ACUERDO No. 016-DIDADPOL-2026

DIRECCIÓN DE ASUNTOS DISCIPLINARIOS POLICIALES DIDADPOL, TEGUCIGALPA

M.D.C. 25 DE MARZO DEL AÑO 2026.

CONSIDERANDO:

Que, la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) es una dependencia desconcentrada de la Secretaría de Estado en el Despacho de Seguridad, con autonomía técnica, administrativa, financiera y operativa, encargada de investigar las faltas graves y muy graves cometidas por miembros de la Carrera Policial y personal de la Secretaría de Seguridad, conforme a su marco legal de creación.

Que, la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL), en cumplimiento de las disposiciones establecidas en la Ley Orgánica del Tribunal Superior de Cuentas (LOTSC), la Ley de Transparencia y Acceso a la Información Pública (LTAIP), Lineamientos de Archivo del IAIP (Acuerdo SO-098-2019), el Marco Rector de Control Interno Institucional de los Recursos Públicos (MARCI), la Ley General de la Administración Pública y demás normativa aplicable, reconoce la importancia de garantizar la privacidad, seguridad, integridad y uso adecuado de los datos personales que administra en el ejercicio de sus funciones.

Que, la presente Política de Privacidad y Protección de Datos Personales se formula en consonancia con la Política de Archivo Institucional y Política de Transparencia de la DIDADPOL, con el fin de asegurar que la gestión documental y el tratamiento de datos personales se realicen bajo criterios uniformes de protección, confidencialidad, conservación, acceso responsable y transparencia.

Que, la Constitución y el marco legal hondureño reconocen el derecho de acceso a la información pública y exigen al Estado preservar la memoria administrativa y facilitar la

rendición de cuentas, sin perjuicio de la protección de la intimidad y de los datos personales cuya divulgación pueda causar perjuicios o vulnerar derechos fundamentales.

Que, la Ley de Transparencia y Acceso a la Información Pública (Decreto No. 170-2006) regula el derecho de acceso a la información pública, establece el deber de informar de las instituciones obligadas, define los conceptos de información pública, reservada y datos personales confidenciales, y dispone obligaciones específicas sobre clasificación, custodia, conservación y sanciones por manejo indebido de datos personales.

Que, la LTAIP obliga a las instituciones obligadas a mantener subsistemas con soporte humano y técnico, a designar un Oficial de Información Pública y a publicar la información que por ley deba difundirse de oficio, pero también contempla la restricción de acceso cuando la divulgación afecte la seguridad del Estado, el interés público o derechos de terceros, incluyendo la protección de datos personales confidenciales.

Que, el Instituto de Acceso a la Información Pública (IAIP) tiene la atribución de regular, emitir lineamientos e instruir a las instituciones obligadas respecto a la clasificación, archivo, custodia y protección de la información pública, y que mediante el Acuerdo SO-098-2019 promulgó los Lineamientos de Archivo que fijan criterios técnicos y procedimentales para la gestión documental en las instituciones obligadas.

Que, los Lineamientos de Archivo del IAIP establecen principios y normas mínimas en materia de gestión documental (clasificación, valoración, expurgo, transferencia y conservación), la necesidad de contar con responsables certificados de archivo, la generación de respaldos digitales periódicos y la elaboración de inventarios e instrumentos de control documental, requisitos que deben integrarse a cualquier política de protección de datos institucional.

Que, el tratamiento de datos personales mediante listas de asistencia a eventos públicos (en soporte papel o digital) constituye operación de datos personales sujeta a normativa de protección; por tanto, su diseño, recolección, custodia, digitalización, periodo de

conservación y eliminación deben ajustarse a los principios de lealtad, licitud, transparencia, minimización, limitación de la finalidad, exactitud, integridad y confidencialidad, y a las indicaciones técnicas y organizativas que emita el IAIP. (Instrucciones del IAIP sobre listas de asistencia).

Que, en atención al principio de minimización y a las obligaciones de seguridad, cuando proceda la recolección de datos para asistencia a eventos públicos se deberá limitar la información a los campos estrictamente necesarios (por ejemplo: nombre, apellido e institución), incluir la debida cláusula informativa (deber de información) y habilitar casillas independientes para consentimientos adicionales (publicidad/comunicaciones), respetando que las casillas de consentimiento no vengan marcadas por defecto. (Directrices prácticas del IAIP sobre recolección en eventos).

Que, la DIDADPOL administra información especialmente sensible en el contexto disciplinario (denunciantes, denunciados, contenido de investigaciones, resultados de pruebas de confianza, dictámenes técnicos administrativos y otros elementos de los expedientes investigativos), lo que exige medidas reforzadas de confidencialidad, control de accesos, conservación segura, trazabilidad de accesos y prohibición de divulgación no autorizada, sin perjuicio de las obligaciones de entrega a autoridades competentes mediante los canales legales correspondientes.

Que, los Lineamientos del IAIP y la LTAIP establecen la obligación de conservar los documentos conforme a un calendario de conservación/expurgo, documentar inventarios de baja documental, realizar procesos de expurgo autorizados y remitir al Archivo Nacional las transferencias secundarias o históricas cuando proceda; dichos procedimientos deben aplicarse con criterios de protección de datos (p. ej. anonimización cuando se transfiera material histórico que contenga datos personales).

Que, la gestión segura de registros en soportes físicos y digitales requiere medidas técnicas y organizativas mínimas: control de acceso físico a hojas de asistencia y expedientes, custodia de las listas en papel por personal designado, digitalización segura y destrucción irreversible del soporte papel una vez cumplido el plazo legal y operativa la digitalización cuando proceda, cifrado y copias de seguridad periódicas en espacios aprobados y restringidos, y registro documental de transferencias y bajas.

Que, la LTAIP prevé un régimen sancionatorio y que el manejo indebido, la divulgación no autorizada, la eliminación irregular o la recolección fuera de marco legal de datos personales confidenciales puede acarrear sanciones administrativas y, cuando corresponda, responsabilidad penal conforme a la normativa aplicable; por ello la política debe establecer controles internos, responsabilidades y mecanismos de auditoría.

Que, la protección efectiva de datos personales requiere la asignación de responsabilidades institucionales claras (Secretaría General, Unidad de Gestión Documental, Oficial de Información Pública, Unidad de Control Interno y Unidad de Auditoría Interna), formación continua del personal en materia de transparencia, archivo y protección de datos, y la publicación accesible de los datos de contacto del responsable del tratamiento para que los titulares puedan ejercer sus derechos (acceso, rectificación, cancelación, oposición y revocación de consentimiento).

ACUERDA:

APROBAR LA SIGUIENTE POLÍTICA INSTITUCIONAL DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE LA DIDADPOL.

POR TANTO, y en uso de las atribuciones que le confiere su normativa orgánica y las disposiciones aplicables en materia de gestión documental y transparencia, la DIDADPOL adopta la presente Política de Privacidad y Protección de Datos Personales, la cual se aplicará a todos los procesos, expedientes, sistemas y actividades de la

institución que impliquen el tratamiento de datos personales, en consonancia con la Ley de Transparencia y los lineamientos del IAIP.

CAPÍTULO I

OBJETIVOS

Artículo 1. Objetivo General. El objetivo general de la presente Política de Privacidad y Protección de Datos Personales es establecer el marco normativo y los lineamientos institucionales que regulen el tratamiento, protección, gestión, conservación, seguridad y disposición final de los datos personales administrados por la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL), integrando dichos procesos dentro del Sistema de Gestión Documental Institucional establecido por la Ley de Transparencia y Acceso a la Información Pública (LTAIP), el Acuerdo SO-098-2019 del Instituto de Acceso a la Información Pública (IAIP) y la Política de Archivo Institucional.

Esta política tiene como finalidad:

- Garantizar que toda actividad de recolección, registro, organización, consulta, conservación, uso, transmisión, digitalización, transferencia, almacenamiento, clasificación, resguardo o eliminación de datos personales incluyendo datos sensibles contenidos en expedientes investigativos, denuncias, resultados de pruebas de confianza, dictámenes técnico-administrativos, listas de asistencia y otros documentos institucionales se realice bajo principios de legalidad, lealtad, transparencia, minimización, confidencialidad, integridad, seguridad y trazabilidad.
- Asegurar que la protección de datos personales forme parte integral de los procesos archivísticos institucionales, de acuerdo con las fases de archivo (trámite, concentración e histórico), los calendarios de conservación y expurgo, los inventarios documentales y los mecanismos de transferencia y organización definidos por el IAIP.
- Proteger la información personal administrada por la DIDADPOL frente a accesos no autorizados, divulgación indebida, pérdida, alteración, uso no autorizado o

destrucción irregular, mediante la implementación de medidas técnicas, organizativas, físicas y administrativas apropiadas al nivel de riesgo y a la sensibilidad de los datos tratados.

- Garantizar que la gestión de datos personales permita simultáneamente el cumplimiento del derecho de acceso a la información pública, la transparencia activa, la rendición de cuentas institucional y la protección efectiva de los derechos fundamentales de las personas cuyas informaciones obra en poder de la DIDADPOL.

