CENTRO NACIONAL DE CIBERSEGURIDAD

Disposición 1/2026

DI-2026-1-APN-CNC#JGM

Ciudad de Buenos Aires, 11/05/2026

VISTO el Expediente N° EX-2026-41496385- -APN-CNC#JGM., y el Decreto 941 del 31 de diciembre de 2025, y

CONSIDERANDO:

Que mediante el Decreto 941/2025 se creó el CENTRO NACIONAL DE CIBERSEGURIDAD (CNC) como organismo descentralizado actuante en la órbita de la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS, con el objeto de planificar, ejecutar y supervisar políticas, programas y acciones en materia de ciberseguridad destinadas a proteger el ciberespacio de interés nacional, las infraestructuras críticas de información, los activos digitales estratégicos del ESTADO NACIONAL y los sistemas tecnológicos empleados en la prestación de servicios públicos esenciales y actividades del Sector Público Nacional.

Que el citado Decreto asigna al CNC el carácter de órgano rector en materia de protección y seguridad integral del ciberespacio de interés nacional, facultándolo para dictar lineamientos y directivas destinadas al Sector Púbico Nacional en materia de planificación y coordinación de la política de protección y seguridad del ciberespacio.

Que la adecuada protection de la information sensible y privada de los ciudadanos de la Nación, así como de los datos de importancia estratégica del ESTADO NACIONAL, requiere la adopción de medidas que permitan direccionar de manera eficiente los esfuerzos de los organismos especializados en la materia.

Que en tal sentido, resulta oportuno aprobar un Reglamento Técnico que establezca los requisitos y características esenciales que deberán cumplir el Sector Público Nacional en la elaboración e implementación de las políticas y planes de contingencia, como así también de los Centros de Procesamiento de Datos Alternativos, con el fin de garantizar la disponibilidad y resiliencia de los sistemas críticos.

Que la adopción de dichos lineamientos contribuirá a promover la adopción de buenas prácticas en materia de gestión de la continuidad operativa, alineadas con estándares internacionales de ciberseguridad y resiliencia digital, fortaleciendo de este modo las capacidades del Estado para prevenir, mitigar y recuperar los servicios digitales ante contingencias o incidentes de seguridad informática.

Que a fin de elevar el nivel de resiliencia cibernética nacional y alinear las presentes disposiciones con las mejores prácticas internacionales, se han tenido en cuenta las recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos de América —en particular las guías NIST SP 800-184 (“Guía para la Recuperación de Eventos de Ciberseguridad”) y NIST SP 800-34 Rev.1 (“Guía de Planificación de Contingencia para Sistemas de Información Federales”), así como los estándares ISO/IEC 27031 e ISO 22301 relativos a la

continuidad de las TIC y la gestión de la continuidad del negocio, y los lineamientos de la Agencia de Ciberseguridad de la Unión Europea (ENISA); todos ellos enfatizan la importancia de la planificación estratégica de la recuperación ante incidentes, el establecimiento de métricas claras de recuperación (tales como objetivos de tiempo y de punto de recuperación, RTO y RPO), la elaboración de procedimientos específicos para distintos escenarios de contingencia (“playbooks”), la realización de pruebas periódicas de los planes de recuperación y la mejora continua de los mismos a partir de las lecciones aprendidas.

Que el Comité de Ciberseguridad, integrado por representantes de la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS, la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la PRESIDENCIA DE LA NACIÓN, el MINISTERIO DE DEFENSA, el MINISTERIO DE SEGURIDAD, el MINISTERIO de RELACIONES EXTERIORES, COMERCIO INTERNACIONAL Y CULTO, y el MINISTERIO DE JUSTICIA, presidido por el Director de este Centro, ha tomado la intervención de su competencia, aprobando la reglamentación en los términos que se propone.

Que el inciso 14 del artículo 24 del Decreto 941/2025 establece entre las funciones de este CNC la de administrar el registro de equipos de respuesta ante incidentes de seguridad informática y elaborar un Plan de Recuperación ante Desastres (PRD) para el Sector Público Nacional.

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

Que la presente medida se dicta en ejercicio de las atribuciones conferidas por el inciso 14 del artículo 24 del Decreto 941/2025.

Por ello,

EL DIRECTOR DEL CENTRO NACIONAL DE CIBERSEGURIDAD

DISPONE:

ARTÍCULO 1° - Apruébase el Reglamento Técnico que establece los requisitos y características esenciales que deberá observar el Sector Público Nacional en la elaboración e implementación de las Politicas de Planes de Contingencias , Planes de Contingencia y Centros de Procesamiento de Datos Alternativos que como ANEXO I (IF-2026-43001297-APN-CNC#JGM) forma parte de la presente medida.

ARTÍCULO 2° - Dispónese que las exigencias establecidas en la presente medida serán de aplicación obligatoria para el Sector Público Nacional definido en el artículo 8° de la Ley N° 24.156 que utilicen centros de datos o infraestructuras de tecnologías de la información.

ARTÍCULO 3° - Encomiéndase a las áreas técnicas competentes del Centro Nacional de Ciberseguridad el seguimiento, asistencia técnica y verificación del cumplimiento de los lineamientos aprobados por la presente disposición, quedando facultadas para dictar normas complementarias y/o aclaratorias que resulten necesarias para su adecuada implementación.

ARTÍCULO 4° - Aclárase que el cumplimiento de las obligaciones establecidas por la presente Disposición no exime a los sujetos alcanzados de la observancia de las demás obligaciones emanadas de otras normas que resulten aplicables a los productos, servicios o sistemas aquí comprendidos.

ARTÍCULO 5° - Disposiciones transitorias. Los sujetos alcanzados por la presente Disposición contarán con un plazo máximo de ciento ochenta (180) días a partir de la entrada en vigencia de la misma para adecuar sus infraestructuras, políticas y planes de contingencia a los lineamientos aprobados en el ANEXO I del artículo primero. Dentro de ese período, deberán presentar ante la Autoridad de Aplicación, un informe de cumplimiento de su Plan de Recuperación de Desastres RD, indicando la ubicación de su centro alternativo cuando sea necesario, las características técnicas implementadas, los resultados de al menos una prueba inicial de conmutación al sitio de respaldo y los parámetros RTO/RPO definidos. Los sujetos alcanzados que ya cuenten con soluciones de recuperación ante desastres deberán verificar y, en su caso, ajustar las mismas para dar plena observancia a los estándares establecidos.

ARTÍCULO 6° - La presente medida entrará en vigencia el día siguiente al de su publicación en el Boletín Oficial.

ARTÍCULO 7° - Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Ariel Waissbein

NOTA: El/los Anexo/s que integra/n este(a) Disposición se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 13/05/2026 N° 31541/26 v. 13/05/2026