



**Comisión de Administración,
Gestión y Modernización Judicial**

Buenos Aires, 16 de julio de 2026

DICTAMEN CAGyMJ N° 35/2026

TAE A-01-00019275-5/2026 s/ Nueva Política General de Seguridad de la Información del PJ de la CABA y Políticas Específicas de Seguridad de la Información del PJ de la CABA.

Mediante Nota 2F DGlyT N° 531/26, la Dirección General de Informática y Tecnología (DGlyT), dirigida a la Secretaría de Administración General y Presupuesto (SAGyP) indicó que por Resolución CM N° 61/2015 se aprobó la “Política de Uso Aceptable de los Recursos Informáticos, Servicios de la Red y de Internet” y las “Políticas de Seguridad y Normas de Confidencialidad” para el Consejo de Magistratura de la Ciudad Autónoma de Buenos Aires.

Agregó que *“El Consejo de Magistratura de la Ciudad Autónoma de Buenos Aires promueve la utilización de tecnologías de la información y la comunicación (TIC) en forma permanente, con el objeto de garantizar la más eficiente prestación del servicio de justicia.*

En consecuencia, describió la situación actual: *“En estos últimos años se ha registrado un incremento sustancial en el uso de las TIC, hasta el punto de volverse indispensables para el desarrollo de todas las actividades, tanto en lo relativo a la gestión interna como a los servicios brindados a la sociedad. El uso intensivo de las TIC incrementa significativamente la superficie de ataque y la exposición a riesgos y amenazas que comprometen la confidencialidad, integridad y disponibilidad de los activos de información y de los sistemas utilizados en todo el Consejo de la Magistratura para el cumplimiento de sus funciones. Evaluando el incremento de la cantidad y la variedad de amenazas y vulnerabilidades que rodean a los activos de informáticos resulta necesario actualizar la normativa vigente a través de la implementación de normas y estándares de seguridad internacional, ya que la ciberseguridad se ha convertido en una herramienta esencial para proteger la información y prevenir ataques cibernéticos”.*

En este marco destacó: *“... dos normas internacionales de suma importancia, la IRAM-ISO/IEC 27001 de Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información y la IRAM-ISO/IEC 27002 de Tecnología de la Información, Técnicas de Seguridad y el Código de Buenas Prácticas para los Controles de la Seguridad de la Información, ambas adquiridas por este Consejo de la Magistratura. La*



**Comisión de Administración,
Gestión y Modernización Judicial**

norma IRAM-ISO-IEC 27001 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) y su objetivo es proporcionar un marco para la gestión de la seguridad de la información de una organización y proteger los activos de información contra amenazas como el robo, la destrucción o la manipulación de datos. Por su parte, la norma IRAM-ISO/IEC 27002 tiene por finalidad garantizar la privacidad de la información y cumplir con las leyes y regulaciones aplicables, además de proporcionar directrices para la implementación de controles requeridos en un SGSI en una organización y enfocarse en las medidas de seguridad necesarias para proteger la información y cubrir una amplia gama de áreas, como la gestión de riesgos, la seguridad física, la seguridad de la red y la seguridad de la información.”

A tales efectos manifestó: “Para certificar las mencionadas normas y estándares resulta necesario dar un paso intermedio, aprobando una Política General Seguridad de la Información y sus Políticas Específicas de Seguridad de la Información del Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia-, las cuales deben estar basadas en las citadas normas “IRAM”, y al mismo tiempo actualizar los términos y alcances de la Resolución CM N° 61/2015, oportunamente aprobada en junio de 2015. La Política General Seguridad de la Información tiene por finalidad establecer los lineamientos para desarrollar e implementar una arquitectura de seguridad de la información con el fin de proteger la disponibilidad, integridad y confidencialidad de la información gestionada por el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires. Por su parte, las Políticas Específicas de Seguridad de la Información establecen objetivos de seguridad alineados con la política general y al mismo tiempo con las normas IRAM-ISO/IEC 27001 e IRAM-ISO/IEC 27002, conteniendo las definiciones de los requisitos y controles necesarios para garantizar la seguridad de la información”.