Artículo 2. Objetivos Específicos. La presente Política de Privacidad y Protección de Datos Personales establece los siguientes objetivos específicos:

1. **Regular el tratamiento integral de los datos personales** administrados por la DIDADPOL, asegurando que toda recolección, registro, organización, uso, conservación, transmisión, consulta, transferencia o eliminación de datos personales se realice conforme a los principios de la LTAIP, la normativa técnica del IAIP y la Política de Archivo Institucional.
2. **Garantizar la protección reforzada de los datos personales sensibles** contenidos en expedientes disciplinarios, denuncias, actuaciones investigativas, dictámenes técnico-administrativos, resultados de pruebas de confianza, registros biométricos, listas de asistencia y demás documentación institucional, aplicando medidas de seguridad adecuadas al nivel de riesgo y sensibilidad de la información.
3. **Incorporar la protección de datos personales dentro del Sistema de Gestión Documental Institucional**, de acuerdo con las fases de archivo (trámite, concentración e histórico), los calendarios de conservación, expurgo y transferencia, así como los procedimientos archivísticos establecidos por el IAIP.
4. **Establecer criterios uniformes para la recolección de datos personales** en formularios, listas de asistencia, plataformas digitales y sistemas institucionales, garantizando el cumplimiento del deber de información, la minimización de

datos, el consentimiento informado cuando proceda y la prohibición de recabar datos innecesarios para la finalidad prevista.

5. **Definir medidas técnicas y organizativas mínimas de seguridad**, tanto físicas como digitales, para prevenir accesos no autorizados, pérdidas, alteraciones, divulgaciones o destrucciones indebidas de datos personales, incluyendo protocolos para archivos físicos, soportes electrónicos, sistemas informáticos y plataformas de recolección digital.
6. **Regular los plazos de conservación, depuración, anonimato, eliminación y baja documental** de los datos personales, según lo establecido por la LTAIP, los Lineamientos de Archivo del IAIP y los calendarios institucionales aprobados para la DIDADPOL.
7. **Establecer responsabilidades institucionales claras** en materia de protección de datos personales, determinando las obligaciones de la Secretaría General, la Unidad de Gestión Documental, el Oficial de Información Pública, la Unidad de Control Interno, la Unidad de Auditoría Interna y cualquier otro personal que intervenga en el tratamiento de datos personales.
8. **Garantizar el ejercicio efectivo de los derechos de los titulares de los datos personales** (acceso, rectificación, cancelación, oposición y revocación del consentimiento cuando corresponda), mediante la publicación de los medios de contacto y procedimientos institucionales definidos para su atención.
9. **Asegurar la trazabilidad documental y el registro de accesos**, movimientos, transferencias, autorizaciones y eliminaciones de documentos que contengan datos personales, de conformidad con los instrumentos archivísticos exigidos por el IAIP.
10. **Facilitar el cumplimiento de auditorías internas y externas**, así como las supervisiones del IAIP y las solicitudes de información pública, garantizando simultáneamente el respeto al régimen de clasificación de la información (pública, reservada, confidencial y datos personales confidenciales).
11. **Promover la responsabilidad institucional y la cultura de protección de datos personales**, mediante la capacitación continua del personal, la adopción de

buenas prácticas y la implementación de mecanismos de mejora continua en materia de privacidad y gestión documental.

Artículo 3. Alcance. La presente Política de Privacidad y Protección de Datos Personales es de aplicación obligatoria en toda la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) y se extiende a todos los procesos, actividades, documentos, registros y sistemas que impliquen el tratamiento de datos personales en el ejercicio de las funciones institucionales. En particular, esta política aplica a:

1. **Todos los datos personales y datos personales sensibles** administrados por la DIDADPOL, incluyendo, entre otros:
    - Información contenida en denuncias y expedientes investigativos.
    - Información de denunciantes, testigos, investigadores y personal involucrado en procesos disciplinarios.
    - Datos personales contenidos en dictámenes técnico-administrativos.
    - Resultados de pruebas de confianza, evaluaciones y otros instrumentos de evaluación técnico-profesional.
    - Datos biométricos, fotográficos, audiovisuales o de identificación utilizados en investigaciones.
    - Registros y listas de asistencia a eventos públicos, reuniones, capacitaciones o actividades institucionales.
    - Formularios físicos y digitales utilizados para la recepción, gestión o documentación de actividades institucionales.
2. **Todos los documentos en cualquier soporte físico o digital** que contengan datos personales o información derivada de actividades disciplinarias o administrativas, incluyendo:
    - Archivos físicos: expedientes, formularios, libros de registro, actas, hojas de asistencia, libros de control.
    - Archivos digitales: bases de datos, documentos electrónicos, imágenes, audios, videos, y cualquier archivo digital administrado por la institución.

3. **Todos los sistemas, plataformas, bases de datos, aplicaciones, equipos y herramientas tecnológicas** utilizados por la DIDADPOL para:
    - Recolectar, almacenar, registrar o procesar datos personales.
    - Generar, custodiar, digitalizar o transmitir documentos institucionales.
    - Organizar expedientes o gestionar el Sistema de Gestión Documental Institucional.
    - Realizar auditorías, consultas internas, controles de acceso o trazabilidad.
4. **Todas las fases del ciclo de vida documental**, desde la creación o recepción del dato personal hasta su disposición final, incluyendo:
    - Archivo de trámite.
    - Archivo de concentración.
    - Archivo histórico (cuando proceda, aplicando mecanismos de anonimización).
    - Procesos de transferencia y expurgo documental establecidos en los lineamientos del IAIP.
5. **Todo el personal que intervenga en el tratamiento de datos personales**, independientemente de su modalidad contractual, incluyendo:
    - Personal permanente o de planta.
    - Personal contratado bajo cualquier modalidad.
    - Investigadores disciplinarios.
    - Funcionarios responsables de archivo y gestión documental.
    - Personal técnico, administrativo y de apoyo.
    - Consultores, proveedores o terceros que, por contrato, tengan acceso a información personal bajo responsabilidad institucional.
6. **Todas las obligaciones derivadas de la relación entre privacidad y transparencia**, en cumplimiento de la LTAIP, incluyendo:
    - Publicación de información de oficio sin vulnerar datos personales confidenciales.
    - Gestión de solicitudes de acceso a la información pública.
    - Aplicación del régimen de clasificación de información (pública, reservada, confidencial y datos personales confidenciales).

- Emisión de versiones públicas cuando proceda.

7. **Todos los mecanismos de seguridad física, lógica y administrativa** relacionados con la protección de datos personales y la gestión documental, incluyendo:
   - Control de accesos a archivos físicos.
   - Sistemas de contraseñas, cifrado, respaldos y seguridad informática.
   - Protocolos de custodia, traslado y destrucción segura de documentos.
   - Supervisión, auditoría y control interno.

En consecuencia, la presente Política será vinculante en todas las áreas de la DIDADPOL y deberá ser implementada, observada y supervisada en todas las operaciones que involucren datos personales, independientemente de su origen, soporte, formato o finalidad.

Artículo 4. Definiciones. Para efectos de la presente Política de Privacidad y Protección de Datos Personales, se adoptan las siguientes definiciones, entendidas conforme a la Ley de Transparencia y Acceso a la Información Pública, los Lineamientos de Archivo del IAIP y la práctica institucional de la DIDADPOL:

1. **Dato Personal:** Cualquier información concerniente a una persona natural identificada o identificable, ya sea en soporte físico o digital. Incluye, entre otros: nombre, identificación, firma, información laboral, académica, audiovisual, biométrica o cualquier otra que permita la identificación directa o indirecta de una persona.
2. **Dato Personal Sensible:** Información cuya divulgación indebida pueda afectar derechos fundamentales o poner en riesgo la integridad, la seguridad, la vida privada o la dignidad de una persona. En la DIDADPOL incluye, sin limitarse a:
   - datos contenidos en expedientes disciplinarios;
   - denuncias y nombres de denunciantes, testigos y denunciados;
   - resultados de pruebas de confianza;
   - dictámenes técnico-administrativos;
   - evaluaciones psicológicas, médicas o de riesgo;

- datos biométricos o información técnica obtenida en procesos investigativos.

3. **Titular de los Datos:** Persona natural a quien corresponden los datos personales objeto de tratamiento.
4. **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones aplicadas a datos personales, automatizadas o no, tales como recolección, registro, organización, almacenamiento, conservación, consulta, uso, análisis, digitalización, transmisión, modificación, depuración, anonimato, bloqueo, supresión, destrucción o disposición final.
5. **Responsable del Tratamiento:** La DIDADPOL, como institución obligada, y específicamente las unidades, funcionarios o servidores públicos que, en el ejercicio de sus funciones, decidan sobre la finalidad, medios y procedimientos aplicables al tratamiento de datos personales.
6. **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que trate datos personales por cuenta de la DIDADPOL, conforme a instrucciones expresas, documentadas y verificables. Incluye proveedores tecnológicos, consultores y personal contratado.
7. **Información Pública:** Toda información generada, administrada o en poder de la DIDADPOL en el ejercicio de sus funciones, salvo aquella clasificada como reservada, confidencial o que contenga datos personales cuya divulgación esté prohibida por ley.
8. **Información Reservada:** Aquella cuya divulgación pueda afectar la seguridad nacional, el interés público, procesos investigativos en curso, estrategias disciplinarias, instancias administrativas o judiciales, o cualquier otra prevista por la LTAIP.
9. **Sistema de Gestión Documental Institucional:** Conjunto de políticas, normas, procesos, procedimientos, técnicas, instrumentos y recursos tecnológicos utilizados para la gestión integral de documentos en todas las fases de su ciclo de vida: generación, clasificación, trámite, conservación, transferencia, acceso, expurgo y archivo histórico.

