado al Senado por el gobierno del Presidente Piñera el 2 de marzo de 2022; una ley con contenido sustancialmente mejorado fue promulgada durante el gobierno del Presidente Boric el 26 de marzo de 2024: apenas dos años y 24 días después [9].

¿De qué se ocupa la Agencia?

En Latinoamérica, la mayor parte de los países tenemos problemas en apariencia mucho más básicos que la ciberseguridad. Según un estudio sobre pobreza multidimensional (que mide no sólo ingreso, sino también salud, vivienda, educación y empleo) presentado por CEPAL y PNUD en abril de este año, alrededor de una cuarta parte de la población de latinoamérica es pobre [10]. Por mucho que nos inquieten escenarios como los de Ejército, ChileCompras o GTD, preocuparse por este tipo de incidentes podría parecer un lujo que sólo pueden darse los países desarrollados, o en vías de desarrollo. Sin embargo, es falso creer que hoy uno puede

preocuparse de una cosa y no de la otra: la mayor parte de las necesidades básicas (agua y alcantarillado, electricidad, transporte, comunicaciones) dependen de Internet para ser provistas. De los factores que mide la pobreza multidimensional, al menos tres (salud, educación y empleo) dependen directa y fuertemente de Internet.

Si una cañería de agua se rompe por mala mantención y deja sin agua a una comunidad, normalmente uno no pensaría en este como un problema de ciberseguridad. Sí lo sería si alguien accediera sin permiso al sistema de control industrial que controla la cantidad de cloro que se agrega al agua para potabilizarla, y tratara de aumentar el nivel de cloro por sobre el límite saludable para la vida humana. Esto, por cierto, ocurrió en 2021 en Florida, Estados Unidos.[11]

Otro ejemplo: en 1999, en el condado de Maroochy, Australia, una persona tuvo una pelea con su jefe y renunció a su trabajo. Pidió al consejo del condado que lo recontrataran para otro rol, lo que no ocurrió. Enojado por esto, intervino el sistema SCADA que controlaba las 142 bombas de drenaje encargadas de llevarse las aguas servidas. Como resultado, las bombas dejaron de generar alarmas, y dejaron de bombear las aguas de desecho, inundando el lugar con más de 750 mil litros de aguas servidas. Los ríos se tiñeron de negro, muchos peces y fauna local murieron, y la población tuvo que soportar la pestilencia de las aguas servidas por semanas [12]. Hoy este es un caso de estudio para la comunidad técnica [13].

Tal como en los casos anteriores, muchos problemas hoy tienen aspectos de ciberseguridad de los que hay que hacerse cargo. Frente a un apagón como el del 25 de febrero de 2025 [14], tenemos que preguntarnos si la causa es la inundación de una planta de generación, un terremoto que botó parte de las torres de transmisión, o un ciberataque, como los que ocurrieron en Ucrania días antes de las navidades de 2015 [15] y 2016 [16]. El día del apagón, parte del equipo nos quedamos en las oficinas atentos a cualquier antecedente que indicara que se trataba de un ciberataque o incidente de ciberseguridad. Si así hubiera sido, habríamos juntado un equipo de analistas para identificar qué servidores o aplicaciones fallaron, dónde estaban físicamente, llamar a las personas encargadas, consultar por el estado de los servidores, y determinar desde ahí cuál era el mejor camino de acción (lo que podría haber incluido ir físicamente donde estuvieran los servidores que habilitaban el servicio, pedir u obtener los logs de las máquinas o de los dispositivos de red, analizarlos y llegar a nuestras propias conclusiones). Afortunadamente nada de eso fue necesario.

El proyecto de ley [que creaba la Agencia Nacional de Ciberseguridad] fue aprobado y promulgado en tiempo récord.

Nuestro ciberespacio es complejo

Nuestro ciberespacio es un sistema complejo; y los sistemas de este tipo tienden a fallar de maneras complejas y difíciles de prever. El aumento de la complejidad de este sistema, unido a una migración acelerada de servicios y procesos hacia el sistema, genera dos efectos: una dependencia creciente de nuestra sociedad de la red, y una incluso mayor complejidad que dificulta aún más el prever qué puede fallar.

Las instituciones que proveen Internet, que desde 2024 es considerado un servicio básico en Chile [17], se han transformado rápidamente en esenciales para la organización y provisión de todo el resto de los servicios, y para la coordinación de procesos, elaboración de productos, y un largo etcétera. Internet se ha transformado en una tecnología de base que posibilita o potencia todo lo demás.

