



ATRIRD

ASOCIACIÓN TRIBUTARIA DE LA
REPÚBLICA DOMINICANA

POLÍTICAS Y PROCEDIMIENTOS INSTITUCIONALES

*Integridad, Independencia y Excelencia Profesional
al Servicio de los Contribuyentes, la Ley y la Sociedad*

Aprobado el mediante acta de Asamblea General del 31 de agosto del 2026
y registrada en la Dirección del Registro Civil y Conservaduría de Hipotecas de
Santo Domingo el 7 de septiembre del 2026 con el registro No. 2026-56151



INTEGRIDAD



OBJETIVIDAD



INDEPENDENCIA



COMPETENCIA
Y DEBIDO CUIDADO



CONFIDENCIALIDAD



CONDUCTA
PROFESIONAL

Compromiso con el interés público

Ética profesional que fortalece la confianza,
el Estado de Derecho y el desarrollo sostenible.

2026

**ASOCIACIÓN TRIBUTARIA DE LA
REPÚBLICA DOMINICANA, INC.**

**POLÍTICAS
Y
PROCEDIMIENTOS INSTITUCIONALES**

**Aprobado el mediante acta de Asamblea General del 31 de agosto del 2026
y registrada en la Dirección del Registro Civil y Conservaduría de Hipotecas de Santo
Domingo el 7 de septiembre del 2026 con el registro No. 2026-56151**

*Este documento excluye de su contenido los Estatutos, el Código de Ética y el Reglamento Disciplinario.
Solo reúne exclusivamente las políticas, reglamento y los procedimientos institucionales*

CLÁUSULA TRANSVERSAL DE LEGALIDAD, DERECHOS FUNDAMENTALES Y PREVALENCIA NORMATIVA

Todos los documentos reunidos en este volumen se interpretarán y aplicarán de conformidad con la Constitución de la República Dominicana, los tratados internacionales de derechos humanos vinculantes para la República Dominicana, la legislación civil, comercial, penal, procesal, tributaria, de asociaciones sin fines de lucro, prevención de lavado de activos, protección de datos personales, protección de consumidores y usuarios y demás normas imperativas que resulten aplicables.

Ninguna disposición interna podrá limitar derechos fundamentales, atribuir a ATRIRD potestades reservadas a autoridades públicas, imponer deberes de denuncia, suministro o revelación de información no exigidos por ley, desconocer el secreto profesional o la confidencialidad legalmente protegida, ni alterar las garantías del debido proceso.

Ante conflicto con una norma imperativa o tratado vinculante aplicable, prevalecerá la norma de superior jerarquía. Los estándares, guías y buenas prácticas internacionales no vinculantes tendrán valor orientador y no crearán por sí solos obligaciones, infracciones, sanciones ni competencias.

Los documentos incluidos están organizados por Títulos y los mismos corresponden a la:

1. Política Institucional de Sostenibilidad, Responsabilidad Social y Gobernanza (ESG)
2. Política de Protección, Gobernanza y uso Ético de la Información
3. Política Institucional de uso Responsable de Inteligencia Artificial y Herramientas Digitales
4. Programa institucional de cumplimiento normativo y prevención de riesgos penales
5. Procedimiento Institucional de Respuesta a Incidentes de Seguridad de la Información

Revisión normativa transversal. Las referencias legales contenidas o implícitas en estos instrumentos deberán entenderse hechas a sus versiones vigentes, modificaciones y normas complementarias. Antes de adoptar protocolos que afecten derechos, información personal, obligaciones tributarias, prevención de lavado de activos, consumidores, relaciones contractuales o procedimientos disciplinarios, ATRIRD deberá verificar la normativa vigente y, cuando la materia lo justifique, obtener revisión jurídica. Los cambios legislativos posteriores prevalecerán sobre cualquier disposición interna incompatible.

Índice

CLÁUSULA TRANSVERSAL DE LEGALIDAD, DERECHOS FUNDAMENTALES Y PREVALENCIA NORMATIVA.....	2
<u>POLÍTICA INSTITUCIONAL DE SOSTENIBILIDAD, RESPONSABILIDAD SOCIAL Y GOBERNANZA (ESG)</u>	<u>7</u>
<u>I. OBJETO, ALCANCE Y PRINCIPIOS.....</u>	<u>8</u>
<u>II. DIMENSIONES AMBIENTALES Y SOCIALES.....</u>	<u>8</u>
<u>III. GOBERNANZA INSTITUCIONAL, DE LA INFORMACIÓN TECNOLÓGICA Y SEGURIDAD.....</u>	<u>9</u>
<u>IV. INTELIGENCIA ARTIFICIAL Y TECNOLOGÍAS EMERGENTES</u>	<u>10</u>
<u>V. OBJETIVOS, RESPONSABILIDADES E INDICADORES</u>	<u>10</u>
<u>VI. INTEGRIDAD DE LAS DECLARACIONES DE SOSTENIBILIDAD.....</u>	<u>10</u>
<u>VII. REFERENCIAS Y ESTÁNDARES INTERNACIONALES</u>	<u>11</u>
<u>VIII. SUPERVISIÓN, SEGUIMIENTO Y REVISIÓN.....</u>	<u>11</u>
<u>IX. INTERPRETACIÓN Y SALVAGUARDA JURÍDICA</u>	<u>12</u>
<u>X. INTEGRACIÓN CON EL SISTEMA DE GOBERNANZA ÉTICA DE ATRIRD</u>	<u>12</u>
<u>XI. ENTRADA EN VIGOR.....</u>	<u>12</u>
<u>POLÍTICA DE PROTECCIÓN, GOBERNANZA Y USO ÉTICO DE LA INFORMACIÓN.....</u>	<u>13</u>
<u>I. OBJETO, ALCANCE Y PRINCIPIOS</u>	<u>14</u>
<u>II. CLASIFICACIÓN DE LA INFORMACIÓN.....</u>	<u>15</u>
<u>III. CONTROL DE ACCESO</u>	<u>15</u>
<u>IV. CICLO DE VIDA DE LA INFORMACIÓN</u>	<u>15</u>
<u>V. USO ÉTICO DE LA INFORMACIÓN</u>	<u>16</u>