10. **Archivo de Trámite:** Área donde se conservan documentos de uso frecuente y que son necesarios para la operación administrativa y las investigaciones en curso.
11. **Archivo de Concentración:** Área donde se conservan documentos cuyo uso ya no es frecuente, pero que deben mantenerse por razones legales, administrativas, técnicas o históricas, por el tiempo establecido en los calendarios de conservación.
12. **Archivo Histórico:** Conjunto de documentos con valor permanente para la memoria institucional. Cuando contengan datos personales o sensibles, deberán realizarse procesos de anonimato, salvo disposiciones específicas legales.
13. **Minimización de Datos:** Principio según el cual solo deben recolectarse los datos estrictamente necesarios para la finalidad específica del tratamiento, especialmente en listas de asistencia y formularios institucionales.
14. **Limitación de la Finalidad:** Obligación de utilizar los datos personales únicamente para los fines previamente informados al titular y definidos por la DIDADPOL, sin que puedan emplearse para fines distintos sin base legal o consentimiento explícito cuando corresponda.
15. **Deber de Información:** Obligación de la DIDADPOL de informar al titular, de manera previa, clara y verificable, sobre el tratamiento de sus datos personales, incluida la finalidad, período de conservación, derechos disponibles y datos de contacto del responsable del tratamiento.
16. **Derechos ARCO:** Derechos que asisten a los titulares de datos personales: **Acceso**, **Rectificación**, **Cancelación** y **Oposición** al tratamiento de sus datos, así como el derecho a la **revocación del consentimiento** cuando éste sea la base legal del tratamiento.
17. **Trazabilidad Documental:** Registro verificable de todas las acciones realizadas sobre documentos que contienen datos personales, tales como accesos, transferencias, digitalizaciones, préstamos internos, expurgo y destrucción.
18. **Expurgo o Baja Documental:** Proceso mediante el cual se eliminan documentos que han cumplido su tiempo de conservación o han perdido su valor

administrativo, de conformidad con calendarios aprobados y procedimientos seguros definidos por el IAIP y la Política de Archivo.

19. **Anonimato:** Procedimiento técnico mediante el cual se elimina o modifica cualquier elemento que permita identificar a una persona dentro de un documento, con el fin de preservar información para fines históricos o estadísticos sin vulnerar la privacidad del titular.

CAPÍTULO II

PRINCIPIOS RECTORES

Artículo 5. Principios de Tratamiento de Datos. El tratamiento de los datos personales administrados por la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) se regirá por los siguientes principios fundamentales, los cuales orientarán toda actuación institucional relacionada con la gestión, archivo, protección, conservación, acceso y disposición final de información que contenga datos personales o datos personales sensibles:

a) **Principio de Legalidad** - Todo tratamiento de datos personales debe realizarse de conformidad con la Ley de Transparencia y Acceso a la Información Pública (LTAIP), el Acuerdo SO-098-2019 del IAIP, la legislación aplicable y las competencias propias de la DIDADPOL.

b) **Principio de Lealtad y Transparencia** - La recolección y uso de datos personales se realizará de manera ética, clara, informada y no engañosa. Los titulares serán informados adecuadamente sobre las finalidades del tratamiento, especialmente en formularios, listas de asistencia o sistemas digitales.

c) **Principio de Limitación de la Finalidad** - Los datos personales solo podrán ser utilizados para los fines previamente definidos e informados al titular. En la DIDADPOL, esto incluye principalmente finalidades disciplinarias, administrativas, investigativas y de gestión institucional. Queda prohibido

utilizar datos personales para fines distintos sin base legal o consentimiento cuando corresponda.

d) **Principio de Minimización de Datos** - Solo se recolectarán los datos estrictamente necesarios según la finalidad establecida. Especial atención se deberá tener en listas de asistencia, evitando la solicitud de datos excesivos o no esenciales como DNI, teléfono, correo electrónico, etnia o género, salvo justificación legal y debida autorización.

e) **Principio de Proporcionalidad** - La cantidad, tipo y alcance del tratamiento de datos personales deberán ser adecuados y no excesivos en relación con las finalidades institucionales. En investigaciones disciplinarias, la recolección debe limitarse a elementos pertinentes para el caso.

f) **Principio de Exactitud** - Los datos personales deben ser veraces, actualizados y exactos.

Los registros incorrectos o desactualizados deben ser rectificados o completados cuando el titular lo solicite o cuando la institución lo detecte.

g) **Principio de Integridad y Confidencialidad** - La DIDADPOL deberá implementar medidas de seguridad físicas, tecnológicas y administrativas que garanticen que los datos personales —especialmente los sensibles— estén protegidos contra pérdida, acceso no autorizado, alteración o divulgación indebida.

Esto incluye:

- Control de accesos a expedientes disciplinarios
- Custodia reforzada de listas de asistencia
- Protocolos seguros de digitalización
- Uso de sistemas con credenciales y restricciones

h) **Principio de Seguridad de la Información** - Todo tratamiento deberá aplicar medidas de seguridad proporcionales al nivel de riesgo: respaldos digitales, cifrado, destrucción segura, resguardo en archivadores cerrados, actualización de software, antivirus, claves de acceso y otros mecanismos de protección.

i) **Principio de Conservación Limitada** -Los datos personales se conservarán únicamente por el tiempo necesario para cumplir con las finalidades del tratamiento y conforme a los calendarios de conservación aprobados por el IAIP.

Concluido el plazo, deberán eliminarse de manera segura o anonimizarse cuando corresponda.

j) **Principio de Responsabilidad Proactiva** - La DIDADPOL deberá demostrar el cumplimiento de esta política mediante registros, controles documentados, auditorías, trazabilidad, capacitación del personal y mecanismos de supervisión establecidos.

k) **Principio de Trazabilidad** - Toda acción realizada sobre documentos o sistemas que contengan datos personales debe quedar registrada: acceso, préstamo, digitalización, transferencia, modificación, expurgo o eliminación.

l) **Principio de Acceso Restringido** - El acceso a datos personales, y especialmente a datos sensibles, solo podrá realizarse por personal autorizado y estrictamente para fines institucionales. Se deberán establecer perfiles, niveles y controles de acceso por área y función.

m) **Principio de Transparencia Pública Responsable** - La DIDADPOL deberá garantizar el acceso a la información pública sin vulnerar datos personales confidenciales. Cuando corresponda, se deberán elaborar versiones públicas o aplicar procesos de anonimato.

n) **Principio de No Discriminación** - El tratamiento de datos personales no podrá generar discriminación directa o indirecta hacia los titulares, especialmente en datos que revelen origen étnico, género, orientación sexual, salud, condición laboral u otras características sensibles.

o) **Principio de Confidencialidad** - La obligación de reserva se mantiene aun cuando la relación laboral o contractual con la DIDADPOL haya concluido, según el tiempo establecido en el Acuerdo de Confidencialidad, suscrito.

CAPÍTULO III

TRATAMIENTO DE LOS DATOS PERSONALES

Artículo 6. Finalidades del Tratamiento. Los datos personales administrados por la DIDADPOL solo podrán ser tratados para las siguientes finalidades institucionales:

1. **Investigación disciplinaria:** análisis, verificación, documentación y resolución de faltas graves y muy graves conforme a la ley.
2. **Gestión administrativa:** trámites internos, control de personal, registros de actividades, procesos de archivo y seguimiento de obligaciones institucionales.
3. **Procesos de transparencia:** elaboración de versiones públicas, atención de solicitudes de información, clasificación documental.
4. **Seguridad institucional:** control de accesos, identificación en instalaciones, custodia de bienes e información.
5. **Gestión de eventos y capacitaciones:** registro de asistencia y organización logística, limitando la finalidad exclusivamente al manejo del evento.
6. **Cumplimiento legal:** entrega de información a autoridades competentes bajo requerimiento formal.
7. **Respaldo y conservación documental:** creación de archivos de trámite, concentración e histórico, conforme al calendario de conservación aprobado.

Queda **prohibido** utilizar datos personales para finalidades distintas a las informadas, salvo que exista una obligación legal o el titular otorgue consentimiento específico cuando proceda.

Artículo 7. Tratamiento de Datos Personales Sensibles en Expedientes Disciplinarios. La DIDADPOL reconoce que los expedientes disciplinarios contienen datos personales altamente sensibles, cuya divulgación o tratamiento inadecuado puede generar riesgos graves para los derechos, integridad o seguridad de los involucrados.

