Buenos Aires, 17 de julio de 2026

RES. CM Nº 141/2026

VISTO:

La Constitución de la Ciudad Autónoma de Buenos Aires, la Ley N° 31, el Dictamen de la Comisión de Administración, Gestión y Modernización Judicial N° 35/2026, la Resolución CM N° 61/2015, las normas internacionales IRAM-ISO/-IEC 27001 e IRAM-ISO/IEC 27002, la actuación TAE A-01-00019275-5/2026, y;

CONSIDERANDO:

Que el artículo 1° de la Ley N° 31 (texto consolidado por la Ley N° 6.764) determina: *"El Consejo de la Magistratura es un órgano permanente de selección de magistrados, gobierno y administración del Poder Judicial de la Ciudad Autónoma de Buenos Aires con la función de asegurar su independencia, garantizar la eficaz prestación del servicio de administración de justicia, promover el óptimo nivel de sus integrantes, y lograr la satisfacción de las demandas sociales sobre la función jurisdiccional del Estado"*.

Que la Resolución CM N° 61/2015 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 .

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.

Que en los 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.

Que 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.

Que, 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.

Que es este marco, se deben destacar 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.

Que la 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.

Que 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.

Que 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.

Que 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.

Que 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.

Que 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.

Que es este marco, 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 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.

Que asimismo, 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.

Que la Dirección General de Asuntos Jurídicos tomó la intervención correspondiente mediante Dictamen DGAJ N° 15014/2026.

Que, en el marco de su competencia, la Comisión de Gestión, Administración y Modernización Judicial consideró la Actuación de referencia y emitió el Dictamen CAGyMJ Nº 35/2026.

Que este Plenario comparte los criterios esgrimidos por la Comisión interviniente, dejándose constancia que la presente decisión se adopta por unanimidad.

Por ello, en ejercicio de las atribuciones otorgadas por la Constitución de la Ciudad Autónoma de Buenos Aires y la Ley N° 31,

EL CONSEJO DE LA MAGISTRATURA
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
RESUELVE:

Artículo 1°: Aprobar 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- que, como Anexo I (Seguridad de la Información) forma parte de la presente Resolución.

Artículo 2°: Aprobar 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- que como Anexo II (Organización de la Seguridad de la Información), Anexo III (Gestión de Incidentes de Seguridad de la Información), Anexo IV (Cumplimiento de Seguridad de la Información), Anexo V (Seguridad de la Información en las Relaciones con los Proveedores), Anexo VI (Seguridad de los Recursos Humanos), Anexo VII (Gestión de Activos), Anexo VIII (Seguridad Criptográfica), Anexo IX (Control de Accesos), Anexo X (Seguridad Física y del Entorno), Anexo XI (Seguridad de las Comunicaciones), Anexo XII (Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información), Anexo XIII (Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de Información) y Anexo XIV (Seguridad de las Operaciones) forman parte de la presente Resolución.

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°: Establecer que 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 artículo 4º de la presente.

Artículo 7°: Derogar la Resolución CM N° 61/2015.

Artículo 8°**:** Regístrese, publíquese en el Boletín Oficial de la Ciudad de Buenos Aires, en el sitio de Internet del Poder Judicial de la Ciudad Autónoma de Buenos Aires (www.consejo.jusbaires.gob.ar), comuníquese a todas las dependencias, a la Secretaría de Administración General y Presupuesto del Poder Judicial, a la Secretaría Legal y Técnica y a la Dirección General de Informática y Tecnología, y, oportunamente, archívese.

RES. CM Nº 141/2026

RES. CM Nº 141/2026 - ANEXO I

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

DGIYT-GOYT-PL-001

Seguridad de la información

Contenido

1. Seguridad de la Información

2. 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.

3. Alcance.

Esta política aplica tanto 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.

4. Documentos relacionados.

4.1. **Ley Nacional N° 25.326** - Protección de datos personales.

4.2. **Ley N° 1.845** - Protección de datos personales.

4.3. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.4. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-002 -** Organización de la Seguridad de la Información.

4.6. **DGIYT-GOYT-PL-003 -** Gestión de Incidentes de Seguridad de la Información.

4.7. **DGIYT-GOYT-PL-004 -** Cumplimiento de Seguridad de la Información.

4.8. **DGIYT-GOYT-PL-005 -** Seguridad de la Información en las Relaciones con los Proveedores.

4.9. **DGIYT-GOYT-PL-006 -** Seguridad de los Recursos Humanos.

4.10. **DGIYT-GOYT-PL-007 -** Gestión de Activos.

4.11. **DGIYT-GOYT-PL-008 -** Seguridad Criptográfica.

4.12. **DGIYT-GOYT-PL-009 -** Control de Accesos.

4.13. **DGIYT-GOYT-PL-010 -** Seguridad Física y del Entorno.

4.14. **DGIYT-GOYT-PL-011 -** Seguridad de las Comunicaciones.

4.15. **DGIYT-GOYT-PL-012 -** Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

4.16. **DGIYT-GOYT-PL-013 -** Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de información.

4.17. **DGIYT-GOYT-PL-014 -** Seguridad de las Operaciones.

5. Definiciones.

5.1. **Información:** la información es la interpretación que se da a los datos. En el caso de la presente política se entenderá como información a toda forma que contenga datos relacionados del organismo.

5.2. **Activos de información:** todo aquello que contiene, procesa, trate y/o manipule información valiosa y que sea necesaria para que el organismo funcione y cumpla con los objetivos establecidos para dicho fin.

5.3. **Confidencialidad:** característica de la información que permite que sea accesible sólo a aquellas personas autorizadas.

5.4. **Disponibilidad:** característica que permite que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

5.5. **Integridad**: característica que permite salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

5.6. **Seguridad de información**: es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información de los diferentes riesgos a los que puede estar expuesta, con el fin de minimizar el daño y garantizar la continuidad operacional.

5.7. **Sistema de Gestión de la Seguridad de la Información (SGSI)**: corresponde al diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la

accesibilidad a la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información minimizando los riesgos de seguridad.

5.8. **Incidente de seguridad de la información**: cualquier evento que afecte la confidencialidad, integridad y disponibilidad de los activos de información del organismo.

5.9. **Clasificación de la información**: acto de asignar a la información alguna de las categorías definidas por el organismo, pudiendo ser: pública, privada, confidencial o secreta.

5.10. **Información pública**: toda información de uso general, que por su contenido o contexto no requiere de protección especial y que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del organismo. Esta no deberá generar daños a terceros, ni a las actividades y/o procesos relacionados.

5.11. **Información privada**: toda información que requiera de cierto nivel de protección, pero que no cumple con los criterios necesarios para ser clasificada como confidencial o secreta y que es única y exclusivamente para uso interno del organismo y para aquellos que sean autorizados por acuerdos de confidencialidad.

5.12. **Información confidencial:** toda información altamente sensible y disponible solamente para un grupo específico del organismo y terceros autorizados explícitamente por el propietario o custodio de la información.

5.13. **Información secreta:** toda información que sea protegida, intransferible e indelegable y que sea prohibido su acceso, distribución, publicación y difusión general de forma permanente, con excepción de las autoridades competentes que, conforme a las regulaciones vigentes del organismo, tengan acceso autorizado a ella.

5.14. **Controles criptográficos**: técnicas y mecanismos utilizados para proteger la información mediante el uso de cifrado de datos. Se emplean para asegurar la confidencialidad, integridad y autenticidad de estos, desde el almacenamiento hasta la transmisión segura.

5.15. **Acuerdo de confidencialidad y no divulgación:** documento en el que se establecen las obligaciones respecto al cuidado que se debe dar a la información que manejarán en el contexto de sus actividades laborales para los empleados, contratados o proveedores.

5.16. **Medios removibles**: todo dispositivo de almacenamiento de información que se pueda conectar y desconectar fácilmente de un activo informático para transferir, almacenar o respaldar datos. Estos medios son portátiles, lo que permite transportarlos entre diferentes dispositivos o ubicaciones cómo, por ejemplo, unidades USB, discos duros portables, tarjetas SD, CD, DVD, etc.

5.17. **Redes informáticas:** sistemas informáticos conectados entre sí mediante una serie de dispositivos los cuales permiten la interconexión de múltiples activos de información, como computadoras, servidores, impresoras y otros equipos, para compartir recursos, datos y servicios facilitando el intercambio de información**.**

5.18. **Infraestructura tecnológica:** conjunto de componentes físicos, lógicos y organizativos conectados que soportan las operaciones, comunicaciones y procesos en una organización o sistema. Cada componente de la infraestructura brinda servicios distintos y es esencial para el

funcionamiento de cualquier entorno tecnológico, ya que proporciona la base sobre la cual se construyen y ejecutan las aplicaciones, servicios y sistemas.

5.19. **Código fuente:** archivo o conjunto de archivos, que contienen instrucciones concretas y declaraciones escritas en un lenguaje de programación y en donde se define el comportamiento y las funciones de un programa de software.

5.20. **Copias de seguridad**: también llamada respaldo o backup, son copias de datos y archivos importantes que se crean con el propósito de proteger la información en caso de pérdida, corrupción o fallo de sistemas.

5.21. **Sistemas de información:** son sistemas compuestos por elementos conectados entre sí que reúnen, procesan, almacenan y distribuyen datos para facilitar la toma de decisiones y la gestión dentro del organismo. Estos sistemas combinan tecnología, personas y procedimientos para gestionar la información de manera eficiente.

5.22. **Propietario de activo de información:** se refiere al organismo, representado por un individuo o área designada, que asume la responsabilidad principal sobre los activos de información. Esto incluye tomar decisiones estratégicas sobre su uso, designar a quienes se encarguen de su administración, protección y valoración. Sin embargo, no implica necesariamente que gestione o utilice directamente el activo.

5.23. **Custodio de los activos de información:** es la entidad que administra física o digitalmente el activo de información. Su función es proteger y gestionar el activo de acuerdo con las regulaciones dictaminadas por el propietario, implementando controles de seguridad que aseguren la disponibilidad, integridad y confidencialidad de este.

5.24. **Riesgo de seguridad:** probabilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

5.25. **Gestión de riesgos**: proceso que tiene como objetivo identificar, analizar, medir y gestionar los riesgos asociados a la seguridad de la información, con el fin de evitar o minimizar sus impactos en el organismo.

6. Roles y Responsabilidades

6.1. **Comité Directivo de Seguridad de la Información (CDSI)**: aprobar técnicamente las prioridades e iniciativas estratégicas de seguridad de la información definidas en la presente política.

6.2. **Responsable de Cumplimiento (RC):** velar por el cumplimiento de los lineamientos especificados en la presente política y mantenerlos actualizados con todos los requerimientos legales y contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad que corresponda.

6.3. **Comité Corporativo de Seguridad de la Información (CCSI):** verificar técnicamente las prioridades e iniciativas estratégicas de seguridad de la información definidas en la presente política y elevar al CDSI para su posterior aprobación.

6.4. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.5. **Jefe de Seguridad de la Información (CISO):** alinear la presente política de acuerdo con la estrategia aprobada por el CDSI y garantizar que se gestionen los riesgos de seguridad de la información.

7. Lineamientos.

7.1. Generalidades.

7.1.1. Considerando que el organismo establece como estrategia de seguridad de la información alinearse con las normas IRAM-ISO/IEC 27001 e IRAM-ISO/IEC 27002, las cuales representan un estándar internacional de Seguridad de la Información, se decidió elaborar la presente Política General de Seguridad de la Información y Trece (13) Políticas Específicas, abarcando las diferentes directrices expresadas en dichas normas.

7.1.2. La presente política representa una síntesis de los lineamientos declarados en las políticas específicas, donde se describen los requisitos y controles necesarios para garantizar la seguridad de la información. Ésta estará compuesta por las siguientes directrices:

- Organización de la seguridad de la información.
- Gestión de incidentes de seguridad de la información.
- Cumplimiento de seguridad de la información.
- Seguridad de la información en las relaciones con los proveedores.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Seguridad criptográfica.
- Control de accesos.
- Seguridad física y del entorno.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Aspectos de seguridad para la gestión de la continuidad de los sistemas de información.
- Seguridad de las operaciones.

7.1.3. Con el fin de garantizar el cumplimiento de dichas directrices, se establecerán normas, procedimientos, instructivos, manuales de usuario, formularios y registros, los cuales estarán subordinados a las políticas de seguridad de la información (general y especificas) y proporcionarán mayor detalle sobre la aplicación de éstas.

7.2. Organización de la seguridad de la información

7.2.1. La organización de la seguridad de la información tiene como objetivo establecer una estructura organizativa para la gestión de la seguridad de la información, definiendo roles, responsabilidades y estrategias que promuevan una cultura de seguridad dentro del organismo.

7.2.2. El organismo deberá:

- Establecer una estructura organizativa definida, aprobada y comprensible para la implementación, operación y gestión de la seguridad de la información.
- Velar por una adecuada segregación de funciones en la estructura organizativa de seguridad de la información y establecer adecuados controles para el cumplimiento de esta.
- Garantizar que sus autoridades se comprometan a impulsar la estrategia de seguridad de la información, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de ésta.

7.3. Seguridad de los Recursos Humanos

7.3.1. La seguridad de los Recursos Humanos tiene como objetivo asegurar que los agentes y/o terceros tengan la formación y la 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.

7.3.2. **Antes del vínculo laboral se deberá**:

- Realizar una verificación de antecedentes de todos los candidatos al puesto de trabajo según las leyes, regulaciones y reglas éticas del organismo.
- Garantizar que los agentes y/o terceros que ejerzan funciones dentro de la DGIYT firmen el acuerdo de confidencialidad y no divulgación, previo al alta de usuario. También podrá ser solicitada la firma, si correspondiera, a agentes y/o terceros de otras dependencias.
- Definir y documentar en los términos y condiciones apropiados antes de la contratación o finalización del contrato, las funciones y responsabilidades de seguridad de todos los agentes y/o terceros sobre los activos de información del organismo.

7.3.3. **Durante el vínculo laboral se deberá**:

- Garantizar que los agentes y/o terceros comprendan sus roles y responsabilidades en materia de seguridad de la información.
- Velar que todos los agentes y/o terceros autorizados que utilicen los activos de información del organismo, implementen las medidas de seguridad en conformidad con la legislación vigente y las políticas de seguridad de la información mencionadas en la presente política.
- Capacitar, educar y concientizar adecuadamente a los agentes y/o terceros sobre las funciones y responsabilidades en materia de seguridad de la información antes de concederles acceso a los activos de información.

7.3.4. **En la desvinculación o cambio de puesto se deberá:**

- Definir y asignar claramente las responsabilidades en materia de separación del servicio, reasignación de tareas y cese de funciones.
- Velar que los agentes y/o terceros devuelvan todos los activos de información del organismo que estén en su posesión al momento de la desvinculación.

- Garantizar que se inhabiliten o modifiquen, según corresponda, los derechos de acceso de todos los agentes y/o terceros autorizados a la información y a los sistemas de información.

7.4. Gestión de activos

7.4.1. La gestión de activos tiene como objetivo identificar y clasificar los activos de información, asegurando que se les asigne la protección adecuada en función de su criticidad y los riesgos asociados.

7.4.2. Se identificarán, documentarán y aplicarán reglas y normas para el uso aceptable de la información y los activos asociados a los sistemas de información.

7.4.3. **En el inventario de activos de información se deberá:**

- Identificar, elaborar y mantener un sistema de gestión de inventario el cual incluya toda la información necesaria que permita implementar las medidas de control y de protección de acuerdo con la criticidad de cada activo.

7.4.4. **En la clasificación de la información se deberá**:

- Clasificar o categorizar en función del valor y criticidad para el organismo, en información pública, privada, confidencial o secreta.
- Elaborar y aplicar lineamientos adecuados para etiquetar y tratar la información crítica.
- Garantizar que la información sea manipulada independientemente del tipo; papel o digital, y siempre contar con las medidas de seguridad apropiadas, de modo de evitar su interceptación o acceso no autorizado.

7.4.5. **En los medios removibles se deberá:**

- Tomar las medidas adecuadas para el almacenamiento y resguardo de los activos de información, con el fin de evitar accesos no autorizados, daños, pérdida de información o extravío de éstos, durante el uso o traslado.

7.4.6. **En los dispositivos móviles se deberá**:

- Garantizar que no se comprometa la información y establecer una protección adecuada para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos.

7.5. Control de acceso

7.5.1. El control de acceso tiene como objetivo restringir el acceso a los sistemas de información únicamente a aquellos agentes y/o terceros que estén autorizados, garantizando que se implementen controles de autenticación y autorización efectivos.

7.5.2. **En el control de acceso a los sistemas de información se deberá:**

- Contar con mecanismos adecuados de control que garanticen la disponibilidad de accesos a los agentes y/o terceros que lo requieran para el desempeño de sus funciones

oficiales. Los derechos de acceso de los usuarios y administradores deben estar alineados al tipo y nivel de criticidad de la información que manipulen.

7.5.3. **En la seguridad de la información de las redes se deberá**:

- Utilizar la identificación automática de equipos para autenticar las conexiones entrantes y salientes para que las comunicaciones sólo puedan iniciarse desde una ubicación o equipos específicos.
- Garantizar que los grupos de servicios de información, usuarios y sistemas de información estén debidamente segregados en las redes.
- Implementar controles de enrutamiento en las redes para garantizar que las conexiones informáticas y los flujos de información no infrinjan la política de control de acceso de las aplicaciones.

7.5.4. En el acceso remoto se deberá:

- Implementar lineamientos y medidas de seguridad adecuadas para proteger la información a la que se accede, procese y almacene en las instalaciones de teletrabajo. Teniendo en cuenta la necesidad de acceso remoto a los sistemas internos y a la criticidad de la información a la que se va a acceder.

7.6. Criptografía

7.6.1. La criptografía tiene como objetivo proteger la información mediante el uso de técnicas criptográficas adecuadas, asegurando la confidencialidad e integridad de los datos durante su almacenamiento y transmisión.

7.6.2. Se deben definir los lineamientos para el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

7.6.3. De corresponder, se debe gestionar la implantación de controles criptográficos durante la adquisición, el desarrollo y el mantenimiento de los sistemas de información.

7.6.4. Se deben utilizar sistemas y técnicas criptográficas para la protección de la información del organismo tanto para su almacenamiento como para su transmisión. Para ello, se requiere el cifrado de toda la información crítica, especialmente cuando ésta sea transmitida fuera del organismo o se encuentre contenida en medios de almacenamiento que se trasladen fuera del mismo.

7.7. Seguridad física y del entorno

7.7.1. La seguridad física y del entorno tiene como objetivo proteger los activos de información y la infraestructura tecnológica mediante controles de seguridad físicos, reduciendo el riesgo de accesos no autorizados, daños y pérdidas.

7.7.2. En las áreas de trabajo se deberá:

- Garantizar que los sistemas de información críticos se encuentren en áreas seguras, protegidas por perímetros de seguridad definidos y controles de entradas adecuados.

7.7.3. En los equipos se deberá:

- Velar que los sistemas de información, el cableado eléctrico y de telecomunicaciones que transporten datos o apoyen servicios, se ubiquen y protejan de forma que se reduzcan los riesgos derivados de amenazas y peligros ambientales, así como de las posibilidades de acceso no autorizado.
- Realizar el correcto mantenimiento de los activos de información para garantizar su disponibilidad e integridad de manera continua. Los mantenimientos sólo podrán ser realizados por los agentes y/o terceros autorizados y se generarán registros adecuados.

7.8. Seguridad de las operaciones

7.8.1. La seguridad de las operaciones tiene como objetivo asegurar que las operaciones de los sistemas de información se realicen de manera segura y eficiente, implementando controles de seguridad que minimicen el riesgo de interrupciones y vulnerabilidades.

7.8.2. Se deben definir los lineamientos para asegurar la operación correcta y segura de los medios de procesamiento de información, así también, evitar la divulgación no autorizada, la corrupción y pérdida de disponibilidad; debido a procedimientos operacionales insuficientes, inadecuados o por canales de comunicación poco eficaces.

7.8.3. Se debe generar documentación de la información y registros referentes a operaciones de tecnología de la información (TI) y de seguridad de la información (SI).

7.8.4. Se debe elaborar un procedimiento de gestión de cambios donde se establezcan medidas para minimizar los riesgos por cambios no autorizados, así como también evitar pérdida de información y proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso.

7.8.5. Se deberán establecer lineamientos de procedimientos asociados a las copias de seguridad para un registro preciso y completo de las mismas, cuya política de retención y frecuencia reflejen las necesidades del organismo.

7.8.6. Se deberá obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que se estén utilizando, se evaluará la exposición a dichas vulnerabilidades y se adoptarán las medidas adecuadas para hacer frente a los riesgos asociados. Siempre que sea posible, se habilitarán sistemas con actualizaciones automáticas para mantener instalados en los sistemas los últimos parches de seguridad de forma expeditiva.

7.8.7. Periódicamente se deben realizar auditorías que permitan detectar desvíos entre los lineamientos planteados y la implementación de éstos.

7.9. Seguridad de las comunicaciones

7.9.1. La seguridad de las comunicaciones tiene como objetivo proteger la información que se transmite a través de redes y sistemas, asegurando que las comunicaciones sean confidenciales, integras y accesibles solo para las partes autorizadas.

7.9.2. Se deben definir los lineamientos para garantizar la protección de la información que se comunica por las redes informáticas y para minimizar los riesgos que pudieran afectar la infraestructura de soporte.

7.9.3. Toda información que se transfiere fuera del organismo, incluyendo la que se transmite a través de los servicios de correo electrónico debe ser protegida de acuerdo con su nivel de criticidad.

7.9.4. Se deben asignar cuentas institucionales a todos los agentes y/o terceros (de corresponder), quienes están obligados a utilizarlas para toda comunicación vinculada a sus funciones.

7.9.5. Se deben identificar e incluir en cualquier acuerdo de servicios de red, los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de éstos.

7.9.6. Se recomienda segregar en más de una red a los grupos de servicios de información, los usuarios y los sistemas de información.

7.10. Adquisición, desarrollo y mantenimiento de los sistemas de información

7.10.1. La adquisición, desarrollo y mantenimiento de los sistemas de información tiene como objetivo garantizar que la seguridad de la información se integre en el proceso de adquisición, desarrollo y mantenimiento de los sistemas de información, considerando el tratamiento de los riesgos y la implementación de controles de seguridad.

7.10.2. Se debe garantizar que se apliquen los principios de seguridad en el desarrollo o adquisición de los sistemas provistos por terceros y que estos sean identificados mediante contratos u otros acuerdos legales.

7.10.3. Se debe garantizar que los sistemas de información (aplicaciones, infraestructuras, servicios, etc.) se diseñen e implementen con la seguridad como componente integral en todos los requisitos específicos del sistema.

7.10.4. Los nuevos sistemas de información y las mejoras de los sistemas deberán ser sometidos a pruebas apropiadas de todos los requisitos de seguridad en un entorno controlado. Las pruebas se documentarán y los resultados de estas se conservarán como activos de información.

7.10.5. Se deberá controlar la instalación de programas informáticos en los sistemas operativos, se definirán responsabilidades específicas para la instalación de software y se asignarán únicamente a usuarios autorizados.

