Buenos Aires, 24 de junio de 2026

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD TECNOLÓGICA NACIONAL

VISTO la necesidad de establecer un marco normativo integral para la gestión de la seguridad de la información en el ámbito de la Universidad Tecnológica Nacional; las actuaciones originadas en el Comité de Seguridad de la Información; la Nota N° 4/2026 de la Unidad de Auditoría Interna de fecha 26 de marzo de 2026; la respuesta elaborada por la Secretaría de Tecnologías de la Información y las Comunicaciones con fecha 16 de abril de 2026; y el Acta N° 1/2026 del Comité de Seguridad de la Información de fecha 30 de abril de 2026, y

CONSIDERANDO

Que la información constituye un recurso esencial para el cumplimiento de las funciones académicas, científicas, administrativas y de gestión de la Universidad Tecnológica Nacional, siendo soporte de los procesos de enseñanza, investigación, extensión y administración.

Que el avance sostenido del proceso de transformación digital ha incrementado exponencialmente la generación, almacenamiento, circulación y uso de información en entornos digitales, ampliando a su vez la superficie de exposición a riesgos tecnológicos, operativos y organizacionales.

Que, en este contexto, resulta necesario fortalecer las capacidades institucionales para prevenir, detectar, responder y recuperarse frente a incidentes que puedan comprometer la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

Que en el marco del Seguimiento de Observaciones del ejercicio 2025, la Unidad de Auditoría Interna ha requerido a esta Universidad información detallada respecto del estado de implementación, formalización y consolidación de la Política de Seguridad de la Información, poniendo de manifiesto la necesidad de fortalecer la gobernanza en la materia.

Que la Secretaría de Tecnologías de la Información y las Comunicaciones ha elaborado una respuesta institucional que sistematiza el marco normativo vigente, la estructura organizativa existente, así como las acciones implementadas y las medidas de mejora en curso, evidenciando un grado significativo de avance, aunque señalando la necesidad de consolidación normativa y documental.

Que la Universidad cuenta con una Política de Seguridad de la Información vigente, con una estructura organizativa basada en el Comité de Seguridad de la Información y con la implementación progresiva de controles técnicos y operativos, configurando un escenario de maduración institucional en la materia.

Que el Comité de Seguridad de la Información, como órgano especializado, ha analizado y avalado la respuesta institucional, recomendando expresamente avanzar en la formulación de un instrumento normativo de jerarquía superior que permita consolidar y dar sostenibilidad a los avances alcanzados.

Que la Universidad ha adoptado los lineamientos establecidos por la Decisión Administrativa N° 641/2021 de la Jefatura de Gabinete de Ministros, que establece los requisitos mínimos de seguridad de la información para organismos del sector público, promoviendo su adecuación a las buenas prácticas vigentes.

Que asimismo se han promovido acciones orientadas a alinear progresivamente la gestión institucional de la seguridad de la información con estándares

internacionales, en particular los establecidos en la familia de normas ISO/IEC 27000, reconocidas por su enfoque sistemático basado en gestión de riesgos y mejora continua.

Que la Política de Seguridad de la Información vigente reconoce expresamente que el conocimiento, los datos y la información constituyen activos estratégicos de la Universidad, en muchos casos de naturaleza intangible, cuya protección resulta esencial para garantizar la continuidad de sus funciones sustantivas.

Que en virtud de lo expuesto, resulta necesario establecer un marco normativo integral, que estructure la gobernanza institucional en materia de seguridad de la información, defina roles y responsabilidades, y promueva un enfoque articulado, federal y progresivo para su implementación.

Que dicho marco permitirá consolidar un sistema institucional orientado a la gestión de riesgos, la trazabilidad de las acciones, la generación de evidencia ante organismos de control y la mejora continua de las prácticas.

Por ello,

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD TECNOLÓGICA NACIONAL

ORDENA:

CAPÍTULO I – OBJETO, ALCANCE Y PRINCIPIOS

ARTÍCULO 1°.- La presente ordenanza tiene por objeto establecer el marco institucional para la gestión integral de la seguridad de la información en la Universidad Tecnológica Nacional, definiendo principios, estructuras de gobernanza, responsabilidades y lineamientos generales orientados a la protección de los activos de información.

ARTÍCULO 2°.- Las disposiciones de la presente serán de aplicación en el ámbito del Rectorado, promoviendo su adopción por parte de las Facultades Regionales, en el marco de un enfoque federal, coordinado y progresivo.

ARTÍCULO 3°.- La gestión de la seguridad de la información se regirá por los principios de:

- protección de los activos de información
- gestión de riesgos
- responsabilidad compartida
- trazabilidad de las acciones
- mejora continua

CAPÍTULO II – ACTIVOS DE INFORMACIÓN

ARTÍCULO 4°.- Reconócese a la información, los datos, el conocimiento institucional y los sistemas que los procesan como activos estratégicos de la Universidad, incluyendo aquellos de naturaleza intangible, esenciales para el cumplimiento de su misión.

ARTÍCULO 5°.- Dichos activos deberán ser identificados, clasificados, valorados y protegidos conforme a criterios de seguridad de la información, en función de su criticidad y sensibilidad, mediante la adopción de esquemas de clasificación que contemplen niveles diferenciados de acceso, tratamiento y resguardo.