<u>VI. INFORMACIÓN TRIBUTARIA Y SECRETO PROFESIONAL</u>	<u>16</u>
<u>VIII. SERVICIOS EN LA NUBE.....</u>	<u>17</u>
<u>IX. ANONIMIZACIÓN Y SEUDONIMIZACIÓN.....</u>	<u>18</u>
<u>X. INCIDENTES DE INFORMACIÓN Y SEGURIDAD</u>	<u>18</u>
<u>XI. CONTINUIDAD, RESPALDO Y RECUPERACIÓN</u>	<u>18</u>
<u>XII. INTELIGENCIA ARTIFICIAL Y HERRAMIENTAS DIGITALES</u>	<u>19</u>
<u>XIV. RESPONSABILIDADES Y GOBERNANZA.....</u>	<u>20</u>
<u>XV. FORMACIÓN, SUPERVISIÓN Y MEJORA CONTINUA</u>	<u>20</u>
<u>XVI. RELACIÓN CON EL RÉGIMEN ÉTICO Y DISCIPLINARIO</u>	<u>20</u>
<u>XVII. DISPOSICIONES FINALES</u>	<u>20</u>
<u>POLÍTICA INSTITUCIONAL DE USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL Y HERRAMIENTAS DIGITALES.....</u>	<u>22</u>
<u>I. OBJETO Y FINALIDAD</u>	<u>23</u>
<u>II. ÁMBITO DE APLICACIÓN.....</u>	<u>24</u>
<u>III. PRINCIPIOS RECTORES</u>	<u>24</u>
<u>IV. INFORMACIÓN, CONFIDENCIALIDAD Y SEGURIDAD</u>	<u>25</u>
<u>V. USO PROFESIONAL EN MATERIA TRIBUTARIA.....</u>	<u>25</u>
<u>VI. TRANSPARENCIA Y TRAZABILIDAD</u>	<u>26</u>
<u>VII. USOS PROHIBIDOS</u>	<u>26</u>
<u>VIII. PROPIEDAD INTELECTUAL.....</u>	<u>27</u>
<u>X. INTELIGENCIA ARTIFICIAL Y PROCEDIMIENTOS DISCIPLINARIOS</u>	<u>27</u>
<u>XI. FORMACIÓN Y CULTURA DIGITAL.....</u>	<u>28</u>

XII. INCIDENTES, ERRORES Y RESPUESTA	28
XIII. GOBERNANZA Y RESPONSABILIDADES.....	28
XIV. RELACIÓN CON EL RÉGIMEN ÉTICO Y DISCIPLINARIO	28
XV. INTERPRETACIÓN Y SALVAGUARDAS	29
XVI. DISPOSICIONES FINALES.....	29
PROGRAMA INSTITUCIONAL DE CUMPLIMIENTO NORMATIVO Y PREVENCIÓN DE RIESGOS PENALES	30
PREÁMBULO.....	31
I. DISPOSICIONES GENERALES.....	31
II. GOBERNANZA DEL PROGRAMA	32
III. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS PENALES	33
IV. CONTROLES PREVENTIVOS.....	33
V. FORMACIÓN Y CULTURA DE CUMPLIMIENTO.....	34
VI. CANALES DE ALERTA Y PROTECCIÓN	34
VII. RECEPCIÓN, INVESTIGACIÓN Y RESPUESTA	35
VIII. DOCUMENTACIÓN, SEGUIMIENTO Y MEJORA.....	36
IX. DISPOSICIONES FINALES	36
PROCEDIMIENTO INSTITUCIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	38
I. OBJETO, PRINCIPIOS Y CONCEPTO	39
II. INFORMACIÓN INICIAL, REGISTRO Y EVALUACIÓN	39
III. CLASIFICACIÓN, CONTENCIÓN Y PRESERVACIÓN.....	40

<u>IV. INVESTIGACIÓN, ANÁLISIS E INFORMACIÓN E INCIDENTES.....</u>	<u>41</u>
<u>V. INCIDENTES.....</u>	<u>41</u>
<u>VI. SEPARACIÓN DE FUNCIONES.....</u>	<u>43</u>
<u>VII. DISPOSICIONES FINALES</u>	<u>44</u>