7.10.6. Se deben realizar auditorías a intervalos regulares sobre los sistemas de información críticos, que permitan detectar deficiencias y vulnerabilidades asegurando el buen funcionamiento de éstas.

7.11. Seguridad de la información en las relaciones con los proveedores

7.11.1. La seguridad de la información en las relaciones con los proveedores tiene como objetivo gestionar los riesgos asociados con proveedores, asegurando que existan controles adecuados para proteger la información compartida.

7.11.2. Se deben establecer los lineamientos para garantizar la protección de los activos de información del organismo a los que tengan acceso los proveedores, evitando así la divulgación no autorizada, la corrupción y la pérdida de información.

7.11.3. Se debe incluir en los pliegos de bases y condiciones particulares, cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte de los proveedores que manipulen información del organismo. Estas cláusulas deben considerar los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización. Los requisitos deben ser acordes a la criticidad de la información y a los servicios, la evaluación de riesgos y el cumplimiento de todas las normas legales y contractuales aplicables.

7.11.4. En caso de corresponder, se implementarán periódicamente mecanismos de control, monitoreos, revisiones y auditorías a los servicios contratados.

7.12. Gestión de incidentes de seguridad de la información

7.12.1. La gestión de incidentes de seguridad de la información tiene como objetivo establecer un proceso para identificación, evaluación y respuesta a incidentes de seguridad de información de manera eficaz, minimizando el impacto y asegurando la mejora continua de la gestión.

7.12.2. Todos los agentes y/o terceros están obligados a notificar la detección y sospecha de vulnerabilidades o incidentes de seguridad de la información.

7.12.3. Se deben implementar procedimientos de notificación y escalado de incidentes de seguridad de la información, para garantizar que se adopten las medidas correctivas oportunas para contener, erradicar y mitigar los riesgos asociados.

7.12.4. Se deben documentar todos los incidentes de seguridad de la información identificados, con el fin de realizar evaluaciones e investigaciones para detectar impactos recurrentes, así como también, como base de consulta para reducir la probabilidad o el impacto de futuros incidentes y reforzar los controles de seguridad.

7.13. Aspectos de seguridad para la gestión de la continuidad de los sistemas de información

7.13.1. Los aspectos de seguridad para la gestión de la continuidad de los sistemas de información tienen como objetivo asegurar que existan planes y procedimientos para mantener la continuidad de las operaciones críticas en caso de incidentes o desastres, mitigando los riegos que puedan vulnerar la disponibilidad e integridad de los activos de información.

7.13.2. Se debe garantizar que el organismo esté preparado para reaccionar ante interrupciones de las operaciones y asegurar la reanudación oportuna de los procesos organizacionales.

7.13.3. Se deberá identificar los procesos críticos y los activos esenciales para el funcionamiento del organismo, evaluar los riesgos y las vulnerabilidades asociadas a estos, para luego

proceder al desarrollo de estrategias y medidas de mitigación para reducir los impactos negativos y minimizar el tiempo de inactividad.

7.13.4. Se deberán realizar pruebas periódicas de los planes de continuidad para evaluar su efectividad y proporcionar entrenamiento regular para familiarizarlos con los procedimientos de respuesta ante emergencias y recuperación ante desastres.

7.14. Cumplimiento

7.14.1. El cumplimiento tiene como objetivo asegurar que se cumplan las leyes, regulaciones y políticas internas relacionadas con la seguridad de la información, evitando sanciones legales y promoviendo la conformidad de los controles que garanticen la integridad, disponibilidad y confidencialidad de la información.

7.14.2. Se debe revisar periódicamente que se cumpla con la legislación vigente, las políticas y las normas de seguridad de la información establecidas.

7.14.3. Se deben realizar auditorías seguridad de la información periódicamente, donde se ejecuten comprobaciones de los sistemas operativos. Las mismas se planificarán cuidadosamente y se acordarán con antelación, para minimizar el riesgo de interrupciones de los procesos funcionales del organismo.

7.14.4. Se debe evitar la violación de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad. El incumplimiento de esto conllevará la aplicación de las normas que establece el Régimen Disciplinario en el Poder Judicial de la Ciudad Autónoma de Buenos Aires – excluido los Ministerios Públicos y el Tribunal Superior de Justicia- , y cualquier otra que pudiera corresponder, según el caso.

7.14.5. Se debe garantizar la privacidad y la protección de los datos personales, según lo requiera la legislación y regulación pertinente, cuando corresponda. Ley Nacional N° 25.326 de Protección de Datos Personales y Ley N° 1.845 de Protección de Datos Personales.

RES. CM Nº 141/2026 - ANEXO II

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Organización de la Seguridad de la Información

DGIYT-GOYT-PL-002

Organización de la seguridad de la información

Contenido

1. Organización de la seguridad de la información

2. Objetivo.

Definir los lineamientos para establecer una estructura organizativa para la gestión de la seguridad de la información, definiendo roles, responsabilidades y estrategias que promuevan una cultura de seguridad dentro del organismo.

3. Alcance.

Esta política aplica tanto 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 ejerzan funciones y responsabilidades en materia de seguridad de la información según lo mencionado en el presente documento.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-005-** Seguridad de la Información en las Relaciones con los Proveedores.

4.5. **DGIYT-GOYT-PL-006** - Seguridad de los Recursos Humanos.

5. Definiciones.

5.1. **Activos de información:** todo aquello que contiene, procesa, trate y/o manipule información valiosa y que sea necesaria para que el organismo funcione y cumpla con los objetivos establecidos para dicho fin.

5.2. **Confidencialidad:** característica de la información que permite que sea accesible sólo a aquellas personas autorizadas.

5.3. **Disponibilidad:** característica que permite que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

5.4. **Integridad:** característica que permite salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

5.5. **Seguridad de información:** es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información de los diferentes riesgos a los que puede estar expuesta, con el fin de minimizar el daño y garantizar la continuidad operacional.

5.6. **Convenio marco y convenio específico:** son tipos de acuerdos que suelen utilizarse en contextos legales y de cooperación entre organismos del Poder Judicial de la CABA, instituciones, entre otros.

5.7. **Acuerdo de confidencialidad y no divulgación:** documento en el que se establecen las obligaciones respecto al cuidado que se debe dar a la información, que manejarán en el contexto de sus actividades laborales para los empleados, contratados o proveedores.

5.8. **Plan de Continuidad del Negocio (BCP):** BCP es la sigla en inglés para "Business Continuity Plan", que se traduce en español como Plan de Continuidad del Negocio. Se trata de un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento y la prestación de servicios brindados en el organismo, después de padecer cualquier tipo de impacto negativo que suponga una interrupción de las actividades y procesos.

5.9. **Plan de Recuperación ante Desastres (DRP):** DRP es la sigla en inglés para "Disaster Recovery Plan", que se traduce al español como Plan de Recuperación ante Desastres. Se trata de un conjunto de procedimientos y estrategias diseñadas para ayudar al organismo a recuperarse y continuar operando después de un desastre o incidente grave, como un ciberataque, una catástrofe natural o una falla tecnológica significativa.

5.10. **DGIYT**: Dirección General de Informática y Tecnología.

6. Roles y Responsabilidades.

6.1. Comité Directivo de Seguridad de la Información (CDSI)

6.1.1. El Comité Directivo de Seguridad de la Información (CDSI), tiene por objetivo promover y garantizar la implementación y la mejora continua de la estrategia de seguridad de la información en el organismo.

6.1.2. El Comité Directivo de Seguridad de la Información (CDSI), debe estar conformado por un representante de la:

- Dirección General de Administración (DGA).
- Dirección General de Informática y Tecnología (DGIYT).
- Dirección General de Factor Humano (DGFH).
- Dirección de Informática y Tecnología (DIT).

6.1.3. El Comité Directivo de Seguridad de la Información (CDSI), entre otras funciones debe:

- Definir, aprobar y demostrar liderazgo y compromiso en la gestión de la estrategia de seguridad de la información.
- Garantizar que se implemente el Comité Corporativo de Seguridad de la Información (CCSI).
- Garantizar que se implemente el rol de Responsable de Cumplimiento (RC).
- Aprobar técnicamente la política general de seguridad de la información.
- Validar la propuesta del proyecto de resolución puesta a consideración por el CCSI, someterla al análisis y dictamen de la Comisión de Administración, Gestión y Modernización Judicial (CAGYMJ), que posteriormente la elevará al Plenario para su aprobación como órgano decisorio final.
- Promover la concientización, capacitación de los agentes y alinear la gestión de los procesos del organismo con la estrategia de seguridad de la información.

- Designar las derogaciones y asignaciones de la estructura organizativa de seguridad de la información cuando sea necesario.

6.2. Responsable de Cumplimiento (RC)

6.2.1. El Responsable de Cumplimiento (RC), tiene como objetivo, garantizar que la información documentada basada en la estrategia de seguridad de la información del organismo, cumpla con los requerimientos legales y contractuales vigentes.

6.2.2. El Responsable de Cumplimiento (RC), está representado por el Jefe de la Oficina de Normas, Procedimientos y Seguridad Informática o a quien el CDSI delegue.

6.2.3. El Responsable de Cumplimiento (RC), entre otras funciones, debe:

- Definir, comunicar al CCSI y mantenerse actualizado con todos los requerimientos legales y contractuales relacionados con la seguridad de la información y de cualquier requisito de seguridad que corresponda.
- Validar la aplicabilidad de las políticas específicas, normas, procedimientos o estándares de seguridad de la información de acuerdo con las regulaciones vigentes.
- Elaborar e implementar un plan de auditoría donde se pueda verificar y revisar el nivel de cumplimiento de las políticas de seguridad de la información.
- Velar por el cumplimiento de los requerimientos especificados en las políticas de seguridad de la información y asesorar al CCSI sobre las problemáticas en términos de cumplimiento legal y contractual, para que se mantengan en consonancia con los controles aplicados, así como también, informar sobre las oportunidades de mejoras identificadas en la estrategia de seguridad de la información.

6.3. Comité Corporativo de Seguridad de la Información (CCSI)

6.3.1. El Comité Corporativo de Seguridad de la Información (CCSI), tiene como objetivo proporcionar una visión integral y a largo plazo sobre cómo proteger los activos de información, asegurando que todos los controles establecidos estén en completa sintonía con los objetivos estratégicos y operacionales generales del organismo.

6.3.2. El Comité Corporativo de Seguridad de la Información (CCSI), debe estar conformado por los siguientes miembros, o a quienes el CDSI delegue:

- El Jefe de Seguridad de la Información (CISO), como representante principal.
- Responsable de Cumplimiento (RC).
- Dirección General de Informática y Tecnología (DGIYT).
- Dirección de Informática y Tecnología (DIT).
- Jefe del Departamento de Aplicaciones (APP).
- Jefe del Departamento de Arquitectura Tecnológica (AT).
- Jefe del Departamento de Planificación e Infraestructura (PEI).
- Jefe del Departamento de Gestión Operativa y Tecnológica (GOYT).
- Jefe del Departamento de Soporte Tecnológico (ST).

- Gestor de Seguridad de la Información (GSI).

6.3.3. El Comité Corporativo de Seguridad de la Información (CCSI), entre otras funciones debe:

- Validar las prioridades, iniciativas y modificaciones en la estrategia de seguridad de la información, y de ser necesario proponer oportunidades de mejoras al CDSI.
- Definir y garantizar la implementación del Grupo de Gestión de Seguridad de la Información (GGSI).
- Definir y garantizar la implementación del rol de Jefe de Seguridad de la Información (CISO).
- Definir y garantizar la implementación del rol de Gestor de Seguridad de la Información (GSI).
- Definir y garantizar la implementación de los roles de los Oficiales de Seguridad de la Información (OSI).
- Verificar según su experticia, las normas, procedimientos y toda la información documentada necesaria para el cumplimiento de la seguridad de la información.
- Verificar técnicamente la política general de seguridad de la información, siendo responsable de esto el representante principal de CCSI, o a quien este delegue.
- Elaborar y formular una propuesta donde se consolide la estrategia de seguridad de la información como proyecto de resolución para luego elevarlo a consideración del CDSI.
- Evaluar y aprobar las herramientas y marcos de trabajo que faciliten el cumplimiento de los requisitos de seguridad de la información.
- Garantizar la implementación de los controles de seguridad, siendo responsable de esto cada representante del CCSI según su experticia dentro del organismo.
- Analizar los informes relacionados con los incidentes de seguridad de la información y proponer, de ser necesario, acciones correctivas y preventivas.

6.4. Grupo de Gestión de Seguridad de la Información (GGSI)

6.4.1. El Grupo de Gestión de Seguridad de la Información (GGSI), tiene como objetivo liderar la implementación de un Plan de Gestión de Crisis cuando ocurra un incidente que provoque la disrupción parcial o total de los sistemas de información del organismo, generando como resultado la continuidad de las operaciones normales.

6.4.2. El Grupo de Gestión de Seguridad de la Información (GGSI), debe estar conformado, sin limitarse a ello, por un representante de:

- Dirección General de Informática y Tecnología (DGIYT).
- Dirección de Informática y Tecnología (DIT).
- Departamento de Arquitectura Tecnológica (AT).
- Departamento de Planificación e Infraestructura Tecnológica (PEI).
- Jefe de Seguridad de la Información (CISO).

6.4.3. El Grupo de Gestión de Seguridad de la Información (GGSI), entre otras funciones debe:

- Elaborar e implementar el Plan de Gestión de Crisis para la continuidad de las operaciones de los activos de información del organismo.
- Proporcionar un marco operacional y establecer procedimientos operativos estandarizados para garantizar que las decisiones y medidas críticas sean implementadas de manera eficiente en la gestión de crisis.
- Desarrollar e implementar planes específicos, como el Plan de Continuidad del Negocio (BCP), el Plan de Recuperación ante Desastres (DRP) y otros que correspondan, incluyendo estrategias para respuestas de emergencia, comunicación en situaciones de crisis y reanudación de las operaciones normales.
- Establecer y mantener una comunicación clara y efectiva con todas las partes interesadas durante y después de un incidente de seguridad de la información.

6.5. Jefe de Seguridad de la Información (CISO).

6.5.1. El Jefe de Seguridad de la Información (CISO), tiene como objetivo ser el punto de contacto para todas las cuestiones relacionadas con la seguridad de la información dentro del organismo. Coordina con otros Departamentos para asegurar que los controles de seguridad se integren de manera efectiva en las operaciones diarias y que se mantenga una cultura de seguridad en las mismas.

6.5.2. El Jefe de Seguridad de la Información (CISO), está representado por el Director General de Informática y Tecnología o a quién este delegue.

6.5.3. El Jefe de Seguridad de la Información (CISO), entre otras funciones, debe:

- Proporcionar el juicio de experto para la toma de decisiones del CDSI.
- Proporcionar el juicio experto para la toma de decisiones del CCSI.
- Proponer al CDSI mejoras en la estrategia de seguridad de la información y que esté en concordancia con el cumplimiento de la misión y visión del organismo.
- Alinear la política general y las específicas en materia de seguridad de la información de acuerdo con la estrategia aprobada por el CDSI.
- Aprobar técnicamente las políticas específicas de seguridad de la información.
- Informar acerca de los incidentes, riesgos, amenazas y vulnerabilidades que puedan afectar transversalmente al organismo, así como también las acciones preventivas y correctivas definidas para su tratamiento.
- Definir acciones preventivas y correctivas eficientes como respuesta a los informes de auditorías de seguridad de la información.
- Garantizar que se implementen las medidas y controles de seguridad necesarios para el tratamiento de los riesgos de seguridad de la información.
- Gestionar planes de capacitación en materia de seguridad de la información para garantizar que todos los agentes y/o terceros comprendan y cumplan las políticas, legislaciones vigentes y mejores prácticas de seguridad.

6.6. Gestor de Seguridad de la Información (GSI)

6.6.1. El Gestor de la Seguridad de la Información (GSI), tiene como objetivo verificar la ejecución práctica y la gestión diaria de la seguridad de la información para asegurar que las medidas y políticas de seguridad se implementen efectivamente.

6.6.2. El Gestor de la Seguridad de la Información (GSI), está representado por el Líder del Programa de Seguridad de la Información de la DGIYT.

6.6.3. El Gestor de la Seguridad de la Información (GSI), entre otras funciones, debe:

- Verificar según corresponda las políticas, normas, procedimientos y toda la información documentada necesaria para el cumplimiento de la seguridad de la información, y luego elevarlas al CCSI para la aprobación técnica.
- Evaluar y proponer al CCSI herramientas y marcos de trabajo que faciliten la labor de la seguridad de la información.
- Analizar y generar un informe al CISO de los indicadores de gestión definidos para los procesos de seguridad de la información.
- Validar el nivel de implementación de la estrategia de seguridad y hacer seguimiento a las acciones correctivas y preventivas de los riesgos de seguridad de la información identificados.
- Hacer seguimiento al cumplimiento de las acciones preventivas y correctivas definidas como respuesta a los informes de auditorías de seguridad de la información.
- Conocer los proyectos de informática a implementar para proponer los lineamientos de seguridad de la información que correspondan.
- Coordinar la gestión de los controles y procesos ejecutados por el Oficial de Seguridad de la Información (OSI).

6.7. Oficial de Seguridad de la Información (OSI)

6.7.1. El Oficial de Seguridad de la Información (OSI), tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de la información del organismo, mediante la monitorización, ejecución y mejora de controles y procesos para el cumplimiento de la estrategia de seguridad.

6.7.2. El Oficial de la Seguridad de la Información (OSI), está representado por un especialista en materia de seguridad de la información (siendo este rol asignado a una o más personas) de la Oficina de Normas, Procedimientos y Seguridad Informática.

6.7.3. El Oficial de la Seguridad de la Información (OSI), entre otras, debe tener las siguientes tareas y responsabilidades:

- Elaborar toda la información documentada en materia de seguridad de la información y realizar las modificaciones necesarias para mantenerla actualizada y someterla posteriormente a su verificación por el representante del CCSI que corresponda según su experticia.

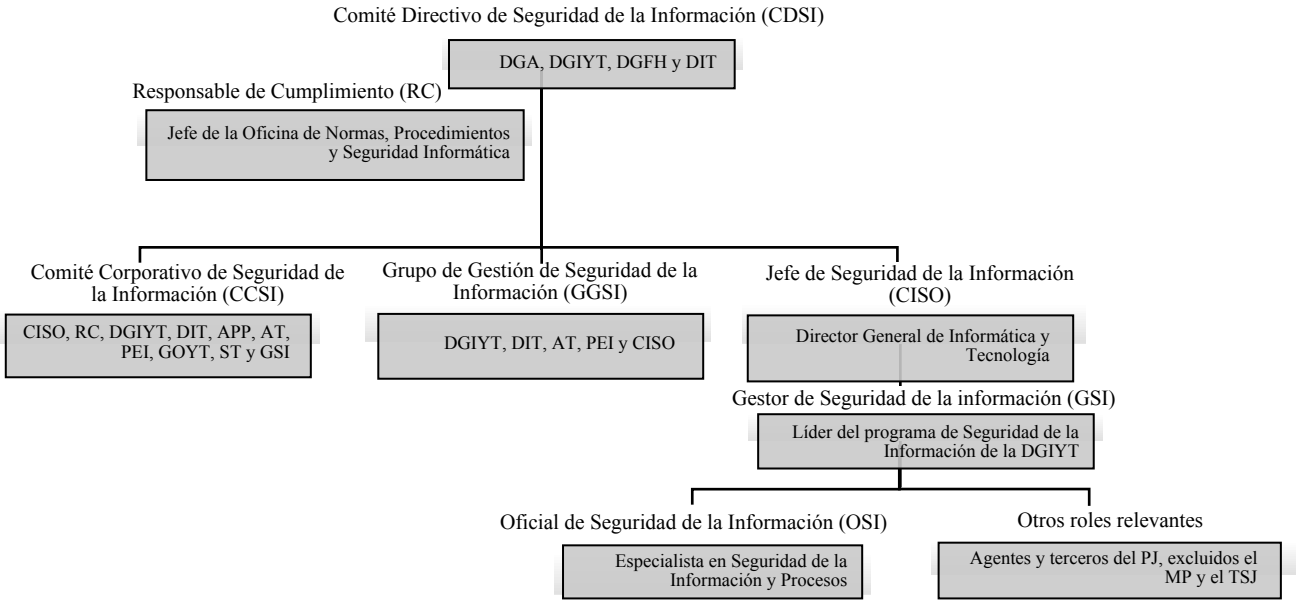
- Establecer una comunicación fluida con el GSI con el fin de mantenerlo actualizado respecto a la gestión de los controles y procesos de seguridad de la información.
- Reportar al GSI, los eventos de seguridad de la información críticos acontecidos en el país.
- Definir y hacer seguimiento de los indicadores de gestión establecidos en los procesos de seguridad de la información, así como también reportar los resultados de éstos al GSI.
- Identificar y reportar al GSI y al CISO los incidentes, riesgos, amenazas y vulnerabilidades que puedan afectar al organismo.
- Implementar las acciones preventivas y correctivas definidas por el CISO como respuesta a los informes de auditorías de seguridad de la información.
- Implementar las medidas y controles de seguridad definidos para el tratamiento de los riesgos de seguridad de la información.
- Monitorear las herramientas de seguridad de la información con el fin de identificar comportamientos anómalos que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información.
- Gestionar las pruebas de arquitectura tecnológica para evaluar la fortaleza de seguridad y detectar las futuras amenazas.

6.8. Otros roles relevantes.

6.8.1. Los sujetos alcanzados por la presente deben:

- Cumplir con las políticas, normas y procedimientos de seguridad de la información que les correspondan según sus roles y funciones.
- Dar el uso adecuado a los activos de información y cumplir con los requisitos de seguridad al momento de utilizarlos según lo establecido en la norma de uso aceptable de los activos y recursos informáticos.
- Reportar cualquier incidente de seguridad, del cual tenga conocimiento en función de sus actividades, a sus respectivas contrapartes o a la Oficina de Normas, Procedimientos y Seguridad Informática.

6.9. Estructura organizativa de seguridad de la información.



7. Lineamientos

7.1. Generalidades.

7.1.1. La DGIYT debe definir, aprobar e implementar controles de seguridad de la información en todas las áreas de procesamiento, almacenamiento y transmisión de información que se encuentre bajo su custodia.

7.1.2. Los roles y las responsabilidades de la estructura organizativa deben estar claramente definidos, asignados y difundidos a las partes interesadas, los mismos deberán ser asignados cuidadosamente según lo establecido en la presente política con el fin de minimizar los problemas de acceso si un rol es eliminado o reasignado a otra área.

7.1.3. El organismo debe emprender acciones destinadas a asegurar que todos los agentes y/o terceros conozcan y cumplan sus responsabilidades en seguridad de la información.

7.1.4. Los agentes y/o terceros que asuman un rol específico en materia de seguridad de la información deben ser competentes en los conocimientos y habilidades requeridos para el mismo, y deberán recibir apoyo del organismo para mantenerse al día con las actualizaciones necesarias para el cumplimiento de sus responsabilidades.

7.1.5. Los agentes y/o terceros con responsabilidades asignadas en la seguridad de la información y que ejerzan funciones en otras áreas, deben garantizar que mantienen la responsabilidad de seguridad y que las tareas sean desempeñadas correctamente.

