ANEXO I - Requisitos técnicos de seguridad de la cadena de suministro para equipamiento destinado a infraestructuras críticas de telecomunicaciones

CAPÍTULO 1: Disposiciones generales

1.1. Definiciones. A los efectos de los presentes REQUISITOS TÉCNICOS se entiende por:

a) Infraestructura crítica de telecomunicaciones: las redes, sistemas y elementos de redes de telecomunicaciones que el CENTRO NACIONAL DE CIBERSEGURIDAD (en adelante, "CNC") identifique como infraestructuras críticas de información conforme al artículo 4° de la presente, incluidos los elementos de comunicaciones que integren infraestructuras críticas de información de otros sectores.

b) Equipamiento alcanzado: los equipos, elementos y componentes de hardware, software y firmware destinados a instalarse en una infraestructura crítica de telecomunicaciones, incluidas sus actualizaciones.

c) Proveedor: quien provea equipamiento alcanzado al Operador. En los términos del punto 1.3, el Proveedor es responsable del cumplimiento de los requisitos del Capítulo 3, aun cuando la información o los procesos exigidos correspondan al fabricante.

d) Operador: quien instale u opere equipamiento alcanzado en una infraestructura crítica de telecomunicaciones, sea una jurisdicción o entidad del Sector Público Nacional, un licenciatario de servicios de Tecnologías de la Información y las Comunicaciones u otra persona humana o jurídica, incluido el Proveedor cuando lo opere por cuenta propia o de terceros, sin perjuicio de lo dispuesto en el punto 1.3.

e) Lista de materiales de software (en adelante, "SBOM"): el inventario estructurado de los componentes de software y firmware de un producto, con su versión, procedencia y dependencias.

f) Nivel de criticidad: la categoría asignada al equipamiento alcanzado conforme al Capítulo 2, con independencia de la clasificación de sistemas prevista en el ANEXO I de la Disposición CNC N° 1/26, sin perjuicio de la regla de articulación del punto 2.3, y cuyos niveles (Crítico, Elevado, Moderado y Reducido) no guardan correspondencia con los de dicha disposición (Alto, Medio y Bajo).

1.2. Principios. Los REQUISITOS TÉCNICOS se aplican durante todo el ciclo de vida del equipamiento alcanzado, desde su diseño y fabricación hasta su retiro y disposición final, con un enfoque basado en riesgo y en proporción a su nivel de criticidad.

1.3. Alcance de las obligaciones. Los Capítulos 3 y 4 son de cumplimiento obligatorio para las jurisdicciones y entidades del Sector Público Nacional alcanzadas por el artículo 2° de la presente. Respecto de las demás personas humanas o jurídicas, incluidos los Proveedores y Operadores privados y los licenciatarios, los requisitos no generan obligaciones directas y solo resultan exigibles a través de los pliegos y contratos del Sector Público Nacional, de las normas que dicte el ENTE NACIONAL DE COMUNICACIONES en ejercicio de sus competencias o de la adhesión voluntaria.

1.4. Información clasificada. Los presentes requisitos se aplican como piso mínimo a las redes y sistemas

que procesen información clasificada, sin perjuicio de los requisitos adicionales que establezca su normativa específica. El CNC coordinará con el MINISTERIO DE DEFENSA, el MINISTERIO DE SEGURIDAD NACIONAL y la SECRETARÍA DE INTELIGENCIA DE ESTADO las medidas complementarias aplicables a dichas redes y la forma de cumplir, conforme a su régimen de clasificación, las obligaciones de información y notificación al CNC.

CAPÍTULO 2: Nivel de criticidad

2.1. Factores. El CNC asignará el nivel de criticidad de cada categoría de equipamiento alcanzado considerando, como mínimo:

a) la función que desempeña en la red.

b) Su exposición a redes públicas o externas.

c) Su capacidad de administración, actualización o modificación local o remota.

d) La información y los servicios que procesa o soporta.

e) El impacto potencial de su compromiso o indisponibilidad.

f) Su dependencia de software, firmware, servicios externos o proveedores terceros.

g) La concentración en un proveedor único o en una cadena de suministro determinada.