Por tanto, se establecen las siguientes obligaciones específicas:

a) El acceso a expedientes disciplinarios será estrictamente limitado al personal autorizado, debidamente designado por la Secretaría General o por la Dirección.
b) Los expedientes deberán mantenerse bajo custodia segura, en archivadores cerrados o sistemas digitales con controles de acceso, contraseñas y trazabilidad.
c) Cuando los expedientes ingresen al Archivo de Concentración, su acceso continuará restringido y sujeto a registro de consulta.
d) Para transferencias al Archivo Histórico, deberá evaluarse si procede **el anonimato** total o parcial cuando el documento no pueda divulgarse sin afectar derechos fundamentales.
e) Ningún dato de denunciantes, testigos, investigadores o personal involucrado podrá divulgarse sin base legal.
f) Los resultados de pruebas de confianza se consideran datos personales sensibles y su tratamiento estará estrictamente regulado; su acceso será autorizado únicamente para fines disciplinarios y administrativos previstos por ley.
g) Todo préstamo o acceso temporal a expedientes deberá quedar registrado en los instrumentos de control archivístico del IAIP.

Artículo 8. Uso, Acceso y Limitaciones. El uso y acceso a datos personales dentro de la DIDADPOL deberá cumplir las siguientes disposiciones:

- El acceso se otorgará exclusivamente al personal cuya función institucional lo requiera.
- Todo acceso deberá ser proporcional y vinculado a una necesidad operativa, administrativa o investigativa.
- Los funcionarios que accedan a datos personales están obligados a guardar absoluta confidencialidad, incluso después de finalizada su relación laboral, de acuerdo al Acuerdo de Confidencialidad, suscrito.
- El personal no podrá copiar, divulgar, fotografiar o transmitir documentos que contengan datos personales sin autorización formal.

- El acceso público a la información se regirá por el régimen de clasificación de la LTAIP; cuando corresponda, se deberá generar una **versión pública**, asegurando el anonimato de datos personales.
- El uso de dispositivos externos (USB, discos duros portátiles, almacenamiento en la nube no autorizado) queda prohibido para documentos que contengan datos personales sin autorización expresa de la institución.
- Las áreas deberán llevar registros de acceso y uso cuando manipulen documentos que contengan datos sensibles, conforme a los lineamientos del IAIP.

Artículo 9. Digitalización, Seguridad y Almacenamiento. El uso y acceso a datos personales dentro de la DIDADPOL deberá cumplir las siguientes disposiciones:

a) El acceso se otorgará exclusivamente al personal cuya función institucional lo requiera.
b) Todo acceso deberá ser proporcional y vinculado a una necesidad operativa, administrativa o investigativa.
c) Los funcionarios que accedan a datos personales están obligados a guardar absoluta confidencialidad, incluso después de finalizada su relación laboral.
d) El personal no podrá copiar, divulgar, fotografiar o transmitir documentos que contengan datos personales sin autorización formal.
e) El acceso público a la información se regirá por el régimen de clasificación de la LTAIP; cuando corresponda, se deberá generar una versión pública, asegurando el anonimato de datos personales.
f) El uso de dispositivos externos (USB, discos duros portátiles, almacenamiento en la nube no autorizado) queda prohibido para documentos que contengan datos personales sin autorización expresa de la institución.
g) Las áreas deberán llevar registros de acceso y uso cuando manipulen documentos que contengan datos sensibles, conforme a los lineamientos del IAIP.

CAPÍTULO IV

CONSERVACIÓN, PLAZOS, EXPURGO Y ELIMINACIÓN

Artículo 10. Plazos de Conservación de los Datos Personales. La DIDADPOL conservará los datos personales únicamente por el tiempo necesario para cumplir con las finalidades del tratamiento y de acuerdo con los calendarios de conservación documental establecidos por la institución y aprobados conforme a los Lineamientos de Archivo del IAIP.

a) Los plazos de conservación deberán definirse considerando:
   - La finalidad del dato.
   - Requerimientos legales o administrativos.
   - Posibles auditorías internas o externas.
   - Tiempos de prescripción relacionados con responsabilidades disciplinarias o legales.
   - La naturaleza sensible del dato.

b) Ningún dato personal podrá conservarse indefinidamente sin justificación legal o archivística.

c) El plazo de conservación deberá ser informado al titular en los casos de recolección directa de datos (formularios, listas de asistencia, plataformas digitales).

d) Para documentos que contengan datos sensibles, el plazo será el indispensable para cumplir con la finalidad disciplinaria, administrativa o investigativa, respetando la seguridad y el carácter reservado de la documentación.

Artículo 11. Conservación Segura y Medidas de Protección. La conservación de documentos físicos y digitales que contengan datos personales deberá realizarse bajo estrictas medidas de seguridad, conforme a los riesgos asociados al tipo de información.

a) Los documentos físicos deberán:

- Guardarse en archivadores cerrados con llave.
- Estar bajo custodia de personal autorizado.
- Contar con control de acceso y registro cuando se trate de expedientes disciplinarios.

b) Los documentos digitales deberán:

- Almacenarse en sistemas institucionales con acceso restringido.
- Utilizar contraseñas seguras, cifrado y antivirus.
- Contar con respaldos periódicos.
- Mantener registros de acceso y modificación.

c) La Secretaría General, la Unidad de Gestión Documental y la Unidad de Tecnología de la Información, deberán garantizar la integridad, autenticidad y disponibilidad de los documentos durante su ciclo de vida.

Artículo 12. Expurgo, Depuración y Anonimato. El expurgo o eliminación de datos personales se realizará únicamente cuando:

1. Haya vencido el plazo de conservación establecido en los calendarios institucionales.
2. El dato personal haya perdido su valor administrativo, legal, técnico, fiscal o disciplinario.
3. Exista resolución o instrucción archivística que así lo disponga.

Todo proceso de expurgo deberá cumplir con:

a) **Autorización formal** de la Secretaría General, con visto bueno de la Unidad de Gestión Documental.
b) **Registro en los instrumentos archivísticos del IAIP**, especialmente el inventario de baja documental.

c) **Destrucción segura**, asegurando la eliminación irreversible del dato personal. Métodos aceptados: trituración, desintegración mecánica, borrado seguro, anonimatos certificados o equivalente aprobado.

Cuando corresponda conservar documentos para fines históricos o estadísticos:

- Se aplicará **el anonimato total o parcial**, eliminando elementos que permitan la identificación del titular.
- La anonimia deberá documentarse como procedimiento archivístico.

Artículo 13. Eliminación y Destrucción Segura de Datos Personales. La eliminación de documentos que contengan datos personales, físicos o digitales, deberá realizarse con métodos que garanticen la imposibilidad de recuperación o reconstrucción de la información.

a) Para documentos físicos, se utilizarán exclusivamente métodos de destrucción irreversible:
    - Trituración industrial.
    - Desintegración mecánica.
    - Corte transversal seguro.
b) Para documentos digitales, la eliminación deberá realizarse mediante:
    - Borrado seguro certificado.
    - Sobreescritura múltiple.
    - Eliminación criptográfica cuando proceda.
c) Ningún documento con datos personales podrá ser destruido sin dejar registro formal del procedimiento, conforme al inventario de baja documental y a los lineamientos del IAIP.
d) La eliminación deberá realizarse por personal autorizado y bajo supervisión documental.
e) Queda prohibida la eliminación informal o no autorizada de cualquier documento que contenga datos personales, especialmente de expedientes disciplinarios, resultados de pruebas de confianza o documentación sensible.

CAPÍTULO V

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Artículo 14. Derechos de Los Titulares (Arco + Revocación). Todo titular cuyos datos personales sean tratados por la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) tiene los siguientes derechos:

a) **Derecho de Acceso:** Conocer si sus datos personales están siendo tratados por la DIDADPOL, obtener descripción del tipo de información procesada y comprender la finalidad del tratamiento. Este derecho se ejercerá sin perjuicio de las restricciones aplicables cuando la información forme parte de expedientes disciplinarios en curso o documentos clasificados conforme a la LTAIP.

b) **Derecho de Rectificación:** Solicitar la corrección, actualización o completación de datos personales inexactos, incompletos o desactualizados que obren en posesión de la DIDADPOL.

c) **Derecho de Cancelación:** Solicitar la eliminación de datos personales cuando:

- Haya vencido el plazo de conservación;
- Los datos ya no sean necesarios para la finalidad original;
- Haya concluido el proceso administrativo o disciplinario sin requerir su conservación;
- Se verifique un tratamiento indebido.

Este derecho se aplicará conforme a los calendarios de conservación y las normas archivísticas del IAIP.

d) **Derecho de Oposición:** Oponerse, por causa legítima, al tratamiento de sus datos personales.

No procederá cuando el tratamiento sea indispensable para el cumplimiento de las funciones disciplinarias, administrativas o legales de la DIDADPOL.

e) **Derecho de Revocación del Consentimiento:** Cuando el tratamiento se base en consentimiento (p. ej., listas de asistencia o usos voluntarios), el titular podrá

revocarlo en cualquier momento, sin efectos retroactivos sobre los tratamientos ya realizados legítimamente.

f) **Derecho a ser Informado:** Recibir información clara, precisa y verificable sobre el tratamiento de sus datos personales, incluyendo finalidad, plazo de conservación, base legal y datos del responsable del tratamiento.