7.1.6. Los roles y responsabilidades en seguridad de la información periódicamente se reevaluarán y actualizarán de ser necesario, con el fin de adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

7.1.7. No se deben dejar brechas entre la estrategia de seguridad definida y las responsabilidades asignadas dentro de la estructura organizativa de seguridad de la información, asegurando que el ciclo de vida de las medidas de seguridad esté cubierto (definición, implementación, operación, revisión y mejora).

7.1.8. El organismo debe garantizar la asignación de los recursos necesarios para la implementación y mejora continua de la estructura organizativa de seguridad de la información.

7.1.9. Para los casos donde sea necesario, el organismo debe mantener contacto con autoridades como, por ejemplo; bomberos, cuerpos de seguridad, organismos reguladores y autoridades supervisoras, con el fin de:

- Gestionar incidentes de seguridad de la información identificados.
- Obtener asesoría para el mejoramiento de las buenas prácticas y controles de seguridad.
- Recibir alertas tempranas, advertencias y parches de seguridad para prevenir posibles incidentes.
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas y/o vulnerabilidades, siempre y cuando se garantice la protección de la información confidencial del organismo.

7.1.10. Se recomienda que el CISO mantenga contacto con los siguientes organismos especializados en temas relativos a la seguridad de la información:

- Oficina Nacional de Tecnologías de Información (ONTI).
- ArCERT (Coordinación de Emergencias en Redes Teleinformáticas).
- Infraestructura de Firma Digital.
- Dirección Nacional de Protección de Datos Personales.
- Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI).
- Otros organismos que sean considerados apropiados según el caso.

7.1.11. Cuando sea necesario intercambiar información con organismos o entidades externas, se deberá realizar cumpliendo con lo establecido previamente en los Convenios Marcos o Convenios Específicos.

7.1.12. Se deberán segregar las obligaciones y áreas de responsabilidad incompatibles para reducir las oportunidades de accesos no autorizados o el mal uso de los activos de información y evitando posibles conflictos de intereses.

7.1.13. El RC debe ser independiente del proceso a auditar, o por una organización tercerizada especializada en auditorías de seguridad, para garantizar que la estrategia de seguridad de la información del organismo continúe siendo correcta, adecuada y eficaz.

7.1.14. Para las personas que ejerzan funciones dentro de la DGIYT, se debe solicitar las firmas del acuerdo de confidencialidad y no divulgación que corresponda. También podrá ser solicitada la firma, si correspondiera, a agentes y/o terceros de otras dependencias.

RES. CM Nº 141/2026 - ANEXO III

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Gestión de Incidentes de Seguridad de la Información

DGIYT-GOYT-PL-003

Gestión de Incidentes de Seguridad de la Información

Contenido

Gestión de Incidentes de Seguridad de la Información

Contenido

1. Gestión de Incidentes de Seguridad de la Información.

2. Objetivo.

Establecer los lineamientos generales para la identificación, evaluación y respuesta a incidentes de seguridad de información de manera eficaz, minimizando el impacto y asegurando la mejora continua de la gestión.

3. Alcance.

Esta política aplica tanto 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 sospechen, detecten y/o gestionen incidentes de seguridad en los activos de información.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001 -** Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002 -** Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-004 -** Cumplimiento de Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-013** - Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de Información.

5. Definiciones.

5.1. **Seguridad de información**: es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información de los diferentes riesgos a los que puede estar expuesta, con el fin de minimizar el daño y garantizar la continuidad operacional.

5.2. **Activos de información**: todo aquello que contiene, procesa, trate y/o manipule información valiosa y que sea necesaria para que el organismo funcione y cumpla con los objetivos establecidos para dicho fin.

5.3. **Incidente de seguridad de la información**: cualquier evento que afecte la confidencialidad, integridad y disponibilidad de los activos de información del organismo.

5.4. **Evento:** es cualquier acción o actividad que tiene lugar en un sistema de información y que puede tener relevancia para la seguridad. No todos los eventos indican un problema o amenaza, pero pueden ser indicativos de comportamientos que necesitan ser monitoreados.

5.5. **Análisis forense de seguridad de la información**: técnicas de investigación y estudios para recolectar, registrar y analizar evidencias de incidentes de seguridad de la información.

5.6. **Contención:** se refiere a las acciones y medidas tomadas para limitar el alcance y el impacto de un incidente de seguridad de la información. Su objetivo principal es evitar que un incidente se propague o cause más daño mientras se trabaja en la resolución y recuperación del problema. La

contención es una parte crucial del proceso de respuesta a incidentes y se realiza para controlar y mitigar el impacto del incidente.

5.7. **Mitigación:** acciones que están encaminadas a reducir y limitar los riesgos de seguridad de la información.

5.8. **Erradicación:** eliminación de las causas del incidente (virus, malware, fallos técnicos, acceso no autorizado, etc.).

5.9. **Plan de Continuidad del Negocio (BCP):** BCP es la sigla en inglés para "Business Continuity Plan", que se traduce en español como Plan de Continuidad del Negocio. Se trata de un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento y la prestación de servicios brindados en el organismo, después de padecer cualquier tipo de impacto negativo que suponga una interrupción de las actividades y procesos.

5.10. **Plan de Recuperación ante Desastres (DRP):** DRP es la sigla en inglés para "Disaster Recovery Plan", que se traduce al español como Plan de Recuperación ante Desastres. Se trata de un conjunto de procedimientos y estrategias diseñadas para ayudar al organismo a recuperarse y continuar operando después de un desastre o incidente grave, como un ciberataque, una catástrofe natural o una falla tecnológica significativa.

6. Roles y Responsabilidades.

6.1. **Comité Corporativo de Seguridad de la información (CCSI):** identificar las oportunidades de mejora en la estrategia de seguridad de información en relación con la gestión de incidentes y velar por el cumplimiento de la implementación de éstas.

6.2. **Grupo de Gestión de Seguridad de la Información (GGSI):** liderar la implementación de un Plan de Gestión de Crisis cuando ocurra un incidente que provoque la disrupción parcial o total de los sistemas de información del organismo y que este plan genere como resultado la continuidad de las operaciones normales.

6.3. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.4. **Jefe de seguridad de la información (CISO):** garantizar que la gestión de los incidentes de seguridad de la información cumpla y este alineada con la estrategia de seguridad de la información del organismo.

6.5. **Gestor de seguridad de la información (GSI):** supervisar la gestión de los eventos e incidentes de seguridad de la información identificando oportunidades de mejora, relevando acciones tomadas y procediendo a corregirlas en caso de requerirse, para poder optimizar los procesos de gestión y tratamientos.

6.6. **Oficial de seguridad de la información (OSI):** monitorear las herramientas de seguridad y gestionar o derivar a quien corresponda, los incidentes de seguridad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

7. Lineamientos.

7.1. Generalidades.

7.1.1. Para que se garantice una respuesta eficiente ante un incidente de seguridad de la información, se deberá cumplir con el procedimiento, los roles y las responsabilidades establecidas en el procedimiento de gestión de incidentes de seguridad de la información.

7.1.2. Con el fin de facilitar la gestión y mitigación de los riesgos, se deberá realizar el registro de todo evento e incidente de seguridad según lo establecido en el procedimiento de gestión de incidentes de seguridad de la información.

7.1.3. Se deberá estandarizar, documentar e implementar un tratamiento según el tipo de incidente, con el fin de mejorar la calidad y la eficiencia operativa.

7.1.4. Durante toda la gestión de los incidentes, se deberá tratar la información de estos de acuerdo con el nivel de clasificación identificado según los lineamientos establecidos en la norma de clasificación de la información

7.1.5. Periódicamente se deberá concientizar a los agentes y/o terceros, para la prevención, detección y reporte de los eventos y/o incidentes de seguridad de la información según las responsabilidades correspondientes, sensibilizando y generando la conciencia necesaria para mejorar la eficiencia en la gestión.

7.1.6. Periódicamente el CISO, deberá presentar un informe al CDSI y al CCSI de los incidentes, riesgos, amenazas y vulnerabilidades que puedan afectar transversalmente al organismo, así como también las acciones preventivas y correctivas definidas para el tratamiento de estos.

7.1.7. Se deben establecer canales de comunicación claros para mantener informados a los agentes y/o terceros necesarios durante el manejo del incidente.

7.1.8. Se deberán garantizar la existencia de múltiples canales de comunicación para asegurar que la misma no sea interrumpida durante la gestión del incidente.

7.1.9. Los incidentes de seguridad deben ser gestionados por el OSI o por cualquier agente y/o tercero que esté expresamente autorizado por la DGIYT.

7.1.10. Para los casos donde sea necesario, el organismo debe mantener contacto con autoridades como, por ejemplo; bomberos, cuerpos de seguridad, organismos reguladores y autoridades supervisoras, con el fin de:

- Gestionar incidentes de seguridad de la información identificados.
- Obtener asesoramiento para el mejoramiento de las buenas prácticas y controles de seguridad.
- Recibir alertas tempranas, advertencias y parches de seguridad para prevenir posibles incidentes.
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas y/o vulnerabilidades, siempre y cuando se garantice la protección de la información confidencial del organismo.

7.1.11. Se recomienda que el CISO mantenga contacto con los siguientes organismos especializados en temas relativos a la seguridad de la información:

- Oficina Nacional de Tecnologías de Información (ONTI).
- ArCERT (Coordinación de Emergencias en Redes Teleinformáticas).
- Infraestructura de Firma Digital, si fuera el caso.
- Dirección Nacional de Protección de Datos Personales.
- Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI).
- Otros organismos que sean considerados apropiados según el caso.

7.1.12. El incumplimiento de estos lineamientos de Seguridad de la Información podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normas vigentes.

7.2. Detección y reporte de eventos e incidentes de seguridad de la información.

7.2.1. El CCSI deberá evaluar y aprobar las herramientas necesarias para el monitoreo y la detección de actividades inusuales o sospechosas que podría poner en riesgo la seguridad de la información.

7.2.2. Se deben monitorear diariamente las herramientas implementadas para la detección de eventos, los cuales pudieran ser clasificados como incidentes de seguridad de la información.

7.2.3. Todo agente y/o tercero debe reportar y canalizar de forma inmediata cualquier evento y/o incidente de seguridad de la información sospechado o detectado.

7.2.4. Entre las situaciones que se pueden reportar como eventos o incidentes de seguridad de la información se encuentran aquellas cuando:

- Se detecten controles de seguridad ineficaces.
- Se detecte el incumplimiento de las expectativas de integridad, confidencialidad y disponibilidad del organismo.
- Se detecte el incumplimiento de los acuerdos de seguridad física.
- Se detecten cambios no controlados ni registrados en los sistemas.
- Se detecte el mal funcionamiento de software o hardware.
- Se haya detectado una violación de acceso.
- Se sospechen eventos que puedan vulnerar la seguridad de la información.

7.3. Identificación y evaluación de eventos e incidentes de seguridad de la información.

7.3.1. Los factores que se deben considerar para la identificación del tipo de incidente, sin limitarse a ello, son los siguientes:

- Naturaleza del incidente: identificar características fundamentales del evento que afectó la confidencialidad, integridad o disponibilidad de los sistemas, datos o servicios del organismo.
- Gravedad y alcance: evaluar la magnitud del incidente, incluyendo daños materiales, personales, ambientales o tecnológicos, y el impacto en las operaciones y la seguridad de la información.

- Causas principales: realizar un análisis para identificar las causas principales del incidente, no solo los síntomas superficiales. Se recomiendan métodos como el análisis de causa raíz.

7.3.2. Cada evento reportado, deberá ser evaluado para identificar si corresponde a un incidente de seguridad de la información, en caso de ser catalogado como un incidente, el OSI deberá realizar un análisis de riesgos, para determinar su clasificación, priorización y tiempo de respuesta, de acuerdo con lo establecido en el procedimiento de gestión de incidentes de seguridad de la información.

7.3.3. Cuando ocurra un incidente de seguridad, se recomienda revisar la Base de conocimientos de Incidentes de Seguridad de la Información existente para analizar cómo se han gestionado incidentes similares en el pasado. Esto permitirá aplicar lecciones aprendidas y mejorar la respuesta actual, optimizando los procedimientos y reduciendo riesgos.

7.3.4. De acuerdo con el nivel de riesgo identificado, el GGSI deberá evaluar la necesidad de activar el Plan de Gestión de Crisis, el BCP, el DRP u otros planes específicos que correspondan a los activos de información afectados. Estos planes deberán contemplar la implementación de medidas de protección y recuperación ante posibles desastres naturales, accidentes, fallos en los equipos y acciones intencionadas, con el fin de minimizar los daños y facilitar el restablecimiento de las operaciones.

7.3.5. De acuerdo con la evaluación realizada, se deberán determinar las acciones de contención, mitigación y erradicación respecto al incidente de seguridad de la información.

7.4. Respuestas a incidentes de seguridad de la información.

7.4.1. Se deberán implementar medidas de contención inmediatas y a corto plazo para limitar la expansión del incidente y asegurar que no siga afectando otros sistemas y servicios mientras se investiga.

7.4.2. Se deberán implementar acciones correctivas a las causas principales del incidente para erradicar las vulnerabilidades que contribuyeron a este.

7.4.3. Se deberán restaurar los sistemas y servicios afectados a su estado normal de operación garantizando que los sistemas estén seguros y que el incidente no vuelva a ocurrir.

7.4.4. Se deberá validar con los responsables de los procesos y activos afectados por el incidente, la correcta operatividad de éstos, luego de la ejecución de acciones aplicadas como respuesta al incidente.

7.4.5. Se deberán implementar medidas a largo plazo para mitigar el riesgo de recurrencia del incidente, con la incorporación de mejores prácticas de seguridad que garanticen la protección continua de los activos de información.

7.4.6. Se deberán utilizar los canales de comunicación previamente definidos por el organismo para mantener informados a los agentes y/o terceros necesarios durante el manejo del incidente.

7.4.7. En casos donde el incidente supera la capacidad de respuesta del equipo inicial, se debe escalar a niveles superiores de gestión o llamar a expertos externos.

7.5. Aprendizaje a partir de los incidentes de seguridad de la información.

7.5.1. Se deben documentar todos los incidentes de seguridad de la información identificados en la Base de conocimientos de Incidentes de Seguridad de la Información, con el fin de realizar evaluaciones e investigaciones para identificar impactos recurrentes, así como también, como base de consulta para reducir la probabilidad o el impacto de futuros incidentes y para reforzar los controles de seguridad.

7.5.2. Se debe concientizar a los agentes en base a la información obtenida de la evaluación de los incidentes de seguridad de la información, con el fin de prevenir nuevas ocurrencias.

7.5.3. El GSI, posterior a la gestión del incidente, deberá revisar de manera habitual la base de conocimientos, identificando oportunidades de mejoras, relevando acciones tomadas y procediendo a corregirlas en caso de requerirse, para poder optimizar los procesos de gestión y tratamientos de los incidentes.

7.5.4. Se deberá verificar si el incidente tuvo implicaciones legales o regulatorias y si se incumplieron normas internas o externas, de ser así, se deberá tomar las acciones pertinentes para regularizar la situación.

7.5.5. Se deberán evaluar qué medidas preventivas existían y si fueron efectivas, así como también las mejoras que puedan aplicarse.

7.6. Recolección de la evidencia.

7.6.1. Durante todo el tratamiento del incidente de seguridad de la información, se deberán capturar y preservar las evidencias del caso como respaldo ante posibles requerimientos de una auditoría interna o externa al organismo. Asimismo, se deberá recopilar la evidencia necesaria para la adopción de medidas administrativas o judiciales posteriores, resguardando la cadena de custodia.

7.6.2. En caso de ser necesario, debe realizar un análisis forense de seguridad de la información, cumpliendo con lo establecido en la norma de análisis forense de seguridad de la información.

7.6.3. Toda evidencia debe ser manejada por personal calificado y herramientas autorizadas por el organismo, con el fin de no modificar el valor de la evidencia preservada.

RES. CM Nº 141/2026 - ANEXO IV

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Cumplimiento de Seguridad de la Información

DGIYT-GOYT-PL-004

Cumplimiento de Seguridad de la Información

Contenido

1. Cumplimiento de la Seguridad de la Información

2. Objetivo.

Establecer los lineamientos para asegurar que se cumplan las leyes, regulaciones y políticas internas relacionadas con la seguridad de la información, evitando sanciones legales y promoviendo la conformidad de los controles que garanticen la integridad, disponibilidad y confidencialidad de la información.

3. Alcance.

Esta política aplica tanto 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, así como también, a toda la información documentada vigente referente a seguridad de la información.

4. Documentos relacionados.

4.1. **Ley Nacional N° 11.723** - Régimen Legal de la Propiedad Intelectual.
4.2. **Ley Nacional N° 24.766** - Confidencialidad sobre Información y Productos que Estén Legítimamente Bajo Control de una Persona y se Divulgue Indebidamente de Manera Contraria a los Usos Comerciales Honestos.
4.3. **Ley Nacional N° 25.326** - Protección de Datos Personales.
4.4. **Ley Nacional N° 25.506** - Firma Digital.
4.5. **Ley N° 1.845** - Protección de Datos Personales.
4.6. **Ley N° 2.095** - Compras y Contrataciones de la CABA.
4.7. **Ley N° 6.357** - Régimen de Integridad Pública.
4.8. **RES. CM N° 170/2014 -** Reglamento Interno del Poder Judicial de CABA.
4.9. **RES. PRESIDENCIA N° 1259/2015** - Convenio Colectivo de Trabajo de los Trabajadores y Trabajadoras del Poder Judicial de CABA.
4.10. **RES. CM N° 20/2016** - Reglamento Disciplinario para Empleados y Funcionarios.
4.11. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.
4.12. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.
4.13. **DGIYT-GOYT-PL-001** - Seguridad de la Información.
4.14. **DGIYT-GOYT-PL-007** - Gestión de Activos.
4.15. **DGIYT-GOYT-PL-008** - Seguridad Criptográfica.
4.16. **DGIYT-GOYT-PL-012** - Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

5. Definiciones.

5.1. **DGIYT**: Dirección General de Informática y Tecnología.

5.2. **Activos de información**: todo aquello que contiene, procesa, trate y/o manipule información valiosa y que sea necesaria para que el organismo funcione y cumpla con los objetivos establecidos para dicho fin.

5.3. **Información:** la información es la interpretación que se da a los datos. En el caso de la presente política, se entenderá como información a toda forma que contenga datos relacionados del organismo

5.4. **Registro:** se entiende por "registro" (o log) a toda la información generada por los sistemas o personas, que permite realizar un seguimiento de actividades realizadas en los sistemas o procesos manuales.

5.5. **Auditoría forense:** en informática, corresponde a una agrupación de técnicas especializadas en las infraestructuras tecnológicas que nos posibilitan realizar una identificación, preservación, análisis de datos y documentación, asegurando la recolección de evidencia que puede ser utilizada en procesos legales cuando se ha detectado la amenaza y/o ataque informático.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información corporativo (CISO):** garantizar la adecuada gestión de los registros y evidencias necesarias para las auditorías de seguridad de la información, asegurando su disponibilidad oportuna cuando se requiera.

6.3. **Responsable de cumplimiento (RC):** verificar el cumplimiento de los lineamientos especificados en las políticas de seguridad de la información, así como también los requerimientos legales y contractuales que puedan impactar en la seguridad de la información para que se mantengan en consonancia con los controles aplicados.

7. Lineamientos.

7.1. Identificación de la legislación aplicable.

7.1.1. Definir, documentar y mantener actualizados todos los requerimientos legales y contractuales relacionados con la seguridad de la información y de cualquier requisito de seguridad.

7.2. Derecho de propiedad intelectual.

7.2.1. Se recomienda implementar los procedimientos apropiados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propios. Ley Nacional N° 11.723 - Régimen Legal de la Propiedad Intelectual.

7.2.2. Para proteger cualquier material, entre otros, se considerarán los siguientes aspectos:

- La adquisición de software solamente a través de fuentes conocidas y con buena reputación, para disminuir el riesgo de que se viole el derecho de propiedad intelectual ("copyright").

- La concientización respecto de las políticas para la protección de los derechos de propiedad intelectual y la notificación de que se implementaran acciones disciplinarias al personal que incurra en incumplimientos.
- El mantenimiento de registros apropiados de activos y la identificación de todos los activos que requieran protección de los derechos de propiedad intelectual.
- El establecimiento de una política para la disposición final o transferencia de software a otros.

7.3. Requerimientos y protección de los registros de auditorías.

7.3.1. El CISO debe identificar todos los registros de auditoría relevantes y definir medidas de protección, para evitar corrupción, modificación o eliminación no autorizada.

7.3.2. Se debe definir el período de retención de los registros sensibles de auditoría y de acuerdo con las regulaciones vigentes, además se deben implementar controles de seguridad de la información para evitar el acceso no autorizado a ellos, durante todo el periodo de retención.

7.3.3. Determinar los sistemas de información críticos y los registros de auditoría, con la finalidad de monitorear e identificar todas las actividades sospechosas. Los mismos deben ser auditados a intervalos regulares y/o ante incidentes de seguridad de la información

7.3.4. Todo sistema de información nuevo (arrendado, adquirido o externalizado sus servicios), debe poder generar registros de auditoría.

7.3.5. El RC, debe establecer un proceso formal de auditoría y un plan de auditoría que al menos contemple la revisión y evaluación de los mecanismos de control para la seguridad de la información (políticas, normas y procedimientos), en virtud de su suficiencia, aplicabilidad, cobertura y profundidad en la mitigación de los riesgos. Considerando revisiones de cumplimiento de los mecanismos de control para la seguridad de la información, sin incurrir en riesgo de interrupción de los procesos, asegurando el acceso adecuado a las herramientas utilizadas para este fin.

7.3.6. El plan de registros de auditorías al menos debe permitir verificar y revisar el nivel de cumplimiento de las políticas y normas de seguridad de la información implementadas.

7.3.7. Las auditorías, del organismo, deben ser realizadas con herramientas confiables y/o de terceros de confianza.

7.3.8. El CISO, debe establecer controles sobre toda la información generada de las auditorías forenses, entiéndase por esta información: metodología usada, resultados de la auditoría, registros y evidencias.

- Toda auditoría forense, producto de cualquier acto ilícito y que pueda ser causa de una investigación o acción judicial, debe ser realizada de acuerdo con la legislación vigente y se debe tener especial cuidado con preservar el estado original de las evidencias.

7.4. Protección de datos personales.

7.4.1. La información personal que es manejada en el organismo debe ser usada sólo con propósitos directamente relacionados con los objetivos del organismo y se les debe dar un tratamiento según las leyes de protección de datos personales vigentes. Ley Nacional N° 25.326 - Protección de Datos Personales y Ley N° 1.845 - Protección de Datos Personales.

7.5. Controles criptográficos.

7.5.1. Se deben establecer controles criptográficos en el organismo, de acuerdo con las leyes y regulaciones vigentes.

7.5.2. Se recomienda asesoramiento legal para garantizar el cumplimiento de la legislación y las regulaciones pertinentes.

7.6. Cumplimiento de las políticas de Seguridad de la Información.

7.6.1. Desde la DGIYT se debe asegurar y verificar que las actividades y procesos se llevan a cabo correctamente y según las directrices de las políticas, normas y procedimientos de seguridad de la información.