Las instituciones que proveen servicios básicos, como el agua potable, la electricidad y el gas licuado o natural, son simplemente vitales y dependen mutuamente entre sí para su provisión: las instalaciones de agua potable dependen de la electricidad y de Internet para proveer agua continuamente; las plantas hidroeléctricas no sólo dependen del agua para generar electricidad: la producción y distribución de energía eléctrica depende de personas que requieren de agua de forma continua; etc. No es difícil imaginar escenarios catastróficos que comienzan con un corte de agua, electricidad o gas total o parcial en una ciudad o comuna.

Las instituciones públicas (que proveen un servicio esencial: la administración del Estado) son las que manejan más información de personas en el país. Por ejemplo, el SII tiene información sensible de personas que en la práctica alcanza a la totalidad de los mayores de 18 años. El Ministerio de Desarrollo Social administra y cautela información sensible de personas que alcanza al 90% del país. Si sólo una pequeña parte de esta información fuera filtrada, modificada o eliminada, generaría un perjuicio enorme a la sociedad.

¿De dónde puede venir el próximo gran problema en la red? Muchas veces los problemas son iniciados (o agravados) por personas con y (más frecuentemente) sin malas intenciones. Tal como Bomberos no puede evitar completamente que personas descuidadas inicien enormes incendios a partir de fogatas pequeñas, la Agencia no puede evitar que el administrador de un sistema SCADA que controla la potabilización de agua tenga "123456" como contraseña de la cuenta principal de administración. Sin embargo, sí puede brindar capacitación a las organizaciones sobre la importancia del uso de buenas contraseñas.

Lo anterior es clave: los seres humanos creamos, formamos parte, e influimos fuertemente en este entramado complejo que llamamos ciberespacio. Y la conducta humana es notoriamente difícil de predecir.

Un riesgo, por definición, implica protegerse contra algo que aún no ha ocurrido. Como los seres humanos preferimos las pérdidas inciertas (p. ej., invertir tiempo algún día en el futuro para aprender a usar un gestor de claves) sobre las pérdidas ciertas (p. ej., aprender a usar un gestor de claves hoy) [18], esto implica que nuestra tendencia natural es a nunca hacernos cargo hoy de un riesgo de ciberseguridad.

La mayor parte de las personas y las organizaciones no está dispuesta a invertir en protegerse, al menos no contra algo tan intangible y abstracto como un ciberataque. Por eso es necesaria una ley: porque el bienestar de todos depende de que las empresas y personas se protejan contra algo de lo que naturalmente no se protegerían.

En los casi 10 meses que llevamos en la ANCI, poco más de un 44% de los incidentes de efecto significativo parten con un compromiso de cuentas. Las medidas usuales que recomendamos para disminuir la probabilidad de pérdida son el uso de gestores de claves y de factores múltiples de autenticación (MFA), el bloqueo geolocalizado de conexiones remotas (VPN), y la configuración de dispositivos de seguridad perimetral para bloquear por defecto, en vez de permitir por defecto. Estimamos que estas medidas por sí mismas podrían detener casi un 70% de los ataques. En la mayor parte de las organizaciones, hemos observado cómo se sobreestima la importancia del antivirus y de los "aparatos" (firewalls, SIEMs, etc.), en detrimento de las medidas que realmente tienen importancia, como tener buenas claves (recordables pero no adivinables).

¿Qué recomendaciones se le puede dar a las organizaciones que quieren mejorar su nivel de seguridad, y cumplir con la ley marco?

La Agencia no puede evitar que el administrador de un sistema [...] tenga "123456" como contraseña [...]. Sin embargo, sí puede brindar capacitación [...] sobre la importancia del uso de buenas contraseñas.

1. **Reporta tus incidentes de ciberseguridad.** Sufrir un incidente no es algo malo: le sucede a todo el mundo, tarde o temprano; como un resfrío o un choque en auto. Hay personas a las que nunca les pasa, pero nadie miraría mal a alguien porque se resfría. Hay que dejar de pensar que es algo que nos muestra débiles, descuidados o ignorantes. Reportar incidentes tiene varias ventajas: si no tienes dinero para contratar a alguien, o no tienes a nadie que sepa algo sobre ciberseguridad, si reportas es probable que el CSIRT Nacional pueda ayudarte (depende de cuánto trabajo tengan en el momento).