Artículo 15.- Restricciones al Ejercicio de los Derechos. Los derechos establecidos en el artículo anterior podrán ser limitados únicamente cuando:

1. La información forme parte de un expediente disciplinario en curso.
2. Exista una investigación activa cuya integridad pueda verse comprometida.
3. La divulgación pueda afectar seguridad institucional, pública o nacional.
4. Se trate de datos personales de terceros involucrados.
5. La documentación esté clasificada como reservada o confidencial según la LTAIP.
6. Exista resolución administrativa o judicial que impida su entrega.

La DIDADPOL deberá garantizar que cualquier limitación sea motivada, documentada y proporcional.

Artículo 16. Procedimiento para Ejercer los Derechos.

a) **Presentación de la solicitud:** El titular deberá presentar su solicitud por escrito, de manera física o electrónica, ante el Oficial de Información Pública de la DIDADPOL o el responsable designado para la atención de derechos de titulares.

b) **Contenido mínimo de la solicitud:**
   - Nombre completo del titular.
   - Número de identidad (solo para fines de verificación).
   - Descripción clara del derecho que desea ejercer.
   - Indicación de los datos o documentos involucrados.
   - Medio para recibir notificaciones.

c) **Plazo de respuesta:** La DIDADPOL deberá responder en un plazo máximo de **10 días hábiles,** prorrogable por hasta **10 días hábiles adicionales** cuando existan circunstancias justificadas, debidamente notificadas al titular.

d) **Verificación de identidad:** Se exigirá verificación de identidad para garantizar la protección de datos personales y evitar divulgaciones indebidas.

e) **Notificación de resolución:** La respuesta será entregada por escrito, física o digitalmente, indicando:

- La decisión adoptada.
- Fundamento legal.
- Procedimientos aplicados.
- Medios para presentar recursos ante el IAIP si el titular no está conforme.

f) **Registro documental:** Toda solicitud y resolución deberá incorporarse a los registros institucionales y documentarse en instrumentos archivísticos conforme al Acuerdo SO-098-2019.

Artículo 17. Datos de Contacto del Responsable del Tratamiento. La DIDADPOL deberá mantener publicados en un lugar accesible (sitio web institucional, cartelera informativa o medios oficiales) los datos del responsable del tratamiento de datos personales, incluyendo:

- Identidad: Dirección de Asuntos Disciplinarios Policiales (DIDADPOL)
- Domicilio: Centro Cívico Gubernamental, Jose Cecilio del Valle, Torre 1 Piso 19
- Correo electrónico oficial: transparencia@didadpol.gob.hn
- Teléfono de contacto: 2242-8645 extensión 44160
- Horario de atención: 7:00 am a 3:00 pm

Estos datos deberán incluirse en todos los formularios, listas de asistencia y medios de recolección de datos personales.

CAPÍTULO VI

RESPONSABILIDADES INSTITUCIONALES

Artículo 18. Responsabilidades de la Secretaría General. La Secretaría General es la responsable directa de coordinar, supervisar y asegurar el cumplimiento de la presente Política de Privacidad y Protección de Datos Personales, con las siguientes funciones:

a) Emitir las directrices internas necesarias para la aplicación de esta política.
b) Aprobar, en coordinación con la Unidad de Gestión Documental, los instrumentos archivísticos institucionales (cuadros de clasificación, tablas de retención, inventarios, calendarios de conservación y expurgo).
c) Garantizar que todas las unidades administrativas cumplan con las obligaciones de protección de datos y gestión documental.
d) Autorizar la eliminación, digitalización o transferencia de documentos que contengan datos personales, conforme a la normativa del IAIP.
e) Coordinar con la Oficialía de Información Pública la aplicación de criterios de clasificación, reserva y confidencialidad.
f) Actuar como máxima instancia administrativa para resolver conflictos internos derivados del manejo de datos personales.

Artículo 19. Responsabilidades de La Unidad de Gestión Documental / Archivo. La Unidad de Gestión Documental y Archivo es la responsable técnica de la administración documental institucional y del tratamiento seguro de datos personales contenidos en documentos y expedientes. Sus funciones son:

a) Implementar y mantener actualizado el Sistema de Gestión Documental conforme a la LTAIP y al Acuerdo SO-098-2019.
b) Realizar clasificación, organización, foliación, registro, resguardo, transferencia, valoración documental y expurgo conforme a la normativa archivística.
c) Asegurar que las listas de asistencia en papel y documentos sensibles se custodien en espacios cerrados, con acceso restringido y controlado.

d) Supervisar los procesos de digitalización y velar por la destrucción segura e irreversible del soporte papel cuando corresponda.
e) Mantener inventarios documentales actualizados con trazabilidad de movimientos, préstamos y transferencias.
f) Garantizar la aplicación de calendarios de conservación y la ejecución de bajas documentales autorizadas.
g) Capacitar periódicamente al personal en materia de archivo, protección de datos y buenas prácticas de custodia documental.

Artículo 20. Responsabilidades del Oficial de Información Pública (OIP). El OIP es la unidad responsable del cumplimiento de la LTAIP y de velar por el correcto tratamiento de los datos personales y la transparencia institucional. Le corresponden las siguientes funciones:

a) Recibir, tramitar y responder solicitudes de ejercicio de derechos ARCO y revocación de consentimiento.
b) Informar al titular sobre sus derechos y los medios disponibles para ejercerlos.
c) Asegurar que todos los formularios, listas de asistencia y mecanismos de recolección incluyan la cláusula de deber de información requerida por el IAIP.
d) Determinar, justificar y registrar formalmente las restricciones de acceso cuando la información esté clasificada como reservada o confidencial.
e) Mantener actualizados los datos de contacto del responsable del tratamiento de datos personales.
f) Coordinar con Secretaría General y la Unidad de Gestión Documental la correcta aplicación de criterios de transparencia, reserva y protección de datos.
g) Llevar control estadístico y documental de las solicitudes recibidas y atendidas.

Artículo 21. Responsabilidades de la Unidad de Tecnologías de la Información. La Unidad de TI es responsable de garantizar la seguridad técnica de los sistemas, equipos y plataformas utilizados para almacenar, procesar o transmitir datos personales. Debe:

a) Asegurar que todos los sistemas utilizados para listas digitales, formularios, expedientes y bases de datos cuenten con medidas de seguridad, protocolos HTTPS, contraseñas robustas, control de accesos y registro de actividad.
b) Realizar respaldos periódicos cifrados y almacenados en espacios institucionales aprobados.
c) Mantener actualizados equipos, software, antivirus y sistemas de protección.
d) Garantizar el borrado seguro de información digital cuando corresponda su eliminación.
e) Verificar que proveedores externos de plataformas o aplicaciones cumplan estándares adecuados de privacidad y seguridad.
f) Apoyar la digitalización certificada y asegurar la integridad de imágenes digitales de expedientes.

Artículo 22. Responsabilidades de la Unidad de Control Interno. La Unidad de Control Interno supervisa la correcta aplicación de esta política como parte del Sistema de Control Interno Institucional. Sus funciones son:

a) Verificar periódicamente el cumplimiento de medidas de seguridad, clasificación, conservación y eliminación de documentos.
b) Evaluar riesgos asociados al manejo de datos personales y proponer controles preventivos.
c) Emitir recomendaciones obligatorias para corregir desviaciones detectadas.
d) Asegurar que la protección de datos personales se incorpore en matrices de riesgos institucionales.

Artículo 23. Responsabilidades de la Unidad de Auditoria Interna. La Auditoría Interna debe:

a) Auditar el cumplimiento de la Política de Privacidad y Protección de Datos Personales.

b) Revisar documentación relativa a digitalización, eliminación o transferencia de expedientes sensibles.
c) Verificar que se cumplan los principios de seguridad, minimización y trazabilidad en auditorías operativas.
d) Emitir informes que identifiquen hallazgos y recomendaciones obligatorias de mejora.

Artículo 24. Responsabilidades del Personal de la DIDADPOL. Todo servidor público de la DIDADPOL que tenga acceso, gestione o manipule datos personales debe:

a) Cumplir estrictamente esta política, la LTAIP y los lineamientos del IAIP.
b) Garantizar confidencialidad, integridad y protección de la información bajo su custodia.
c) Firmar los compromisos de confidencialidad correspondientes.
d) Reportar inmediatamente incidentes, pérdidas, accesos no autorizados o riesgos detectados.
e) Abstenerse de divulgar, copiar o usar información personal para fines distintos a los autorizados.

Artículo 25. Responsabilidades de las Jefaturas. Las jefaturas de cada unidad administrativa deberán:

a) Supervisar el cumplimiento de esta política en su área.
b) Velar porque el personal reciba capacitación adecuada sobre transparencia y protección de datos.
c) Garantizar el uso de formularios, listas y registros que cumplan con los principios de minimización y seguridad.
d) Facilitar la implementación de controles internos y atender recomendaciones de auditoría y control interno.