Título I

Política Institucional de Sostenibilidad, Responsabilidad Social y Gobernanza (ESG)

Documento de desarrollo del sistema de gobernanza ética institucional que articula la sostenibilidad y los criterios ESG con la ética profesional, la gobernanza de la información, la seguridad, la prevención de conflictos de interés, la transparencia, el uso responsable de la inteligencia artificial, el cumplimiento normativo y el procedimiento de respuesta a incidentes de seguridad, preservando en todo momento la jerarquía de los Estatutos Sociales

I. Objeto, Alcance y Principios

Artículo 1. **Objeto, naturaleza y alcance.** La Asociación Tributaria de la República Dominicana, Inc. (ATRIRD) promoverá la adopción e implementación de una Política Institucional de Sostenibilidad, Responsabilidad Social y Gobernanza (ESG), adecuada a su naturaleza jurídica de asociación sin fines de lucro, a sus fines estatutarios, a la dimensión de sus operaciones y a los recursos razonablemente disponibles para su ejecución.

La presente Política tiene por objeto incorporar progresivamente criterios ambientales, sociales y de gobernanza en la gestión institucional, procurando que las actuaciones de ATRIRD sean coherentes con los principios de responsabilidad, transparencia, integridad, sostenibilidad, buena administración y conducta ética que informan sus Estatutos Sociales, su Código de Ética y las demás normas internas aplicables.

La aplicación de esta Política se regirá por los principios de proporcionalidad, materialidad, razonabilidad, transparencia, verificabilidad y mejora continua.

En consecuencia, ATRIRD evitará trasladar mecánicamente obligaciones, metodologías o estructuras concebidas para sociedades comerciales, entidades reguladas o grandes organizaciones cuando estas no resulten compatibles con su naturaleza asociativa, su estructura institucional o su capacidad material.

II. Dimensiones Ambientales y Sociales

Artículo 2. **Dimensiones Ambientales.** En su dimensión ambiental, ATRIRD procurará el uso responsable de los recursos empleados en sus actividades y fomenta prácticas razonables dirigidas a prevenir o reducir los impactos ambientales que puedan derivarse de su funcionamiento institucional.

Estas prácticas comprenden, entre otras, la reducción del consumo innecesario de papel, la digitalización de documentos y procedimientos, el uso eficiente de energía y otros recursos, la adecuada disposición de residuos, la consideración de criterios ambientales en la selección de proveedores cuando resulte viable y la incorporación de prácticas sostenibles en la organización de congresos, jornadas, seminarios, reuniones y demás actividades institucionales.

Las medidas ambientales deberán concebirse como objetivos de implementación progresiva y evaluación periódica.

No constituirán compromisos absolutos ni declaraciones de resultados ambientales que excedan la capacidad material de ATRIRD o que no puedan ser razonablemente demostrados.

Artículo 3. **Dimensiones Sociales.** En su dimensión social, ATRIRD promoverá el respeto de la dignidad humana, la igualdad de trato, la no discriminación, la inclusión, el desarrollo profesional, la educación tributaria, el respeto de los derechos de los contribuyentes y la

generación y difusión responsable de conocimiento que contribuya al fortalecimiento de la cultura tributaria y del Estado de derecho.

La Política reconoce especialmente la función educativa y profesional de ATRIRD y su capacidad para contribuir al desarrollo de sus miembros y de la comunidad tributaria mediante actividades académicas, investigación, capacitación, cooperación institucional, intercambio profesional y difusión responsable del conocimiento.

ATRIRD procurar asimismo condiciones institucionales que favorezcan la participación equitativa, el respeto profesional y la prevención del acoso, la discriminación, las represalias y demás conductas incompatibles con sus principios éticos.

III. Gobernanza institucional, de la información Tecnológica y seguridad

Artículo 4. **Gobernanza Institucional.** En materia de gobernanza, ATRIRD promueve estructuras y procedimientos que fortalezcan la transparencia, la rendición de cuentas, la integridad institucional, la adecuada administración de recursos, la prevención y gestión de conflictos de interés, la independencia en la toma de decisiones, el cumplimiento normativo y la trazabilidad de las actuaciones institucionales relevantes.

La implementación de este componente respeta estrictamente la distribución de competencias establecida en los Estatutos Sociales, el Código de Ética, el Reglamento Disciplinario y las demás normas internas válidamente adoptadas.

Ninguna disposición de esta Política podrá alterar las atribuciones de la Asamblea General, la Junta Directiva, el Comité Disciplinario u otros órganos de ATRIRD.

La gobernanza sostenible comprende también mecanismos razonables para la identificación, declaración, prevención y gestión de conflictos de interés, así como controles orientados a prevenir corrupción, soborno, fraude, utilización indebida de recursos institucionales y otras actuaciones contrarias a los principios éticos de ATRIRD.

Artículo 5. **Gobernanza de la Información, tecnología y seguridad.** La presente Política articula con la Política de Protección, Gobernanza y Uso Ético de la Información y con las demás normas institucionales relacionadas con información y seguridad.