ARTÍCULO 6°.- La Universidad promoverá la incorporación progresiva de los activos de información en los sistemas de gestión patrimonial institucional, conforme a las definiciones y mecanismos que establezca la reglamentación.

CAPÍTULO III – GOBERNANZA INSTITUCIONAL

ARTÍCULO 7°.- La gobernanza de la seguridad de la información se estructura en los siguientes niveles:

- El Consejo Superior, como órgano normativo
- El Comité de Seguridad de la Información, como órgano responsable de la dirección estratégica y supervisión
- La Secretaría de Tecnologías de la Información, como autoridad de aplicación
- Las dependencias y Facultades Regionales, como responsables de implementación

Sección I – Comité de Seguridad de la Información

ARTÍCULO 8°.- El Comité de Seguridad de la Información será el órgano responsable de la dirección estratégica, definición, revisión y supervisión de las políticas institucionales en la materia.

ARTÍCULO 9°.- Son funciones del Comité de Seguridad de la Información:

- Proponer políticas, lineamientos y normativa institucional en la materia;
- Supervisar la implementación de la Política de Seguridad de la Información en el ámbito universitario;
- Evaluar periódicamente el estado de situación y los riesgos asociados;
- Emitir recomendaciones a las autoridades competentes;
- Promover la mejora continua de las prácticas institucionales;
- Asegurar la coherencia, uniformidad y alineamiento institucional en la aplicación de las políticas de seguridad de la información en todo el ámbito de la Universidad.

ARTÍCULO 10°.- El Comité desarrollará sus actividades con dependencia funcional del Rectorado y dará cuenta de sus actuaciones al Consejo Superior.

Sección II – Secretaría de Tecnologías de la Información

ARTÍCULO 11°.- La Secretaría TIC será la autoridad de aplicación de la presente ordenanza.

ARTÍCULO 12°.- Son sus funciones:

- implementar políticas definidas
- dictar normas técnicas y procedimientos
- ejecutar controles
- monitorear cumplimiento
- elaborar informes

ARTÍCULO 13°.- Articulará su accionar con el Comité de Seguridad de la Información en el marco de las funciones asignadas.

CAPÍTULO IV – ORGANIZACIÓN INSTITUCIONAL

ARTÍCULO 14°.- Las dependencias del Rectorado y las Facultades Regionales deberán designar responsables en materia de seguridad de la información, quienes actuarán como referentes en la implementación de las políticas, la coordinación con la Secretaría TIC y la articulación con el Comité de Seguridad de la Información, conforme a lo que establezca la reglamentación.

ARTÍCULO 15°. - Se promoverá un esquema de responsabilidad compartida entre las distintas áreas que gestionan información institucional.

CAPÍTULO V – POLÍTICAS Y MARCO NORMATIVO

ARTÍCULO 16°.- (Marco Normativo y de Referencia)

La gestión de la seguridad de la información en el ámbito de la Universidad Tecnológica Nacional se desarrollará en concordancia con un marco normativo integral que articula:

a) La Política de Seguridad de la Información institucional vigente, que establece los principios, lineamientos organizativos, roles y responsabilidades para la protección de los activos de información en toda la Universidad;

b) La normativa nacional aplicable, en particular la Decisión Administrativa N° 641/2021 de la Jefatura de Gabinete de Ministros, sus normas complementarias y modificatorias, en cuanto establecen requisitos mínimos de seguridad de la información para organismos del sector público, promoviendo un enfoque basado en el control interno, la gestión de riesgos y la evidencia documental;

c) Los estándares internacionales reconocidos, especialmente los comprendidos en la familia de normas ISO/IEC 27000, que orientan la implementación de sistemas de gestión

de la seguridad de la información basados en buenas prácticas, mejora continua y enfoque sistemático.

La articulación de estos instrumentos garantiza que la Universidad adopte un enfoque coherente, progresivo y alineado con los requerimientos institucionales, normativos y técnicos vigentes.

La Universidad promoverá la construcción progresiva de un Sistema de Gestión de Seguridad de la Información (SGSI), conforme a estándares internacionales reconocidos, orientado a la mejora continua, la gestión de riesgos y la trazabilidad institucional.

Artículo 17°.- (Componentes del Sistema de Seguridad de la Información)

Las políticas, normas y procedimientos que se dicten en el marco de la presente ordenanza deberán configurar un sistema integral de gestión de la seguridad de la información, contemplando de manera articulada y consistente, como mínimo, los siguientes componentes:

a) Gestión de activos de información

Comprende la identificación, registro, clasificación, valoración y protección de los activos de información, incluyendo la definición de categorías según su criticidad y sensibilidad,, tales como datos, conocimientos, sistemas y procesos, en función de su criticidad y sensibilidad para la Institución.

b) Gestión de riesgos

Implica la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la seguridad de la información, permitiendo establecer medidas de prevención y mitigación acordes al nivel de exposición y a la tolerancia institucional al riesgo.

