CENTRO NACIONAL DE CIBERSEGURIDAD

- **SEGURIDAD PÚBLICA**

Di-2026-7-APN-CNC#JGM.
Infraestructuras Críticas de Telecomunicaciones.
Requisitos Técnicos de Seguridad de la Cadena
de Suministro para Equipamiento. Aprobación.

Disposición Nº 7/2026
Ciudad de Buenos Aires, 5 de noviembre de 2026
Boletín Oficial: 6-11-2026

VISTO el Expediente N° EX-2026-107484323- -APN-CNC#JGM, la Ley N° 27.078, los Decretos Nros. 267/15, 577/17 y sus modificatorios y 941/25, las Resoluciones del ENTE NACIONAL DE COMUNICACIONES Nros. 682/23, 57/26 y 843/26, la Resolución de la ex SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN N° 1523/19, la Decisión Administrativa N° 641/21, la Disposición de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD N° 1/22 y la Disposición del CENTRO NACIONAL DE CIBERSEGURIDAD N° 1/26, y

CONSIDERANDO:

Que mediante el Decreto N° 941/25 se creó el CENTRO NACIONAL DE CIBERSEGURIDAD como organismo descentralizado actuante en la órbita de la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS, en carácter de autoridad nacional en materia de ciberseguridad.

Que el artículo 24 del citado decreto asigna a este Centro, entre otras funciones, las de dictar lineamientos y directivas para las jurisdicciones y organismos del Sector Público Nacional en materia de ciberseguridad, definir las infraestructuras críticas de información, impulsar su resiliencia, promover estándares y buenas prácticas, y entender en la adopción de medidas técnicas y de organización en materia de ciberseguridad que permitan gestionar, con el menor índice de riesgo, las redes y sistemas que se utilizan para prestar servicios de telecomunicaciones.

Que la Resolución de la ex SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN N° 1523/19 definió las infraestructuras críticas y las infraestructuras críticas de información, con SIETE (7) criterios de impacto y ONCE (11) sectores, entre ellos el de Tecnologías de la Información y las Comunicaciones, por lo que la identificación prevista en la presente se articula con dicho marco y con la intervención del Comité de Ciberseguridad, creado por el Decreto N° 577/17 y sus modificatorios.

Que las redes de telecomunicaciones sustentan servicios públicos, actividades económicas, sistemas de emergencia y comunicaciones institucionales, y su seguridad depende no solo de las medidas adoptadas durante su operación, sino también de la integridad y trazabilidad de los productos y servicios que integran su cadena de suministro.

Que los riesgos de la cadena de suministro se extienden a todo el ciclo de vida del equipamiento, desde su diseño y fabricación hasta su retiro, y comprenden vulnerabilidades derivadas, entre otros factores, de productos falsificados, componentes no autorizados, alteraciones de software o firmware y deficiencias en los procesos de desarrollo, actualización y soporte.

Que la TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA) desarrolló la norma SCS 9001, un sistema de gestión de seguridad de la cadena de suministro orientado a las tecnologías de la información y las comunicaciones, cuyo esquema de certificación por terceros permite verificar las prácticas de fabricantes y proveedores, sin sustituir la evaluación técnica del equipamiento.

Que la lista de materiales de software (SBOM, por sus siglas en inglés) es un registro formal y estructurado de los componentes de software y firmware que integran un producto, con sus versiones, proveedores y relaciones de dependencia, que permite correlacionarlos con vulnerabilidades conocidas y determinar con rapidez la exposición del equipamiento ante nuevas vulnerabilidades durante todo su ciclo de vida.

Que los mecanismos de actualización, el acceso remoto de fabricantes o terceros, la gestión de vulnerabilidades y la finalización del soporte constituyen vectores de riesgo que requieren controles proporcionales a la criticidad del equipamiento.

Que los requisitos deben aplicarse con un enfoque basado en riesgo, de manera proporcional, objetiva y técnicamente fundada, en consonancia con el Acuerdo sobre Obstáculos Técnicos al Comercio de la ORGANIZACIÓN MUNDIAL DEL COMERCIO, aprobado por la Ley N° 24.425, cuyo artículo 2.2 reconoce los imperativos de la seguridad nacional como objetivo legítimo de los reglamentos técnicos.

Que la referencia a la norma TIA SCS 9001 obedece a que se trata de un esquema específico de gestión de seguridad de la cadena de suministro de las tecnologías de la información y las comunicaciones, certificable por terceros, que evalúa los procesos del fabricante a lo largo de toda la cadena, a diferencia de los esquemas de evaluación de seguridad de producto, como Common Criteria (ISO/IEC 15408) o NESAS/SCAS, que verifican un producto determinado y no resultan equivalentes a ese fin.

Que, si el ENTE NACIONAL DE COMUNICACIONES incorporara los REQUISITOS TÉCNICOS con carácter obligatorio a la homologación, deberá evaluarse previamente su notificación en los términos del artículo 2.9 del Acuerdo sobre Obstáculos Técnicos al Comercio y su conformidad con la normativa del MERCOSUR.

