RED
DE GOBERNANZA PARA
ARGENTINA

GOBERNANZA TI

EL TRÍPODE DE LA APN

Febrero 2025

Jorge Nunes
redgobernanzaparaargentina@gmail.com

Introducción

El crecimiento exponencial de los ciberdelitos y el aumento del número de personas afectadas en el País evidencian no solo la vulnerabilidad de los sistemas digitales, sino también la deficiente gestión de la información sensible. Ejemplos recientes ilustran la magnitud del problema: el ataque de ransomware al Hospital Churruca; al Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (PAMI); la filtración de imágenes y datos personales del Registro Nacional de las Personas (RENAPER) y el incidente reportado por la Comisión Nacional de Energía Atómica (CNEA), que puso en riesgo información estratégica con potencial impacto en la seguridad nacional.

Desde una perspectiva jurídica, el marco normativo argentino presenta deficiencias para hacer frente a estas amenazas. La Ley 25.326 de Protección de Datos Personales, vigente desde el año 2000, ha quedado obsoleta ante los avances tecnológicos, al igual que la tipificación de los delitos en las disposiciones del Código Penal Argentino modificadas por la Ley 26.388 en 2008, que deja sin herramientas para enfrentar la realidad de los ciberataques.

Asimismo, el ciberdelito se ha consolidado como una actividad delictiva altamente organizada, en la que operan redes criminales con sofisticadas capacidades de ataque y motivaciones predominantemente económicas. Un fenómeno preocupante en este contexto es la creciente disponibilidad de la "ciberdelincuencia como servicio", que permite a individuos sin conocimientos avanzados en informática acceder a herramientas ilícitas en mercados clandestinos, reduciendo la necesidad de estructuras criminales complejas para la comisión de delitos.

Ante este escenario, resulta imperativo fortalecer los recursos humanos y tecnológicos destinados a la ciberseguridad y a la investigación del ciberdelito. La formación, capacitación y entrenamiento de profesionales especializados, junto con el desarrollo de una infraestructura tecnológica adecuada, son elementos clave para enfrentar estos desafíos. Del mismo modo, se requiere la implementación de mecanismos de prevención e investigación articulados y coordinados entre distintos organismos.

En respuesta a esta problemática, el 8 de enero de 2025, el Ministerio de Seguridad de la Nación emitió la Resolución 19/2025 (RESOL-2025-19-APN-MSG), mediante la cual se creó el Programa de Fortalecimiento en Ciberseguridad e Investigación del Ciberdelito (ForCIC). Este programa, dependiente de la Dirección de Ciberdelito y Asuntos Cibernéticos de la Unidad Gabinete de Asesores del Ministerio, completa un “trípode” normativo que incluye la Disposición Administrativa DA/641/2021 y la Resolución 3/2023 de la Dirección Nacional de Ciberseguridad. En conjunto, estas normativas buscan fortalecer la capacidad de los organismos públicos para prevenir, detectar y mitigar los riesgos cibernéticos que afectan la integridad de la información en la Administración Pública Nacional (APN).

En este informe se analiza el contenido y la obligatoriedad de cumplimiento de estas normativas, destacando su importancia en el contexto de la ciberseguridad nacional y los desafíos que enfrenta su implementación.

1. Disposición Administrativa DA/641 de la Dirección Nacional de Ciberseguridad (DNCS)

La DA/641 establece un marco normativo integral para la protección de los sistemas de información en el ámbito de la Administración Pública Nacional, alcanzando también a sus proveedores. Su objetivo principal es garantizar la protección de infraestructuras críticas y datos sensibles, así como promover una respuesta coordinada ante los incidentes de ciberseguridad que pudieran afectarlos.

Características principales:

- Marco normativo y de coordinación: La DA/641 proporciona un marco legal para la protección de sistemas de información en entidades públicas, fomentando una estructura organizada para la respuesta a incidentes cibernéticos a nivel nacional.

- Fortalecimiento de la infraestructura de ciberseguridad: Establece principios y políticas para la protección de infraestructuras tecnológicas críticas, como redes, sistemas y servicios esenciales.

- Desarrollo de capacidades: Promueve la creación de capacidades en el sector público y privado para enfrentar riesgos cibernéticos, incluyendo la implementación de centros de monitoreo y respuesta ante incidentes.

- Colaboración interinstitucional: Fomenta la cooperación entre entidades gubernamentales, organismos internacionales y empresas privadas para compartir información relevante sobre ciberseguridad.

- Adopción de estándares internacionales: La normativa exige la adopción de mejores prácticas internacionales, como las establecidas en la norma ISO/IEC 27001:2013, adaptándolas al contexto nacional.

Obligaciones a cumplir:

1. Implementación de medidas preventivas: Las instituciones públicas deben adoptar medidas como la actualización de software, uso de firewalls, sistemas de detección de intrusiones y técnicas de encriptación.

2. Gestión de riesgos y vulnerabilidades: Se requiere un proceso continuo de identificación y evaluación de riesgos para reducir la exposición a ciberataques.

3. Planes de contingencia y respuesta: Las organizaciones deben contar con planes detallados para la gestión de incidentes, incluyendo procedimientos de detección, contención, erradicación y recuperación.

