EL MERCURIO Legal

Versión para imprimir El Mercurio.com

Legal |
Opinión | Artículo 2 de 2

La coordinación de ciberseguridad en marcha: el “Plan de Acción” y el caso de telecomunicaciones

"...Es una virtud de la legislación sobre ciberseguridad el hecho de ser consciente de esta complejidad regulatoria que involucra su transversalidad. El mecanismo que ha dispuesto para coordinarla así lo atestigua. Con la reciente Resolución Exenta 28 de la ANCI este mecanismo ha dado un paso muy simbólico en su desarrollo. La ejecución del Plan de Acción en el tiempo será un buen indicador de cuán virtuoso es el mecanismo en la práctica..."

Miércoles, 1 de octubre de 2025 a las 10:40

Lucas Sierra

La Ley Marco de Ciberseguridad (LMC) diseñó un complejo mecanismo para lidiar con el hecho de que ella se extiende sobre distintos sectores sujetos a leyes especiales, por ejemplo, sobre telecomunicaciones y sobre el sector eléctrico. Su objeto es evitar que este hecho devengue conflictivo. Hace algún tiempo, la puesta en práctica de este mecanismo de coordinación alcanzó un hito con la publicación del “Plan de Acción” del Comité Interministerial contemplado por la LMC.

Antes de ir al Plan de Acción, una mención a otros elementos del mecanismo de “coordinación regulatoria”, como lo llama la LMC. Piénsese, por ejemplo, en la relación entre la Agencia Nacional de Ciberseguridad (ANCI), el órgano regulatorio propio de la LMC, y el regulador sectorial de las telecomunicaciones Subtel.

Cuando alguna de estas dos autoridades quiera dictar una norma de ciberseguridad para el respectivo sector, deberá pedir un informe a la otra para prevenir “conflictos normativos”. Lo mismo ocurre para la declaración de Operadores de Importancia Vital (OIV), proceso que se encuentra hoy en marcha para algunos servicios esenciales como, por ejemplo, los de telecomunicaciones.

Además, si una autoridad sectorial dicta normas sobre ciberseguridad cuyos efectos son “a lo menos

equivalentes” a los efectos de las normas dictadas por la ANCI, la autoridad sectorial podrá fiscalizar y sancionar a los sujetos regulados de acuerdo con su propia regulación. Es decir, cumplida esa condición de equivalencia, prevalecerá la ley especial. La competencia de la ANCI es supletoria.

Ahora bien. La coordinación regulatoria también se expresa en el mencionado Comité Interministerial sobre Ciberseguridad. En él participan las subsecretarías de Defensa, Relaciones Exteriores, Segpres, Telecomunicaciones, Hacienda, Ciencia y Tecnología; además, el director de la Agencia Nacional de Inteligencia (ANI) y el director de la ANCI, que lo preside. Entre las funciones de este comité está “coordinar la implementación de la Política Nacional de Ciberseguridad”.

La Política Nacional de Ciberseguridad fue definida por decreto supremo en 2023, hasta 2028. Ella se materializa por medio de un Plan de Acción elaborado por el Comité Interministerial, en el que, dentro del conjunto de medidas posibles que contempla la Política Nacional se han incorporado algunas medidas de acuerdo con un criterio de “viabilidad en su implementación”. El Comité Interministerial las eligió a fines de marzo pasado mediante un acuerdo. Más de tres meses después, el 11 de julio pasado, la ANCI dictó la Resolución Exenta 28, mediante la que se “implementa” dicho acuerdo. Esta se publicó en el Diario Oficial el 6 de agosto pasado.

Se trata de 15 medidas. Algunas tienen como objeto a los órganos de la Administración del Estado, otras al sistema general afecto a riesgos de ciberseguridad y otras, en fin, a dos sectores regulados específicos: telecomunicaciones y el sector eléctrico. Este variopinto conjunto da cuenta de los esfuerzos de coordinación que la ciberseguridad demanda en términos regulatorios.