7.6.2. Se debe sancionar administrativamente a quien viole lo dispuesto en la política **DGIYT-GOYT-PL-001** - Seguridad de la Información y todas las políticas específicas nombradas en dicho documento.

- **Ley Nacional N° 24.766** - Confidencialidad sobre Información y Productos que Estén Legítimamente Bajo Control de una Persona y se Divulgue Indebidamente de Manera Contraria a los Usos Comerciales Honestos
- **Ley N° 6.357**- Régimen de Integridad Pública.
- **RES. CM N° 170/2014** - Reglamento Interno del Poder Judicial de CABA.
- **RES. PRESIDENCIA N° 1259/2015** – Convenio Colectivo de Trabajo de los Trabajadores y Trabajadoras del Poder Judicial de CABA, artículos: 30, 31, 32 y 33.
- **RES. CM N° 20/2016** - Reglamento Disciplinario para Empleados y Funcionarios.

7.6.3. Los agentes que no den debido cumplimiento a sus deberes indicados en estas políticas de seguridad de la información podrían incurrir también en responsabilidad civil o patrimonial, cuando se ocasione un daño que debe ser indemnizado y/o en responsabilidad penal, cuando su conducta constituya un comportamiento considerado delito por el código penal y leyes especiales.

7.6.4. Los terceros que no den cumplimiento a las políticas de seguridad de la información del organismo podrán ser sancionados según los términos que rijan la contratación. Ley N° 2.095 - Compras y contrataciones de la CABA.

7.7. Revisión del cumplimiento técnico.

7.7.1. Se debe garantizar que se revisen periódicamente los sistemas de información para verificar que cumplan con las políticas y las normas de seguridad de la información.

7.7.2. Se recomienda que las revisiones de cumplimiento técnico sean con la asistencia de herramientas automatizadas, las cuales generan informes técnicos para la subsiguiente interpretación por parte de un especialista.

7.7.3. Cualquier revisión de cumplimiento técnico debe ser realizado sólo por personas competentes y autorizadas, o bajo la supervisión de tales personas.

7.8. Revisión independiente de la seguridad de la información.

7.8.1. Se recomienda que el RC revise el enfoque del organismo para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), en forma independiente a intervalos planificados o cuando ocurran cambios significativos.

7.8.2. La revisión de la seguridad de la información se podría llevar a cabo por personal competente, independiente del área a auditar, o por una organización de terceras partes especializada en tales revisiones, para garantizar que el enfoque del organismo continúe siendo correcto, adecuado y eficaz. La revisión debe incluir la evaluación de las oportunidades de mejora.

7.8.3. Se recomienda que los resultados de la revisión independiente se registren, mantengan y reporten al Comité Corporativo de Seguridad de la Información (CCSI).

RES. CM Nº 141/2026 - ANEXO V

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de la Información en las Relaciones con los Proveedores

DGIYT-GOYT-PL-005

Seguridad de la información para las relaciones con los proveedores

Contenido

1. Seguridad de la Información para las Relaciones con los Proveedores

2. Objetivo.

Establecer los lineamientos de seguridad de la información en las relaciones con los proveedores con el fin de proteger los activos de información frente a amenazas internas o externas, deliberadas o accidentales, que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información.

3. Alcance.

Esta política aplica a terceros vinculados directa o indirectamente con el Poder Judicial de la Ciudad Autónoma de Buenos Aires -excluido el Ministerio Público y el Tribunal Superior de Justicia-, que brinden servicios informáticos y que para la ejecución de sus funciones manejen y/o requieran acceder a la información.

4. Documentos relacionados.

4.1. **Ley N° 2.095-** Compras y Contrataciones de la CABA.

4.2. **IRAM-ISO/IEC 27001 -** Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.3. **IRAM-ISO/IEC 27002 -** Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-003 -** Gestión de Incidentes de Seguridad de la Información.

4.6. **DGIYT-GOYT-PL-004 -** Cumplimiento de Seguridad de la Información.

4.7. **DGIYT-GOYT-PL-006 -** Seguridad de los Recursos Humanos.

4.8. **DGIYT-GOYT-PL-007 -** Gestión de Activos.

4.9. **DGIYT-GOYT-PL-009 -** Control de Accesos.

4.10. **DGIYT-GOYT-PL-014 -** Seguridad de las Operaciones.

5. Definiciones.

5.1. **Contrato de prestación de servicios o provisión de bienes:** documento jurídico que genera derechos y obligaciones donde se describen los acuerdos establecidos entre las partes interesadas para la ejecución de una obra material, la prestación de un servicio o la adquisición de un bien físico.

5.2. **Acuerdo de confidencialidad y no divulgación:** documento en el que se establecen las obligaciones respecto al cuidado que se debe dar a la información, que manejarán en el contexto de sus actividades laborales para los empleados, contratados o proveedores.

5.3. **Proveedor:** persona física o jurídica que proporciona bienes, productos y/o servicios al organismo.

5.4. **DGIYT:** Dirección General de Informática y Tecnología.

5.5. **ABM:** Altas, bajas y modificación.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que los acuerdos de nivel de servicio con los proveedores cumplan con los requisitos y estándares establecidos para la seguridad de la información.

6.3. **Gestor de servicio:** responsable de gestionar y velar por el cumplimiento de los acuerdos de nivel de servicio entre el organismo y el proveedor de servicios.

7. Lineamientos.

7.1. Generalidades.

7.1.1. Todo proveedor de servicios informáticos se compromete a garantizar que su personal o terceros subcontratados y que presten servicios directamente al organismo, cumplan con sus políticas de seguridad de la información. En este sentido, el proveedor se compromete a capacitar y a poner a disposición las políticas, procedimientos, normas, instructivos, manuales de usuario, formularios y registros aplicables, incluyendo, aunque no limitándose a los siguientes:

- DGIYT-GOYT-PL-001 - Seguridad de la Información.
- DGIYT-GOYT-PL-009 - Control de Accesos.
- DGIYT-GOYT-PL-004 - Cumplimiento de Seguridad de la Información.
- DGIYT-GOYT-PL-003 - Gestión de Incidentes de Seguridad de la Información.
- DGIYT-GOYT-PL-007 - Gestión de Activos.
- DGIYT-GOYT-PL-014 -Seguridad de las Operaciones.

7.1.2. Cualquier tipo de intercambio de información que se produzca entre el organismo y el proveedor, se entenderá que ha sido realizada dentro del marco establecido por el contrato de prestación de servicios o provisión de bienes y el acuerdo de confidencialidad. Además, se establece que el medio oficial para llevar a cabo el intercambio de información será el uso de correo electrónico del dominio del organismo. En caso de que el proveedor requiera usar otra herramienta de comunicación, deberá ser notificado al CISO para ser evaluada, garantizando que se mantenga la integridad, disponibilidad y confidencialidad de la información.

7.1.3. Todos los recursos que la DGIYT pone a disposición del proveedor, son exclusivamente destinados para cumplir con las obligaciones y propósitos del servicio contratado.

7.1.4. La DGIYT deberá determinar un responsable (Gestor de Servicio) para cada proveedor.

7.1.5. El incumplimiento de los lineamientos de Seguridad de la Información podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normativas vigentes.

7.2. Acuerdo de confidencialidad.

7.2.1. En el acuerdo de confidencialidad se establecerán todos los requisitos de seguridad de la información pertinentes con cada proveedor y deberá ser firmado por todo el personal que se involucre en el servicio prestado. El mismo deberá ser validado por el CISO.

7.2.2. Entre otros, en el acuerdo de confidencialidad se deberá considerar que:

- Se describa la información a la que se va a tener acceso y los métodos para suministrar dicha información o para acceder a ella.
- La información generada cumpla con los lineamientos de la norma correspondiente sobre clasificación de la información.
- Se describa y asegure que se cumplan los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor.

7.3. Vulnerabilidades e incidentes de seguridad de información.

7.3.1. El proveedor debe reportar toda vulnerabilidad, evento o incidente que pudiera afectar la confidencialidad, integridad o disponibilidad de la información del organismo.

7.3.2. Cuando el proveedor conozca de cualquier pérdida, uso no autorizado, revelación de la información u otra circunstancia que pudiera afectar la seguridad de la información del organismo, deberá cumplir con los lineamientos establecidos en el instructivo sobre cómo informar un incidente de seguridad de la información

7.4. Control y revisión de la provisión de servicios.

7.4.1. La DGIYT se reserva el derecho de implementar periódicamente mecanismos de control, monitoreo, revisiones y auditorías a los servicios contratados de acuerdo con lo especificado en la norma sobre gestión de riesgos de seguridad de la información, con el fin de:

- Asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, que los incidentes y problemas de seguridad de la información se gestionen apropiadamente.
- Hacer seguimiento y control a los reportes, auditorías del proveedor, registros de eventos de seguridad de la información, problemas operacionales, incidentes e interrupciones relacionadas con el servicio entregado.
- Revisar los aspectos de seguridad de la información de las relaciones de los proveedores con terceros.

7.4.2. Los terceros que no den cumplimiento a las políticas de seguridad de la información del organismo podrán ser sancionados según los términos que rijan la contratación. Ley N° 2.095 - Compras y contrataciones de la CABA.

7.5. Gestión de cambios en la provisión de servicios.

7.5.1. La DGIYT administrará los cambios, evaluará la necesidad y justificación del cambio, los riesgos asociados y su impacto en los servicios ya existentes, incluido el mantenimiento y

la mejora de las políticas, procedimientos y controles de seguridad de la información, teniendo en cuenta la criticidad de la información y los sistemas y procesos involucrados del organismo.

7.5.2. De presentarse un cambio en la provisión del servicio, el proveedor lo informará por escrito (sea por alta, baja, sustitución, cambio de funciones, responsabilidades o alcance) y de corresponder deberá cumplir la presente política.

7.6. Acceso a activos de información del organismo.

7.6.1. Todos los accesos serán autorizados según los lineamientos establecidos en la política DGIYT-GOYT-PL-009 - Control de Accesos.

7.6.2. Cada persona con acceso a la información del organismo es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él derive.

7.6.3. De requerirse una gestión de ABM de usuarios, el gestor del servicio del proveedor deberá generar la solicitud, cumpliendo con los lineamientos establecidos en el procedimiento de gestión de ABM de usuarios.

7.6.4. Los proveedores de servicios de tecnología, con acceso a las aplicaciones del organismo que requieran gestionar contraseñas, deberán regirse por los lineamientos establecidos en la norma sobre gestión de claves seguras.

7.6.5. El proveedor deberá garantizar la protección de los activos de información del organismo bajo su uso, garantizando su seguridad tanto durante su utilización como cuando se encuentren inactivos.

7.6.6. El proveedor no deberá, sin autorización explícita, realizar pruebas para detectar, utilizar o explotar una debilidad o vulnerabilidad en un sistema del organismo.

7.6.7. En los casos en que el proveedor requiera que se dé la baja o reasigne un activo del organismo, deberá regirse por los lineamientos establecidos en el procedimiento de gestión de activos.

7.7. **Tratamiento de riesgos relacionados con proveedores.**

7.7.1. La DGIYT identificará y evaluará los riesgos asociados con los proveedores, probabilidades e impactos, definirá estrategias y acciones para mitigar y/o controlar los riesgos y garantizará mecanismos de monitoreos y seguimiento continuo, procurando proveedores confiables, la mitigación de riesgos y la continuidad del suministro.

7.8. Especificaciones técnicas en los contratos.

7.8.1. Entre otros, en los contratos de prestación de servicios o provisión de bienes con proveedores se debe considerar de forma explícita lo siguiente:

- Controles de seguridad de la información.
- Requisitos de seguridad según lo establecido en la norma sobre desarrollo seguro.

- Divulgación por parte de los proveedores de las prácticas y requisitos de seguridad a lo largo de la prestación del servicio.
- Derecho del organismo, de auditar los procesos y controles de los proveedores, relacionados con el acuerdo de prestación de servicios.
- Reglas para compartir cualquier tipo de información entre el organismo y los proveedores.
- Implementación de procesos específicos para la gestión del ciclo de vida y la disponibilidad de componentes de tecnología de información, comunicación y de los riesgos de seguridad asociados.
- Derecho del organismo a solicitar el cambio de personal o de disolver el contrato en caso de incumplimiento por parte del proveedor, según lo establecido en el Pliego de Base de Condiciones Particulares de la contratación vigente.
- Lista detallada de personal del proveedor autorizado para tener acceso o recibir información del organismo.
- Obligación del proveedor que desarrolle o modifique un sistema informático de entregar todos los archivos ejecutables, el código fuente, los manuales de uso y las indicaciones técnicas correspondientes, además de proporcionar las capacitaciones necesarias para el adecuado uso del sistema.

7.9. Finalización de contrato.

7.9.1. Todo proveedor garantiza que, al momento de la culminación del servicio, inmediatamente cesará de sus servicios y el uso de toda la información proporcionada, entregando la misma que obre en su poder y destruyendo toda copia que haya realizado. Asimismo, entregará una confirmación por escrito, la cual tendrá calidad de declaración jurada.

RES. CM Nº 141/2026 - ANEXO VI

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de los Recursos Humanos

DGIYT-GOYT-PL-006

Seguridad de los Recursos Humanos

Contenido

1. Seguridad de los Recursos Humanos

2. Objetivo.

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.

3. Alcance.

Esta política aplica tanto 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 contratados directa o indirectamente con él, que desempeñen funciones y/o actividades relacionadas con la gestión de personal los cuales tengan acceso a información de éste.

4. Documentos relacionados.

4.1. **RES. PRESIDENCIA N° 1.259/2015 -** Convenio Colectivo de Trabajo de los Trabajadores y Trabajadoras del Poder Judicial de CABA.

4.2. **IRAM-ISO/IEC 27001 -** Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.3. **IRAM-ISO/IEC 27002 -** Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-004 -** Cumplimiento de Seguridad de la Información.

4.6. **DGYIT-GOYT-PL-005 -** Seguridad de la Información en las Relaciones con los Proveedores.

5. Definiciones.

5.1. **DGIYT**: Dirección General de Informática y Tecnología.

5.2. **DGFH:** Dirección General de Factor Humano.

5.3. **Acuerdo de Confidencialidad y No Divulgación:** documento en el que se establecen las obligaciones respecto al cuidado que se debe dar a la información, que manejarán en el contexto de sus actividades laborales para los agentes y/o terceros.

5.4. **Información Confidencial:** toda información altamente sensible y disponible solamente para un grupo específico del organismo y terceros autorizados explícitamente por el propietario o custodio de la información.

5.5. **Información privada:** toda información que requiera de cierto nivel de protección, pero que no cumple con los criterios necesarios para ser clasificada como confidencial o secreta y que es única y exclusivamente para uso interno del organismo y para aquellos que sean autorizados por acuerdos de confidencialidad.

5.6. **Información Secreta:** toda información que sea protegida, intransferible e indelegable y que sea prohibido su acceso, distribución, publicación y difusión general de forma permanente, con

excepción de las autoridades competentes que, conforme a las regulaciones vigentes del organismo, tengan acceso autorizado a ella.

5.7. **Agente:** Se refiere toda persona vinculada con el organismo y/o que desempeñe tareas en el mismo.

5.8. **Seguridad de información:** es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información de los diferentes riesgos a los que puede estar expuesta, con el fin de minimizar el daño y garantizar la continuidad operacional.

5.9. **Propietario de activo de información**: se refiere al organismo, representado por un individuo o área designada, que asume la responsabilidad principal sobre los activos de información. Esto incluye tomar decisiones estratégicas sobre su uso, designar a quienes se encarguen de su administración, protección y valoración. Sin embargo, no implica necesariamente que gestione o utilice directamente el activo.

5.10. **Custodio de los activos de información**: es la entidad que administra física o digitalmente el activo de información. Su función es proteger y gestionar el activo de acuerdo con las regulaciones dictaminadas por el propietario, implementando controles de seguridad que aseguren la disponibilidad, integridad y confidencialidad de este.

5.11. **Proveedor:** persona física o jurídica que proporciona bienes, productos y/o servicios al organismo.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de Seguridad de la Información Corporativo (CISO):** gestionar planes de capacitación en materia de seguridad de la información para garantizar que todos los agentes y/o terceros comprendan y cumplan las políticas, legislaciones vigentes y mejores prácticas de seguridad.

6.3. **Director General de Factor Humano:** implementar los lineamientos establecidos en esta política, según le corresponda de acuerdo con sus funciones. Así como también informar las altas, traslado o desvinculación del personal a la DGIYT.

6.4. **Gestor de Servicio / Superior Jerárquico:** supervisar y garantizar que los agentes y/o terceros bajo su responsabilidad cumplan con los lineamientos de seguridad de la información establecidos en esta política.

7. Lineamientos.

7.1. Antes del vínculo laboral.

7.1.1. La DGFH entre otras funciones, debe:

- Realizar una verificación de antecedentes de todos los candidatos al puesto de trabajo según las leyes, regulaciones y reglas éticas del organismo.
- Establecer en los vínculos laborales con los agentes y/o terceros contratados, de corresponder, los términos y condiciones laborales y/o de servicios donde se detallen

las responsabilidades de este y del organismo para con la seguridad de la información, de acuerdo con la política general.

7.1.2. La DGIYT, así como cualquier otra área que en el futuro lo considere necesario, debe asegurar que todas las personas que ejerzan funciones dentro de éstas firmen el acuerdo de confidencialidad y no divulgación que corresponda, previo a darle el alta de usuario.

7.2. Durante el vínculo laboral.

7.2.1. El organismo deberá comunicar los requerimientos a los agentes y/o terceros contratados que deben aplicar de acuerdo con las políticas y normas establecidas de Seguridad de la Información.

7.2.2. El superior jerárquico de los agentes deberá brindar todas las facilidades necesarias para su participación en cursos o capacitaciones relacionados con la seguridad de la información.

7.2.3. Se deben comunicar las directrices y actividades que respalden el buen uso de los activos informáticos, para reducir los daños ocasionados por incidentes de seguridad de la información y/o mal funcionamiento, producto de errores humanos o desconocimiento.

7.2.4. Los agentes y cuando sea pertinente, los terceros contratados, deben recibir concientización y capacitación apropiadas de Seguridad de la Información que sean pertinentes a su tarea.

7.2.5. Para todo proceso de capacitación en temas de seguridad de la información, el CISO debe velar por la correcta implementación integral del proceso de capacitación.

7.2.6. Para sancionar a aquellos que hayan incumplido las políticas y normas de Seguridad de la Información, se debe aplicar un proceso disciplinario formal.

7.2.7. Todos los agentes deben asistir a las capacitaciones de seguridad de la información, de acuerdo con las necesidades del área donde se desempeñen.

7.2.8. Todos los agentes deben informar cualquier violación de seguridad de la información a sus superiores jerárquicos directos o al área de seguridad de la información, inmediatamente cuando se detecte, de lo contrario, se pueden aplicar sanciones disciplinarias según lo establecido en la política DGIYT-GOYT-PL-004 - Cumplimiento de seguridad de la información.

7.2.9. Debe existir una comunicación constante y efectiva entre la DGFH y la DGIYT, con el fin de tener un seguimiento controlado de las altas, bajas y modificaciones de usuarios.

7.2.10. El superior jerárquico del nuevo agente o el gestor de servicio del proveedor deberá solicitar la gestión del ABM de accesos y permisos a los sistemas correspondientes de acuerdo con lo establecido en el procedimiento de gestión de ABM de usuarios.

7.2.11. El superior jerárquico del nuevo agente deberá garantizar que el mismo use adecuadamente los sistemas informáticos a los que le haya solicitado el acceso, según las políticas de seguridad de la información vigente.

7.3. Desvinculación o cambio de puesto.

7.3.1. Se debe definir, comunicar y hacer cumplir a los agentes y/o terceros contratados, las responsabilidades y las obligaciones relativas a la Seguridad de la Información que continúan estando vigentes luego de la desvinculación o cambio de puesto.

7.3.2. En caso de baja de los agentes o terceros contratados, el superior jerárquico o el gestor de servicio donde estuvo designada la persona, deberá informar inmediatamente a la DGIYT, siguiendo los pasos del procedimiento de gestión de ABM de usuarios.

7.3.3. El agente que deja de prestar servicios para al organismo, debe restituir todos los activos de información y elementos de identificación del organismo de corresponder. Refiriéndose entre otros a: información del organismo en todos sus medios de almacenamiento y en caso de incumplimiento podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normas vigentes.

7.3.4. La inhabilitación (ya sea temporal o definitiva) debe realizarse en el momento del cese, por lo cual las comunicaciones deberán efectuarse oportunamente, siendo responsables el superior jerárquico o el gestor de servicio donde estuvo designada la persona.

7.3.5. Si en opinión del superior jerárquico existe riesgo de la seguridad de la información, se debe informar a quien corresponda que el agente desvinculado no tiene autorización para actuar en representación del organismo.

7.3.6. En caso de transferencia o reasignación de agentes, los derechos de accesos y privilegios del antiguo rol se deben bloquear o remover, según lo establecido en el procedimiento de gestión de ABM de usuarios. En caso de incumplimiento, se procederá con sanciones de acuerdo con lo establecido en la política DGIYT-GOYT-PL-004 - Cumplimiento de Seguridad de la Información.

RES. CM Nº 141/2026 - ANEXO VII

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Gestión de Activos

DGIYT-GOYT-PL-007

Gestión de Activos

Contenido

1. Gestión de Activos

2. Objetivo.

Establecer los lineamientos para identificar y clasificar los activos de información, asegurando que se les asigne la protección adecuada en función de su criticidad y los riesgos asociados.

3. Alcance.

Esta política aplica para todos los activos de información gestionados por el 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. La no inclusión explícita en el presente documento no constituye argumento para no proteger activos de información que se encuentren en otras formas.

4. Documentos relacionados.

4.1. **RES. PRESIDENCIA N° 557/2014** - Creación de la Dirección General de Informática y Tecnología.

4.2. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.3. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-004** - Cumplimiento de Seguridad de Información.

4.6. **DGIYT-GOYT-PL-009 -** Control de Accesos.

4.7. **DGIYT-GOYT-PL-014** - Seguridad de las Operaciones.

5. Definiciones.

5.1. **DGIYT**: Dirección General de Informática y Tecnología.

5.2. **Buen uso:** se entiende por "buen uso" de los sistemas de información del organismo, a las expectativas con respecto al cuidado que su personal debe procurar a los activos de información que se ponen a su alcance. Por esto se entiende, usar los activos de información exclusivamente para los fines para los cuales se otorgó el acceso, evitando la modificación, divulgación, destrucción intencional, salvo expresa autorización.

5.3. **Ciclo de vida de un activo**: etapas de la relación de un activo, desde la adquisición, pasando por la puesta en marcha, la operación y la eliminación.

5.4. **Activos de información:** todo aquello que contiene, procesa, trate y/o manipule información valiosa y que sea necesaria para que el organismo funcione y cumpla con los objetivos establecidos para dicho fin.

5.5. **Tipos de activos de información:**

- **Activos primarios**: procesos y actividades de servicio.

- **Activos de soporte**: hardware, software, redes, personal, ubicación y estructura del organismo.

5.6. **Activos de software:** software de aplicaciones, sistemas, herramientas de desarrollo, utilitarios, entre otros.

