Comisión de Transformación Digital
ACTUALIZACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Resolución CE Nº 2004/26
Buenos Aires, 5 de agosto de 2026

VISTO:
la actualización del documento "Política de seguridad de la información" elaborado por la Comisión de Transformación Digital;
la Resol. CE N° 1669/22; y

CONSIDERANDO:
que la resolución mencionada en el visto aprobó el documento denominado "Políticas de Seguridad de la Información" y su guía de instrucciones en el 2022;
que, en consecuencia de los desarrollos de tipo tecnológico, normativo, organizacional y de gestión corresponde una adecuación de las políticas al nuevo escenario;
que la Comisión de Transformación Digital, a través del trabajo de la Subcomisión de Ciberseguridad, propone el documento que contiene la actualización de los aspectos señalados en el considerando precedente;
que se trata de una guía para que cada Casa de Altos Estudios pueda utilizar adaptándola a su contexto y normativa;
que este cuerpo considera debe proveerse de conformidad a lo recomendado.
Por ello,

EL COMITÉ EJECUTIVO
DEL CONSEJO INTERUNIVERSITARIO NACIONAL
Resuelve:

Artículo 1º: Aprobar la actualización del documento denominado "Políticas de Seguridad de la Información en las instituciones universitarias públicas" que como anexo se agrega a la presente.

Artículo 2º: Regístrese, dese a conocer y archívese.

Mario Miguel F. Gimelli, Secretario Ejecutivo
Franco Bartolacci, Presidente

Consejo Interuniversitario Nacional

Resol. CE N° 2004/26 – anexo

Política de seguridad de la información de las instituciones universitarias

Introducción

El conocimiento es el activo más importante de la UUNN. Estos conocimientos se adquieren gracias al análisis y el proceso de los datos e información que se generan en archivos digitales o papeles, con el fin de dar cumplimiento a la misión estratégica. En el contexto de transformación digital en el que se encuentra avanzando la UUNN, se hace indispensable para su organización tener un control sobre sus archivos, manteniendo y asegurando su integridad, confidencialidad y disponibilidad de la información.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. También se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por fallos técnicos o, porque no, por catástrofes naturales.

Es por ello, que esta política establece un marco organizativo y operacional para fortalecer la seguridad de los sistemas, los datos y los servicios prestados por la UUNN, alineada a la DA 641/21 de la Jefatura de Gabinete de Ministros "Requisitos mínimos de Seguridad de la Información para Organismos".

La UUNN debe estar preparada para prevenir, detectar, responder y recuperarse de incidentes.

Prevención

La UUNN debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad propuestas para los organismos nacionales así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estas medidas, los roles y las responsabilidades de seguridad de la información de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de esta Política, la UUNN debe:

- Establecer los mecanismos para autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Realizar continuas campañas de concientización a los miembros de la comunidad universitaria.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.
La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Las instituciones universitarias públicas debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la universidad.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias Informáticas o CERT (Computer Emergency Response Team) reconocidos a nivel nacional e internacional.

Recuperación

Para garantizar la disponibilidad de los servicios críticos, la UUNN debe desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

A partir de lo expuesto hasta aquí se propone el siguiente modelo de Política de Seguridad de la Información para las universidades, que puede ser tomado como base y adaptado por cada institución.

CiN Consejo Interuniversitario Nacional

ÍNDICE

Introducción 2
ÍNDICE 4
1. Misión 5
2. Alcance 5
3. Marco Normativo 5
Leyes relacionadas a la ciberseguridad 5
Normativas vinculadas a las funciones de la Dirección Nacional de Ciberseguridad
Otras normativas relacionadas a la ciberseguridad
4. Organización de la seguridad de la información 6
4.1 Roles, funciones y responsabilidades de seguridad 6
Propietario de la Información 7
Responsables de los servicios 7
Responsable de Seguridad de la Información 7
Responsables de los sistemas 7
Responsable del Área de Recursos Humanos 8
Responsable del Área Informática 8
Responsable del Área Legal o Jurídica 8
Toda la comunidad 8
4.2 Conformación del Comité de Seguridad 9
Funciones y Responsabilidades 9
Coordinador del comité de seguridad de la información 10
5. Gestión de riesgos 10
6. Obligaciones de la comunidad universitaria 10
7. Terceras partes 10
8. Normativas de seguridad 11

1. Misión

Cada institución universitaria pública debe incluir la misión definida en el estatuto.

2. Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la institución universitaria pública.
Debe ser conocida y cumplida por todos los miembros de la Institución, tanto se trate de personal como de estudiantes, desde funcionarios políticos hasta técnicos, y sea cual fuere su nivel jerárquico y su situación de revista; y terceros vinculados a la misma.

3. Marco Normativo

Son de aplicación las leyes y normativas nacionales, provinciales y municipales en relación con seguridad de la información, protección de datos personales, propiedad intelectual y uso de herramientas de comunicaciones informáticas[1].

Leyes relacionadas a la ciberseguridad

3.1 Legislación Nacional

- Ley 25.326 – Protección de Datos Personales.
- Decreto 1558/2001 – Reglamenta la Ley 25.326.
- Leyes 27.483 y 27.699 – Convenio 108 y Protocolo 108+.
- Ley 26.388 – Delitos Informáticos.
- Ley 26.904 – Grooming.
- Ley 25.506 – Firma Digital.
- Decreto 2628/2002 – Reglamenta la Ley 25.506.
- Ley 11.723 – Propiedad Intelectual.

[1] https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

3.2 Normativa del Sector Público Nacional

• Decisión Administrativa 641/2021 – Requisitos Mínimos de Seguridad de la Información (RMSI).
• Resolución 44/2023 – Segunda Estrategia Nacional de Ciberseguridad.
• Disposición ONTI 3/2013 – Política de Seguridad de la Información Modelo.
• Disposición 1/2021 – Estructura del CERT.ar.
• Disposición 6/2021 – Comité para Desarrollo Seguro.
• Disposición 8/2021 – Guía para Desarrollo Seguro de Aplicaciones Web.
• Resolución 580/2011 – Programa Nacional de Protección de Infraestructuras Críticas.
• Resolución 1523/2019 – Infraestructuras Críticas de Información.

3.3 Estrategia y Gobernanza Nacional de Ciberseguridad

• Decreto 577/2017 – Comité de Ciberseguridad.
• Decreto 480/2019 – Actualización del Comité de Ciberseguridad.

3.4 Estándares Técnicos y Marcos Internacionales de Referencia

• ISO/IEC 27001:2022 – SGSI.
• ISO/IEC 27002:2022 – Controles de Seguridad.
• ISO/IEC 27005:2022 – Gestión de Riesgos.
• NIST CSF 2.0 (2024) – Marco de Ciberseguridad.
• NIST SP 800-61r2 – Gestión de Incidentes.

4. Organización de la seguridad de la información

La UUNN establecerá roles y responsabilidades claras a fin de garantizar la gestión adecuada de la seguridad de la información en toda la institución.

4.1 Roles, funciones y responsabilidades de seguridad

4.1.1 Autoridad Superior

La Autoridad Superior (Rector, Consejo Superior o quien corresponda) será responsable de:

• Aprobar esta Política y sus actualizaciones.
• Proveer los recursos necesarios para su implementación.
• Designar al Responsable de Seguridad de la Información.
• Supervisar el cumplimiento institucional.

4.1.2 Propietario de la Información

Cada área será responsable de su propia información y deberá:

• Determinar la clasificación del activo.
• Definir requisitos de seguridad.
• Aceptar o rechazar riesgos residuales.
• Trabajar con el RSI y TI en la protección del activo.

4.1.3 Responsable de Seguridad de la Información (RSI)

Será responsable de:

• Coordinar la implementación de esta Política.
• Elaborar normativa complementaria.
• Gestionar incidentes y participar en la respuesta.
• Monitorear el cumplimiento de medidas de seguridad.
• Coordinar el proceso de análisis y gestión de riesgos.
• Mantener relación con CERT.ar y organismos externos.
• Promover la concientización institucional.

4.1.4 Responsable de Tecnología de la Información (TI)

Será responsable de:

• Implementar las medidas técnicas de seguridad.
• Administrar infraestructura y sistemas.
• Aplicar controles de acceso, respaldos, parches y monitoreo.
• Asegurar que los sistemas operen conforme a los niveles de clasificación establecidos.
• Mantener documentación técnica actualizada.