Que el ENTE NACIONAL DE COMUNICACIONES tiene a su cargo la homologación y certificación de los equipos de telecomunicaciones con el objeto de garantizar la integridad y calidad de las redes de telecomunicaciones, conforme al artículo 16 de la Ley N° 27.078, así como la regulación de los lineamientos técnicos relativos a la infraestructura y los equipos que se conecten a dichas redes, conforme a los incisos c) y h) del artículo 81 de la citada ley.

Que, en particular, el artículo 21 del Anexo I de la Resolución ENACOM N° 682/23 dispone que los equipos y sistemas de radiocomunicaciones, así como las actividades

vinculadas con su fabricación o comercialización, con los alcances establecidos en la reglamentación específica, deberán estar inscriptos en el Registro de Actividades y Materiales de Telecomunicaciones (RAMATEL).

Que la Resolución ENACOM N° 57/26 aprobó el nuevo Reglamento de dicho registro, cuya entrada en vigor fue postergada hasta el 1° de diciembre de 2026 por la Resolución ENACOM N° 843/26, rigiendo hasta entonces las inscripciones del régimen anterior, por lo que el ENTE NACIONAL DE COMUNICACIONES constituye el ámbito adecuado para que, en ejercicio de sus competencias, incorpore los requisitos aprobados respecto del equipamiento comercializado en el país y de los licenciatarios de servicios de Tecnologías de la Información y las Comunicaciones.

Que la presente medida no modifica la Disposición CNC N° 1/26, que regula la continuidad operativa del Sector Público Nacional, y se aplica sin perjuicio de ella, articulándose con su clasificación de sistemas conforme al punto 2.3 del ANEXO I.

Que la Decisión Administrativa N° 641/21 y la Disposición de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD N° 1/22 establecen, respectivamente, requisitos mínimos de seguridad de la información para las jurisdicciones y entidades comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 y un modelo referencial de política de seguridad de la información, cuyos requisitos alcanzan también, conforme al artículo 2° de la Decisión Administrativa N° 641/21, a los proveedores que contratan con el Estado, por lo que los REQUISITOS TÉCNICOS se aplican como norma especial en lo relativo a la seguridad de la cadena de suministro del equipamiento alcanzado, sin perjuicio de los controles de aquellas.

Que el servicio jurídico permanente ha tomado la intervención que le compete.

Que la presente se dicta en ejercicio de las facultades conferidas por los incisos 3, 7, 9, 10 y 15 del artículo 24 del Decreto N° 941/25.

Por ello,

EL DIRECTOR EJECUTIVO DEL CENTRO NACIONAL DE CIBERSEGURIDAD

DISPONE:

ARTÍCULO 1°.- Apruébanse los Requisitos Técnicos de Seguridad de la Cadena de Suministro para Equipamiento Destinado a Infraestructuras Críticas de Telecomunicaciones (en adelante, los “REQUISITOS TÉCNICOS”), que como ANEXO I (IF-2026-107939563-APN-CNC#JGM) forman parte de la presente.

ARTÍCULO 2°.- Establécese que los REQUISITOS TÉCNICOS son de aplicación obligatoria para el Sector Público Nacional definido en el artículo 8° de la Ley N° 24.156, incluidas las empresas y sociedades del Estado, en la adquisición, contratación, instalación y operación de equipamiento destinado a infraestructuras críticas de telecomunicaciones a su cargo, en lo relativo a la seguridad de su cadena de suministro. Los organismos contratantes incorporarán los REQUISITOS TÉCNICOS en los pliegos de bases y condiciones particulares y en los contratos, y fundarán en el nivel de criticidad del equipamiento toda exigencia de certificación o evaluación. Los

REQUISITOS TÉCNICOS no establecen obligaciones directas para las personas humanas o jurídicas ajenas al Sector Público Nacional, a quienes sólo resultarán exigibles por alguna de las siguientes vías: a) los pliegos y contratos del Sector Público Nacional; b) las normas que, en ejercicio de sus competencias, dicte el ENTE NACIONAL DE COMUNICACIONES; o c) la adhesión voluntaria.

ARTÍCULO 3°.- Establécese que los REQUISITOS TÉCNICOS constituyen el estándar técnico de referencia, obligatorio para el Sector Público Nacional en los términos del artículo 2° y de carácter orientativo y de adhesión voluntaria para los demás sujetos, en materia de seguridad de la cadena de suministro del equipamiento destinado a infraestructuras críticas de telecomunicaciones. La aplicación de los presentes REQUISITOS TÉCNICOS se efectuará sin perjuicio de las competencias propias del ENACOM en materia de homologación, registro y fiscalización de materiales de telecomunicaciones.