CAPÍTULO VII

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 26.- Disposiciones Generales de Seguridad. La Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) implementará medidas de seguridad técnicas, organizativas, físicas y administrativas adecuadas al riesgo, sensibilidad y volumen de los datos personales que administra, garantizando su confidencialidad, integridad, disponibilidad y trazabilidad.

Las medidas deberán aplicarse tanto a documentos físicos como digitales.

Artículo 27. Seguridad Física. La DIDADPOL deberá adoptar, como mínimo, las siguientes medidas:

a) **Control de acceso a áreas de archivo y resguardo:** Solo personal autorizado podrá ingresar a las áreas de archivo, con registro de acceso cuando existan expedientes disciplinarios, denuncias o documentos sensibles.
b) **Resguardo seguro de listas de asistencia:** Las listas en papel deberán estar bajo custodia inmediata de una persona designada durante el evento y almacenadas después en archivadores cerrados con llave.
c) **Protección de expedientes físicos:** Todos los expedientes investigativos, pruebas de confianza, dictámenes y documentación sensible deberán mantenerse en gavetas o depósitos bajo llave, protegidos contra humedad, incendio, manipulación indebida o acceso no autorizado.
d) **Vigilancia y resguardo de espacios críticos:** Las áreas que almacenen expedientes disciplinarios o bases de datos sensibles deberán estar bajo mecanismos de seguridad institucional (vigilancia, cámaras, controles físicos).

Artículo 28. Seguridad Organizativa y Administrativa.

a) **Designación de responsables:** Cada unidad deberá tener personal específicamente designado para el manejo de información sensible.
b) **Compromisos de confidencialidad:** Todo el personal con acceso a datos personales deberá firmar compromisos de confidencialidad y resguardar de forma estricta dicha información.
c) **Protocolos de préstamo, traslado y devolución:** Todo movimiento de expedientes deberá registrarse mediante inventarios, actas de préstamo o sistemas de control documental.
d) **Clasificación documental:** La información será clasificada conforme a la LTAIP y los lineamientos del IAIP (pública, reservada o confidencial).
e) **Capacitación periódica:** La DIDADPOL capacitará periódicamente al personal en temas de protección de datos, transparencia, archivo y seguridad.

Artículo 29. Seguridad Digital o Tecnológica. La Unidad de TI garantizará, como mínimo:

a) **Uso obligatorio de protocolos HTTPS** en formularios digitales, plataformas de registro y sistemas de almacenamiento.
b) **Control de accesos basado en roles**, con credenciales individuales, contraseñas robustas y renovación periódica.
c) **Cifrado de información** almacenada y en tránsito en sistemas que contengan expedientes disciplinarios, denuncias o listas digitales.
d) **Respaldos periódicos** cifrados y almacenados en infraestructura institucional autorizada.
e) **Actualización permanente** de antivirus, sistemas operativos y herramientas de seguridad.
f) **Borrado seguro de información digital**, utilizando métodos que impidan su recuperación.
g) **Auditoría y registro de accesos**, manteniendo evidencia de quién accede, cuándo y para qué.

Artículo 30. Seguridad en el Uso de Formularios y Listas de Asistencia.

a) **Minimización de datos:** Formularios físicos o digitales solo podrán solicitar nombre, apellido e institución, salvo necesidad justificada.

b) **Cláusula informativa obligatoria:** Todo formulario deberá incluir el texto: "Sus datos serán tratados por la DIDADPOL para gestionar su asistencia a este evento, basándonos en nuestro interés legítimo. Puede ejercer sus derechos en [correo]. Más información en nuestra política de privacidad disponible en [URL]."

c) **Consentimientos separados:** Cualquier consentimiento adicional (publicidad, comunicaciones) deberá estar en casilla independiente, desmarcada por defecto.

d) **Custodia física:** La hoja de asistencia no podrá circular entre participantes; deberá ser llenada o gestionada únicamente por personal autorizado.

e) **Digitalización segura:** En caso de digitalizar, deberá realizarse en equipo seguro y eliminar el papel mediante trituración o desintegración mecánica cuando corresponda.

Artículo 31. Conservación y Eliminación Segura.

a) **Plazos de conservación:** Se aplicarán los calendarios de conservación documental aprobados conforme a los lineamientos del IAIP y con criterios de minimización y riesgo.

b) **Destrucción segura:** Al finalizar el plazo, los documentos físicos deberán ser destruidos de forma irreversible (trituración, compactación o método certificado).

   La eliminación digital deberá realizarse mediante borrado seguro, certificando su irreversibilidad.

c) **Registro de eliminación:** Toda eliminación deberá documentarse en actas de baja documental, inventarios y reportes firmados por el personal autorizado.

d) **Anonimato en transferencias:** Cuando la normativa requiera transferir material histórico al Archivo Nacional, se deberá dar anonimato a la información que contenga datos personales salvo obligación legal en contrario.

Artículo 32. Protección de Información Especialmente Sensible. Debido a la naturaleza disciplinaria de la DIDADPOL, se aplicarán medidas reforzadas para información contenida en:

a) Expedientes investigativos.
b) Denuncias y datos de denunciantes.
c) Datos de denunciados, testigos y terceros.
d) Pruebas de confianza y sus resultados.
e) Dictámenes técnico-administrativos.
f) Información biométrica o de identificación especial.

Estas medidas incluyen:

a) Mayor restricción de acceso (solo personal estrictamente autorizado).
b) Prohibición absoluta de copias no autorizadas.
c) Accesos documentados, auditables y trazables.
d) Prohibición de divulgación sin fundamento legal.
e) Mayor responsabilidad administrativa ante filtraciones o mal uso.

Artículo 33. Gestión de Incidentes de Seguridad.

a) **Reporte obligatorio:** Todo incidente, pérdida, acceso no autorizado o riesgo deberá reportarse inmediatamente a la Secretaría General, TI y Control Interno.
b) **Evaluación del incidente:** Se analizará la naturaleza del evento, los datos comprometidos y el impacto institucional.
c) **Medidas correctivas:** Se aplicarán medidas inmediatas para mitigar daños, bloquear accesos, reforzar controles y evitar reincidencias.

d) **Documentación del incidente:** Todo incidente deberá registrarse y conservarse en expediente especial para auditoría y seguimiento.

CAPÍTULO VIII

CONSERVACIÓN, TRANSFERENCIA Y ELIMINACIÓN DOCUMENTAL

Artículo 34. Disposiciones Generales. La gestión documental de la DIDADPOL se regirá estrictamente por la Ley de Transparencia y Acceso a la Información Pública (LTAIP), el Acuerdo SO-098-2019 del IAIP (Lineamientos de Archivo), la Política de Archivo Institucional y la presente Política de Privacidad.

Toda actividad de conservación, valoración, expurgo, transferencia o eliminación de documentos deberá integrar criterios de protección de datos personales, garantizando la reducción de riesgos y la protección de la información sensible.

Artículo 35. Calendarios de Conservación y Expurgo.

a) La DIDADPOL contará con un **Calendario de Conservación y Expurgo** aprobado por la Secretaría General y la Unidad de Gestión Documental, conforme a los lineamientos del IAIP.
b) Cada serie documental deberá tener definido su tiempo de conservación según su valor administrativo, legal, fiscal, disciplinario o histórico.
c) Los expedientes con datos personales sensibles (investigaciones, denuncias, pruebas de confianza) deberán tener plazos de conservación reforzados y ser evaluados antes de su transferencia o eliminación.
d) Ningún documento podrá ser destruido sin estar incluido en el calendario y sin cumplir con los procedimientos de baja documental.

CAPÍTULO IX

CONSERVACIÓN, TRANSFERENCIA, VALORACIÓN Y ELIMINACIÓN DOCUMENTAL

Artículo 36. Disposiciones Generales. La gestión documental de la DIDADPOL se regirá estrictamente por la Ley de Transparencia y Acceso a la Información Pública (LTAIP), el Acuerdo SO-098-2019 del IAIP (Lineamientos de Archivo), la Política de Archivo Institucional y la presente Política de Privacidad.

Toda actividad de conservación, valoración, expurgo, transferencia o eliminación de documentos deberá integrar criterios de protección de datos personales, garantizando la reducción de riesgos y la protección de la información sensible.

Artículo 37. Calendarios de Conservación y Expurgo.

1. La DIDADPOL contará con un **Calendario de Conservación y Expurgo** aprobado por la Secretaría General y la Unidad de Gestión Documental, conforme a los lineamientos del IAIP.
2. Cada serie documental deberá tener definido su tiempo de conservación según su valor administrativo, legal, fiscal, disciplinario o histórico.
3. Los expedientes con datos personales sensibles (investigaciones, denuncias, pruebas de confianza) deberán tener plazos de conservación reforzados y ser evaluados antes de su transferencia o eliminación.
4. Ningún documento podrá ser destruido sin estar incluido en el calendario y sin cumplir con los procedimientos de baja documental.

Artículo 38. Transferencia Documental. (Archivo de Trámite, Archivo de Concentración y Archivo Histórico)

1. Cada área generadora deberá transferir sus documentos al **Archivo de Concentración** conforme a los tiempos definidos.