5.7. **Activos hardware:** equipamiento de computación, comunicaciones, medios removibles, entre otros.

5.8. **Medios removibles:** todo dispositivo de almacenamiento de información que se pueda conectar y desconectar fácilmente de un activo informático para transferir, almacenar o respaldar datos. Estos medios son portátiles, lo que permite transportarlos entre diferentes dispositivos o ubicaciones cómo, por ejemplo, unidades USB, discos duros portables, tarjetas SD, CD, DVD, etc.

5.9. **Clasificación de la información:** acto de asignar a la información alguna de las categorías definidas por el organismo, pudiendo ser: pública, privada, confidencial o secreta.

5.10. **Información pública**: toda información de uso general, que por su contenido o contexto no requiere de protección especial y que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del organismo. Ésta no deberá generar daños a terceros, ni a las actividades y/o procesos relacionados.

5.11. **Información privada**: toda información que requiera de cierto nivel de protección, pero que no cumple con los criterios necesarios para ser clasificada como confidencial o secreta y que es única y exclusivamente para uso interno del organismo y para aquellos que sean autorizados por convenios.

5.12. **Información confidencial:** toda información altamente sensible y disponible solamente para un grupo específico del organismo y terceros autorizados explícitamente por el propietario o custodio de la información.

5.13. **Información secreta:** toda información que sea protegida, intransferible e indelegable y que sea prohibido su acceso, distribución, publicación y difusión general de forma permanente, con excepción de las autoridades competentes que, conforme a las regulaciones vigentes del organismo, tengan acceso autorizado a ella.

5.14. **Dispositivo móvil:** aparato de dimensiones relativamente pequeñas, diseñado para ser portátil y vincularse con otros equipos mediante Bluetooth o conectividad Wi-Fi, estos dispositivos pueden ser transportados con frecuencia y facilidad y poseen la capacidad de enviar y recibir datos sin ningún tipo de cableado

5.15. **Propietario de activo de información**: se refiere al organismo, representado por un individuo o área designada, que asume la responsabilidad principal sobre los activos de información. Esto incluye tomar decisiones estratégicas sobre su uso, designar a quienes se encarguen de su administración, protección y valoración. Sin embargo, no implica necesariamente que gestione o utilice directamente el activo.

5.16. **Custodio de los activos de información**: es la entidad que administra física o digitalmente el activo de información. Su función es proteger y gestionar el activo de acuerdo con las

regulaciones dictaminadas por el propietario, implementando controles de seguridad que aseguren la disponibilidad, integridad y confidencialidad de este.

5.17. **Usuario:** cualquier cargo, proceso, sistema o área, que genere, obtenga, transforme, conserve o utilice información del organismo para propósitos propios de su labor.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** responsable de la custodia de los activos informáticos asignados de acuerdo con Resolución Presidencia N° 557/2014 – Creación de la Dirección General de Informática y Tecnología, así como también garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que todos los activos de información cuenten con los controles de seguridad apropiados según su nivel de criticidad, asegurando su protección frente a riesgos y cumpliendo con las mejores prácticas en seguridad de la información.

6.3. **Oficial de seguridad de la información (OSI):** monitorear los activos de información correspondientes y gestionar de manera integral los controles de seguridad necesarios en cada etapa de su ciclo de vida, desde su creación o adquisición hasta su baja operativa.

7. Lineamientos.

7.1. Generalidades de la seguridad de los activos de información.

7.1.1. Todas las áreas pertenecientes al organismo deben considerar las directrices de la presente política.

7.1.2. Los agentes del Poder Judicial de la CABA o terceros tienen por obligación proteger físicamente los activos, así como también proteger la información.

7.1.3. Todos los activos deben estar protegidos para que cualquier información procesada y/o almacenada en ellos permanezca segura, que la integridad del activo no se vea comprometida y que esté disponible para cuando se necesite.

7.1.4. El uso de los activos para propósitos ilegales y/o inapropiados para el ambiente de trabajo está estrictamente prohibido y puede resultar en acciones disciplinarias de acuerdo con lo establecido en la política DGIYT-GOYT-PL-004 - Cumplimiento de Seguridad de Información.

7.1.5. Todo activo debe pasar por un análisis de riesgos para determinar su nivel de criticidad y a su vez evaluar las medidas de mitigación de estos, según lo establecido en la norma de gestión de riesgos de seguridad de la información.

7.2. Inventario de activos de información.

7.2.1. Al recibir un activo informático se deberá garantizar que el alta de este sea registrada en el sistema de gestión de inventario de manera inmediata.

7.2.2. Se deberá mantener un sistema de gestión de inventario de activos actualizado, debiendo ser revisado periódicamente.

7.2.3. Se debe dar cumplimiento del procedimiento de gestión de activos que regula y asegura la actualización permanente del activo de información y la aplicación de controles.

7.2.4. En el sistema de gestión inventario de activos de información se debe incluir toda información necesaria, que permita implementar las medidas de control y de protección de acuerdo con la sensibilidad de cada activo.

7.3. Propiedad de los activos de información.

7.3.1. Todo activo de información debe ser asociado a un propietario, que le asigne un valor apropiado a su sensibilidad e importancia y que garantice la protección efectiva del mismo de acuerdo con los riesgos que lo afectan.

7.3.2. Los propietarios de los activos de información deben velar por el cumplimiento de clasificación de la información que se encuentra bajo su responsabilidad en función de su sensibilidad y criticidad, cumpliendo los lineamientos establecidos en la norma de clasificación de la información.

7.3.3. El propietario de los activos de información puede delegar en un custodio la administración, uso y protección de este. Sin embargo, la responsabilidad de éste sigue siendo del propietario.

7.3.4. Para toda información, el propietario o el custodio asignado por el mismo, deberá asegurar las medidas necesarias para garantizar el acceso a ella, en cualquiera de sus formatos, sólo por las personas autorizadas.

7.4. **Uso aceptable de los activos de información.**

7.4.1. Los agentes del Poder Judicial de la CABA o terceros deben notificar al OSI toda debilidad, incidente o evento asociado a actividades no permitidas o malas prácticas de acceso, que pudieran derivar en un posible incumplimiento, uso indebido o poner en riesgo la seguridad de un activo.

7.4.2. Todos los agentes del Poder Judicial de la CABA o terceros deberán hacer uso aceptable de los activos informáticos y cumplir los requisitos de seguridad al momento de utilizarlos según lo establecido en la norma de uso aceptable de los activos y recursos informáticos.

7.4.3. De no cumplirse los lineamientos establecidos respecto a la norma de uso aceptable de los activos y recursos informáticos se aplicarán sanciones en función de la política DGIYT-GOYT-PL-004 - Cumplimiento de Seguridad de la Información.

7.5. **Devolución de activos de información,**

7.5.1. La baja operativa de los activos deberá ser debidamente registrada siguiendo los lineamientos del procedimiento de gestión de activos.

7.5.2. La toma de decisión de la desincorporación de los activos de hardware deberá ser tomada por el organismo de acuerdo con lo analizado en el informe del estado de los activos.

7.5.3. El CISO deberá garantizar que a todo activo de hardware que requiera ser dado de baja operativa, antes de ser llevado a su estado final, le sea eliminada toda información que contenga.

7.6. Clasificación de activos de información.

7.6.1. Los agentes del Poder Judicial de la CABA, ante el desconocimiento del nivel de clasificación o etiquetado de la información recibida, procesada o mantenida, debe asumir siempre una clasificación o etiquetado confidencial.

7.6.2. La información debe ser clasificada de acuerdo con los lineamientos establecidos en la norma de clasificación de la información.

7.6.3. Todo acceso a información clasificada como secreta o confidencial debe ser restringida y autorizada explícitamente por el propietario o custodio del activo.

7.7. Etiquetado y manipulado de información.

7.7.1. La información, independiente del tipo; papel o digital, que requiera ser transmitida, siempre debe contar con las medidas de seguridad apropiadas, de modo de evitar su interceptación o acceso no autorizado.

7.7.2. El organismo deberá regirse por los lineamientos de etiquetado y manipulado de activos de información, establecidos en la norma de clasificación de la información.

7.7.3. Se debe hacer una verificación del inventario físico de activos informáticos del organismo para validar que no se hayan efectuado retiros no autorizados.

7.8. Divulgación de la información.

7.8.1. Si se requiere divulgar información, sólo los propietarios o custodios de dicha información deben autorizar su divulgación, el medio y quién lo realiza.

7.8.2. Si se divulga oralmente información en una reunión, seminario, discurso o presentación, el expositor debe señalar la clasificación de la información y exigir discreción de corresponder.

7.9. Medios removibles.

7.9.1. Solo es permitido el uso de medios removibles (pendrive, disco duro externo, almacenamientos virtuales, cintas magnéticas, discos externos, entre otros) a aquellos usuarios autorizados que lo requieran por el tipo de labores que realizan y para uso exclusivo del organismo, el incumplimiento de esto será sancionado de acuerdo con lo establecido por la política DGIYT-GOYT-PL-004 - Cumplimiento de seguridad de información.

7.9.2. Es responsabilidad del custodio y usuario autorizado del medio removible, tomar las medidas adecuadas para el almacenamiento y resguardo del activo, con el fin de evitar accesos no autorizados, daños, pérdida de información o extravío del medio, durante el uso

o traslado de este. Si algo de esto ocurriera, se considera un incidente de seguridad de la información y debe ser reportado inmediatamente al OSI.

7.9.3. Se recomienda que los medios de almacenamiento removible sean protegidos por contraseñas seguras, cumpliendo con lo establecido en la norma de gestión de claves seguras, evitando el acceso no autorizado a la información.

7.9.4. Toda información que requiera ser almacenada en medios removibles, debe realizarse en los medios que son de propiedad del organismo.

7.9.5. Todo medio removible debe ser escaneado mediante un antivirus, cada vez que sea conectado a un equipo en red del organismo y se deben monitorear y registrar todas las transferencias de información que se realicen.

7.9.6. Los activos de información clasificados como “confidencial” o “secreto” y que se transporten en un medio de almacenamiento removible, sólo podrán ser transportados por personal autorizado por el organismo, quien debe proteger la integridad del activo y su contenido contra accesos no autorizados, mal uso o corrupción durante el transporte. Se deben llevar los registros de la transportación, los involucrados y la recepción de destino.

7.9.7. Los medios de almacenamiento deberán ser destruidos físicamente de manera apropiada, para que la información contenida, no pueda ser recuperada.

7.9.8. Para la eliminación de medios de almacenamiento, se debe cumplir con lo establecido en la norma borrado seguro de la información.

7.10. **Dispositivos móviles.**

7.10.1. Se deben establecer los controles de seguridad necesarios para evitar que el uso de los dispositivos móviles sea causa de infección y distribución de código malicioso dentro del organismo, y así prevenir que éstos sean el origen de accesos no autorizados a las redes informáticas. Para ello, es necesario el cumplimiento de las directivas que se describen a continuación:

- Los dispositivos móviles deben estar inventariados.
- Los dispositivos móviles deben estar cifrados.
- Los dispositivos móviles deben contar con mecanismos de protección contra código malicioso.
- Los sistemas o servicios que puedan ser accedidos mediante dispositivos móviles deben estar identificados.
- Los dispositivos móviles deben contar con bloqueo mediante contraseña, pin u otro medio robusto de autenticación.
- Se debe reportar la pérdida o extravío de dispositivos móviles de forma inmediata a la toma de conocimiento, de acuerdo con los procedimientos y/o protocolos establecidos.
- Los dispositivos móviles deben tener un sistema operativo obtenido por canales oficiales o instalados de fábrica y contar con la última actualización instalada.

- Las aplicaciones instaladas en el dispositivo deben ser aprobadas por el organismo y con el licenciamiento debido.
- Se recomienda que se implementen instrumentos y herramientas técnicas (hardware, software) que permitan bloquear y/o borrar la información de forma remota. Se deberá evaluar puntualmente los riesgos asociados al uso de dispositivos que no permitan el cumplimiento de este control.
- Se debe contar con procedimientos para la reutilización y/o eliminación de dispositivos (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible allí almacenada.

RES. CM Nº 141/2026 - ANEXO VIII

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Seguridad Criptográfica

DGIYT-GOYT-PL-008

Seguridad criptográfica

Contenido

1. Seguridad Criptográfica

2. Objetivo.

Establecer los lineamientos para el uso de técnicas criptográficas adecuadas con el fin de proteger la confidencialidad, autenticidad e integridad de los datos e información durante su almacenamiento y transmisión.

3. Alcance.

Esta política aplica tanto 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, los cuales gestionen el cifrado de datos e información.

4. Documentos relacionados.

4.1. **Ley Nacional N° 25.326** - Protección de Datos Personales.

4.2. **Ley Nacional N° 25.506** - Firma Digital.

4.3. **Ley N° 1.845**- Protección de Datos Personales.

4.4. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.5. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.6. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.7. **DGIYT-GOYT-PL-006 -** Seguridad de los Recursos Humanos.

5. Definiciones.

5.1. **Criptografía:** técnica que permite alterar y modificar el código lingüístico y/o tecnológico habitual de mensajes y/o datos, recurriendo a un cifrado o a una codificación diferente, con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo.

5.2. **Cifrado:** proceso para convertir información en un formato ilegible aplicando un algoritmo criptográfico.

5.3. **Controles criptográficos:** técnicas y mecanismos utilizados para proteger la información mediante el uso de cifrado de datos. Se emplean para asegurar la confidencialidad, integridad y autenticidad de estos, desde el almacenamiento hasta la transmisión segura.

5.4. **Firma Digital:** es un mecanismo criptográfico que se implementa utilizando dos (2) claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

5.5. **No repudio:** capacidad de demostrar o probar la participación de las partes (origen y destino), mediante su identificación, en una comunicación o en la realización de una determinada acción.

5.6. **Claves criptográficas:** cadena de caracteres utilizados por un algoritmo criptográfico para transformar texto plano (legible) en texto cifrado o viceversa. Puede ser secreta o pública.

5.7. **Clave secreta (criptografía simétrica):** cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

5.8. **Clave pública (criptografía asimétrica):** cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que la gestión de los procedimientos relacionados con los controles y claves criptográficas se realicen en cumplimiento con los lineamientos de seguridad establecidos en esta política.

7. Lineamientos.

7.1. Controles criptográficos

7.1.1. Se realizarán evaluaciones de riesgo a todo nuevo sistema, dispositivo informático y servicio del organismo, con el fin de identificar los datos sensibles que requieran protección criptográfica, determinando los requerimientos de resguardo y mecanismos de encriptación, tanto para su almacenamiento, transporte, validación y control de acceso.

7.1.2. Todos los sistemas de acceso públicos deben prever que la información que se obtenga procese y proporcione, sea de acuerdo con las normativas vigentes, en especial la Ley Nacional N° 25.326- Protección de datos personales. y Ley N° 1.845- Protección de datos personales.

7.1.3. El CISO deberá garantizar el uso de controles criptográficos para maximizar los beneficios, como la autenticación, el no repudio, la integridad y la confidencialidad de la información. Entre otros, los controles serán utilizados en los siguientes casos:

- Para la protección de los datos que se trasmiten, procesen y/o almacenen.
- Para la protección de las credenciales de los usuarios.
- Para permitir comunicaciones seguras, entre sistemas y/o dispositivos.
- Para las verificaciones, autenticaciones, identificaciones y validaciones.

7.1.4. Para la aplicación efectiva de los controles criptográficos, se tomará en cuenta lo siguiente:

- Se deben definir los algoritmos criptográficos que podrán utilizarse en el interior del organismo, como aplicación directa o como parte de la configuración de otros productos de seguridad comerciales, tomando en cuenta el tipo, la calidad de los algoritmos criptográficos utilizados y la longitud de las claves criptográficas.

7.1.5. Periódicamente los controles criptográficos serán evaluados con el fin de identificar riesgos y vulnerabilidades.

7.1.6. En casos de daño, compromiso o pérdida de información cifrada o de claves, deberá ser reportada de manera inmediata al organismo.

7.1.7. Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular. Las firmas y certificados digitales se rigen por la legislación vigente como la Ley Nacional N° 25.506- Firma Digital.

7.2. Claves criptográficas

7.2.1. Las claves criptográficas deben gestionarse y protegerse de forma segura a lo largo de su ciclo de vida, desde su generación y almacenamiento iniciales, hasta su recuperación, distribución, retirada y destrucción final.

7.2.2. Se recomienda utilizar un certificado de clave pública administrada por una entidad denominada Autoridad Certificante (AC) para la administración segura de las claves secretas y privadas.

7.2.3. El acceso a las claves criptográficas debe ser limitado únicamente a personal autorizado.

7.2.4. El CISO deberá garantizar que las solicitudes de claves criptográficas sean debidamente autorizadas, proporcionadas a tiempo y registradas adecuadamente.

7.2.5. Cada clave criptográfica tendrá un ciclo de vida, el cual dependerá del nivel de complejidad de esta y de la clasificación de la información o equipo que se desea proteger, debe ser definida con el fin de reducir la probabilidad del uso inapropiado.

7.2.6. Se recomienda que el ciclo de vida de la clave criptográfica dure por un lapso no mayor a doce (12) meses.

7.2.7. Los algoritmos criptográficos, la longitud de las claves y su uso, deben ajustarse a lo establecido en la norma de gestión de claves seguras.

7.2.8. Para la protección de las claves criptográficas durante su uso, se tomarán en cuenta los siguientes lineamientos:

- Todas las claves deben ser protegidas contra modificación y destrucción.
- Las claves secretas y privadas deben ser protegidas contra copia o divulgación no autorizada.
- Las claves públicas deben ser protegidas mediante el uso de su correspondiente certificado.
- Los activos utilizados para generar, almacenar y archivar las claves deben ser protegidos adecuadamente.

7.2.9. Si los datos en un medio de almacenamiento se encuentran cifrados incluso en modo de respaldo, las llaves de cifrado deben ser almacenadas en otro medio de almacenamiento separado (cuando sea necesario).

7.2.10. Toda información protegida debe ser transferida por un medio distinto al utilizado para transferir las llaves criptográficas.

7.2.11. En el caso de que un usuario sea desvinculado del organismo, la clave criptográfica existente debe ser revocada de forma inmediata, anulada o desactivada.

7.2.12. En los casos donde la clave criptográfica se vea comprometida, deberá ser revocada y se debe generar una nueva clave para evitar la fuga de datos.

7.2.13. Todas las actividades relativas a la gestión de claves deben ser registradas para control interno.

7.2.14. Los acuerdos y contratos con proveedores externos de servicios criptográficos deben definir la responsabilidad legal, confiabilidad y tiempos de respuesta para la prestación de los servicios.

7.2.15. En la norma de gestión de claves seguras se definen los lineamientos de los siguientes aspectos:

- Asignación de claves de forma segura a los usuarios que corresponda, incluyendo información de cómo deben activarse cuando se reciban.
- Almacenamiento de claves, incluyendo la forma de acceso a éstas por parte del personal autorizado.
- Actualización de claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las mismas.
- Revocación de claves, incluyendo cómo deben retirarse o desactivarse.

RES. CM Nº 141/2026 - ANEXO IX

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Control de Accesos

DGIYT-GOYT-PL-009

Control de Accesos

Contenido

1. Control de Accesos

2. Objetivo.

Establecer los lineamientos generales para restringir el acceso a los sistemas de información exclusivamente a aquellos que estén autorizados, garantizando la implementación de controles de autenticación y autorización efectivos.

3. Alcance.

Esta política aplica tanto 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 según sus roles y funciones requieran acceso lógico a los activos de información de éste. La no inclusión explícita en el presente documento no constituye argumento para no controlar el acceso a los activos de información que se encuentren en otras formas.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

5. Definiciones.

5.1. **DGIYT:** Dirección General de Informática y Tecnología.

5.2. **DGFH:** Dirección General de Factor Humano.

5.3. **ABM:** alta, baja o modificación.

5.4. **Activos de información:** todo aquello que contiene, procesa, trate y/o manipule información valiosa y que sea necesaria para que el organismo funcione y cumpla con los objetivos establecidos para dicho fin.

5.5. **Acceso:** permiso para ingresar a un recurso, sistema, aplicación o red.

5.6. **Dirección General de informática y tecnología (DGIYT):** es el órgano técnico responsable de proponer proyectos de tecnología innovadores que permitan mejorar la calidad de los procesos judiciales y procedimientos administrativos de gestión del Poder Judicial de la CABA.

5.7. **Derechos de accesos:** conjunto de permisos dados a un usuario para acceder a un determinado recurso de acuerdo con su rol y función.

5.8. **Derechos privilegiados:** conjunto de permiso o atributos dados a un usuario, quien de acuerdo con sus funciones y/o tareas encomendadas, puede acceder a un determinado recurso.

5.9. **Permiso:** autorización que mantiene un usuario para realizar determinadas acciones dentro de un sistema informático especifico.

5.10. **Acceso remoto:** capacidad de acceder a datos, correo, información y aplicaciones desde fuera del entorno del organismo.

5.11. **Teletrabajo:** trabajo que se realiza desde fuera de las oficinas del organismo, mediante sistemas de telecomunicación.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que la gestión de los procedimientos relacionados con el control de acceso a los sistemas de información se realice en cumplimiento con los lineamientos de seguridad establecidos en esta política.

6.3. **Oficial de Seguridad de la Información (OSI):** asegurar la adecuada implementación y cumplimiento de los controles de acceso establecidos, verificando que estos se apliquen correctamente conforme a los lineamientos en esta política.

7. Lineamientos.

7.1. Generalidades.

7.1.1. El control de acceso a la información se realizará teniendo en cuenta los niveles de clasificación determinados en la norma de clasificación de la información.

7.1.2. El acceso a los activos y servicios de información serán otorgados de acuerdo con las funciones y responsabilidades de cada usuario, serán asignados con el menor privilegio y únicamente por el tiempo que sea necesario.

7.1.3. Para la habilitación de permisos y accesos de los usuarios, es necesario contemplar la segregación de funciones, evitando accesos no autorizados. Entre otros, se deben considerar los siguientes principios:

- Otorgar el acceso a la información requerida para la ejecución de las tareas asignadas.
- Otorgar el acceso a las instalaciones de procesamiento de información que necesita para la ejecución de las tareas.

7.1.4. El OSI deberá revisar los derechos de acceso asignados o en curso de todos los usuarios de los sistemas o plataformas, pudiendo recomendar cambios en los permisos y accesos de los usuarios.

7.1.5. Los derechos de acceso para usuarios privilegiados deberán ser revisados detalladamente y con una mayor frecuencia.

7.2. Acceso a las redes y servicios de red.

7.2.1. Los usuarios deben tener acceso a la red y a los servicios que han sido autorizados específicamente, lo cual debe quedar establecido en la asignación de privilegios correspondiente según sus funciones y responsabilidades.

7.2.2. Todos los accesos tanto internos como externos y desde cualquier lugar u origen, deberán ser previamente aprobados, registrados y controlados periódicamente, garantizando que no se comprometa la seguridad de la información.

7.3. ABM de usuarios,

7.3.1. Todo usuario que requiera acceder a los recursos, datos o información del organismo deberá poseer un código de usuario vinculado a la red del organismo (denominado "usuario" o "nombre de usuario"). Dicho código es personal e intransferible, siendo su propietario responsable por su uso y por toda actividad realizada con el mismo. Los códigos de usuario no deberán indicar ningún indicio del nivel de privilegio otorgado.