Respecto de los órganos de la Administración del Estado, las medidas ordenan dictar guías para orientar a estos órganos en materias de ciberseguridad, crear becas para la “formación de talentos” en estas materias, fomentar la práctica de ejercicios de ciberseguridad en colaboración con organizaciones nacionales e internacionales, dictar un protocolo a seguir por dichos órganos para comunicar al público el hecho de haber sufrido un incidente de ciberseguridad, generar una agenda a seguir para las relaciones internacionales relativas a ciberseguridad, desarrollar un programa de tutorías sobre “educación y autocuidado digital” y actualizar la “Política de Ciberdefensa 2024-2028”.

Respecto del sistema general expuesto a riesgos de ciberseguridad, las medidas ordenan elaborar un reporte anual sobre la “realidad nacional en ciberseguridad”, elaborar una metodología para evaluar estos riesgos que quede a disposición del público, organizar en conjunto con el mundo educacional ferias estudiantiles sobre ciberseguridad, proponer una carrera técnica sobre ciberseguridad para la educación media técnico-profesional y elaborar un informe con las áreas cuya investigación debería reforzarse a objeto de disminuir riesgos de ciberseguridad en Chile.

Dos medidas se refieren a sectores regulados específicos. Una ordena la dictación de una norma técnica de ciberseguridad para el sector eléctrico, y la segunda se refiere a telecomunicaciones y es bien específica: el establecimiento de exigencias de ciberseguridad en los concursos públicos mediante los cuales se adjudica el espectro radioeléctrico. Esta última medida es interesante.

Ella busca que la Subtel establezca dichas exigencias a fin de dar cumplimiento, en los concursos públicos de espectro, a la Resolución Exenta 1318 que la propia Subtel dictó en 2020 como norma técnica de ciberseguridad para el diseño, instalación y operación de redes y sistema usados por los servicios de

telecomunicaciones. Esto da cuenta del hecho de que la ciberseguridad es una preocupación de las telecomunicaciones desde antes que se dictara la LMC en 2024. Hay aquí una clara competencia sectorial en la materia.

La Subtel deberá primero determinar si está concursando espectro para operadores que serán declarados “relevantes” o no desde el punto de vista de vista de la ciberseguridad, o que serán declarados como “infraestructura crítica”. Según la citada Resolución Exenta 1318 de 2020, todos los servicios públicos, intermedios y limitados de telecomunicaciones están sujetos a deberes de ciberseguridad, pero estos son más extensos e intensos para aquellos declarados como relevantes o como infraestructura crítica. ¿Cuántos deberes se van a exigir en las bases de los concursos públicos que se llamen para asignar espectro?

Es una pregunta difícil, que la Subtel deberá contestar con prudencia, pues es razonable que imponga exigencias para intentar asegurar que quien se adjudique un concurso tenga luego un buen estándar desde el punto de vista de la ciberseguridad. Pero, al mismo tiempo, un exceso de exigencias en esta etapa tan temprana puede limitar artificialmente la competencia por un recurso escaso como es el espectro radioeléctrico.

Como veíamos más arriba, junto con esta medida para el sector de telecomunicaciones, el Plan de Acción contempla un conjunto de otras medidas, cada una con propios objetivos. Esto, de nuevo, refleja la complejidad de una materia que, como la ciberseguridad, se extiende a través del sistema jurídico. Basta ver la cantidad de órganos públicos que el plan menciona como “responsables” de la ejecución de las medidas. Además de la ANCI, siete ministerios están involucrados: Hacienda, Segegob, Defensa, Educación, Energía, Transportes y Telecomunicaciones, y Ciencia y Tecnología. Si consideramos, además, que la ANCI se relaciona con el Presidente de la República a través del Ministerio de Seguridad Pública, son ocho los ministerios responsables.

Con todo, y como se apuntó al inicio, es una virtud de la legislación sobre ciberseguridad el hecho de ser consciente de esta complejidad regulatoria que involucra su transversalidad. El mecanismo que ha dispuesto para coordinarla así lo atestigua. Con la reciente Resolución Exenta 28 de la ANCI este mecanismo ha dado un paso muy simbólico en su desarrollo. La ejecución del Plan de Acción en el tiempo será un buen indicador de cuán virtuoso es el mecanismo en la práctica.

** Lucas Sierra Iribarren es abogado, socio de Lupa Legal y profesor de Derecho de las Telecomunicaciones en la Universidad de Chile.*