En consecuencia, la gobernanza institucional comprende, según corresponda, la clasificación de información, control de accesos, conservación y eliminación segura, gestión del ciclo de vida de la información, administración de terceros, seguridad de los servicios tecnológicos y en la nube, respuesta frente a incidentes, mecanismos de anonimización o seudonimización cuando resulten pertinentes y medidas razonables para preservar la confidencialidad, integridad y disponibilidad de la información.

La gestión de información observar los deberes de confidencialidad, secreto profesional, protección de datos y demás obligaciones que resultan aplicables conforme al ordenamiento jurídico dominicano y a las normas internas de ATRIRD.

IV. Inteligencia Artificial y Tecnologías Emergentes

Artículo 6. **Inteligencia Artificial y Tecnologías emergentes.** ATRIRD promueve un uso responsable de la inteligencia artificial, sistemas automatizados y demás tecnologías emergentes en sus actividades institucionales y profesionales.

Su utilización se sujeta, según la naturaleza del caso, a criterios de supervisión humana, confidencialidad, seguridad, exactitud razonable, transparencia, trazabilidad y responsabilidad profesional.

El uso de herramientas tecnológicas no sustituirá el juicio profesional ni liberará a la persona que las utilice de las responsabilidades éticas o profesionales que le correspondan.

Cuando se utilicen sistemas tecnológicos para procesar información confidencial o datos de terceros, se adoptan medidas razonables para evitar divulgaciones, accesos, reutilizaciones o tratamientos incompatibles con la finalidad legítima para la cual la información fue obtenida.

V. Objetivos, responsabilidades e indicadores

Artículo 7. **Objetivos, responsabilidades e indicadores.** La Política no se limita a una declaración programática. ATRIRD procura identificar progresivamente objetivos concretos y razonablemente medibles, asignar responsabilidades institucionales para su ejecución y establecer mecanismos periódicos de seguimiento y evaluación.

Los indicadores son proporcionales a la naturaleza, capacidad y materialidad de las actividades de ATRIRD. Comprenden, entre otros aspectos, participación en programas de formación ética y profesional, actividades educativas desarrolladas, avances en digitalización, cumplimiento de declaraciones de conflictos de interés, gestión de incidentes de información, participación institucional, cumplimiento de políticas de gobernanza y otras métricas razonables que permiten evaluar la evolución de los objetivos adoptados.

La ausencia de indicadores complejos o de metodologías internacionales de reporte empresarial no constituirá por sí misma incumplimiento cuando dichos instrumentos no resulten materialmente adecuados a la naturaleza asociativa de ATRIRD.

VI. Integridad de las declaraciones de sostenibilidad

Artículo 8. **Integridad de las declaraciones de sostenibilidad.** ATRIRD observará especial prudencia en toda comunicación pública relativa a sostenibilidad, responsabilidad social, impacto ambiental, gobernanza o cumplimiento de criterios ESG.

Ninguna comunicación institucional presentará como alcanzado un objetivo que constituya únicamente una aspiración, ni atribuirá a ATRIRD certificaciones, niveles de cumplimiento, reducciones de impacto, resultados ambientales, sociales o de gobernanza que no puedan ser razonablemente sustentados mediante información verificable.

Cuando se comuniquen metas futuras, se deberán identificar claramente como tales y, cuando resulte apropiado, indicarse su alcance, metodología, limitaciones y horizonte temporal.

ATRIRD evitará afirmaciones engañosas o susceptibles de inducir a error respecto de su desempeño ambiental, social o de gobernanza, incluyendo prácticas comúnmente identificadas como ecolavado (greenwashing), lavado ético (social washing) u otras formas de representación inexacta del desempeño institucional.

Cuando una actividad, publicación, capacitación, certificación, servicio o relación institucional quede comprendida en el ámbito de la legislación de protección de consumidores o usuarios, ATRIRD observa los deberes imperativos de información veraz, suficiente y no engañosa, trato digno y no discriminatorio, protección de intereses legítimos y demás garantías aplicables.

Esta referenciará no implica calificar automáticamente como relación de consumo toda actividad asociativa, académica o profesional de ATRIRD; dicha calificación dependerá de la ley y de las circunstancias de cada caso.

VII. Referencias y estándares internacionales

Artículo 9. **Referencias y estándares internacionales.** ATRIRD podrá utilizar como referencias orientadoras principios, marcos y buenas prácticas nacionales e internacionales en materia de sostenibilidad, responsabilidad social, gobernanza, integridad, anticorrupción y conducta profesional, siempre que resulten compatibles con el ordenamiento jurídico dominicano, sus Estatutos Sociales y su naturaleza institucional.

La referencia a un estándar, marco o iniciativa internacional no implicará, por sí misma, certificación, adhesión formal, cumplimiento integral ni asunción de obligaciones que ATRIRD no haya aceptado válidamente.

Cuando ATRIRD comunique públicamente la utilización de un estándar o marco de referencia, deberá describir con precisión el alcance real de dicha utilización y evitar afirmaciones que puedan razonablemente interpretarse como una certificación o reconocimiento inexistente.

VIII. Supervisión, seguimiento y revisión

Artículo 10. **Supervisión, seguimiento y revisión.** La Junta Directiva, dentro de las atribuciones que le confieran los Estatutos Sociales, promoverá la implementación de esta Política y determinará las responsabilidades administrativas necesarias para su seguimiento, sin invadir las competencias atribuidas estatutariamente a otros órganos.