   Existe la creencia de que luego de reportar llegarán las multas de la Agencia. A pesar de que cada caso debe analizarse en su propio mérito, hoy existe una tendencia fuerte a no multar a los que reportan. Hoy es muy difícil esconder que se ha sufrido un incidente: es por tanto un riesgo no reportar. Por el contrario: la tendencia es a fiscalizar a las instituciones que evidentemente han sufrido incidentes y no los han reportado. Ante la duda sobre si un incidente debe o no reportarse, es mejor reportar.

2. **¿Prestas un servicio esencial?** Los servicios esenciales están descritos en el artículo 4 de la ley: electricidad, transporte, agua potable, telecomunicaciones, etc. Si se provee un servicio esencial, las obligaciones que hay que cumplir son esencialmente dos: aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad; y reportar los incidentes de ciberseguridad. Ambas están pensadas para ser cumplidas por todo el mundo. Si crees o sabes que no puedes cumplir alguna, acude al CSIRT Nacional por ayuda.

3. **¿Fuiste nombrado un Operador de Importancia Vital (OIV)?** Los OIV están definidos en el artículo 5 de la ley. En esencia, se trata de aquellos prestadores de servicios esenciales que son considerados tan importantes, que su operación no puede ser detenida por un incidente de ciberseguridad. Ser OIV no es malo. La ley fue diseñada para permitirle a instituciones de distintos niveles de recursos cumplir con ella. Es fundamental tener una persona responsable de las medidas que hay que cumplir. No importa que esta persona no sea experta: puedes optar por el entrenamiento que brinda el CSIRT para cumplir con las obligaciones que la ley impone.

Algunas organizaciones han usado el hecho de haber sido nombradas OIV como un reconocimiento explícito a su importancia para la sociedad. Si vas a invertir tiempo y esfuerzo en esto, ¡haz que al menos valga la pena en términos de marketing!

La ciberseguridad y la salud

La ciberseguridad es ante todo una responsabilidad personal. Una analogía entre ciberseguridad y salud puede ser útil: para ser adultos funcionales, todas las personas tenemos que tener ciertas nociones de higiene básica, independientemente de que la mayor parte de nosotros no seamos profesionales de la salud. Tenemos que saber reconocer cuando estamos enfermos (cuando hay fiebre, por ejemplo), y cuando requerimos de la ayuda de un profesional de la salud. La misión del Estado en esto es asegurarle a todos la posibilidad de obtener prestaciones de salud. Para ello, debe asegurar que exista infraestructura pública de salud (hospitales y clínicas), y que los prestadores de salud, tanto públicos como privados, sigan las normas establecidas. A pesar de que el Estado no puede prohibir a alguien que se haga alcohólico tomando en exceso todos los días, o que coma grasas y azúcares en exceso, sabemos que una persona alcohólica, o con diabetes o dislipidemia no sólo se daña a sí misma y a su familia, sino al resto de la sociedad. Una persona enferma requerirá de tratamiento médico, medicamentos, terapias físicas, o tal vez de todas las anteriores. Utilizará servicios escasos y caros en una sociedad, y le quitará a otra persona la posibilidad de usarlos.

De manera similar, todas las personas tenemos que saber hacernos cargo de nuestro propio bienestar en términos de ciberseguridad. La misión de la Agencia es asegurarse de que la infraestructura más importante del país esté bien protegida en términos de ciberseguridad. La Agencia no puede prohibir a las personas que se hagan daño a sí mismas; por ejemplo, usando malas claves y haciendo sencillo el que otras personas sean capaces de adivinar esas claves, capturar sus cuentas y hacerles pasar un muy mal rato. Sin embargo, sí puede obligar a las instituciones que ofrecen servicios autenticados a cumplir con ciertas normas; por ejemplo, con un segundo factor de autenticación para que sea más difícil para un criminal tener acceso a las cuentas, incluso si las personas siguen usando malas claves.

En ciberseguridad, tal como en salud, hay algunos problemas que es posible prevenir (p. ej., que adivinen o exfiltren

credenciales de usuario), y algunos que sólo es posible remediar (p. ej., las denegaciones de servicio distribuidas). Prevenir un problema es usualmente más efectivo que lidiar con las consecuencias. Una forma práctica de prevenir incidentes es monitoreando el tráfico entrante (¡y saliente!) de los servicios públicos en búsqueda de patrones de tráfico maliciosos. Esto permite disminuir la cantidad de formas en que agentes de amenaza pueden afectar nuestros activos, y (en algunos casos) disminuir también el impacto sobre nuestros activos si estos llegan a ser afectados. B

Referencias

[1] Ley 21.663 (08/04/2024). Ley Marco de Ciberseguridad, Art. 10. https://bcn.cl/3isi2.