Finalmente indicó: “En consecuencia con la aprobación de la mentada Política General de Seguridad de la Información junto a las Políticas Específicas de Seguridad de la Información, resultará oportuno continuar con el proceso de actualización, a través de la elaboración de procedimientos, instructivos, manuales de usuario, registros y formularios de Seguridad de la Información, que brinden operatividad para la efectiva implementación de los lineamientos impartidos respecto a seguridad y tecnología. Es en este marco, que resulta pertinente instruir a la Dirección General de Informática y Tecnología, en su calidad de área técnica competente, a que desarrolle la Política General de Seguridad de la Información junto a las Políticas Específicas de Seguridad de la Información y elabore y mantenga actualizados



**Comisión de Administración,
Gestión y Modernización Judicial**

los procedimientos, instructivos, manuales de usuario, registros y formularios de Seguridad de la Información, y eleve los mismos a la Secretaría de Administración General y Presupuesto del Poder Judicial para su aprobación. La Dirección General de Informática y Tecnología deberá incorporar y publicar los documentos aprobados en materia de Seguridad de la Información en el Repositorio de Documentos de Seguridad de la Información, además de su comunicación a los destinatarios que correspondan según el instrumento, y la realización de capacitaciones permanentes a la totalidad de los actores involucrados en cada proceso”.

En tal sentido, adjuntó un proyecto de Resolución CM que aprueba la *“Política General de Seguridad de la Información del Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia- y las Políticas Específicas de Seguridad de la Información del Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia”* – Adjuntos Nros. 94436/26 y 94437/26 -.

La SAGyP tomo conocimiento de la situación expuesta por la Dirección General de Informática y Tecnología (DGIT), e incorporó un nuevo proyecto de acto administrativo obrante en el Adjunto N° 96323/26 y mediante Memo N° 3501/26, elevó lo actuado a la Secretaría de la Comisión de Administración, Gestión y Modernización Judicial, para la intervención de dicho órgano.

Consecuentemente, intervino la Dirección General de Asuntos Jurídicos emitiendo el Dictamen DGAJ N° 15014/26, sin realizar observaciones al proyecto propuesto por la SAGyP.

En tal estado, llega lo actuado a la Comisión de Administración, Gestión y Modernización Judicial.

El presente acto se encuadra en el artículo 116 inciso 3° de la Constitución de la Ciudad Autónoma de Buenos Aires, que establece la competencia del Consejo de la Magistratura para dictar los reglamentos internos del Poder Judicial.

Concordantemente con ello, la Ley 31 le atribuye competencia al Consejo para: *“Dictar su reglamento interno, y los reglamentos internos del Poder Judicial, excepto los del Tribunal Superior y Ministerio Público”* (art. 2 inciso 3).



**Comisión de Administración,
Gestión y Modernización Judicial**

Asimismo, entre las facultades asignadas al Plenario de Consejeros en el artículo 20 inc. 3 se consigna: *“Dictar el Reglamento interno del Consejo de la Magistratura y de las Comisiones del Consejo; los Reglamentos de Funcionamiento de los Tribunales de Primera Instancia, las Cámaras de Apelaciones y los Reglamentos Generales del Poder Judicial, excluidos los correspondientes al Tribunal Superior y al Ministerio Público”*.

La ley 31 establece en el art. 37 las competencias de la Comisión de Administración, Gestión y Modernización Judicial, que están involucradas en el proyecto objeto del presente dictamen: Supervisar el diseño de la política de informática y telecomunicaciones que se lleve adelante. Disponer los reglamentos necesarios para organizar y mantener un sistema informático único, en todo el Poder Judicial, que permita llevar adelante la gestión administrativa y judicial bajo un expediente digital con firma digital y agenda única, que asegure el registro de todos los expedientes y actuaciones brindando acceso a todos los usuarios y agentes del servicio de Justicia a información precisa, permanente y actualizada de acuerdo a sus competencias (inc. 8); proponer reformas normativas que resulten necesarias para la modernización de la administración de justicia (inc. 11); y dictaminar sobre los reglamentos generales del Poder Judicial y elevarlos al Plenario (inc. 12).

Atento lo dispuesto en las normas citadas precedentemente, la Comisión es competente para dictaminar sobre la reglamentación de la Política General de Seguridad de la Información junto a las Políticas Específicas de Seguridad de la Información.

El proyecto impulsado por la SAGyP, en relación a la Política General de Seguridad de la Información, tiene por objetivo *“Establecer los lineamientos para desarrollar e implementar una arquitectura de seguridad de la información con el fin de proteger la disponibilidad, integridad y confidencialidad.”* Y su alcance abarca a los agentes del Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia- como a terceros vinculados directa o indirectamente con él, que gestionen activos de información del mencionado organismo.