ARTÍCULO 4°.- Dentro de los NOVENTA (90) días de la entrada en vigencia de la presente, el CENTRO NACIONAL DE CIBERSEGURIDAD, previa intervención del Comité de Ciberseguridad, identificará las Infraestructuras Críticas de Información, en ejercicio de la función prevista en el inciso 7 del artículo 24 del Decreto N° 941/25 y conforme a las definiciones, los criterios de impacto y los sectores establecidos por la Resolución de la ex SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN N° 1523/19, y asignará el nivel de criticidad de las categorías de equipamiento alcanzado conforme al Capítulo 2 del ANEXO I de la presente. Se publicarán en el BOLETÍN OFICIAL las categorías de equipamiento y sus niveles de criticidad. Solo podrá reservarse el listado nominal de instalaciones, que se notificará a los Operadores comprendidos y les será oponible desde dicha notificación. Hasta que el CENTRO NACIONAL DE CIBERSEGURIDAD asigne el nivel de criticidad de una categoría de equipamiento, se aplicará con carácter provisorio el nivel que resulte del punto 2.4 del ANEXO I de la presente. Cuando se trate de infraestructuras, redes, sistemas, servicios o equipamiento vinculados al sector de las telecomunicaciones, dicha identificación y clasificación se realizará en coordinación con el ENTE NACIONAL DE COMUNICACIONES, cuando correspondan al ámbito de sus competencias sectoriales propias de cada organismo.

ARTÍCULO 5°.- Aclárase que el cumplimiento de los REQUISITOS TÉCNICOS no exime a los Proveedores y Operadores definidos en el ANEXO I de las demás obligaciones que les resulten aplicables. En particular, no los exime de las obligaciones de la Disposición CNC N° 1/26 ni de los requisitos mínimos de seguridad de la información aprobados por la Decisión Administrativa N° 641/21 y del Modelo Referencial de Política de Seguridad de la Información aprobado por la Disposición N° 1/22 de la Dirección Nacional de Ciberseguridad.

En caso de superposición con estos últimos, los REQUISITOS TÉCNICOS serán de aplicación especial en lo relativo a la seguridad de la cadena de suministro del equipamiento alcanzado, y el CENTRO NACIONAL DE CIBERSEGURIDAD publicará, dentro de los NOVENTA (90) días de la entrada en vigencia de la presente, una matriz de correlación entre los REQUISITOS TÉCNICOS y los controles de dichas normas, tomando como referencia el Marco de Ciberseguridad (CSF) y las directrices sobre gestión de riesgos de la cadena de suministro del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos de América y la norma ISO/IEC 27001.

ARTÍCULO 6°.- Encomiéndase a las áreas técnicas competentes de este Centro el seguimiento, la asistencia técnica y la verificación del cumplimiento de la presente, quedando facultadas para dictar normas aclaratorias. La actualización del ANEXO I conforme a la evolución tecnológica y a las buenas prácticas internacionales se aprobará por disposición del Director Ejecutivo. Las actividades de seguimiento y verificación que involucren materiales sujetos a homologación, registro o fiscalización por parte del ENACOM se desarrollarán en coordinación con dicho organismo, en el ámbito de sus respectivas competencias.

ARTÍCULO 7°.- Establécese que los REQUISITOS TÉCNICOS se aplicarán a los procedimientos de adquisición o contratación que se inicien a partir de los NOVENTA (90) días de la entrada en vigencia de la presente. El equipamiento instalado solo quedará sujeto a medidas de adecuación conforme al Capítulo 5 del ANEXO I. Las medidas de adecuación respecto del equipamiento instalado se determinarán considerando su nivel de criticidad, exposición, ciclo de vida, soporte disponible y riesgo asociado, fijándose plazos de adecuación razonables y sujetos a la disponibilidad presupuestaria del organismo responsable. El reemplazo del equipamiento instalado solo procederá mediante disposición fundada.

ARTÍCULO 8°.- La presente medida entrará en vigencia el día siguiente al de su publicación en el BOLETÍN OFICIAL.

ARTÍCULO 9°.- Comuníquese la presente al ENTE NACIONAL DE COMUNICACIONES a fin de que, en ejercicio de sus competencias, evalúe la incorporación de los REQUISITOS TÉCNICOS a los procedimientos de homologación de materiales y a las obligaciones de los licenciatarios de servicios de Tecnologías de la Información y las Comunicaciones.

ARTÍCULO 10°.- Comuníquese la presente a la OFICINA NACIONAL DE CONTRATACIONES a fin de que, en el marco de sus competencias, evalúe la incorporación de los REQUISITOS TÉCNICOS a los pliegos y modelos de contratación del Sector Público Nacional.

ARTÍCULO 11°.- Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Walter Fabián Agüero.

Nota: La presente disposición se publica sin su correspondiente anexo. Si desea consultarlo puede ingresar en www.revistarap.com, o bien solicitar el envío del mismo a edicion@revistarap.com.