2.2. El CNC determinará el nivel de criticidad mediante la ponderación conjunta de los factores del punto 2.1. La exposición, la capacidad de administración o modificación remota, las dependencias y la concentración podrán elevar el nivel que correspondería atendiendo solo al impacto potencial. El nivel de criticidad podrá ser:

a) Crítico: equipamiento cuyo compromiso podría afectar funciones centrales de la red o la prestación de servicios esenciales a escala nacional.

b) Elevado: equipamiento cuyo compromiso podría afectar servicios esenciales a escala regional o a un número significativo de usuarios.

c) Moderado: equipamiento cuyo compromiso tendría efectos adversos acotados, manejables mediante medidas alternativas.

d) Reducido: equipamiento cuyo compromiso tendría un impacto limitado y no afectaría servicios esenciales.

2.3. Articulación con la Disposición CNC N° 1/26. La clasificación del equipamiento es independiente de la clasificación de sistemas de la Disposición CNC N° 1/26, pero el nivel de criticidad del equipamiento no podrá ser inferior al que resulte de la siguiente equivalencia mínima respecto del sistema más crítico que soporte: sistema de nivel Alto, equipamiento Crítico; sistema de nivel Medio, equipamiento Elevado; sistema de nivel Bajo, equipamiento Moderado.

2.4. Nivel provisorio. Hasta que el CNC asigne el nivel de criticidad de una categoría de equipamiento, se aplicará con carácter provisorio el nivel que resulte del punto 2.3 o, si el equipamiento no soportara sistemas clasificados conforme a la Disposición CNC N° 1/26, el nivel Moderado.

CAPÍTULO 3: Requisitos del equipamiento y del Proveedor

3.1. Certificación del sistema de gestión. Para el equipamiento de nivel elevado o crítico, el Proveedor deberá acreditar que el fabricante cuenta con un sistema de gestión de seguridad de la cadena de suministro certificado conforme a la norma TIA SCS 9001. Durante los primeros TREINTA Y SEIS (36) meses posteriores a la entrada en vigencia de la presente, se aceptará, en lugar de la certificación, la confirmación directa de la TIA que acredite que el fabricante se ha registrado para iniciar el proceso de certificación, acompañada de una declaración jurada del fabricante y un plan de certificación. A estos fines, no se admitirán otras certificaciones o esquemas como equivalentes. La exigencia de certificación deberá fundarse, en cada procedimiento, en el nivel de criticidad del equipamiento, y no deberá restringir la competencia de manera injustificada.

3.2. Integridad. El equipamiento alcanzado deberá contar con mecanismos que preserven la autenticidad, integridad y trazabilidad de su hardware, software y firmware y que permitan identificar las versiones instaladas. Las actualizaciones deberán permitir verificar su procedencia, autenticidad e integridad antes de su aplicación. Para los niveles elevado y crítico, cuando resulte técnicamente aplicable, se exigirán arranque seguro, firma y verificación criptográfica del firmware y controles de integridad.

3.3. SBOM. Para el equipamiento de nivel elevado o crítico, el Proveedor deberá entregar al Operador y, a su requerimiento, al CNC, una SBOM en un formato de archivo estructurado que permita su procesamiento automatizado, tales como SPDX, conforme a la norma ISO/IEC 5962, o CycloneDX, conforme a la norma ECMA-424, y actualizarla ante toda modificación relevante del software o firmware. Para el nivel moderado, deberá mantenerla a disposición del Operador y del CNC. La SBOM tendrá carácter confidencial en los términos de las excepciones del artículo 8° de la Ley N° 27.275, sin perjuicio de lo cual el personal del CNC y de los Operadores que acceda a ella estará obligado a guardar reserva, y los contratos deberán incluir cláusulas de confidencialidad en tal sentido, y solo podrá utilizarse para evaluación de riesgo, gestión de vulnerabilidades y respuesta ante incidentes.