4. Gobernanza en ciberseguridad: Se insta a las organizaciones a establecer una estructura de gobernanza que designe responsables para supervisar las políticas de seguridad.

5. Capacitación del personal: Es obligatorio capacitar a empleados y funcionarios en materia de ciberseguridad para promover buenas prácticas y prevenir incidentes.

6. Protección de datos y privacidad: Se deben implementar medidas para proteger datos sensibles, cumpliendo con normativas locales e internacionales, como la Ley de Protección de Datos Personales de Argentina.

7. Auditorías y revisión de políticas: Las entidades deben realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas.

La DA/641 representa un avance significativo en la ciberseguridad nacional, aunque su implementación enfrenta desafíos relacionados con la falta de recursos y la necesidad de actualización constante frente a las amenazas emergentes.

2. Disposición 3/2023 de la ex-Subsecretaria de Tecnologías de la Información (DNCS)

La Disposición 3, aprobada el 4 de julio de 2023, establece la Guía de Notificación y Gestión de Incidentes de Ciberseguridad. Esta guía busca estandarizar los procesos de notificación y gestión de incidentes en los organismos públicos.

Características principales:

- Estandarización de procesos: Proporciona pautas claras para la notificación y gestión de incidentes, unificando los procedimientos de reporte al Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar).

- Taxonomía y clasificación: Establece una clasificación común de incidentes basada en estándares internacionales como los del NIST, ISO y ENISA.

- Pautas de notificación: Define procedimientos y plazos para la notificación de incidentes, facilitando una respuesta rápida y coordinada.

Obligaciones a cumplir:

1. Notificación obligatoria: Los organismos de la APN deben notificar al CERT.ar cualquier incidente de ciberseguridad, siguiendo las pautas establecidas.

2. Gestión de incidentes: Se deben implementar procedimientos internos alineados con las recomendaciones de la guía, asegurando la confidencialidad, integridad y disponibilidad de la información.

La Disposición 3/2023 fortalece la capacidad de respuesta ante incidentes cibernéticos, promoviendo una gestión más eficiente y coordinada en el ámbito público.

3. Resolución 19/2025 del Ministerio de Seguridad de la Nación

La Resolución 19/2025 crea el Programa de Fortalecimiento en Ciberseguridad e Investigación del Ciberdelito (ForCIC), cuyo objetivo es coordinar, asistir y brindar asesoramiento en materia de seguridad digital e investigación de ciberdelitos.

Objetivos principales:

- Incrementar las capacidades de prevención, detección, análisis y respuesta ante incidentes cibernéticos.
- Fortalecer las actividades de investigación de ciberdelitos en las fuerzas policiales y de seguridad federales.
- Elaborar métricas específicas sobre la situación de ciberseguridad y su impacto en la seguridad nacional.
- Promover la colaboración interjurisdiccional y la concientización sobre ciberseguridad.

El ForCIC representa un avance hacia una estrategia nacional integral en ciberseguridad, aunque su éxito dependerá de la asignación de recursos, el compromiso de los responsables de cada organismo y la coordinación efectiva entre los distintos actores involucrados.

Conclusión

Con el análisis de las normativas, se evidencia que constituyen un marco normativo que permite fortalecer la ciberseguridad en la APN. No obstante, su implementación efectiva enfrenta desafíos considerables, entre los que se destacan la insuficiencia de recursos financieros y humanos, la carencia de mecanismos de control eficaces y la necesidad de desarrollar un programa integral de capacitación y concientización, especialmente dirigido al personal jerárquico.

Para superar estos obstáculos, resulta imperativo:

- Asignar recursos adecuados que permitan la implementación efectiva de las medidas de seguridad propuestas.
- Fomentar la cooperación interinstitucional y garantizar la participación activa de todas las jurisdicciones, con especial atención a las regiones del interior del País.
- Actualizar las normativas en línea con los estándares y avances internacionales en materia de ciberseguridad.
- Promover una cultura organizacional de ciberseguridad mediante programas continuos de capacitación y concientización, enfocados en todos los niveles de la administración.

La situación actual puede ilustrarse mediante la analogía de un trípode, donde cada pata representa una de las normativas clave analizadas. La estabilidad de esta estructura depende del equilibrio y la complementariedad entre estos tres pilares normativos, los cuales sostienen la protección integral de los sistemas, datos y servicios de la APN. Si una de las patas se debilita o desalinea, la estructura completa se ve comprometida, exponiendo a riesgos significativos su seguridad.

En un contexto de digitalización de trámites y de la gestión, y en el que las amenazas cibernéticas evolucionan constantemente y se tornan cada vez más sofisticadas, la APN debe adoptar un enfoque proactivo y estratégico que garantice la protección de sus activos digitales. Si bien los marcos normativos actuales (el trípode) aún no se encuentran plenamente alineados y equilibrados, es posible alcanzar una gobernanza eficiente en ciberseguridad mediante una gestión adecuada y un compromiso firme por parte de todos los actores involucrados.

El camino hacia una implementación efectiva es complejo y está plagado de desafíos, pero no es insuperable. Con una visión clara, una planificación estratégica y una ejecución coordinada, la APN puede avanzar hacia un modelo de ciberseguridad robusto y resiliente, capaz de enfrentar los retos del entorno digital actual y futuro.