4.1.5 Responsable de los Sistemas

Para cada sistema, deberá:

• Administrar su ciclo de vida (implementación, operación, cambios).
• Coordinar con TI y RSI las medidas de seguridad aplicables.
• Mantener registros y configuración autorizada.
• Supervisar incidentes técnicos relacionados con el sistema.

4.1.6 Responsable del Área Personal

Será responsable de:

• Informar al personal sobre responsabilidades y normativa de seguridad.
• Gestionar compromisos de confidencialidad.
• Coordinar acciones de capacitación y concientización.

4.1.7 Responsable del Área Legal

Será responsable de:

• Asegurar que los contratos y acuerdos incorporen requisitos de seguridad.
• Asesorar sobre aspectos legales vinculados a protección de datos, incidentes, propiedad intelectual y normativa aplicable.

4.1.8 Responsables de Proveedores y Terceras Partes

Deberán:

• Verificar que los proveedores cumplan los requisitos de seguridad aplicables.
• Supervisar contratos, acuerdos y niveles de servicio.
• Garantizar que los proveedores manejen la información conforme a su clasificación.

4.1.9 Comité de Seguridad de la Información

Será responsable de:

• Revisar periódicamente esta Política.
• Evaluar riesgos relevantes e incidentes graves.
• Aprobar metodologías y criterios en materia de seguridad.
• Coordinar acciones interáreas y resolver conflictos.
• Elevar informes a la Autoridad Superior.

4.1.10 Toda la Comunidad Universitaria

Toda persona que acceda a sistemas o información de la UUNN deberá:

• Conocer y cumplir esta Política.
• Respetar los niveles de clasificación de la información.
• Reportar incidentes de seguridad.
• Participar en actividades de capacitación obligatoria.

4.2 Conformación del Comité de Seguridad

La conformación aquí establecida incluye los roles que son necesarios mínimamente. Cada organización también podrá incluir otros roles que lo conformarán de acuerdo con sus características y funcionamiento.

1. Responsable de seguridad de la información.
2. Responsable(s) de TI (del área central).
3. Responsable del área Personal.
4. Responsable del área legal.
5. Responsable del área económica.
6. Rector o a quien éste delegue.

El Comité podrá incorporar a sus reuniones a las personas que considere oportuno en función de los temas a tratar.
El Comité propondrá la designación del Coordinador que será aprobado por las autoridades de la UUNN.

Funciones y Responsabilidades

- Revisar y proponer a la máxima autoridad para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Controlar cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área[2].
- Acordar y aprobar metodologías y procesos relativos a seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información; evaluará y coordinará la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Resolver los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

[2] Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo con sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

Coordinador del comité de seguridad de la información

- Coordinar las acciones del Comité de Seguridad de la Información; y de
- Impulsar la implementación y cumplimiento de la Política de seguridad de la información y de toda la normativa que se desprenda de ella.

5. Gestión de riesgos

La Institución evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.
Se debe repetir la evaluación:

- Regularmente, con la frecuencia que el Comité de Seguridad de la Información defina.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados, o cuando haya un cambio significativo en la plataforma tecnológica.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

6. Obligaciones de la comunidad universitaria

Todos los miembros de la UUNN tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados definidos en el alcance de la presente política.
Se debe establecer un programa de concientización continua para atender a todos los miembros de la comunidad universitaria, en particular a los de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

7. Terceras partes

Cuando la UUNN preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la respuesta ante incidentes de seguridad.
Cuando la UUNN utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la referida normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concientizado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se refiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los propietarios de la Información y de los responsables de los servicios afectados antes de seguir adelante.

8. Normativas de seguridad

La política se desarrollará en normativas específicas que permitan la implementación de la presente política.
Se proponen las siguientes temáticas:

- Controles Organizacionales;
- Controles Personales;
- Controles Físicos;
- Controles Técnicos.

Las normativas a desarrollarse deben incluir las temáticas anteriormente listadas pero no limitarse a ellas.

Hoja de firmas