La Política será objeto de revisión periódica atendiendo a la evolución de las actividades de ATRIRD, sus riesgos institucionales, los cambios normativos y las buenas prácticas nacionales e internacionales que resulten pertinentes.

Los resultados de su implementación podrán incorporarse, cuando resulte razonable, a los mecanismos institucionales de rendición de cuentas. Toda información divulgada deberá ser

objetiva, comprensible, verificable y proporcional a la naturaleza y capacidad institucional de ATRIRD.

IX. Interpretación y salvaguarda jurídica

Artículo 11. **Interpretación y salvaguarda Jurídica.** La incorporación de criterios ESG al sistema de gobernanza de ATRIRD no tendrá por efecto crear obligaciones jurídicas no establecidas por la legislación dominicana, los Estatutos Sociales o los compromisos válidamente asumidos por la Asociación.

Los criterios contenidos en esta Política se interpretarán como instrumentos de buena gobernanza y desarrollo institucional, salvo aquellos aspectos cuyo cumplimiento resulte obligatorio por disposición legal, estatutaria, contractual o reglamentaria.

Ninguna disposición de esta Política podrá interpretarse de manera que modifique indirectamente los Estatutos Sociales, amplíe las competencias de los órganos institucionales, cree infracciones o sanciones disciplinarias por vía administrativa, o altere las garantías establecidas en el Código de Ética y el Reglamento Disciplinario.

Cuando exista contradicción entre esta Política y una norma de superior jerarquía aplicable a ATRIRD, prevalecerá esta última.

X. Integración con el sistema de gobernanza ética de ATRIRD

Artículo 12. **Integración con el sistema de gobernanza ética de ATRIRD.** La presente Política deberá aplicarse de manera coordinada con el Código de Ética, el Reglamento Disciplinario, la Política de Protección, Gobernanza y Uso Ético de la Información, las políticas de conflictos de interés, los programas de educación profesional continua y los demás instrumentos de cumplimiento y gobernanza que adopte ATRIRD.

Esta integración tiene por finalidad evitar duplicidades, contradicciones o sistemas paralelos de cumplimiento y procurar que las dimensiones ambientales, social y de gobernanza formen parte de un único marco institucional de integridad, responsabilidad profesional, protección de información, cumplimiento normativo y rendición de cuentas.

XI. Entrada en vigor

Artículo 13. **Entrada en Vigor.** La presente Política entrará en vigor en la fecha y mediante el mecanismo de aprobación que corresponda de conformidad con los Estatutos Sociales y las competencias de los órganos de ATRIRD.

Su implementación podrá realizarse de manera progresiva, atendiendo a la materialidad de los riesgos, las prioridades institucionales y los recursos razonablemente disponibles, sin perjuicio del cumplimiento inmediato de aquellas obligaciones que deriven directamente de la legislación aplicable o de normas institucionales vigentes.

Título II

POLÍTICA DE PROTECCIÓN, GOBERNANZA Y USO ÉTICO DE LA INFORMACIÓN

Clasificación de información, control de accesos, ciclo de vida, gestión de terceros, incidentes, nube y anonimización

Preámbulo

La Asociación Tributaria de la República Dominicana, Inc. (ATRIRD) reconoce que la información constituye un activo esencial para el cumplimiento de sus fines institucionales, académicos, profesionales y administrativos y que su adecuada protección constituye una responsabilidad fundamental de buena gobernanza.

La naturaleza de las actividades desarrolladas por ATRIRD puede implicar el tratamiento de información institucional, profesional, tributaria, financiera, académica, administrativa y personal, así como documentos y comunicaciones cuya divulgación, alteración, pérdida, utilización indebida o acceso no autorizado pudiera afectar derechos individuales, obligaciones profesionales, intereses legítimos de terceros o la integridad y reputación de la Asociación.

ATRIRD adopta, en consecuencia, la presente Política de Protección, Gobernanza y Uso Ético de la Información, con el propósito de establecer principios, responsabilidades y controles razonables aplicables durante todo el ciclo de vida de la información, desde su creación u obtención hasta su archivo, anonimización o eliminación.

La Política deberá interpretarse coordinadamente con los Estatutos Sociales, el Código de Ética, el Reglamento Disciplinario, la Política Institucional de Sostenibilidad y ESG, la Política Institucional de Uso Responsable de Inteligencia Artificial y Herramientas Digitales y las demás disposiciones internas aplicables.

I. Objeto, Alcance y Principios

Artículo 14. **Objeto.** La presente Política tiene por objeto establecer el marco institucional para la obtención, creación, clasificación, utilización, almacenamiento, acceso, transmisión, conservación, protección, archivo, anonimización y eliminación de información bajo responsabilidad de ATRIRD.

Artículo 15. **Ámbito de aplicación.** Será aplicable a la información tratada por ATRIRD independientemente de su soporte físico o digital, lugar de almacenamiento, tecnología utilizada, origen interno o externo, persona autorizada que la gestione o proveedor tecnológico utilizado para su procesamiento o almacenamiento. Será igualmente aplicable a los órganos, directivos, funcionarios, empleados, colaboradores, comités, comisiones, contratistas y demás personas que accedan legítimamente a información bajo control de ATRIRD.