3.4. Gestión de vulnerabilidades. El Proveedor deberá contar con procedimientos para identificar las vulnerabilidades que afecten al equipamiento alcanzado, evaluar su impacto, desarrollar y distribuir medidas de mitigación o actualizaciones y registrar las acciones de remediación, durante el período de soporte previsto en el punto 3.5. Las vulnerabilidades críticas que afecten equipamiento de nivel elevado o crítico deberán comunicarse dentro de las SETENTA Y DOS (72) horas de tomar conocimiento de ellas al CNC, a través de su centro de respuesta a incidentes (CERT.ar o el que lo suceda) y a los Operadores afectados. A los fines de esta disposición, se consideran vulnerabilidades críticas aquellas con una puntuación CVSS igual o superior a 9,0 o con explotación activa conocida.

3.5. Soporte. El Proveedor deberá informar las condiciones de soporte y la fecha prevista de finalización de las actualizaciones de seguridad. Para el equipamiento de nivel moderado, elevado o crítico, deberá garantizar actualizaciones de seguridad por un plazo no inferior a TRES (3) años para el nivel moderado y a CINCO (5) años para los niveles elevado y crítico, o a la vida útil declarada del equipamiento si está fuera mayor, desde su provisión. Esta obligación podrá cumplirse mediante la puesta a disposición por el fabricante de las actualizaciones y avisos de seguridad, sin que se requiera un contrato de mantenimiento integral.

3.6. Trazabilidad de fabricación. Para el equipamiento de nivel elevado o crítico, el Proveedor deberá mantener registros que permitan verificar la identidad y procedencia del producto y de sus componentes relevantes, incluidos números de serie, versiones de software y firmware y modificaciones efectuadas, desde la fabricación hasta la entrega al Operador.

3.7. Evaluación técnica independiente. Para el equipamiento de nivel crítico, el Proveedor deberá presentar un informe de evaluación de seguridad del producto emitido por un laboratorio de ensayos acreditado conforme a la norma ISO/IEC 17025 y reconocido por el CNC para la evaluación de ciberseguridad conforme al esquema que este apruebe, sin perjuicio de las competencias del ENACOM respecto de los laboratorios de homologación. Hasta que el CNC apruebe dicho esquema, se admitirán los informes emitidos por laboratorios acreditados conforme a la norma ISO/IEC 17025 bajo alguno de los esquemas Common Criteria (ISO/IEC 15408), NESAS/SCAS, IEC 62443-4-2 o ETSI EN 303 645, por el plazo de transición que fije el CNC.

CAPÍTULO 4: Obligaciones del Operador

4.1. Acceso remoto. El acceso remoto de Proveedores o terceros para administración, mantenimiento o soporte estará sujeto a controles de autenticación, autorización y registro de actividades, conforme a los controles de acceso de terceros de la Decisión Administrativa N° 641/21 y la Disposición DNCIB N° 1/22, y con autenticación multifactor e identificación individual de quienes acceden. Para el equipamiento de nivel elevado o crítico, dicho acceso permanecerá deshabilitado por defecto y se habilitará solo a demanda y con autorización del Operador, y sus registros se conservarán por un plazo no inferior a UN (1) año. Los servicios tercerizados de integración, instalación y mantenimiento gestionado del equipamiento alcanzado quedan sujetos a los mismos controles, y el Operador deberá exigirlos contractualmente a sus contratistas.

4.2. Recepción e inventario. El Operador mantendrá un único inventario, integrado al inventario de sistemas exigido por la Disposición CNC N° 1/26, que incluirá el equipamiento alcanzado instalado, con su nivel de criticidad, números de serie y versiones de software y firmware. Al recibir equipamiento de nivel elevado o crítico, verificará su integridad y su correspondencia con los registros del Proveedor.