7.3.2. Se debe evitar la existencia de múltiples códigos de usuario para un mismo agente, en caso de excepciones deberá ser evaluado y aprobado por el OSI.

7.3.3. Para la solicitud de gestión de ABM de usuarios se deberá cumplir con los lineamientos establecidos en el procedimiento de gestión de ABM de usuarios.

7.3.4. Periódicamente se harán revisiones y auditorías identificando los usuarios redundantes y los que ya no son necesarios, con el fin de eliminarlos y/o deshabilitarlos.

7.3.5. De forma inmediata se deshabilitarán los permisos de accesos de usuarios que cambien su rol, se desvinculen del organismo o sufran la pérdida/robo de sus credenciales de acceso.

7.3.6. Los terceros que requieran un usuario para el desempeño de sus tareas deberán contar con permisos temporales; los cuales no pueden superar el tiempo máximo del contrato establecido con el organismo.

7.3.7. Debe existir una comunicación constante y efectiva entre la DGFH y la DGIYT, con el fin de tener un seguimiento controlado de las altas, bajas y modificaciones de usuarios.

7.3.8. Previamente antes de asignar o revocar un acceso a un usuario para uso de un sistema o servicio de información, se deberá contar con la autorización del superior jerárquico del usuario, siguiendo lo indicado en el procedimiento de gestión de ABM de usuarios.

7.3.9. De presentarse un cambio, traslado o modificación de un usuario, se ajustarán todos los derechos de acceso en base al nuevo rol y función de este, garantizando que se deshabilitan los permisos a los accesos anteriores.

7.3.10. Cuando se desvincule un agente que sea administrador de sistemas del organismo, se deberá modificar de forma inmediata las contraseñas de los equipos, sistemas y servicios vinculados con el mismo y se deberá informar a todos los usuarios involucrados para que no continúen compartiendo información con la persona en cuestión.

7.4. Accesos de Administrador y Superadministrador.

7.4.1. Los usuarios con permisos privilegiados para ver, eliminar o modificar registros deberán autenticarse mediante herramientas de autenticación de múltiples factores para autorizar su acceso.

7.4.2. Dado su alto riesgo, frecuentemente se limitará y controlará de forma detallada la asignación y el uso de los accesos con privilegios especiales o de administradores de cada sistema,

proceso o servicio y se identificarán las cuentas con privilegios redundantes con el fin de eliminarlas.

7.4.3. Se deberá utilizar los privilegios elevados o de administración únicamente cuando éstos representen el único medio para realizar la tarea requerida.

7.4.4. Los usuarios con acceso privilegiado deberán contar con una identificación diferente a la que utilizan habitualmente en sus actividades usuales, donde no requieren de una cuenta privilegiada.

7.5. Gestión de la información crítica para la autenticación del usuario.

7.5.1. Se debe garantizar la implementación de claves de accesos y factores de autenticación, con el fin de validar la identidad de un usuario para el acceso a las instalaciones o servicios de información.

7.5.2. Los agentes y/o terceros deberán cumplir con los lineamientos establecidos en la norma de gestión de claves seguras

7.5.3. Las claves temporales de acceso a los sistemas y servicios de información serán compartidas al usuario por medios de comunicación seguros y establecidos en el procedimiento de gestión de ABM de usuarios.

7.5.4. Se harán controles de los sistemas de información con el fin de garantizar que no se permita el uso de contraseñas débiles.

7.5.5. La información crítica para la autenticación otorgada por proveedores o fabricantes de sistemas debe ser cambiada de forma inmediata luego de cada instalación; a su vez deben ser cambiadas de forma inmediata si existe un posible indicio de compromiso del sistema o de cualquier incidente de seguridad relacionado con la clave y debe ser notificado de forma inmediata al OSI.

7.5.6. Las claves utilizadas por los usuarios deben ser robustas con el fin de evitar que sean comprometidas fácilmente. Las mismas no deben estar basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, datos generales o del organismo.

7.6. Procedimiento seguro de inicio de sesión.

7.6.1. El CISO debe establecer los mecanismos necesarios para garantizar el acceso controlado y seguro a los sistemas, aplicaciones y activos de información.

7.6.2. Se deben utilizar métodos de autenticación para cada sistema o servicio de información con el fin de validar las identidades de un usuario durante el proceso de inicio de sesión.

7.6.3. Los mecanismos de acceso a los activos de información deben ser sometidos a pruebas periódicas de seguridad, con el propósito de identificar y gestionar los riesgos y vulnerabilidades.

7.6.4. Todo inicio se sesión quedará registrado en los logs de cada sistema o aplicación del organismo.

7.7. Sistema de gestión de contraseña.

7.7.1. Las contraseñas asignadas a una nueva cuenta de usuario deben ser creadas de forma provisoria y el usuario tiene la obligación de cambiarla durante su primer inicio de sesión.

7.7.2. Está prohibido que los usuarios de los sistemas compartan sus contraseñas, las actividades que se ejecuten con ese usuario son entera responsabilidad del dueño o responsable de la cuenta de usuario.

7.7.3. En aquellos casos en que el usuario olvide su contraseña o ésta se encuentre bloqueada, debe solicitar el reemplazo o desbloqueo según sea el caso a través de Mesa de Ayuda.

7.8. Uso de utilitarios con privilegios.

7.8.1. Se debe restringir y controlar el uso de los programas utilitarios que poseen la capacidad de sobrepasar, anular o evitar los controles de acceso a los sistemas y aplicaciones.

7.8.2. Los programas utilitarios deben estar documentados y separados de las aplicaciones del sistema.

7.9. Control de acceso al código fuente de los programas.

7.9.1. El acceso al código fuente debe ser restringido y controlado con el fin de prevenir la introducción de funcionalidades no autorizadas y evitar cambios no intencionales.

7.9.2. Los cambios realizados deben estar sujetos a los procedimientos estrictos de control de cambios y se debe mantener un registro de todas las actividades.

7.10. Acceso remoto.

7.10.1. Se debe garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información del organismo, tanto para agentes o terceros autorizados a trabajar en esta modalidad, y definir las condiciones y restricciones del teletrabajo. Para ello, es necesario el cumplimiento de las siguientes directrices:

- Definir una lista de servicios, redes y sistemas de información que pueden ser accedidos remotamente por un personal autorizado.
- Contar con un inventario de accesos remotos otorgados, identificando al usuario que cuenta con el acceso, el motivo por el cual se le otorgó y el plazo por el cual está autorizado.
- Se debe contar con una lista de equipos desde los cuales se puede acceder remotamente.
- Se debe utilizar comunicaciones seguras para el acceso remoto.
- Los equipos utilizados para el acceso remoto deben contar con protección ante software malicioso y estar encriptados con algún mecanismo robusto.
- Se deben definir los procedimientos y protocolos para la realización de teletrabajo, así como los contactos con soporte técnico para resolución de problemas.

- Se debe definir un procedimiento de revisión periódica de las condiciones de uso del acceso remoto y de los usuarios que hacen uso de éste, que contemple la revisión de los puntos anteriores.

RES. CM Nº 141/2026 - ANEXO X

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Seguridad Física y del Entorno

DGIYT-GOYT-PL-010

Seguridad Física y del Entorno

Contenido

1. Seguridad Física y del Entorno

2. Objetivo.

Establecer los lineamientos para proteger los activos de información y la infraestructura tecnológica mediante controles de seguridad físicos, reduciendo el riesgo de accesos no autorizados, daños y pérdidas.

3. Alcance.

Esta política aplica tanto 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 o accedan a las áreas donde se encuentre información clasificada como privada, confidencial o secreta. La no inclusión explícita en el presente documento no constituye argumento para no proteger los activos de información.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-004** - Cumplimiento de la Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-006** - Seguridad de los Recursos Humanos.

4.6. **DGIYT-GOYT-PL-007** - Gestión de Activos.

4.7. **DGIYT-GOYT-PL-009 -** Control de Accesos.

4.8. **DGIYT-GOYT-PL-013 -** Aspectos de Seguridad para Gestión de la Continuidad de los Sistemas de Información.

4.9. **DGIYT-GOYT-PL-014** - Seguridad de las Operaciones.

5. Definiciones.

5.1. **DGIYT**: Dirección General de Informática y Tecnología.

5.2. **Seguridad perimetral:** corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en áreas seguras.

5.3. **Áreas seguras:** áreas donde se almacene o procese información.

5.4. **Equipos de UPS / Grupos electrógenos:** fuente de energía eléctrica que permite brindar servicio alternativo por el tiempo que exista un corte de luz o un problema eléctrico en la infraestructura.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de Seguridad de la Información (CISO):** garantizar que la gestión de los procedimientos relacionados con el control de acceso físico se realice en cumplimiento con los lineamientos de seguridad establecidos en esta política.

6.3. **Oficial de Seguridad de la Información (OSI):** asegurar la adecuada implementación y cumplimiento de los controles de acceso físico establecidos, verificando que estos se apliquen correctamente conforme a los lineamientos en esta política.

6.4. **Director de Seguridad:** gestionar e implementar, de corresponder, los controles de seguridad física detallados en la presente política.

6.5. **Jefe del Departamento de Planificación e Infraestructura (PEI):** asegurar y proporcionar las condiciones físicas y ambientales óptimas en los centros de cómputo, con el propósito de proteger los activos de información, garantizando su integridad, disponibilidad y confidencialidad.

7. Lineamientos.

7.1. Perímetro de seguridad física

7.1.1. La Dirección de Seguridad debe garantizar que los perímetros de seguridad del edifico y de los sitios que contengan las instalaciones de procesamiento de información estén adecuadamente protegidos.

7.1.2. El perímetro de seguridad de las instalaciones de procedimientos de información del organismo debe ser físicamente seguro, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción.

7.1.3. Todo aquel que acceda a las áreas seguras, deberá asegurarse de que las puertas y ventanas de éstas se encuentren cerradas con llave al momento de finalizar sus actividades.

7.1.4. El organismo debe contar con un área de recepción atendida por personas u otros medios de control de acceso físico, tener vigilancia mediante Circuito Cerrado de Televisión (CCTV) y ser monitoreado por el personal de vigilancia, se debe tener en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de las áreas seguras.

7.1.5. Todas las puertas de emergencia deben estar señalizadas, tener alarma y deben cumplir lineamientos de acuerdo con las normas legales vigentes y pertinentes en cuanto a la seguridad del personal.

7.1.6. Se recomienda que se cuente con sistemas adecuados de detección de intrusos, los mismos deben ser probadas periódicamente para garantizar su funcionamiento y protección de los sitios donde se almacene o procese información.

7.1.7. Se recomienda que las instalaciones de procesamiento de información gestionadas por terceras partes sean separadas de las instalaciones gestionadas por el organismo.

7.2. Control de acceso físico.

7.2.1. El acceso a los sitios que contengan instalaciones de procesamiento de información debe ser protegido por mecanismos que garanticen la entrada exclusivamente al personal autorizado, por ejemplo: mecanismos de autenticación de dos factores tales como tarjetas de acceso, números de identificación (PIN), entre otros. Complementando con los lineamientos establecidos en la política **DGIYT-GOYT-PL-009 -** Control de Accesos.

7.2.2. Se debe deshabilitar o modificar de forma inmediata, los privilegios de acceso físico a las instalaciones de procesamiento de información, en los casos de desvinculación o ausencia transitoria, de acuerdo con la política de **DGIYT-GOYT-PL-006** - Seguridad de los Recursos Humanos.

7.2.3. Se debe contar con el registro de todos los accesos a las áreas seguras que permitan la trazabilidad para casos de auditorías.

7.2.4. Todos los agentes que ingresen al centro de cómputos y centros de cableado deberán cumplir con los lineamientos del procedimiento de gestión de acceso físico o cuando se trate de personal externo no vinculado al organismo deberán estar acompañado por personal

autorizado, el cual se hará responsable de la estadía del personal ajeno durante el tiempo que permanezca en las instalaciones.

7.2.5. Se recomienda establecer mecanismos para asegurar que, en la entrada y salida de personas, no se genere un riesgo en la disponibilidad, integridad y confidencialidad de los activos de información.

7.2.6. El ingreso de equipos pertenecientes a las áreas seguras debe contar con autorización expresa, ser debidamente registrado y se debe llevar a cabo de acuerdo con lo establecido en el procedimiento de gestión de activos.

7.3. Seguridad de las oficinas, recintos e instalaciones.

7.3.1. Se debe proteger toda información, independientemente del medio en que se encuentre, bajo controles de seguridad e instalaciones adecuadas para evitar el acceso no autorizado.

7.3.2. Los responsables del acceso a las áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen del organismo deben asegurar que no se tomen fotografías o grabaciones de videos, a menos que esté expresamente autorizado. El incumplimiento podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normas vigentes.

7.3.3. El organismo debe garantizar que las instalaciones estén diseñadas o configuradas para evitar que sean visibles y/o audibles desde el exterior.

7.3.4. Se deben supervisar las actividades de limpieza en las áreas seguras, especialmente: centro de datos y centros de cableado, brindando orientación al personal de limpieza acerca de las precauciones mínimas a seguir durante el proceso de limpieza.

7.4. Protección contra amenazas externas y del entorno.

7.4.1. El organismo debe asegurar las condiciones físicas y medioambientales necesarias como: sistemas de control ambiental de temperatura/humedad, de detección y extinción de incendios, de descarga eléctrica y de vigilancia, entre otros, para asegurar la protección y correcta operación de los centros de cómputos. Estos sistemas se deben monitorear de manera permanente.

7.4.2. El CISO debe diseñar e implementar planes de acción frente a desastres naturales, ataques intencionales o accidentales.

7.4.3. Se debe garantizar que el centro de cómputo o de cableado, se encuentre separado de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios y mantenerlos libres de objetos o elementos que no sean propios de la operación.

7.4.4. En caso de desastres naturales o contingencias, se deberá cumplir con los procedimientos establecidos por la DGIYT.

7.5. Trabajo en áreas seguras.

7.5.1. Para contribuir con la seguridad en un área, se recomienda cumplir, entre otros, los siguientes lineamientos:

- Los visitantes deberían estar acompañados y/o previamente autorizados por un representante del organismo.
- El ingreso de equipos de fotografía, videos, audios o equipamientos de grabación deberían ser previamente autorizados.
- Los agentes y/o terceros al finalizar su horario laboral deberían asegurar no dejar a la vista información del organismo con un nivel de clasificación, secreto, privado o confidencial.

7.6. Área de carga y descarga.

7.6.1. Se recomienda que las áreas de cargas y descargas se encuentren alejadas de las áreas donde se almacenen o procese información del organismo, con el fin de evitar riesgos en la disponibilidad, integridad y confidencialidad de ésta.

7.6.2. Los activos de información asignados a la custodia de la DGIYT deben ser registrados y gestionados de acuerdo con el procedimiento de gestión de activos.

7.7. Ubicación y protección de equipos.

7.7.1. Los equipamientos deben ubicarse de manera que no obstruyan el acceso a otras áreas y que minimicen el riesgo de exposición de la información a personas no autorizadas durante su uso.

7.7.2. De observarse algún incidente donde se genere un riesgo a la disponibilidad, integridad y confidencialidad de los activos de información, el mismo debe ser informado de acuerdo con el instructivo de cómo informar un incidente de seguridad de la información. De lo contrario se generarán sanciones disciplinarias según lo establecido en la política **DGIYT-GOYT-PL-004 -** Cumplimiento de la Seguridad de la Información.

7.7.3. Se debe implementar protección contra rayos en todos los edificios y adaptar filtros de protección contra éstos en todas las líneas de comunicaciones externas.

7.8. Elementos de soportes.

7.8.1. Se deben instalar sistemas de protección eléctrica para asegurar los equipos, el centro de cómputo y comunicaciones contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos.

7.8.2. Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.

7.8.3. Se debe asegurar la operación permanente de los servidores alojados en los centros de cómputos, de igual forma proteger la información almacenada en los sistemas de almacenamiento, para que esté segura y disponible.

7.8.4. Los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento del centro de cómputos, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.

7.8.5. El organismo debe disponer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

7.9. Seguridad del cableado.

7.9.1. El cableado de energía y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interferencias o daños.

7.9.2. Los cables de energía y los cables de comunicaciones deben instalarse por separado para evitar interferencias y garantizar la seguridad y eficiencia de los sistemas eléctricos y de telecomunicaciones.

7.9.3. Se debe asegurar que los centros de cableado y/o cuarto eléctrico cumplan con las condiciones físicas y medioambientales establecidas en las políticas del organismo y en las normativas de seguridad vigentes.

7.9.4. La instalación y mantenimiento de los cables de energía y líneas de telecomunicaciones, debe ser realizada por personal capacitado y autorizados que sigan los estándares de calidad y seguridad.

7.10. Mantenimiento del equipamiento.

7.10.1. Los equipos de cómputo y comunicaciones deben seguir programas de mantenimiento adecuados con el objeto de garantizar su disponibilidad e integridad continua.

7.10.2. Se debe asegurar que las labores de mantenimiento y cambios en las áreas seguras sean realizadas por personal idóneo y autorizado previamente.

7.10.3. Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo realizado a los equipamientos.

7.10.4. En el mantenimiento de equipos se considerará, entre otros:

- Elaborar planes de mantenimiento de acuerdo con las especificaciones del proveedor y/o las definidas por el organismo.
- Validar que la información sensible se encuentre debidamente respaldada previo a la realización de mantenimientos.

7.11. Retiro de activos.

7.11.1. El retiro de equipos o soportes de información debe ser autorizado formalmente, registrado y llevado a cabo según el procedimiento de gestión de activos.

7.11.2. Se debe asegurar la implementación de controles de seguridad para detectar y prevenir retiros no autorizados de activos de información.

7.11.3. El retiro de equipos debe ser realizado por personal autorizado y capacitado, garantizando que el procedimiento no genere riesgos para los demás equipos presentes en el área.

7.12. Seguridad del equipamiento y de los activos fuera del organismo.

7.12.1. Los activos de información deben ser correctamente utilizados de modo de asegurar la continuidad, disponibilidad e integridad de este, cumpliendo con lo establecido en la norma de uso aceptable de los activos y recursos informáticos.

7.12.2. Se debe informar inmediatamente los casos de pérdida o robo de activos de información, siguiendo lo establecido en el instructivo de cómo informar incidente de seguridad de la información.

7.13. Baja operativa segura o reutilización del equipamiento.

7.13.1. Cuando un activo sea reasignado o dado de baja, debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar una recuperación no autorizada de la misma.

7.13.2. Al momento de reasignar o dar de baja un activo de información, se deberá evaluar la necesidad de realizar una copia de respaldo de la información que se encuentra almacenada en el mismo.

RES. CM Nº 141/2026- ANEXO XI

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de las Comunicaciones

DGIYT-GOYT-PL-011

Seguridad de las Comunicaciones

Contenido

1. Seguridad de las Comunicaciones

2. Objetivo.

Establecer los lineamientos para proteger la información que se transmite a través de redes y sistemas asegurando que las comunicaciones sean confidenciales, integras y accesibles solo para las partes autorizadas.

3. Alcance.

Esta política aplica tanto 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, los cuales gestionen las redes e infraestructuras de éste.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-004** - Cumplimiento de Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-006 -** Seguridad de los Recursos Humanos.

4.6. **DGIYT-GOYT-PL-009** - Control de Accesos.

5. Definiciones.

5.1. **DGIYT**: Dirección General de Informática y Tecnología.

5.2. **Perímetro de la red:** límite entre la red interna segura del organismo e Internet, o cualquier otra red externa no controlada.

5.3. **Red pública:** sistema de comunicación distribuida que está libremente disponible para uso público. Esta red se construye utilizando protocolos de comunicación estandarizados, lo que permite a los dispositivos conectarse y compartir información entre ellos. Las redes públicas permiten a los usuarios acceder a recursos digitales, comunicarse entre sí y compartir contenido.

5.4. **Red privada:** sistema de comunicación distribuida que solo está disponible para los miembros autorizados dentro de un entorno particular. Estas redes normalmente están cerradas al exterior y son administradas por el propietario de esta. Los usuarios tienen control completo sobre la infraestructura y los datos que pasan a través de ella, lo que les da mayor seguridad y privacidad.

5.5. **Seguridad de la información:** es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información de los diferentes riesgos a los que puede estar expuesta, con el fin de minimizar el daño y garantizar la continuidad operacional.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de Seguridad de la Información (CISO):** garantizar que la gestión de los procedimientos relacionados a la seguridad de las comunicaciones se realice en cumplimiento con los lineamientos de seguridad establecidos en esta política.

6.3. **Jefe del Departamento de Arquitectura Tecnológica (AT):** implementar los controles de seguridad en la configuración y monitoreo de las redes y los servicios de red del organismo.

6.4. **Oficial de Seguridad de la Información (OSI):** asegurar la adecuada implementación y cumplimiento de la seguridad de las comunicaciones, verificando que se apliquen correctamente conforme a los lineamientos establecidos en esta política.

7. Lineamientos.

7.1. Generalidades.

7.1.1. El departamento de AT garantizará que todos los agentes del organismo y terceros tengan sus cuentas de red debidamente configuradas para acceder a los distintos servicios de red, de acuerdo con su perfil (cargo) y funciones.

7.1.2. Se deberán definir los procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el responsable de la unidad organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

7.1.3. Las solicitudes de permisos especiales o adicionales para utilizar redes o servicios de red deben ser realizadas y regirse por los lineamientos establecido en la política de **DGIYT-GOYT-PL-009-** Control de Accesos.

7.1.4. El acceso a las redes debe ser utilizado con propósitos autorizados o con el destino por el cual fue provisto.

7.1.5. El organismo se reserva el derecho de bloquear el acceso a ciertos sitios de web que no estén relacionadas con funciones propias de mismo.

7.1.6. Se generarán registros de los accesos de los usuarios a las redes, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Para ello, el CISO junto con el AT, analizará las medidas a ser implementadas para hacer efectivo dicho control.

7.2. Controles de red.

7.2.1. Se establecerán e implementarán controles con el fin de garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra accesos no autorizados.

7.2.2. Se garantizará la implementación de los controles a las aplicaciones que procesen información clasificada, aplicaciones críticas o a usuarios que utilicen el acceso desde sitios de alto riesgo, con el fin de identificar las acciones que puedan afectar la confidencialidad

y la integridad de los datos que se transmiten y para la protección de los sistemas y aplicaciones conectadas.

7.2.3. Se recomienda que los accesos externos se realicen a través de redes privadas virtuales y deben ser registradas.

7.2.4. Se recomiendan que para las redes inalámbricas (WIFI), deben cumplir con las siguientes configuraciones:

- Dos nombres de acceso, una para los usuarios del organismo y otra para visitas.
- Permisos restringidos y temporales para las visitas o terceros que solicitan conectarse a la red del organismo.

7.2.5. Se deberán evaluar los riesgos e implementar todos los controles necesarios antes de permitir conexiones de redes internas con terceros. Así mismo se deberán implementar controles de seguridad de la información, para asegurar que las redes externas autorizadas sólo tienen acceso a los sistemas o servicios permitidos y que sean activadas solo cuando es necesario.