Artículo 16. **Principios.** La gobernanza de información se regirá por los principios de legalidad, finalidad legítima, proporcionalidad, minimización, exactitud, confidencialidad, integridad, disponibilidad, responsabilidad, trazabilidad, seguridad, necesidad de acceso, conservación limitada y utilización ética. La información no deberá ser obtenida, utilizada, compartida o conservada simplemente porque técnicamente sea posible hacerlo.

II. Clasificación de la Información

Artículo 17. **Clasificación.** ATRIRD establecerá un sistema de clasificación proporcional al nivel de sensibilidad, riesgo y consecuencias derivadas de un acceso, modificación, pérdida o divulgación no autorizados. La información podrá clasificarse, como mínimo, en: a) pública; b) de uso interno; c) confidencial; y d) restringida o especialmente protegida.

Artículo 18. **Información especialmente protegida.** Podrán recibir esta clasificación, atendiendo a su naturaleza, los datos personales sensibles o de especial protección conforme al derecho aplicable; información tributaria o financiera confidencial; expedientes disciplinarios; credenciales y mecanismos de autenticación; información protegida por secreto profesional; investigaciones internas; estrategias jurídicas; información relativa a incidentes de seguridad; bases de datos que permitan identificar personas; y cualquier otra información cuya divulgación pueda producir daños relevantes. La clasificación dependerá de la naturaleza real de la información y no exclusivamente del nombre asignado al documento.

III. Control de Acceso

Artículo 19. **Necesidad de conocimiento.** El acceso a información deberá limitarse a quienes razonablemente lo necesiten para el cumplimiento de funciones legítimas. La condición de miembro, directivo, funcionario o colaborador de ATRIRD no otorgará por sí sola acceso irrestricto a la información institucional.

Artículo 20. **Mínimo privilegio.** Los permisos tecnológicos y administrativos deberán limitarse al nivel mínimo razonablemente necesario para el desempeño de las funciones correspondientes.

Artículo 21. **Gestión de usuarios.** ATRIRD procurará establecer procedimientos para creación y autorización de cuentas, asignación de permisos, modificación de accesos cuando cambien las funciones, revisión periódica de privilegios, revocación oportuna cuando finalice la relación que justificaba el acceso y utilización de mecanismos adecuados de autenticación.

Artículo 22. **Credenciales.** Las credenciales de acceso serán personales cuando la naturaleza del sistema lo permita. No deberán compartirse contraseñas ni utilizarse mecanismos destinados a eludir controles de seguridad. ATRIRD promoverá mecanismos de autenticación reforzada para sistemas o información de mayor riesgo cuando resulte técnica y económicamente razonable.

IV. Ciclo de Vida de la Información

Artículo 23. **Principio de ciclo de vida.** La protección de la información comprenderá todas sus etapas: creación u obtención, clasificación, utilización, almacenamiento, transmisión, modificación, conservación, archivo, anonimización o eliminación.

Artículo 24. **Obtención.** ATRIRD procurará obtener únicamente la información razonablemente necesaria para finalidades institucionales legítimas. La obtención indiscriminada de información que no responda a una finalidad identificable deberá evitarse.

Artículo 25. **Exactitud.** Cuando la exactitud de determinada información pueda afectar decisiones institucionales o derechos de terceros, deberán establecerse mecanismos razonables para verificarla y, cuando corresponda, corregirla.

Artículo 26. **Conservación.** La información deberá conservarse durante el período requerido por disposiciones legales, obligaciones fiscales o contables, obligaciones contractuales, necesidades institucionales legítimas, ejercicio o defensa de derechos, preservación histórica institucional o cualquier otra finalidad jurídicamente válida. La conservación indefinida no deberá utilizarse como regla general cuando haya desaparecido la finalidad legítima que justificaba mantener la información.

Artículo 27. **Eliminación.** Cumplido el período legítimo de conservación, la información deberá ser eliminada, destruida o anonimizada mediante mecanismos razonablemente apropiados a su sensibilidad y soporte. La eliminación deberá procurar impedir la reconstrucción o recuperación no autorizada cuando la naturaleza de la información así lo requiera.

V. Uso Ético de la Información

Artículo 28. **Limitación de finalidad.** La información obtenida para una finalidad legítima no deberá reutilizarse para propósitos materialmente incompatibles sin fundamento jurídico suficiente.

Artículo 29. **Prohibición de utilización indebida.** Ninguna persona podrá utilizar información obtenida en razón de su cargo, función, participación institucional o acceso autorizado para obtener ventajas indebidas; beneficiar ilegítimamente a terceros; perjudicar a otra persona; realizar operaciones basadas en información reservada cuando ello resulte ilícito o éticamente improcedente; ejercer represalias; manipular procedimientos institucionales; o realizar cualquier finalidad incompatible con los principios éticos de ATRIRD.

Artículo 30. **Deber de confidencialidad.** La obligación de confidencialidad subsistirá después de finalizar el cargo, función, contrato o relación institucional cuando la naturaleza de la información o una obligación jurídica así lo requiera.