2. La transferencia al **Archivo Histórico** solo procederá cuando el documento haya agotado su valor administrativo, disciplinario o legal.
3. Toda transferencia deberá documentarse mediante actas o inventarios aprobados por la Unidad de Gestión Documental.
4. Antes de transferir documentos históricos, deberá **anonimizarse** cualquier dato personal que no sea indispensable para su valor histórico, salvo disposición legal expresa que exija mantener la identidad.

Artículo 39. Valoración Documental.

1. La Unidad de Gestión Documental efectuará procesos de valoración periódica para determinar si un documento:

    a) conserva valor administrativo o legal,
    b) debe transferirse al archivo histórico, o
    c) debe someterse a expurgo o eliminación.

2. En expedientes investigativos, pruebas de confianza y documentación disciplinaria, la valoración deberá considerar:
    - riesgos para los derechos de las personas,
    - sensibilidad de la información,
    - impacto institucional y legal,
    - obligaciones de confidencialidad.
3. Toda valoración deberá quedar documentada y fundamentada.

Artículo 40. Eliminación o Baja Documental.

1. La eliminación de documentos se realizará únicamente cuando haya vencido su plazo de conservación y tras una valoración formal.
2. La Unidad de Gestión Documental elaborará un **Acta de Baja Documental**, firmada por:

- Secretaría General,
- Unidad de Gestión Documental,
- Unidad de Control Interno.

3. No podrá eliminarse ningún documento que:

   a) esté sujeto a auditoría, inspección o investigación,

   b) esté requerido como evidencia,

   c) tenga valor histórico,

   d) contenga datos personales cuya eliminación requiera medidas especiales.

Artículo 41. Eliminación Segura de Documentos Físicos.

1. La destrucción deberá ser **irreversible**, mediante:
   - trituración cruzada,
   - compactación industrial,
   - desintegración mecánica,
   - o métodos equivalentes certificados.
2. Se prohíbe la eliminación mediante:
   - quema,
   - disposición en basura ordinaria,
   - o métodos que permitan reconstrucción parcial.
3. La eliminación deberá realizarse en presencia de personal autorizado y dejar constancia documental.

Artículo 42. Eliminación Segura de Información Digital.

1. La eliminación digital deberá garantizar que la información no pueda recuperarse mediante:
   - sobreescritura segura,
   - borrado criptográfico,
   - o destrucción del soporte cuando sea necesario.

2. La Unidad de TI certificará el proceso mediante documento técnico que deberá adjuntarse al Acta de Baja Documental.
3. En ningún caso se permitirá:
    - formateo simple,
    - borrado estándar,
    - eliminación sin registro.

Artículo 43. Registro Obligatorio de Baja Documental.

1. Toda eliminación deberá registrarse en el **Inventario de Baja Documental** institucional.
2. Dicho registro contendrá:
    - serie documental,
    - volumen,
    - fecha de creación y eliminación,
    - método utilizado,
    - responsables,
    - observaciones especiales.
3. El registro será auditable por el IAIP, Auditoría Interna y Control Interno.

Artículo 44. Prohibición de Eliminación Irregular. Se prohíbe la destrucción, alteración, ocultamiento o eliminación de documentos fuera de los procedimientos establecidos.

Toda eliminación irregular constituye falta grave y puede generar responsabilidad administrativa, civil o penal.

Artículo 45. Integración con la Protección de Datos Personales. Los procesos de conservación, transferencia y eliminación deberán:

1. Respetar el principio de minimización.

2. Evitar conservar información personal por periodos mayores a los necesarios.
3. Proteger especialmente los datos sensibles.
4. Garantizar que toda eliminación reduzca el riesgo al titular de los datos.
5. Priorizar la seguridad, trazabilidad y documentación de cada etapa.

Artículo 46. Verificación y Auditoría.

1. La Unidad de Control Interno y la Auditoría Interna verificarán anualmente el cumplimiento de los lineamientos establecidos en este capítulo.
2. Podrán emitir recomendaciones, observaciones y medidas correctivas obligatorias.
3. Los informes deberán elevarse a la Máxima Autoridad para su seguimiento.

CAPÍTULO X

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Artículo 47. Derechos Fundamentales de los Titulares. Toda persona cuyos datos personales sean recolectados, registrados, almacenados, utilizados, transmitidos, conservados o eliminados por la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) tiene los siguientes derechos:

1. **Derecho de Acceso:** A conocer si la DIDADPOL trata sus datos personales, la naturaleza de dichos datos, su origen, finalidad, destinatarios previstos y el tiempo estimado de conservación.
2. **Derecho de Rectificación:** A solicitar la corrección de datos personales inexactos, incompletos o desactualizados.
3. **Derecho de Cancelación:** A solicitar la supresión de sus datos personales cuando:

   a) hayan dejado de ser necesarios para la finalidad por la que fueron recabados,

b) haya vencido el plazo de conservación,

c) el tratamiento sea ilícito,

d) así lo determine una autoridad competente.

No aplicará cuando la conservación sea necesaria para fines disciplinarios, legales, probatorios o en cumplimiento de una obligación institucional.

4. **Derecho de Oposición:** A oponerse al tratamiento de sus datos por causa legítima, salvo cuando el tratamiento sea indispensable para el ejercicio de la función disciplinaria, la seguridad interna o el interés público institucional.
5. **Derecho de Revocación del Consentimiento:** A retirar el consentimiento otorgado para tratamientos basados en dicha base legal (ej.: comunicaciones, finalidades adicionales), sin efectos retroactivos.
6. **Derecho a la Información:** A ser informado sobre el tratamiento de sus datos en formularios, expedientes, sistemas digitales o listas de asistencia.
7. **Derecho a la Protección de Datos Sensibles:** A un tratamiento reforzado cuando se trate de resultados de pruebas de confianza, datos biométricos, información investigativa, denuncias o datos de terceros involucrados.

Artículo 48. Ejercicio de los Derechos.

a) Los derechos podrán ejercerse mediante solicitud presentada en:
b) Oficinas de la DIDADPOL,
c) Correo institucional del Responsable del Tratamiento de Datos,
d) El Sistema de Acceso a la Información Pública habilitado por el IAIP.
e) La solicitud deberá contener:
   - Identificación del titular
   - Descripción clara del derecho que desea ejercer
   - Medios para recibir respuesta
   - Documentación probatoria cuando corresponda.
f) La DIDADPOL proporcionará formularios para facilitar el ejercicio de derechos, tanto en formato físico como digital.

Artículo 49. Plazos de Respuesta.

a) La DIDADPOL deberá responder toda solicitud en un plazo máximo de **10 días hábiles**, prorrogables por 5 días adicionales en casos complejos.
b) La prórroga deberá ser debidamente motivada y comunicada al solicitante.
c) La falta de respuesta injustificada podrá ser considerada incumplimiento sujeto a responsabilidad conforme a la LTAIP.

Artículo 50. Restricciones al Ejercicio de los Derechos. Los derechos de acceso, rectificación, cancelación, oposición o revocación podrán denegarse total o parcialmente cuando:

1. Su ejercicio comprometa una investigación disciplinaria en curso.
2. Exista obligación legal de conservar los datos.
3. La información forme parte de un expediente en reserva conforme a la LTAIP.
4. Se trate de datos sobre terceros cuya identidad debe protegerse (denunciantes, testigos, víctimas).
5. Exista orden o requerimiento de autoridad competente que limite el acceso.

Artículo 51. Gratuidad. El ejercicio de los derechos será gratuito para el titular, salvo que:

1. requiera copias físicas extensas,
2. solicite reproducción certificada con costos asociados,
3. presente solicitudes manifiestamente infundadas o repetitivas.

En tales casos podrán cobrarse únicamente los costos estrictamente necesarios.

Artículo 52. Deber de Información. La DIDADPOL garantizará que toda recolección de datos personales incluya una cláusula informativa clara que indique:

a) identidad y datos de contacto del responsable del tratamiento,
b) finalidad del tratamiento,
c) base legal,
d) destinatarios previstos,
e) plazo de conservación,
f) derechos del titular y cómo ejercerlos,
g) si los datos serán usados para finalidades secundarias,
h) si se requiere consentimiento adicional.

Artículo 53. Registro y Trazabilidad de Solicitudes.

a) La institución llevará un **Registro de Solicitudes de Derechos de Titulares**, que deberá incluir:
   - fecha de presentación,
   - tipo de derecho solicitado,
   - estado de la solicitud,
   - acciones realizadas,
   - fecha y contenido de la respuesta.

b) El registro será auditable por el IAIP, Auditoría Interna y Control Interno.

Artículo 54. Garantías Especiales para Información Sensible.

a) Las solicitudes relacionadas con información de expedientes investigativos o disciplinarios deberán recibir un tratamiento reforzado para evitar:
   - riesgos a denunciantes,
   - afectación de investigaciones,
   - exposición indebida de terceros.

b) Cuando sea posible, la DIDADPOL brindará acceso **parcial**, aplicando técnicas de:
   - tarja,
   - supresión de datos,
   - proceso de anonimato,

- versiones públicas.