7.2.6. La gestión de accesos para los usuarios deberá comprender lo establecido en el procedimiento de gestión de ABM de usuarios.

7.2.7. De forma periódica se realizarán evaluaciones o análisis de vulnerabilidades en todas las redes internas y se implementarán controles sobre las debilidades detectadas que pongan en riesgo la disponibilidad, confidencialidad y/o integridad de la información que circula en ellas.

7.3. Seguridad en los servicios de red.

7.3.1. Se controlará el uso de los servicios de red y la información enviada o recibida de los sistemas utilizados, a fin de reducir los riesgos asociados.

7.3.2. Las pautas para garantizar la seguridad de los servicios de red tanto públicos como privados, deben ser definidas y para ello se tendrá en cuenta, entre otras, las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

7.3.3. Todos los dispositivos de comunicaciones sean físicos o virtuales deben contar con características de auditoría para monitorear su funcionamiento y efectuar investigaciones en cuanto a violaciones detectadas o potenciales de las políticas de seguridad de la red.

7.3.4. En lo servicios expuestos se deberán implementar soluciones que detecten, alerten y prevengan ataques del tipo DoS/DDoS y/o abusos; el OSI deberá orientar las implementaciones para responder a detecciones conocidas, así como también aquellas que surjan del análisis por comportamiento anómalo.

7.4. Segregación de redes.

7.4.1. Con el fin de restringir el acceso indebido a los datos, se deberá segregar el tráfico de datos que circulan por las redes del organismo y se hará en base a la función que tengan las aplicaciones que residan en dicho segmento.

7.4.2. Para controlar la seguridad en redes extensas, se recomienda segmentar en dominios de red separados, para esto, se definirán y documentarán los perímetros de seguridad que sean convenientes.

7.4.3. Se recomienda que las redes sean segmentadas por dispositivos físicos o lógicos, el punto de interconexión estará particularmente asegurado, mantenido y monitorizado.

7.5. Seguridad en los perímetros de red.

7.5.1. Se deberá garantizar el uso de herramientas de seguridad de red para monitorear y controlar el tráfico de entrada y salida entre diferentes redes, con el fin de:

- Establecer reglas de filtro y navegación para los usuarios internos.
- Permitir configurar publicaciones de servicios internos hacia internet en forma segura.
- Filtrar correos (Antispam) y bloquear mensajes no deseados en tiempo real.
- Filtrar navegaciones y restringir accesos WEB de usuarios, de acuerdo con el contenido de los sitios y proteger contra sitios maliciosos.
- Filtrar virus, revisión de tráfico WEB y email de protección perimetral contra malware, entre otros.
- Servicio de conectividad remota segura a través de VPN.
- Integrar con Active Directory, para controlar y agrupar por tipo los diferentes niveles de acceso a internet por parte de los usuarios.

7.5.2. Por otra parte, se gestionarán a través de recursos propios o de terceros, las siguientes tareas en orden de mantener la seguridad perimetral en permanente operación:

- Resumen de incidentes y requerimientos por mes.
- Principales eventos de seguridad detectados, criticidad, origen de estos y recomendaciones.
- Análisis de actualizaciones y parches para la plataforma administrada.
- Monitoreo y reportes de actualizaciones generales de componentes.
- Registro de conexiones denegadas.
- Registro y reportes de bloqueo de sitios web no autorizados.
- Registro y reportes de sitios web más visitados.
- Registro y reportes de ranking de los usuarios con mayor actividad.
- Registro y reportes de eventos ocurridos en el firewall.

7.6. Transferencia de información.

7.6.1. El CISO garantizará procedimientos y controles con el fin de proteger la transferencia de información a través de cualquier medio de comunicación.

7.6.2. Para el uso aceptable de la transferencia de información se deberá cumplir los lineamientos establecidos en las normas vigentes de uso aceptable de los activos y recursos informáticos y de clasificación de la información.

7.6.3. En los controles para la transferencia de información se tendrá en cuenta, entre otros, los siguientes aspectos:

- Protección a la información transferida de actos no autorizados de intercepción, copia, modificación, ruteo incorrecto y destrucción.
- Protección y detección de códigos maliciosos.
- Restricciones y uso aceptable de las instalaciones de comunicaciones.
- Técnicas criptográficas para transacciones que lo ameriten.

7.6.4. Se debe informar en el registro de incidentes de seguridad cualquier detección de falla, uso o acceso malintencionado de información. El incumplimiento podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normas vigentes.

7.6.5. El uso aceptable de los activos deberá ser informado a todo el personal y terceros del organismo según lo establecido en la política **de DGIYT-GOYT-PL-006 -** Seguridad de los Recursos Humanos.

7.7. Regulaciones por correo electrónico.

7.7.1. El correo electrónico tendrá un estándar de capacidad limitada de espacio de almacenamiento para cada usuario de correo. Las excepciones deben ser solicitadas a través de mesa de ayuda y deben ser evaluadas según las políticas y procedimientos del organismo.

7.7.2. En caso de que la comunicación lo amerite, por su contenido o por el cargo de los participantes, el correo electrónico debiese generarse firmado digitalmente y/o cifrado.

7.7.3. El organismo debe concientizar, capacitar y gestionar a los agentes que sean moderadores de difusión de correos masivos en las diferentes listas de correo electrónico del Poder Judicial de la CABA, con el fin de evitar la transmisión de información que pueda poner en riesgo la confidencialidad, disponibilidad e integridad de la información.

7.7.4. Se recomienda que, en los controles de seguridad de la información para la mensajería electrónica, se tome en cuenta, los siguientes aspectos:

- Protección de mensajes contra accesos y modificaciones no autorizadas.
- Controles de autenticación para los accesos desde redes accesibles al público.

7.7.5. El envío y recepción de archivos ejecutables estarán restringidos y serán bloqueados durante el proceso de transmisión en el servidor de correo electrónico.

7.7.6. Todo mensaje recibido que no pueda ser entregado a su destinatario, debe ser devuelto a su remitente, garantizando la notificación correspondiente.

7.7.7. Se debe hacer uso de la mensajería electrónica propiedad del organismo exclusivamente para actividades de trabajo relacionadas a sus funciones, entre otros, se prohibirá el uso a las siguientes actividades:

- Distribución y explotación de información confidencial del organismo sin previo consentimiento o autorización y dependerá del nivel de clasificación de la información.
- Actividades ilícitas.
- Fin de lucro ajeno al organismo.
- Acoso y con fines racistas.
- Fines personales.
- Entretenimiento.
- Envío de propaganda.
- Contenido sexual explícito.

RES. CM Nº 141/2026 - ANEXO XII

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

DGIYT-GOYT-PL-012

Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Contenido

1. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

2. Objetivo.

Establecer los lineamientos generales para garantizar que la seguridad de la información se integre en el proceso de adquisición, desarrollo y mantenimiento de los sistemas de información, considerando el tratamiento de los riesgos y la implementación de controles de seguridad.

3. Alcance.

Esta política aplica tanto 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 participen en los procesos de adquisición, desarrollo y mantenimiento de los sistemas de información.

4. Documentos relacionados.

4.1. **Ley Nacional N° 11.723** - Régimen Legal de la Propiedad Intelectual.

4.2. **Ley Nacional N° 25.326** - Protección de Datos Personales.

4.3. **Ley N° 1.845** - Protección de Datos Personales.

4.4. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.5. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.6. Código de Buenas Prácticas en el Desarrollo de Software Público de la ONTI.

4.7. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.8. **DGIYT-GOYT-PL-004** - Cumplimiento de Seguridad de la Información.

4.9. **DGIYT-GOYT-PL-007 -** Gestión de Activos.

4.10. **DGIYT-GOYT-PL-008 -** Seguridad Criptográfica.

5. Definiciones.

5.1. **Desarrollo seguro:** requisito para generar un servicio en: arquitectura, software y sistema seguro, desde la perspectiva del resguardo de la información.

5.2. **Software crítico:** aquellos componentes de software desarrollados interna o externamente, que son activos sensibles del organismo.

5.3. **Paquetes de software:** conjunto de aplicaciones informáticas diferentes pero relacionadas entre sí que se distribuyen de forma conjunta.

5.4. **Red pública:** sistema de comunicación distribuida que está libremente disponible para uso público. Esta red se construye utilizando protocolos de comunicación estandarizados, lo que permite a los dispositivos conectarse y compartir información entre ellos. Las redes públicas permiten a los usuarios acceder a recursos digitales, comunicarse entre sí y compartir contenido.

5.5. **Red privada:** sistema de comunicación distribuida que solo está disponible para los miembros autorizados dentro de un entorno particular. Estas redes normalmente están cerradas al exterior y son administradas por el propietario de esta. Los usuarios tienen control completo sobre la

infraestructura y los datos que pasan a través de ella, lo que les da mayor seguridad y privacidad.

5.6. **DGIYT**: Dirección General de Informática y Tecnología.

5.7. **AT:** Arquitectura Tecnológica.

5.8. **APP:** Aplicaciones.

5.9. **GOYT:** Gestión Operativa y Tecnológica.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que la gestión de los procedimientos relacionados con los sistemas de información se realice en cumplimiento con los lineamientos de seguridad establecidos en esta política.

6.3. **Oficial de seguridad de la información (OSI):** asegurar la adecuada implementación y cumplimiento de los controles para identificar y evaluar las vulnerabilidades de seguridad en los sistemas de información, verificando que estos se apliquen correctamente conforme a los lineamientos en esta política.

6.4. **Jefes de departamento de AT/APP/GOYT**: implementar los controles establecidos en esta política según corresponda, de acuerdo con las funciones de cada departamento.

7. Lineamientos.

7.1. Análisis y especificación de requisitos de seguridad de la información.

7.1.1. El CISO deberá garantizar que los requisitos para la seguridad de la información sean incluidos en la fase de planificación para sistemas de información, teniendo en cuenta la seguridad y las funcionalidades requeridas por una aplicación o sistema antes de su fase de desarrollo.

7.1.2. En los requisitos de seguridad de la información para sistemas nuevos, existentes, propios o de terceros, se deberán contemplar que se realicen análisis de los niveles de riesgo, de la criticidad, además del nivel de protección, los controles de seguridad que requieren los datos y las aplicaciones que lo compongan.

7.2. Seguridad de los servicios de aplicaciones en redes públicas.

7.2.1. Toda la información implicada en los servicios de aplicaciones que circulen por redes públicas debe estar protegida contra actividades fraudulentas, divulgación y modificación no autorizada.

7.2.2. Los sistemas con acceso público deben ser monitoreados y probados contra fallas, eventos y vulnerabilidades, antes que la información sea publicada.

7.2.3. En los controles de seguridad de la información para los servicios de aplicaciones sobre redes públicas, se debe tener en cuenta los siguientes aspectos:

- Método de autenticación seguro (criptografía de clave pública, firmas digitales, entre otros).
- Requisitos de protección frente a ataques (denegación de servicio "DoS", entre otros).
- Acuerdos entre partes (terceros) sustentados en documentación.
- Se deben implementar algoritmos y protocolos necesarios para brindar una comunicación segura.
- Realizar como mínimo una vez al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados o cuando se realice un cambio en el sistema.
- Cada sistema de información debe cumplir con tiempos máximos de inactividad, debiendo solicitar un nuevo proceso de autenticación para ingresar.
- Todos los escaneos de vulnerabilidades y pruebas de penetración deben ser ejecutadas por la persona autorizada para realizar dicha actividad.

7.2.4. Las amenazas encontradas mediante evaluaciones, controles y monitoreos deben ser analizadas y documentadas para el registro interno del organismo.

7.2.5. De presentarse algún incidente de seguridad, se deberá cumplir con lo establecido en el instructivo de cómo informar un incidente de seguridad de la información. El incumplimiento de esto podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normas vigentes.

7.2.6. La integridad de la información disponible en un sistema con acceso público debe protegerse de modificaciones no autorizadas. Se tendrá en cuenta lo siguiente, pero sin limitarse a ello:

- Los sitios web del organismo serán desarrollados y mantenidos por personal debidamente calificado y autorizado.
- Todos los cambios en el sitio web deben documentarse y procesarse a través de la norma de gestión de cambios.

7.3. Protección de las transacciones.

7.3.1. Toda la información implicada en las transacciones en línea estará protegida para evitar transmisión incompleta, el enrutamiento erróneo, la divulgación de la información, la alteración de los datos, duplicación o reproducción no autorizada de mensajes.

7.3.2. Para todas las transacciones, las partes deberán tener en cuenta lo siguiente:

- Verificación de una autenticación segura.
- Cifrado de la ruta de comunicación.
- Preservación de la privacidad de los datos.
- Confidencialidad de las transacciones.

7.4. Procedimiento de control de cambios.

7.4.1. Se deberá controlar y documentar los cambios a los sistemas dentro del ciclo de vida de desarrollo garantizando que estén debidamente justificados, autorizados y documentados.

7.4.2. Al presentarse un cambio, se deberá controlar el mismo, realizando una evaluación de riesgos, un análisis de impacto y una especificación de controles de seguridad, con el fin de garantizar la integridad de los sistemas.

7.4.3. En el análisis de impacto se debe considerar pruebas y revisiones de sistemas críticos ya instalados, con el fin de asegurar su adecuada operación y garantizando que la seguridad y los procesos de controles existentes no se ponen en peligro.

7.4.4. Se deberá considerar los riesgos de integridad y disponibilidad del sistema y evitar el uso de actualizaciones automáticas sobre sistemas críticos.

7.5. Revisión técnica de las aplicaciones tras los cambios de los sistemas operativos.

7.5.1. Las versiones nuevas o diferentes a los sistemas operativos deberán ser registradas debidamente de acuerdo en lo establecido en la norma de gestión de cambios.

7.5.2. Antes de efectuar algún cambio en los sistemas operativos, se deberá notificar previamente a las partes involucradas con el fin de poder realizar pruebas y revisiones apropiadas antes de la implementación.

7.6. Restricciones a los cambios en los paquetes de software.

7.6.1. Las modificaciones de los paquetes de software se controlarán estrictamente antes de su implementación.

7.6.2. Se recomienda que los paquetes de software suministrados por proveedores deben ser utilizados sin modificaciones, con el fin de minimizar la posibilidad de generar incidentes.

7.6.3. De generarse la necesidad de un cambio, se conservará el software original y los cambios serán aplicados a una copia designada.

7.6.4. Todos los cambios o instalaciones de un nuevo software deberán ser probados en un entorno de prueba seguro, el cual debe estar totalmente separado del entorno de producción.

7.6.5. Se implantará un proceso de gestión de parches de software para garantizar que los parches se encuentran aprobados y actualizados.

7.7. Requisitos de seguridad en el desarrollo de sistemas.

7.7.1. El OSI definirá y documentará los requisitos de seguridad para todas las capas de diseño de la arquitectura, dichos requisitos serán revisados y actualizados periódicamente con el fin de contrarrestar cualquier amenaza.

7.7.2. Los principios de seguridad en el desarrollo de los sistemas provistos por terceros deberán ser aplicados mediante contratos u otros acuerdos legales.

7.7.3. Se aplicarán técnicas de seguridad como controles de validación adecuados, para las aplicaciones que poseen interfaces de entrada y salida de datos, con el fin de:

- Validar los datos de entrada y salida.
- Detectar la corrupción de la información, tanto si se debe a errores de procesamiento como a actos deliberados.
- Validar el tratamiento correcto y adecuado de la información almacenada.

7.7.4. Se deberá definir y documentar las responsabilidades de todo el equipo técnico, desarrolladores, analistas de sistemas, diseñadores de sistemas y de todos los implicados en los procesos de entrada y salida de datos en los proyectos.

7.7.5. Se recomienda que los desarrolladores estén capacitados con el fin de que tengan el conocimiento adecuado acerca de las prácticas seguras de programación para que pueda evitar, encontrar y resolver las vulnerabilidades en los desarrollos de software y sistemas.

7.7.6. La información generada en los sistemas deberá ser clasificada según la norma de clasificación de la información.

7.7.7. Todo activo de información debe tener asociado un propietario, que le asigne un valor apropiado a su sensibilidad e importancia y que garantice la protección efectiva de dicho activo de acuerdo con los riesgos que lo afectan. El propietario de los activos de información puede delegar en un custodio la responsabilidad de administrar, usar y proteger el mismo. Sin embargo, la responsabilidad del activo de información siempre permanece con el propietario.

7.7.8. Los datos personales gestionados en los sistemas de información deben protegerse considerando lo establecido en la Ley Nacional N° 25.326 - Protección de Datos Personales y la Ley N° 1.845 - Protección de Datos Personales.

7.7.9. Los servicios que deben operar con alta disponibilidad deben ser identificados y periódicamente se les implementarán controles de seguridad, con el fin de identificar las acciones que puedan afectarlos, garantizando así, la continuidad de los servicios incluso en situaciones de deficiencia.

7.7.10. Periódicamente se harán copias de resguardo y pruebas de recuperación de datos de acuerdo con los lineamientos del procedimiento de administración de copias de resguardo y de recuperación de datos.

7.7.11. Se debe garantizar la implementación de controles apropiados relacionados con los derechos de propiedad intelectual y el uso de productos de software propios. Ley Nacional N° 11.723 - Régimen Legal de la Propiedad Intelectual.

7.7.12. Se deben realizar auditorías a intervalos regulares sobre los sistemas e información crítica, que permitan detectar deficiencias y vulnerabilidades asegurando el buen funcionamiento de éstas.

7.8. Entorno de desarrollo seguro.

7.8.1. La DGIYT establecerá y garantizará la protección de un entorno de desarrollo seguro (que incluya personas, procesos y tecnología) como parte de los requisitos del ciclo de vida de desarrollo de los sistemas. Los requisitos abarcarán entre otros, los siguientes aspectos:

- Sensibilidad de los datos a procesar, almacenar e intercambiar por el sistema.

- Aplicabilidad de políticas internas y normativas externas. Código de Buenas prácticas en el desarrollo de software público de la ONTI.
- Aplicación de las medidas de seguridad.
- Segregación entre los distintos entornos de desarrollo.
- Control de acceso al entorno de desarrollo y métodos de autenticación.
- Control de cambios.
- Copias de resguardo.
- Transferencia de datos desde y hacia el entorno de desarrollo.

7.8.2. Los niveles de protección deben ser notificados y proporcionados a todas las personas que lo necesiten.

7.8.3. Se recomienda que en el caso de los desarrollos internos se consideren los siguientes ambientes:

- Ambiente de Desarrollo.
- Ambiente de Pruebas.
- Ambiente Pre-Producción.
- Ambiente Producción.

7.9. Desarrollo tercerizado.

7.9.1. Se deberá supervisar las actividades de desarrollo de los sistemas provistos por terceras partes, con el fin de garantizar el cumplimiento de lo establecido en los contratos de servicios.

7.9.2. Se recomienda para el caso de los desarrollos tercerizados, para la transferencia de software se considere lo siguiente:

- Ambiente de Desarrollo.
- Ambiente de Pruebas.
- Ambiente Pre-Producción.
- Ambiente Producción.

7.9.3. Los aspectos para evaluar cuando el desarrollo es llevado a cabo por un tercero incluirán, entre otros, lo siguiente:

- Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual.
- Cumplimiento de una metodología aceptable de desarrollo y mantenimiento de sistemas.
- Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba.
- Controles de prueba de seguridad de aplicaciones.
- Evaluación de vulnerabilidad y tratamiento.

7.10. Pruebas de seguridad del sistema.

7.10.1. Los sistemas nuevos de información y actualizaciones se someterán a pruebas y verificaciones de seguridad durante su fase de desarrollo, donde se probarán las características y funciones de seguridad teniendo en cuenta los siguientes aspectos:

- Métodos de control de acceso y autenticación.
- Asignación y gestión de privilegios.
- Copia de seguridad y recuperación de datos.
- Cifrado y privacidad de datos.

7.10.2. Las pruebas deben ser realizadas aplicando criterios y datos generados aleatoriamente en archivos, de modo de permitir la verificación rápida y repetitiva.

7.10.3. Para los desarrollos internos, el equipo de desarrollo es el responsable de realizar las pruebas de seguridad, seguido de pruebas de aceptación, garantizando que el sistema funcione de acuerdo con lo previsto.

7.11. Pruebas de aceptación de sistemas.

7.11.1. Se deberá garantizar que los requisitos y criterios de pruebas de aceptación de nuevos sistemas, actualizaciones y versiones nuevas, estén claramente definidos, acordados, documentados y probados. Se recomienda tomar en cuenta, entre otros, los siguientes criterios:

- Requisitos de rendimiento y capacidad del sistema.
- Recuperación de errores, procedimientos de reinicio y planes de contingencia.
- Preparación y ensayo de procedimientos operativos rutinarios.
- Conjunto acordado de controles de seguridad establecidos.
- Disposiciones para la continuidad de las actividades.
- Pruebas de que la instalación del nuevo hardware no afecta negativamente a los sistemas de control y automatización existentes, especialmente en las horas críticas de procesamiento.
- Formación sobre el funcionamiento o uso de los nuevos equipos.
- Garantías y soporte para el mantenimiento.

7.11.2. Las pruebas de aceptación deben contemplar las pruebas de requisitos de seguridad y el cumplimiento de las prácticas de seguridad en el desarrollo de sistemas.

7.11.3. Las pruebas de aceptación de sistemas se deberán realizar en un entorno de prueba, de tal forma que permita, garantizar que el sistema no introducirá vulnerabilidades al entorno del organismo. Asimismo, se debe asegurar, que las pruebas sean realistas y confiables.

7.11.4. Para realizar las pruebas de aceptación de sistemas, se podrán utilizar herramientas automatizadas, como el análisis de códigos o los escáneres de vulnerabilidad.

7.12. Protección de los datos de las pruebas.

7.12.1. Se debe garantizar la cuidadosa selección, protección y control de los datos de prueba que se utilicen para los desarrollos de sistemas de información en el organismo.

7.12.2. Se debe evitar el uso de datos productivos que contengan información de datos personales o cualquier otra información confidencial para propósitos de prueba, en caso donde se utilice esta información, todos los detalles y contenidos sensibles se deben enmascarar, eliminándose de forma inmediata después de finalizar las pruebas.

7.12.3. A las aplicaciones en sistemas de prueba se le deben aplicar los procedimientos de control de acceso aplicados a los sistemas de información productivos.

RES. CM Nº 141/2026 - ANEXO XIII

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de Información
DGIYT-GOYT-PL-013

Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de Información

Contenido

1. Aspectos de Seguridad para la Gestión de la Continuidad de los Sistemas de Información

2. Objetivo.

Establecer los lineamientos generales para asegurar que existan planes y procedimientos que mantengan la continuidad de las operaciones críticas en caso de incidentes o desastres, mitigando los riegos que puedan vulnerar la disponibilidad e integridad de los activos de información.

3. Alcance.

Esta política aplica tanto 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 la continuidad de las operaciones de los activos de información.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-DIT-PL-001 -** Gestión de Incidentes - ITIL.

4.4. **DGIYT-GOYT-PL-001** - Seguridad de la Información.

4.5. **DGIYT-GOYT-PL-002 -** Organización de Seguridad de Información.

4.6. **DGIYT-GOYT-PL-003** - Gestión de Incidentes de Seguridad de la Información.