[2] Sepúlveda, N. (22/09/2022). Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa. Ciper Chile. https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/.

[3] Ver por ejemplo: Caro, I., Gómez, R. (21/09/2022). Ministra Maya Fernández regresa de urgencia al país desde Nueva York tras hackeo a correos de las Fuerzas Armadas. La Tercera. https://www.latercera.com/politica/noticia/ministra-fernandez-interrumpe-gira-en-la-onu-y-regresa-de-urgencia-al-pais-tras-hackeo-a-correos-de-las-fuerzas-armadas/EQZJS4W2PVCHTL3FPOHTWN6FTY/; y Díaz, F. (21/09/2022). Ministra de Defensa retorna de emergencia a Chile tras hackeo a correos del Estado Mayor Conjunto. Biobio Chile. https://www.biobiochile.cl/noticias/nacional/chile/2022/09/21/ministra-de-defensa-deja-ny-y-vuelve-de-emergencia-a-chile-tras-hackeo-a-correos-de-fuerzas-armadas.shtml.

[4] Ver la alerta del CSIRT de Gobierno del 12/09/2023 (https://csirt.gob.cl/alertas/10cnd23-00108-01/), y el artículo de INCIBE del 06/10/2023 (https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-ransomware-contra-ifx-networks).

[5] El Mostrador (24/10/2023). GTD: reportan ciberataque a empresa de telecomunicaciones que ofrece servicios al Gobierno. El Mostrador. https://www.elmostrador.cl/noticias/pais/2023/10/24/ciberataque-a-empresa-de-telecomunicaciones-gtd-gobierno-reporta-servicios-publicos-afectados/.

[6] Fossa, L. (22/09/2023). Lo que se sabe y lo que no del ciberataque que afectó a Mercado Público en Chile. Interferencia. https://interferencia.cl/articulos/lo-que-se-sabe-y-lo-que-no-del-ciberataque-que-afecto-mercado-publico-en-chile.

[7] Cárdenas, L. (14/11/2023). Agencia de ciberseguridad del gobierno califica ataque a GTD como un "incidente grave y masivo" y Subtel alista reunión con gerentes. La Tercera. https://www.latercera.com/pulso-pm/noticia/agencia-de-ciberseguridad-del-gobierno-califica-ataque-a-gtd-como-un-incidente-grave-y-masivo-y-subtel-alista-reunion-con-gerentes/GUQERJ7OJBH6NOSUDG76M7DEQE/.

[8] Riquelme, I. (21/02/2025). Leyes y proyectos de ley pertenecientes a la agenda de seguridad del Gobierno del Presidente Gabriel Boric Font. Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/36983/1/BCNSeleccionPL_AgendaSeguridad.pdf.

[9] Biblioteca del Congreso Nacional (08/04/2024). Historia de la Ley N° 21.663. https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8286/.

[10] CEPAL (02/04/2025). CEPAL y PNUD presentan un nuevo Índice de Pobreza Multidimensional para América Latina. Sitio web CEPAL. https://www.cepal.org/es/noticias/cepal-pnud-presentan-un-nuevo-indice-pobreza-multidimensional-america-latina.

[11] BBC (08/02/2021). Hacker tries to poison water supply of Florida city. Sitio web de BBC. https://www.bbc.co.uk/news/world-us-canada-55989843.

[12] Levi, R. (07/02/2016). What the Maroochy Incident taught us about Cyber Warfare. Medium. https://medium.com/curious-minds/what-the-maroochy-incident-taught-us-about-cyber-warfare-4a1abd6abcfc.

[13] Ver, por ejemplo: Abrams, M., Weiss, J. Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. Case #08-1145, MITRE. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf; y Sayfayn, N., Madnick, S. (mayo de 2017). Cybersafety Analysis of the Maroochy Shire Sewage Spill. Working Paper CISL #2017-09. MIT Sloan School of Management. https://web.mit.edu/smadnick/www/wp/2017-09.pdf.

[14] Wikipedia (español), artículo "Apagón de Chile de 2025". https://es.wikipedia.org/wiki/Apag%C3%B3n_de_Chile_de_2025.

[15] Wikipedia (inglés), artículo "2015 Ukraine power grid hack". https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack.

[16] Wikipedia (inglés), artículo "2016 Kyiv cyberattack". https://en.wikipedia.org/wiki/2016_Kyiv_cyberattack.

[17] Ley 21.678 (03/07/2024). Establece el acceso a Internet como servicio público de telecomunicaciones. https://bcn.cl/3kr7q.

[18] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 47(2), 363-391.