La DGAJ examinó el proyecto propiciado por la DGIT sin formular observaciones, resaltando la competencia de esta Comisión para analizar su pertinencia. Además, cabe destacar, que este órgano tiene como prioridad el resguardo de la información sensible en todas las dependencias del Poder Judicial de la Ciudad, por lo que resulta necesario incorporar nuevas normas de seguridad y confidencialidad.



**Comisión de Administración,
Gestión y Modernización Judicial**

A continuación, se detallan los documentos relacionados: 1. Ley Nacional N° 25.326 - Protección de datos personales. 2. Ley N° 1.845 - Protección de datos personales. 3. IRAM-ISO/IEC 27001 - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos. 4. IRAM-ISO/IEC 27002 - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información. 5. DGIYT-GOYT-PL-002 - Organización de la Seguridad de la Información. 6. DGIYT-GOYT-PL-003 - Gestión de Incidentes de Seguridad de la Información. 7. DGIYT-GOYT-PL-004 - Cumplimiento de Seguridad de la Información. 8. DGIYT-GOYT-PL-005 - Seguridad de la Información en las Relaciones con los Proveedores. 9. DGIYT-GOYT-PL-006 - Seguridad de los Recursos Humanos. 10. DGIYT-GOYT-PL-007 - Gestión de Activos. 11. DGIYT-GOYT-PL-008 - Seguridad Criptográfica. 12. DGIYT-GOYT-PL-009 - Control de Accesos. 13. DGIYT-GOYT-PL-010 - Seguridad Física y del Entorno. 14. DGIYT-GOYT-PL-011 - Seguridad de las Comunicaciones. 15. DGIYT-GOYT-PL-012 - Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información. 16. DGIYT-GOYT-PL-013 - Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de información. 17. DGIYT-GOYT-PL-014 - Seguridad de las Operaciones.

Se establece las diferentes definiciones, los roles y responsabilidades de las entidades involucradas en la organización y cumplimiento del reglamento bajo estudio, y finalmente, se describen los lineamientos aplicados.

En cuanto a las Políticas Específicas de Seguridad de la Información, involucra la seguridad de los Recursos Humanos, que tiene por objeto *“definir las directrices para asegurar la formación y conciencia adecuada sobre la seguridad de la información, así como gestionar los controles necesarios para mitigar los riesgos relacionados antes, durante y después del vínculo laboral con el organismo.”*, con idéntico alcance que el General, y los documentos relacionados son los siguientes: 1. RES. PRESIDENCIA N° 1.259/2015 - Convenio Colectivo de Trabajo de los Trabajadores y Trabajadoras del Poder Judicial de CABA. 2. IRAM-ISO/IEC 27001 - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos. 3. IRAM-ISO/IEC 27002 - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información. 4. DGIYT-GOYT-PL-001 - Seguridad de la Información. 5. DGIYT-GOYT-PL-004 - Cumplimiento de Seguridad de la Información. 6. DGIYT-GOYT-PL-005 - Seguridad de la Información en las Relaciones con los Proveedores.



**Comisión de Administración,
Gestión y Modernización Judicial**

Además, se definen las entidades involucradas, la confidencialidad y privacidad de la información, los roles y responsabilidades, y finalmente lineamientos del vínculo laboral.

Por otra parte, se propone lo siguiente: “*Artículo 3°: Encomendar a la Dirección General de Informática y Tecnología el diseño y planificación del Cronograma de Implementación de las Política General de Seguridad de la Información aprobada en el Artículo 2° de la presente Resolución. Artículo 4°: Encomendar a la Dirección General de Informática y Tecnología la elaboración y actualización de los procedimientos, instructivos, manuales de usuario, registros y formularios de Seguridad de la Información, que correspondan a la Política General de Seguridad de la Información y cada una de las Políticas Específicas de Seguridad de la Información, dispuestas en la presente Resolución, junto a su incorporación y publicación en el Repositorio de Documentos de Seguridad de la Información, además de su comunicación a los destinatarios que correspondan según el instrumento, y la realización de capacitaciones permanentes a la totalidad de los actores involucrados en cada proceso. Artículo 5°: Delegar en la Secretaría de Administración General y Presupuesto del Poder Judicial la aprobación de los procedimientos, instructivos, manuales de usuario, registros y formularios de Seguridad de la Información, que correspondan a la Política General de Seguridad de la Información y cada una de las Políticas Específicas de Seguridad de la Información, elaborados por la Dirección General de Informática y Tecnología. Artículo 6°: Derogar la Resolución CM N° 61/2015.*”.