c) Control de accesos y gestión de identidades

Refiere al conjunto de mecanismos destinados a asegurar que el acceso a la información y a los sistemas se realice exclusivamente por parte de usuarios autorizados, conforme a sus funciones, garantizando autenticación, autorización y trazabilidad.

d) Seguridad de sistemas, redes y comunicaciones

Abarca la protección de la infraestructura tecnológica, incluyendo sistemas, aplicaciones, redes y comunicaciones, mediante la implementación de controles técnicos que permitan prevenir, detectar y mitigar amenazas y vulnerabilidades.

e) Gestión de incidentes de seguridad

Comprende el establecimiento de procedimientos para la detección, registro, análisis, respuesta y recuperación ante eventos que comprometan o puedan comprometer la seguridad de la información, asegurando una gestión coordinada y documentada.

f) Continuidad operativa y recuperación

Implica la planificación y ejecución de medidas que permitan asegurar la continuidad de los servicios críticos y la recuperación de la información ante situaciones adversas, incluyendo respaldos, planes de contingencia y pruebas periódicas.

g) Gestión de terceros y proveedores

Refiere a la definición de condiciones, controles y responsabilidades en la relación con terceros que acceden o procesan información institucional, asegurando el cumplimiento de las políticas de seguridad adoptadas por la Universidad.

h) Capacitación y concientización

Comprende el desarrollo de acciones sistemáticas destinadas a formar y sensibilizar a la comunidad universitaria en materia de seguridad de la información, reconociendo el factor humano como componente crítico del sistema.

i) Auditoría, monitoreo y mejora continua

Incluye la evaluación periódica del cumplimiento de las políticas y controles implementados, la generación de evidencias, y la adopción de acciones correctivas y de mejora que permitan fortalecer el sistema de seguridad de la información en forma progresiva.

j) Cumplimiento normativo

Comprende la identificación, registro, clasificación, valoración y protección de los activos de información, incluyendo la definición de categorías según su

criticidad y sensibilidad, asegurando la adecuación permanente de las prácticas de seguridad a los requerimientos establecidos por los organismos de control y el marco jurídico aplicable.

CAPÍTULO VI – IMPLEMENTACIÓN Y CONTROL

ARTÍCULO 18°.- La implementación será progresiva, basada en riesgos y priorización institucional.

ARTÍCULO 19°.- La autoridad de aplicación establecerá mecanismos de monitoreo, evaluación y auditoría periódica, orientados a verificar el cumplimiento de las políticas y controles implementados, generar evidencia documental suficiente y promover la adopción de acciones correctivas y de mejora continua en el ámbito institucional.

CAPÍTULO VII – CONTINUIDAD Y RESPUESTA

ARTÍCULO 20°.- La Universidad deberá contar con procedimientos formales de gestión de incidentes. La autoridad de aplicación elaborará informes periódicos sobre el estado de la seguridad de la información en la Universidad, los cuales serán elevados al Rector y puestos en conocimiento del Consejo Superior, a fin de garantizar la adecuada supervisión institucional.

ARTÍCULO 21°.- Se implementarán planes de continuidad y recuperación, asegurando la continuidad de los servicios críticos y de las funciones académicas, de investigación, extensión y gestión de la Universidad.

CAPÍTULO VIII – CAPACITACIÓN

ARTÍCULO 22°.- Se implementarán programas permanentes de capacitación y concientización.

CAPÍTULO IX – ADHESIÓN

ARTÍCULO 23°.- Invítase a las Facultades Regionales a adherir.

ARTÍCULO 24°.- Se establece un proceso de adecuación progresiva.

CAPÍTULO X – DISPOSICIONES FINALES

ARTÍCULO 25°.- Apruébase el ANEXO I – Lineamientos Generales de Seguridad de la Información, el cual forma parte integrante de la presente ordenanza y establece criterios orientadores para la implementación progresiva de las políticas definidas.

ARTÍCULO 26°.- La presente normativa entrará en vigor a partir de su aprobación. Las disposiciones de la presente ordenanza deberán interpretarse en forma dinámica, conforme a la evolución de las tecnologías de la información, los estándares

aplicables y la normativa vigente, promoviendo su adecuación continua en el marco de los principios establecidos.

ARTÍCULO 27°.- Facúltase a la Secretaría TIC a dictar normativa reglamentaria.

ARTÍCULO 28°.- Registrese,comuniquese. Archivese.

ORDENANZA N°2243

ANEXO I

ORDENANZA N°2243

LINEAMIENTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

A fin de orientar la implementación de la presente ordenanza, se establecen los siguientes lineamientos generales:

1. Identificación y clasificación de la información institucional según su nivel de criticidad y sensibilidad.
2. Definición de responsables de los activos de información.
3. Implementación de controles de acceso basados en funciones.
4. Establecimiento de procedimientos de gestión de incidentes de seguridad.
5. Desarrollo de mecanismos de respaldo y recuperación de la información.
6. Implementación de medidas de seguridad en sistemas, redes y comunicaciones.
7. Evaluación periódica de riesgos asociados a la información.
8. Registro y monitoreo de actividades relevantes.
9. Capacitación continua de los usuarios.
10. Promoción de la mejora continua del sistema de seguridad de la información.