Artículo 31. **Derechos de las personas respecto de sus datos.** Cuando ATRIRD trate datos personales, deberá facilitar, en los casos y condiciones previstos por la legislación aplicable, el ejercicio de los derechos de acceso, rectificación, actualización, oposición o cancelación/supresión que correspondan, así como los mecanismos de hábeas data y demás garantías legalmente reconocidas. Las solicitudes deberán tramitarse con verificación razonable de identidad, protección de terceros y observancia de las excepciones legales, sin utilizar esta Política para restringir derechos reconocidos por la Constitución o la ley.

VI. Información Tributaria y Secreto Profesional

Artículo 32. **Protección reforzada.** La información tributaria, financiera, patrimonial o profesional relativa a contribuyentes o terceros recibirá protección reforzada cuando esté sometida a deberes legales, contractuales o profesionales de confidencialidad.

Artículo 33. **Secreto profesional.** Ninguna disposición de esta Política deberá interpretarse como autorización para revelar información protegida por secreto profesional. Cuando exista un requerimiento de autoridad, deberá determinarse previamente su validez, alcance y fundamento jurídico, así como las limitaciones que resulten aplicables.

VII. Gestión de Terceros

Artículo 34. **Principio de responsabilidad.** La contratación de un tercero para procesar, almacenar, transportar, administrar o acceder a información no eliminará las responsabilidades institucionales que correspondan a ATRIRD.

Artículo 35. **Evaluación de terceros.** Antes de permitir acceso a información confidencial o restringida, ATRIRD procurará evaluar proporcionalmente la naturaleza del servicio, información involucrada, medidas de seguridad, obligaciones de confidencialidad, utilización de subcontratistas, localización y almacenamiento de información, mecanismos de recuperación y eliminación, gestión de incidentes, continuidad del servicio y condiciones aplicables a la terminación contractual.

Artículo 36. **Obligaciones contractuales.** Cuando resulte materialmente necesario, los contratos deberán establecer obligaciones adecuadas sobre confidencialidad, seguridad, finalidad del tratamiento, acceso autorizado, subcontratación, notificación de incidentes, devolución o eliminación de información y cooperación al finalizar la relación.

Artículo 37. **Relaciones civiles y comerciales.** Las políticas institucionales no modificarán por sí solas contratos, obligaciones civiles o comerciales ni derechos adquiridos de terceros. Toda obligación contractual sobre información, tecnología, confidencialidad, propiedad intelectual, servicios o responsabilidad deberá resultar del contrato, de la ley o de una modificación válidamente consentida, respetando las normas imperativas aplicables.

VIII. Servicios en la Nube

Artículo 38. **Uso de servicios en la nube.** La utilización de servicios de almacenamiento, colaboración o procesamiento en la nube deberá responder a una finalidad institucional legítima y a una evaluación proporcional del riesgo de la información involucrada.

Artículo 39. **Evaluación de nube.** Antes de alojar información confidencial o restringida en servicios de nube, ATRIRD procurará considerar las condiciones de seguridad y privacidad del proveedor, localización y transferencias de datos, mecanismos de cifrado cuando resulten pertinentes, autenticación y control de accesos, copias de seguridad, recuperación, continuidad, exportación y eliminación de información y condiciones contractuales aplicables.

Artículo 40. **Transferencias y alojamiento transfronterizo.** La utilización de proveedores o infraestructuras ubicados fuera de la República Dominicana deberá evaluarse conforme a la legislación aplicable, la naturaleza de los datos, las garantías contractuales y técnicas disponibles, los derechos de los titulares y las obligaciones de confidencialidad o secreto profesional. La mera conveniencia tecnológica no constituirá fundamento suficiente para realizar una transferencia incompatible con una prohibición legal, contractual o profesional.

Artículo 41. **Cuentas institucionales.** Cuando resulte razonablemente posible, la información institucional deberá gestionarse mediante cuentas, repositorios y servicios autorizados por ATRIRD, evitando su almacenamiento innecesario en cuentas personales o servicios no aprobados.

IX. Anonimización y Seudonimización

Artículo 42. **Anonimización.** Cuando una finalidad legítima pueda alcanzarse sin identificar a las personas involucradas, ATRIRD procurará utilizar información anonimizada. La anonimización deberá procurar reducir razonablemente la posibilidad de reidentificación teniendo en cuenta la naturaleza, contexto y medios razonablemente disponibles.

Artículo 43. **Seudonimización.** Cuando la anonimización completa no resulte adecuada, podrán sustituirse identificadores directos por códigos u otros mecanismos deseudonimización. La información necesaria para revertir laseudonimización deberá mantenerse separada y protegida cuando resulte razonablemente posible.

Artículo 44. **Datos para formación, investigación y tecnología.** La información utilizada para actividades académicas, estadísticas, demostraciones, pruebas tecnológicas o sistemas de inteligencia artificial deberá anonimizarse o minimizarse cuando la identificación de personas no sea necesaria para la finalidad perseguida.

X. Incidentes de Información y Seguridad

Artículo 45. **Concepto de incidente.** Se considerará incidente cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de información o sistemas, incluyendo pérdida, acceso no autorizado, divulgación, alteración, destrucción, envío a destinatario incorrecto, compromiso de credenciales, malware o indisponibilidad significativa.