La creciente utilización de tecnologías de la información y comunicación (TIC), que **agrupan al conjunto de herramientas, redes, programas y dispositivos tecnológicos que permiten crear, procesar, almacenar, transmitir y recuperar información de forma digital**, al punto de volverse indispensables para el desarrollo de todas las actividades, tanto en lo relativo a la gestión interna como a los servicios brindados a la sociedad, justifican la actualización de las políticas de seguridad.

Además, corresponde considerar que el Consejo adquirió las normas IRAM-ISO/IEC 27001 de Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información y la IRAM-ISO/IEC 27002 de Tecnología de la Información, Técnicas de Seguridad y el Código de Buenas Prácticas para los Controles de la Seguridad de la Información, lo cual motiva la modernización normativa promovida por la DGIT.

Por lo expuesto, se observa que atento la situación planteada por la DGIT, dependencia que por su idoneidad cumple el requisito de órgano



**Comisión de Administración,
Gestión y Modernización Judicial**

técnico en la materia objeto del presente, corresponde actualizar las disposiciones de la Res. CM N° 61/2015, ya que la misma contempla normativas que por el transcurso del tiempo perdieron efectividad.

Conforme lo expuesto, no existen razones de hecho ni derecho que impidan dar continuidad al presente trámite.

Sin perjuicio de ello, en virtud de las competencias de la Comisión establecidas en el art. 37 inc. 8 y 11 de la ley 31, resulta conveniente que este órgano sea informado de las acciones desarrolladas por la Dirección General de Informática y Tecnología.

En virtud de lo expuesto, la Comisión de Administración, Gestión y Modernización Judicial, propone el Plenario, en el marco de lo propuesto en el Adjunto N° 96323/26 aprobar lo siguiente:

- 1.- La Política General de Seguridad de la Información del Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia-
- 2.- Las Políticas Específicas de Seguridad de la Información del Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia-
- 3.- Encomendar a la Dirección General de Informática y Tecnología el diseño y planificación del Cronograma de Implementación de la Política General de Seguridad de la Información.
- 4.- Encomendar a la Dirección General de Informática y Tecnología la elaboración y actualización de los procedimientos, instructivos, manuales de usuario, registros y formularios de Seguridad de la Información, que correspondan a la Política General de Seguridad de la Información y cada una de las Políticas Específicas de Seguridad de la Información, dispuestas en la presente Resolución, junto a su incorporación y publicación en el Repositorio de Documentos de Seguridad de la Información, además de su comunicación a los destinatarios que correspondan según el instrumento, y la realización de capacitaciones permanentes a la totalidad de los actores involucrados en cada proceso. Todo ello deberá ser informado a la Comisión de Administración Gestión y Modernización Judicial.
- 5.- Delegar en la Secretaría de Administración General y Presupuesto del Poder Judicial la aprobación de los procedimientos, instructivos, manuales de usuario, registros y formularios de Seguridad de la Información, que correspondan a la Política General de Seguridad de la Información y cada una de las Políticas Específicas de Seguridad de la Información, elaborados por la Dirección general de Informática y Tecnología.



**Comisión de Administración,
Gestión y Modernización Judicial**

6.- La Dirección General de Informática y Tecnología deberá informar a la Comisión de Administración, Gestión y Modernización Judicial, sobre las modificaciones implementadas en el marco de la facultad dispuesta en el punto 4º.

7.- Derogar la Resolución CM N° 61/2015.

DICTAMEN CAGyMJ N° 35/2026



FIRMAS DIGITALES



**CORTI Horacio
Guillermo Aníbal**
PRESIDENTE DE
COMISION
CONSEJO DE LA
MAGISTRATURA DE LA
CIUDAD AUTONOMA DE
BUENOS AIRES



CLIENTI Maria Lorena
VOCAL
CONSEJO DE LA
MAGISTRATURA DE LA
CIUDAD AUTONOMA DE
BUENOS AIRES



MEIS Marcelo Fernando
CONSEJERO/A
CONSEJO DE LA
MAGISTRATURA DE LA
CIUDAD AUTONOMA DE
BUENOS AIRES