CAPÍTULO XI

RESPONSABLES DEL TRATAMIENTO Y OBLIGACIONES INTERNAS

Artículo 55. Responsable del Tratamiento de Datos Personales. La Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) actúa como Responsable del Tratamiento de Datos Personales, siendo la autoridad obligada a garantizar la protección, confidencialidad, integridad, disponibilidad y uso legítimo de los datos personales que administra en el ejercicio de sus funciones disciplinarias y administrativas.

Artículo 56. Secretaría General. La Secretaría General tendrá las siguientes responsabilidades:

a) Supervisar la implementación de esta Política en toda la Institución.
b) Garantizar que las unidades cumplan con la LTAIP y los lineamientos del IAIP.
c) Autorizar las transferencias documentales, expurgos y procesos de eliminación.
d) Validar las actas de baja documental y los inventarios oficiales.
e) Coordinar con el Oficial de Información Pública la atención a solicitudes de derechos de titulares.
f) Asegurar que se publiquen y mantengan actualizados los datos de contacto del Responsable del Tratamiento.

Artículo 57. Unidad de Gestión Documental. La Unidad de Gestión Documental será responsable de:

a) Cumplir y hacer cumplir los Lineamientos de Archivo del IAIP (Acuerdo SO-098-2019).
b) Aplicar el Cuadro de Clasificación Documental, inventarios, calendarios de conservación y expurgo.

c) Custodiar, organizar y conservar adecuadamente documentos físicos y electrónicos.
d) Verificar la aplicación de medidas de seguridad reforzadas para expedientes investigativos, denuncias y datos sensibles.
e) Documentar transferencias, préstamos, devoluciones y movimientos de expedientes.
f) Elaborar actas de baja documental y registros de eliminación segura.
g) Colaborar con TI en la preservación y resguardo digital.

Artículo 58. Oficial de Información Pública (OIP). El Oficial de Información Pública deberá:

a) Gestionar el derecho de acceso a la información pública conforme a la LTAIP.
b) Atender solicitudes de derechos de titulares de datos personales.
c) Emitir versiones públicas de documentos, aplicando tarja o anonimización cuando corresponda.
d) Asesorar a las unidades sobre clasificación de información (pública, reservada o confidencial).
e) Garantizar el registro y trazabilidad de solicitudes.
f) Coordinar con Gestión Documental y Control Interno para asegurar respuestas dentro de los plazos legales.
g) Reportar al IAIP cualquier incumplimiento relevante cuando sea exigido por ley.

Artículo 59. Unidad de Tecnologías de la Información (TI). TI será responsable de:

a) Implementar las medidas tecnológicas de seguridad digital establecidas en esta Política.
b) Mantener sistemas, plataformas y bases de datos en ambientes seguros (HTTPS, cifrado, backups, control de accesos).
c) Registrar accesos, monitorear actividad y reportar incidentes digitales.
d) Garantizar la eliminación segura de información digital.

e) Evaluar herramientas y proveedores para asegurar el cumplimiento de estándares de privacidad.
f) Resguardar bases de datos sensibles (expedientes, denuncias, listas digitalizadas).
g) Apoyar procesos de digitalización con criterios de seguridad documental.

Artículo 60. Unidad de Control Interno. Control Interno deberá:

a) Verificar el cumplimiento de esta Política de manera periódica.
b) Evaluar riesgos relacionados con el tratamiento de datos personales y la gestión documental.
c) Emitir recomendaciones obligatorias para corregir incumplimientos o debilidades.
d) Supervisar procesos de préstamo, traslado, custodia y devolución de expedientes.
e) Revisar trámites de baja documental y eliminación segura.

Artículo 61. Unidad de Auditoría Interna. Auditoría Interna será responsable de:

a) Realizar auditorías anuales sobre el manejo de datos personales.
b) Verificar el cumplimiento de la LTAIP, el Acuerdo SO-098-2019 y esta Política.
c) Emitir informes con hallazgos y recomendaciones obligatorias.
d) Revisar especialmente:
    1. custodia de expedientes investigativos,
    2. manejo de información sensible,
    3. listas de asistencia,
    4. formularios digitales,
    5. sistemas de acceso y control.
e) Reportar hallazgos a la Máxima Autoridad y, si la normativa lo exige, al IAIP.

Artículo 62. Unidades Generadoras de Documentos. Toda unidad que genere o administre datos personales deberá:

a) Aplicar los principios y obligaciones de esta Política.
b) Usar únicamente los formularios aprobados que incluyan cláusulas informativas.
c) Limitar la recolección a los datos estrictamente necesarios.
d) Evitar la reproducción innecesaria de expedientes o información sensible.
e) Reportar incidentes de seguridad.
f) Remitir periódicamente documentos al Archivo de Concentración.
g) Garantizar la custodia temporal adecuada de documentos de trámite.

Artículo 63. Obligaciones de Todo el Personal. Todo funcionario o empleado de la DIDADPOL deberá:

a) Tratar los datos personales conforme a los principios de lealtad, licitud, minimización y confidencialidad.
b) Evitar divulgar información sin autorización expresa.
c) Firmar compromisos de confidencialidad cuando corresponda.
d) Reportar irregularidades, incidentes o pérdidas de información.
e) Cumplir las instrucciones del Responsable del Tratamiento.
f) Custodiar adecuadamente cualquier documento o expediente bajo su responsabilidad.
g) Participar en capacitaciones institucionales sobre privacidad y archivo.

Artículo 64. Responsabilidad Institucional. Las violaciones a esta Política pueden derivar en responsabilidades:

- administrativas,
- civiles,
- disciplinarias,

- o penales,

conforme a la normativa hondureña, la LTAIP, la LOTSC y demás leyes aplicables.

CAPÍTULO XII

PUBLICACIÓN, VIGENCIA, REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

Artículo 65. Publicación y Difusión.

a) La presente Política de Privacidad y Protección de Datos Personales será publicada en:
   - El sitio web oficial de la DIDADPOL,
   - El Portal Único de Transparencia administrado por el IAIP,
   - Las instalaciones físicas de la institución, en un lugar visible para el público.

b) La Secretaría General garantizará que la política esté disponible, accesible y actualizada para todas las personas interesadas.

c) Las unidades internas deberán difundir esta política entre su personal, asegurando su comprensión y aplicación.

Artículo 66. Entrada en Vigencia.

a) La presente Política entrará en vigencia a partir de la fecha de su aprobación mediante Acuerdo emitido por la Dirección de la DIDADPOL.

b) A partir de su entrada en vigor, todas las unidades deberán adecuar sus procedimientos, formularios, sistemas y prácticas al contenido de esta Política.

c) Cualquier normativa interna existente que contradiga esta Política quedará sin efecto en lo relativo al tratamiento y protección de datos personales.

Artículo 67. Revisión Periódica.

a) La política será revisada **al menos una vez cada dos años** o antes si:
   - se producen reformas a la LTAIP,
   - se emiten nuevos lineamientos del IAIP,
   - cambian las funciones o atribuciones de la DIDADPOL,
   - se identifican riesgos relevantes o incidentes de seguridad.

b) La revisión estará a cargo de:
   - Secretaría General,
   - Unidad de Gestión Documental,
   - Oficial de Información Pública,
   - Unidad de TI,
   - Unidad de Control Interno.

Artículo 68. Actualización y Mejora Continua.

a) Toda modificación, actualización o ampliación deberá aprobarse mediante Acuerdo emitido por la Dirección de la DIDADPOL.

b) El proceso de actualización deberá considerar:
   - avances tecnológicos,
   - mejores prácticas internacionales,
   - recomendaciones de Auditoría Interna,
   - resoluciones u observaciones del IAIP.

c) Las unidades deberán recibir capacitación cuando se realicen actualizaciones que afecten sus actividades.

Art. 69.- Aplicación Preferente. En caso de conflicto entre esta Política y cualquier otro procedimiento interno, prevalecerá esta Política en todo lo relativo al tratamiento, protección, conservación y eliminación de datos personales.

Artículo 70. Responsabilidad por Incumplimiento.

a) El incumplimiento de las disposiciones contenidas en esta Política constituye falta administrativa y podrá generar:
   - sanciones internas,
   - responsabilidad disciplinaria,
   - responsabilidad civil o penal,

   conforme a la normativa aplicable.

b) La DIDADPOL podrá remitir al IAIP los casos de incumplimiento cuando así lo exija la LTAIP o cuando el Instituto lo requiera.

Artículo 71. Disposiciones Finales.

a) Todo personal de la Institución deberá actuar con apego a los principios de legalidad, lealtad, transparencia, confidencialidad y protección integral de los datos personales.

b) La presente Política forma parte obligatoria del Sistema de Gestión Documental de la DIDADPOL y deberá aplicarse de manera armónica con la Política de Archivo Institucional.

c) Las situaciones no previstas en esta Política serán resueltas por la Dirección de la DIDADPOL conforme al marco jurídico aplicable y a los lineamientos del IAIP.

Abogada Silvia Marcela Amaya Escoto
Directora DIDADPOL

Abogada Sharon Ivette Bardales Rubio
Secretaria General DIDADPOL