5. Definiciones.

5.1. **Plan de Continuidad del Negocio (BCP):** BCP es la sigla en inglés para “Business Continuity Plan", que se traduce en español como Plan de Continuidad del Negocio. Se trata de un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento y la prestación de servicios brindados en el organismo, después de padecer cualquier tipo de impacto negativo que suponga una interrupción de las actividades y procesos.

5.2. **Plan de Recuperación ante Desastres (DRP):** DRP es la sigla en inglés para "Disaster Recovery Plan", que se traduce al español como Plan de Recuperación ante Desastres. Se trata de un conjunto de procedimientos y estrategias diseñadas para ayudar al organismo a recuperarse y continuar operando después de un desastre o incidente grave, como un ciberataque, una catástrofe natural o una falla tecnológica significativa.

5.3. **Redundancia:** disposición de más de un recurso, normalmente de similares características a otro ya existente, para la ejecución de una misma tarea que se considera crítica o prioritaria, de esta manera y en caso de fallos, la función vital igualmente podrá ser asegurada y cumplida.

5.4. **BIA:** Business Impact Analysis o Análisis de Impacto en el Negocio en español, es un proceso fundamental dentro de la gestión de la continuidad de los sistemas de información. Su objetivo principal es identificar y evaluar los efectos que una interrupción significativa podría tener en las operaciones del organismo.

5.5. **DGIYT:** Dirección General de Informática y Tecnología.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que la gestión de los planes y procedimientos relacionados con la continuidad de los sistemas de información críticos, en caso de incidentes o desastres, se realice en cumplimiento con los lineamientos de seguridad establecidos en esta política.

6.3. **Grupo de Gestión de Seguridad de la Información (GGSI):** encargado de liderar la elaboración e implementación del Plan de Gestión de Crisis cuando ocurra un incidente que provoque la disrupción parcial o total de los sistemas de información del organismo, generando como resultado la continuidad de las operaciones normales.

7. Lineamientos.

7.1. **Generalidades.**

7.1.1. Ante la ocurrencia de un incidente de seguridad de la información, y en función del nivel de riesgo evaluado, el GGSI deberá determinar la necesidad de activar los planes de respuestas establecidos. En dicho caso, se deberá priorizar la protección de los activos de información afectados y asegurar la rápida reanudación de las operaciones críticas.

7.1.2. Los incidentes que afecten la infraestructura tecnológica administrada por la DGIYT deberán ser gestionados conforme a lo establecido en la política **DGIYT-DIT-PL-001 -** Gestión de incidentes – ITIL.

7.1.3. En los casos en los que no se justifique la activación de los planes mencionados, se deberá seguir lo establecido en la política **DGIYT-GOYT-PL-003** - Gestión de Incidentes de Seguridad de la Información, asegurando una respuesta proporcionada, documentada y coherente con el nivel de impacto.

7.1.4. El GGSI será responsable de garantizar la existencia de los planes BCP, DRP y otros que correspondan, asegurando que dichos planes respondan adecuadamente a los requerimientos del organismo y estén disponibles para su activación ante escenarios disruptivos. La elaboración detallada, pruebas, mantenimiento y actualización continua de dichos planes se abordarán en los ítems siguientes.

7.1.5. La DGIYT deberá asegurar la provisión de infraestructura, herramientas tecnológicas y servicios necesarios para sostener la operación continua de los sistemas críticos ante una interrupción o incidente.

7.1.6. Todos los sistemas de gestión considerados críticos deberán contar con copias de seguridad actualizadas, verificadas y almacenadas de forma segura, garantizando su disponibilidad para procesos de recuperación en situaciones adversas.

7.1.7. El personal con roles asignados dentro de los planes de continuidad y recuperación deberá recibir formación continua, participar en ejercicios prácticos y estar plenamente capacitado para responder con eficacia ante eventos que afecten la continuidad operativa.

7.1.8. Todos los procesos relacionados con la continuidad de los sistemas de información y la recuperación ante desastres deberán ser revisados y actualizados periódicamente, integrando lecciones aprendidas, nuevos riesgos identificados y cambios en la tecnología o estructura organizacional.

7.2. Planificación de la continuidad de las operaciones.

7.2.1. El CISO garantizará que se realice un BIA a los sistemas de información pertenecientes o relacionados al organismo, con el fin de determinar los requisitos necesarios de seguridad de la información y de la continuidad de las operaciones aplicables en los casos de situaciones adversas.

7.2.2. Se deberá elaborar un BCP, DRP y todos los planes que correspondan para proporcionar una guía clara y práctica con el fin de gestionar y superar interrupciones, garantizando que el organismo continúe operando con la mínima disrupción posible.

7.2.3. Todos los procesos, procedimientos y controles requeridos para la continuidad de la seguridad de la información, deben ser debidamente documentados y se debe garantizar que la documentación se mantenga, revise, actualice y se pruebe en un proceso de mejora continua. La documentación se actualizará siempre que se produzcan cambios significativos en las personas, procesos, tecnologías o estructura organizativa de los sistemas de información.

7.2.4. Se deberán establecer procedimientos específicos de respuesta ante cada posible incidente detectado, y constantemente evaluar nuevos posibles escenarios.

7.2.5. Se definirán a los agentes y/o terceros responsables y las distintas funciones dentro de los planes de continuidad de los sistemas de información y recuperación de desastres, contemplando la gestión de los incidentes, el mantenimiento de los niveles de seguridad y restauración de los sistemas de información.

7.2.6. Se deberá establecer un GGSI el cual tendrá como objetivo liderar la implementación de un Plan de Gestión de Crisis cuando ocurra un incidente que provoque la disrupción parcial o total de los sistemas de información del organismo y que este plan genere como resultado la continuidad de las operaciones normales.

7.2.7. El GGSI, deberá estar conformado de acuerdo con lo establecido en la política establecida en la **DGIYT-GOYT-PL-002 -** Organización de Seguridad de la Información.

7.2.8. El GGSI deberá establecer y liderar Equipos de Gestión de Crisis (EGC) con responsables técnicos tanto interno como externos de acuerdo con los diferentes escenarios que se puedan presentar como incidentes.

7.2.9. Se deberán establecer responsables sustitutos en caso de que los principales no se encuentren disponibles al momento de afrontar una crisis. Para ello, será importante garantizar que haya

agentes y/o terceros capacitados con las habilidades y conocimientos necesarios para cubrir.

7.2.10. Se deberá establecer y proporcionar un espacio centralizado desde el cual se pueda coordinar la respuesta a desastres, permitiendo una toma de decisiones rápida y efectiva.

7.2.11. Se deben establecer canales de comunicación claros para mantener informados a los agentes y/o terceros necesarios durante el manejo del incidente.

7.2.12. Se deberán garantizar la existencia de múltiples canales de comunicación para asegurar que la misma no sea interrumpida durante una crisis.

7.2.13. Las aplicaciones y servicios que soportan los procesos principales del organismo deberán ser identificados, documentados y debidamente protegidos. La irrupción de alguno de estos servirá como criterio claro para que el GGSI de inicio a la activación del plan.

7.2.14. Se deberá mantener actualizado y disponible en diferentes medios una matriz de contactos tanto internos y externos que puedan ser necesarios ante posibles incidentes.

7.2.15. Se deberá verificar que los servicios tercerizados o en la nube que soportan procesos críticos del organismo cuenten con sus propios mecanismos de continuidad operativa, y que dichos mecanismos estén alineados con los requerimientos del organismo. Esta evaluación deberá realizarse previamente a la contratación y de forma periódica.

7.3. Verificación, revisión y evaluación de la continuidad de las operaciones.

7.3.1. Periódicamente, se llevará a cabo una evaluación y se realizarán pruebas de funcionalidad en los procesos, procedimientos y controles relacionados con la continuidad de la seguridad de la información. De este modo garantizar que los mecanismos establecidos para proteger la información sigan siendo eficaces y adecuados.

7.3.2. Las pruebas deben incluir simulaciones de incidentes y escenarios de crisis para verificar la capacidad de respuesta y recuperación de los sistemas, lo cual permitirá identificar áreas de mejora y ajustar las estrategias de seguridad según sea necesario, asegurando que se mantenga un nivel aceptable de protección en la seguridad de la información.

7.3.3. Cada vez que se realicen cambios en los sistemas de información del organismo, se deberá llevar a cabo una evaluación minuciosa para determinar si estos cambios impactan los controles de continuidad de la seguridad de la información. Este proceso implica revisar los cambios propuestos o implementados para identificar cualquier efecto potencial sobre los controles existentes, la integridad del sistema, y la capacidad de recuperación en caso de incidente.

7.3.4. Todas las verificaciones, revisiones y evaluaciones realizadas a los procesos de continuidad de las operaciones deben ser registrados para control interno y sirve como evidencia durante auditorías. La documentación debe incluir los resultados de las pruebas, las observaciones realizadas, las acciones correctivas adoptadas, y cualquier recomendación para mejorar los controles y procedimientos.

7.3.5. Luego de cada simulacro, se deberá realizar un informe de lecciones aprendidas, que incluya oportunidades de mejora, debilidades detectadas y recomendaciones para ajustes en los procedimientos.

7.4. Instalaciones de procesamiento de información.

7.4.1. Cuando no se puede garantizar disponibilidad usando la arquitectura de los sistemas ya existentes, se deberá considerar la activación de un plan de contingencia acorde.

7.4.2. Periódicamente se realizarán pruebas de funcionamientos a los sistemas de información redundantes, asegurando que se puedan hacer transiciones sin interrupciones de un componente a otro al momento de presentarse un incidente, falla o casos de situaciones adversas.

7.4.3. En las pruebas de funcionamientos a los sistemas de información redundantes, se debe considerar sin limitarse a ello, la verificación de la sincronización de datos, la integridad de la información transferida, y la capacidad de los sistemas para operar de manera independiente si es necesario.

7.4.4. El CISO deberá asegurar que las instalaciones de procesamiento de información del organismo mantengan una alta disponibilidad en todo momento. Esto implica la implementación de estrategias y soluciones que garanticen que los sistemas de información estén operativos y accesibles cuando se necesiten, minimizando al máximo posible cualquier tiempo de inactividad.

7.4.5. El CISO debe garantizar que se lleven a cabo evaluaciones detalladas de los sistemas de información actuales para identificar cuáles, debido a su diseño o arquitectura, no pueden cumplir con los requisitos de disponibilidad establecidos por los procesos y operaciones del organismo. Esta evaluación debe considerar factores como la capacidad de los sistemas para manejar cargas de trabajo, la redundancia incorporada, la capacidad de recuperación ante fallos, y cualquier limitación inherente en la infraestructura tecnológica.

7.4.6. En los casos en que la arquitectura de los sistemas de información existentes no pueda garantizar la disponibilidad requerida, el CISO deberá considerar la activación de un plan de contingencia adecuado. Este plan debe estar diseñado para abordar y mitigar los riesgos asociados con la falta de disponibilidad y garantizar que los procesos críticos del organismo puedan continuar funcionando incluso en caso de fallos importantes en los sistemas de procesamiento de información.

7.4.7. Los planes de contingencia deben ser documentados y probados regularmente para asegurar que se ajusten según las necesidades cambiantes del organismo y la evolución de la tecnología.

RES. CM Nº 141/2026 - ANEXO XIV

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de las Operaciones

DGIYT-GOYT-PL-014

Seguridad de las Operaciones

Contenido

1. Seguridad de las Operaciones

2. Objetivo.

Establecer los lineamientos para asegurar que las operaciones de los sistemas de información se realicen de manera segura y eficiente, implementando controles de seguridad que minimicen el riesgo de interrupciones y vulnerabilidades.

3. Alcance.

Esta política aplica tanto 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 las operaciones de los sistemas de información.

4. Documentos relacionados.

4.1. **IRAM-ISO/IEC 27001** - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.

4.2. **IRAM-ISO/IEC 27002** - Tecnología de la Información - Técnicas de Seguridad - Código de Buenas Prácticas para los Controles de la Seguridad de la Información.

4.3. **DGIYT-GOYT-PL-001 -** Seguridad de la Información.

4.4. **DGIYT-GOYT-PL-004** - Cumplimiento de Seguridad de Información.

4.5. **DGIYT-GOYT-PL-005 -** Seguridad de la Información en las Relaciones con Proveedores.

4.6. **DGIYT-GOYT-PL-008 -** Seguridad Criptográfica.

4.7. **DGIYT-GOYT-PL-012 -** Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

5. Definiciones.

5.1. **Sincronización de relojes en los sistemas:** consiste en garantizar que los procesos se ejecuten en forma cronológica y a la misma vez respetando el orden de los eventos dentro del sistema.

5.2. **Información documentada**: hace referencia a la información que el organismo considera importante, la misma debe ser consolidada en un espacio físico o digital.

5.3. **Copias de seguridad**: también llamada respaldo o backup, son copias de datos y archivos importantes que se crean con el propósito de proteger la información en caso de pérdida, corrupción o fallo de sistemas.

5.4. **Registro:** se entiende por "registro" (o log) a toda la información generada por los sistemas o personas, que permite realizar un seguimiento de actividades realizadas en los sistemas o procesos manuales.

5.5. **DGIYT:** Dirección General de Informática y Tecnología.

5.6. **AT:** Arquitectura Tecnológica.

5.7. **APP:** Aplicaciones.

5.8. **GOYT:** Gestión Operativa y Tecnológica.

5.9. **ST:** Soporte Técnico.

6. Roles y Responsabilidades.

6.1. **Director General de Informática y Tecnología:** garantizar la eficiente asignación y uso de los recursos necesarios para asegurar la implementación adecuada de esta política.

6.2. **Jefe de seguridad de la información (CISO):** garantizar que la gestión de los procedimientos relacionados con la seguridad de las operaciones de los activos de información se realice en cumplimiento con los lineamientos de seguridad establecidos en esta política.

6.3. **Oficial de Seguridad de la Información (OSI):** monitorear continuamente las operaciones de los activos de información identificando patrones o comportamientos anómalos con el fin de detectar y gestionar posibles incidentes de seguridad.

6.4. **Jefes de departamento de AT/APP/GOYT/ST**: implementar los controles establecidos en esta política según corresponda, de acuerdo con las funciones de cada departamento.

6.5. **Responsable de Cumplimiento (RC):** asegurar el cumplimiento de los lineamientos establecidos en los procedimientos de seguridad de las operaciones, mediante la planificación y ejecución de auditorías de seguridad.

7. Lineamientos.

7.1. Procedimientos operativos documentados.

7.1.1. Se deberá garantizar la debida documentación y actualización de procedimientos e instructivos de actividades operativas, asociadas a las instalaciones de procesamiento de información y comunicaciones, garantizando su disposición a todo aquel que lo necesite.

7.1.2. Los cambios a la información documentada de los procedimientos operativos deben ser autorizados previamente, cualquier procedimiento inadecuado o incorrectamente documentado puede dar lugar a errores del usuario provocando la pérdida de disponibilidad, integridad y confidencialidad de la información.

7.1.3. Se recomienda que los procedimientos operativos documentados se desarrollen proporcionando diagramas de flujo de información actualizados.

7.1.4. La información documentada se mantendrá almacenada de forma segura y de acuerdo con el nivel de clasificación de la información que contenga, con el fin de proteger el acceso no autorizado.

7.2. Gestión de cambios.

7.2.1. Se recomienda que todos los cambios sean controlados previamente, realizando una evaluación de riesgos y un análisis de impacto, con el fin de identificar los cambios que puedan afectar la seguridad de la información.

7.2.2. Cuando sea necesario realizar cambios, actualizaciones o reconfiguraciones, se deberá cumplir con los lineamientos establecidos en la norma de gestión de cambios.

7.2.3. Se deberán garantizar procedimientos para la implementación rápida y controlada de cambios de emergencias y procedimientos para la recuperación ante cambios no exitosos o eventos imprevistos.

7.2.4. Cuando se realicen cambios, se deberá conservar un registro de actividad que contenga toda la información pertinente para auditorias y control interno del organismo.

7.3. Gestión de la capacidad.

7.3.1. Se deben hacer proyecciones de futuros requisitos de capacidad tecnológica para asegurar el desempeño de los sistemas de información y evitar la pérdida de disponibilidad o rendimiento por falta de capacidad.

7.3.2. Se debe controlar el uso de los recursos informáticos, para ello, se recomienda que se tome en cuenta, entre otros, los siguientes aspectos:

- Medición y seguimiento.
- Previsión de uso a futuro.
- Optimización.
- Vida útil.

7.4. **Separación de los ambientes.**

7.4.1. Los entornos deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.

7.4.2. Se debe garantizar el acceso autorizado a los ambientes, con el fin de evitar cambios no intencionales al software o a la información.

7.5. Controles contra código malicioso.

7.5.1. El CISO garantizará que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso, mediante la implementación de controles de detección, prevención y recuperación.

7.5.2. Se deberán establecer e implementar controles que prevengan o detecten el uso de software no autorizados y de sitios web conocidos o sospechados como maliciosos.

7.5.3. Se deberá realizar monitoreos de software y de los datos de la red, con el fin de identificar las vulnerabilidades que el código malicioso pueda explotar.

7.5.4. Se utilizarán antivirus como medida de protección a la red, controlando los archivos que se procesen en esta.

7.5.5. La última versión del software antivirus debe estar correctamente instalado sin posibilidad de ser desactivado o modificado por los usuarios.

7.6. Resguardo de la información.

7.6.1. Las copias de seguridad de la información, el software y los sistemas, serán probados periódicamente de acuerdo con lo establecido en el procedimiento de administración de copias de resguardo y recuperación de datos.

7.6.2. Para el respaldo de la información se tomarán en cuenta, entre otros, los siguientes aspectos:

- Se generarán registros exactos y completos de las copias de resguardo y procedimientos de restauración documentados.

- Las copias de resguardo serán almacenadas en un lugar físico y no cercano al principal, evitando cualquier daño producido en éste. Y deberán ser protegidas adecuadamente con el mismo nivel de seguridad que el activo de información original, evitando su acceso o destrucción no autorizado.
- Los medios de resguardo serán probados regularmente para garantizar su disponibilidad en los casos de emergencia.
- Se recomienda que en situaciones de confidencialidad y de ser necesario, las copias de resguardo sean protegidas por medios de cifrado y de acuerdo con el estándar de criptografía del organismo.

7.6.3. Se deberá garantizar la realización de campañas de capacitación y concientización, dando a conocer las obligaciones del personal, respeto a la seguridad de la información, con el fin de que puedan detectar y reportar incidentes y/o eventos que pongan en riesgo la seguridad de la información.

7.7. Registro de eventos

7.7.1. Se registrarán y protegerán las actividades de los administradores y operadores de sistemas, dichas activades serán revisadas de manera regular para mantener la trazabilidad de los usuarios con privilegios, evitando que los registros de actividades sean manipulados o alterados.

7.7.2. Los administradores de sistemas no tendrán permiso para borrar o desactivar los registros de sus propias actividades, a menos que sea explícitamente autorizado por el organismo. El incumplimiento de esto podrá implicar, si correspondiere, procesos disciplinarios y/o sancionatorios según los términos de las normas vigentes.

7.7.3. Se recomienda que los registros de eventos incluyan, entre otros, los siguientes aspectos:

- Intentos de accesos exitosos y fallidos.
- Desconexiones del sistema.
- Acciones ejecutadas.
- Archivos accedidos y tipo de acceso.
- Alertas por fallos en los sistemas.
- Fecha y hora en que se producen los eventos.
- Tiempos de detención.
- Personas involucradas.
- Causas.

7.8. Protección de registros.

7.8.1. Las instalaciones de registro y la información de registro de las actividades deben estar protegidas contra la manipulación y el acceso no autorizado.

7.8.2. En caso de ser necesario modificar o eliminar los registros deberá ser autorizado por la DGIYT y deberá generarse un respaldo de dicha información.

7.8.3. Se recomienda el uso de software de monitoreo de integridad de archivos o detección de cambios, con el fin de garantizar que los datos de registro existentes sean cambiados o manipulados sin autorización.

7.9. Sincronización de relojes.

7.9.1. Se debe mantener sincronizado los relojes de todos los sistemas de procesamiento de información pertenecientes al organismo, de acuerdo con la ubicación geográfica correspondiente.

7.9.2. El Jefe de departamento de Arquitectura Tecnológica garantizará la sincronización de relojes de los diferentes equipos.

7.10. Instalación del software en los sistemas en producción.

7.10.1. Todos los activos de software deberán ser debidamente inventariados, detallando su funcionamiento y propietario.

7.10.2. La instalación, monitoreo y desinstalación de software, será gestionada según lo establecido en el procedimiento de gestión de activos.

7.10.3. La actualización del software operativo, las aplicaciones y las bibliotecas de programas, solo serán realizadas por administradores capacitados y autorizados.

7.10.4. Se establecerá e implementará un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema.

7.10.5. Se recomienda que las versiones antiguas del software sean archivadas, junto con toda la información y los parámetros requeridos, los procedimientos, los detalles de configuración y el software de soporte.

7.10.6. El acceso físico y lógico a los proveedores para dar servicio de soporte deberá ser otorgado solo por el tiempo necesario.

7.11. Gestión de las vulnerabilidades técnicas.

7.11.1. Se identificarán las vulnerabilidades técnicas de los sistemas de información utilizados, se evaluará la exposición del parque informático del organismo a dichas vulnerabilidades y se tomarán las medidas apropiadas de acuerdo con la clasificación de la información del activo.

7.11.2. Periódicamente y después de cualquier cambio significativo en la red interna y externa, se establecerá un proceso para identificar vulnerabilidades de seguridad.

7.11.3. Se deben definir los roles y responsabilidades para la gestión de las vulnerabilidades técnicas, contemplado el monitoreo, la evaluación de los riesgos, los parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.

7.12. Restricciones a la instalación del software.

7.12.1. Los lineamientos que rigen la instalación y las actividades que involucran la verificación de los sistemas deberán ser planificados y acordados cuidadosamente para minimizar las interrupciones en los procesos.

7.12.2. Se deberán identificar y documentar los tipos de instalaciones de software que estén homologadas por el organismo.

7.13. Controles de auditoría de los sistemas de información.

7.13.1. Periódicamente se realizan auditorías que permitan detectar desvíos entre los lineamientos planteados y la implementación de éstos, de acuerdo con lo establecido en la política **DGIYT-GOYT-PL-004** - Cumplimiento de Seguridad de Información.

7.13.2. Las auditorías a los sistemas de información deben ser acordadas con las personas involucradas previamente a su ejecución y el alcance debe ser acordado y controlado.

7.13.3. Las pruebas de auditoría deben limitarse al acceso de sólo lectura de la información debidamente monitoreada y registrada.

7.13.4. Las pruebas de auditoría que, de acuerdo con el análisis previo, puedan afectar a la disponibilidad de los sistemas de información, deben ser ejecutadas fuera de horarios laborales.

FIRMAS DIGITALES

Firmado digitalmente por:
LEGUIZAMON, ISABELLA KARINA
PRESIDENTE/A
CMCABA
Fecha: lunes, 20 julio 2026 16:25:40

Firmado digitalmente por:
CORTI, HORACIO GUILLERMO ANIBAL
VICEPRESIDENTE/A
CMCABA
Fecha: lunes, 20 julio 2026 16:31:18