

Ciberseguridad: la ley para evitar ataques en Mendoza con un equipo anti-hacker

03/07/2026



El **Gobierno** envió este jueves a la **Legislatura** un proyecto de **Ley de Ciberseguridad** que busca establecer una política de **Estado** para proteger la infraestructura digital de los tres poderes provinciales, los servicios públicos esenciales y los sistemas informáticos que sostienen el funcionamiento del Estado.

La iniciativa, impulsada por el Ministerio de Seguridad y Justicia, crea un esquema integral de prevención, monitoreo y respuesta ante ciberataques, en un contexto en el que este tipo de delitos registra un crecimiento sostenido a nivel mundial.

La presentación se realizó en el Salón Azul de la Legislatura y estuvo encabezada por la ministra de Seguridad y Justicia, **Mercedes Rus**, quien sostuvo que la Provincia debe prepararse frente a una amenaza que ya afecta a organismos públicos y privados. Como ejemplo, recordó el ataque sufrido por el **Registro Nacional de las Personas (RENAPER)** y otros episodios registrados contra poderes judiciales de distintas provincias.

Rus señaló además que en **Argentina** las organizaciones privadas reciben cerca de 2.800 intentos de ataques informáticos por semana. *“Tenemos que estar preparados. Buscar estar mejor preparados que el atacante para poder llevar adelante esto”*, remarcó.

Las claves

El proyecto establece obligaciones para el **Poder Ejecutivo, el Poder Legislativo y el Poder Judicial**, además de alcanzar a proveedores tecnológicos y prestadores de servicios críticos esenciales que operen con el **Estado provincial**. También invita a los municipios a adherir a la normativa respetando su autonomía.

Entre sus principales herramientas crea un **Comité de Conducción Estratégica de Ciberseguridad**, encargado de elaborar el **Plan Provincial de Ciberseguridad**, definir estándares técnicos y supervisar su cumplimiento, mientras que una Autoridad de Ejecución Operativa tendrá a su cargo la respuesta concreta frente a incidentes informáticos.

Rus explicó que uno de los aspectos centrales de la iniciativa es la diferenciación entre las funciones de planificación y control y las tareas operativas. *“Va a haber un plan de ciberseguridad que deberá elaborar el comité ejecutivo, además de las guías y estándares. La norma diferencia claramente las funciones de elaboración, fiscalización y auditoría respecto*

de las tareas de ejecución operativa”, indicó.

La ministra agregó que la futura autoridad operativa será **la responsable de ejecutar las acciones de ciberseguridad dentro del Estado, coordinar la respuesta ante incidentes y supervisar cómo reaccionan los distintos organismos frente a un ataque.**

El proyecto contempla además la creación de un **Centro de Operaciones de Seguridad (SOC)**, un **Equipo de Respuesta ante Incidentes (CSIRT)** y un **Registro Provincial de Incidentes de Ciberseguridad**, destinado a centralizar la información sobre vulnerabilidades y ataques para mejorar la capacidad de respuesta institucional.

La iniciativa incorpora además un régimen de gobierno de datos **que obliga a proteger la información pública durante todo su ciclo de vida, desde su creación hasta su eliminación**, e impone estándares mínimos de seguridad para los organismos estatales y las empresas que administren infraestructura tecnológica vinculada con el Estado.

También prevé la identificación de **infraestructura digital** crítica, cuya interrupción podría comprometer servicios esenciales como **salud, seguridad, justicia, educación, transporte o energía.**

La explicación de Rus

Durante la presentación, Rus diferenció el alcance de esta ley de las reformas penales vinculadas al ciberdelito. Explicó que Mendoza ya elevó propuestas al Ministerio de Seguridad de la Nación para actualizar el Código Penal en materia de sustitución de identidad y ciberestafas, pero aclaró que la nueva norma tiene un objetivo distinto.

“Esta ley adopta una política de Estado para proteger los sistemas digitales de los que dependen servicios públicos

esenciales. Si un ataque afecta el sistema del transporte, el problema ya no es solamente si funciona el servicio, sino que puede generar accidentes y poner en riesgo la integridad física de las personas”, ejemplificó.

La funcionaria sostuvo además que el crecimiento del crimen informático obliga a modificar las prioridades de seguridad pública. *“Hoy el ciberdelito avanza más rápido que el robo y más rápido que el narcotráfico. A nivel internacional ya se lo considera la principal forma de criminalidad organizada porque evoluciona a la misma velocidad que la tecnología”, afirmó.*

En los fundamentos del proyecto, el Ejecutivo destaca que Mendoza ya desarrolló herramientas específicas para investigar delitos informáticos, entre ellas fiscalías especializadas, el agente encubierto digital, el allanamiento digital y un Laboratorio Forense Digital destinado al análisis de evidencia tecnológica.

También menciona inversiones en inteligencia artificial aplicada a videovigilancia, identificación biométrica, análisis predictivo y capacitación junto a universidades y organismos internacionales. Según el texto, la nueva ley busca consolidar todas esas acciones bajo un marco institucional permanente y convertirlas en una política de Estado.

La iniciativa consta de 42 artículos y deberá comenzar ahora su tratamiento legislativo que iniciará en el Senado. De ser aprobada, Mendoza se convertiría en la primera provincia del país en contar con una ley integral de ciberseguridad para proteger la infraestructura digital estatal y garantizar la continuidad de los servicios públicos frente a ataques informáticos.

Fuente: El Sol –
<https://www.elsol.com.ar/mendoza/ciberseguridad-la-ley-para-evitar-ataques-en-mendoza-con-un-equipo-anti-hacker/>