4.3. Retiro y disposición final. Antes del retiro, reutilización o disposición final del equipamiento alcanzado, el Operador eliminará de manera segura la información, credenciales, configuraciones y datos residuales, y dejará constancia de ello. La reutilización solo procederá previa verificación de dicha eliminación, que será autorizada por el responsable de seguridad de la información del Operador y registrada en el

inventario del punto 4.2. La eliminación segura se ajustará a los procedimientos de disposición de medios de la Decisión Administrativa N° 641/21.

4.4. Notificación de incidentes. Para el equipamiento de nivel elevado o crítico, el Operador notificará al CNC los incidentes de ciberseguridad que lo afecten dentro de las VEINTICUATRO (24) horas de tomar conocimiento de ellos, sin perjuicio de otras obligaciones de notificación aplicables.

CAPÍTULO 5: Reevaluación

5.1. Supuestos. El CNC podrá disponer la reevaluación del equipamiento alcanzado ante:

a) vulnerabilidades críticas;

b) modificaciones sustanciales de hardware, software o firmware;

c) cambios relevantes en el Proveedor o en la cadena de suministro;

d) pérdida, suspensión o modificación de la certificación exigida;

e) finalización del soporte;

f) cambios en las condiciones de exposición o en el nivel de criticidad;

g) cualquier otra circunstancia debidamente fundada que incremente significativamente el riesgo.

5.2. Procedimiento y efectos. La reevaluación se sustanciará con intervención del Proveedor y del Operador. Respecto del Sector Público Nacional, podrá concluir en la exigencia de medidas de mitigación con plazos de adecuación razonables, que se fijarán expresamente en cada caso, o, mediante disposición fundada, en el reemplazo del equipamiento. Cuando el equipamiento se encuentre inscripto en el RAMATEL, el CNC comunicará el resultado al ENACOM y, cuando corresponda, coordinará con dicho organismo las medidas que resulten procedentes en el ámbito de sus respectivas competencias. Respecto de los sujetos ajenos al Sector Público Nacional, la reevaluación no genera obligaciones directas y solo podrá producir efectos por las vías previstas en el punto 1.3.

CAPÍTULO 6: Requisitos mínimos por nivel de criticidad

Requisito	Reducido	Moderado	Elevado	Crítico
3.1 Certificación SCS 9001	-	-	Sí	Sí
3.2 Integridad y actualizaciones verificables	Sí	Sí	Sí	Sí
3.2 Arranque seguro y firma de firmware	-	-	Sí	Sí
3.3 SBOM	-	A disposición	Entrega	Entrega
3.4 Gestión de vulnerabilidades	Sí	Sí	Sí	Sí

3.4 Comunicación de vulnerabilidades críticas al CNC (CERT.ar)	-	-	Sí	Sí
3.5 Información de soporte	Sí	Sí	Sí	Sí
3.5 Soporte mínimo de actualizaciones de seguridad	-	3 años	5 años	5 años
3.6 Trazabilidad de fabricación	-	-	Sí	Sí
3.7 Evaluación técnica independiente	-	-	-	Sí
4.1 Controles de acceso remoto	Sí	Sí	Sí	Sí
4.1 Acceso remoto deshabilitado por defecto	-	-	Sí	Sí
4.2 Inventario	Sí	Sí	Sí	Sí
4.2 Verificación en la recepción	-	-	Sí	Sí
4.3 Retiro seguro	Sí	Sí	Sí	Sí
4.4 Notificación de incidentes	-	-	Sí	Sí

República Argentina - Poder Ejecutivo Nacional
Año de la Grandeza Argentina

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2026-107939563-APN-CNC#JGM

CIUDAD DE BUENOS AIRES
Jueves 5 de Noviembre de 2026

Referencia: ANEXO I - Requisitos técnicos de seguridad de la cadena de suministro para equipamiento destinado a infraestructuras críticas de telecomunicaciones

---

El documento fue importado por el sistema GEDO con un total de 6 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.11.05 15:44:36 -03:00

Walter Fabián AGÜERO
Director Ejecutivo
Centro Nacional de Ciberseguridad
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.11.05 15:44:36 -03:00