Artículo 46. **Deber de comunicación.** Quien tenga conocimiento de un incidente relacionado con información de ATRIRD deberá comunicarlo oportunamente por los canales institucionales establecidos. La comunicación de buena fe de un posible incidente no dará lugar a represalias.

Artículo 47. **Respuesta.** ATRIRD procurará establecer un procedimiento de respuesta que contemple identificación, contención, evaluación, preservación de evidencia cuando corresponda, recuperación, documentación, análisis de causas, medidas correctivas y determinación de obligaciones de comunicación a personas afectadas, proveedores, aseguradores o autoridades cuando jurídicamente proceda.

Artículo 48. **Registro de incidentes.** Los incidentes relevantes deberán documentarse de manera proporcional, incluyendo naturaleza, información afectada, medidas adoptadas, consecuencias conocidas y acciones preventivas posteriores.

XI. Continuidad, Respaldo y Recuperación

Artículo 49. **Continuidad.** ATRIRD procurará adoptar medidas razonables para preservar la disponibilidad de información necesaria para sus funciones esenciales.

Artículo 50. **Copias de seguridad.** La información institucional crítica deberá estar sujeta, cuando resulte apropiado, a mecanismos de respaldo y recuperación cuya frecuencia y protección sean proporcionales a su importancia.

Artículo 51. **Recuperación.** Los mecanismos de recuperación deberán ser revisados periódicamente para determinar razonablemente que la información puede restaurarse cuando sea necesaria.

XII. Inteligencia Artificial y Herramientas Digitales

Artículo 52. **Coordinación.** El tratamiento de información mediante inteligencia artificial y herramientas digitales se regirá conjuntamente por esta Política y por la Política Institucional de Uso Responsable de Inteligencia Artificial y Herramientas Digitales.

Artículo 53. **Información en sistemas de inteligencia artificial.** No deberá introducirse información confidencial, restringida, protegida por secreto profesional o perteneciente a terceros en herramientas cuya seguridad, condiciones de tratamiento, retención o utilización posterior de los datos no hayan sido razonablemente evaluadas.

Artículo 54. **Minimización tecnológica.** Antes de utilizar información en sistemas automatizados deberá evaluarse si la finalidad puede alcanzarse mediante datos anonimizados, seudonimizados, sintéticos o reducidos.

XIII. Transferencia y Comunicación de Información

Artículo 55. **Transferencia.** La transmisión de información confidencial o restringida deberá realizarse mediante mecanismos razonablemente adecuados al nivel de riesgo, verificando cuando corresponda la identidad y legitimidad del destinatario.

Artículo 56. **Divulgación externa.** La información institucional no pública solo podrá comunicarse externamente cuando exista autorización, obligación legal, fundamento contractual o finalidad institucional legítima compatible con su clasificación.

Artículo 57. **Requerimientos de autoridades.** Los requerimientos de información provenientes de autoridades deberán ser evaluados atendiendo a su competencia, fundamento jurídico, alcance y formalidades aplicables, preservando las garantías, privilegios y deberes de confidencialidad reconocidos por el ordenamiento jurídico.

Artículo 58. **Información tributaria, cooperación e intercambio internacional.** Ninguna disposición de esta Política autoriza a ATRIRD a ejercer facultades de fiscalización, requerimiento, asistencia administrativa mutua o intercambio internacional de información reservadas a la Administración Tributaria u otras autoridades competentes. La entrega o transferencia de información tributaria a autoridades nacionales o extranjeras solo procederá cuando exista fundamento jurídico aplicable, requerimiento válido o consentimiento jurídicamente suficiente, según corresponda, y con respeto de las garantías del contribuyente, la confidencialidad, el secreto profesional y las limitaciones de uso previstas por el ordenamiento.

XIV. Responsabilidades y Gobernanza

Artículo 59. **Junta Directiva.** La Junta Directiva, dentro de las atribuciones que le confieran los Estatutos Sociales, promoverá la implementación de esta Política y la asignación de responsabilidades administrativas para la gobernanza de información.

Artículo 60. **Responsables de información.** ATRIRD podrá designar responsables funcionales o custodios para categorías de información o sistemas relevantes, sin que tales designaciones modifiquen las competencias estatutarias de sus órganos.

Artículo 61. **Deber individual.** Toda persona con acceso autorizado deberá proteger la información bajo su control, utilizarla únicamente para finalidades legítimas, respetar su clasificación y comunicar incidentes o riesgos relevantes de los que tenga conocimiento.

XV. Formación, Supervisión y Mejora Continua

Artículo 62. **Formación.** ATRIRD promoverá formación periódica y proporcional sobre confidencialidad, protección de datos, seguridad digital, phishing, manejo documental, nube, inteligencia artificial, incidentes y demás riesgos relevantes.

Artículo 63. **Revisión de controles.** Los controles y procedimientos de información deberán revisarse periódicamente atendiendo a cambios tecnológicos, organizativos, jurídicos y de riesgo.

Artículo 64. **Mejora continua.** Los incidentes, auditorías, revisiones y experiencias de implementación deberán utilizarse para mejorar razonablemente el sistema de protección y gobernanza de información.

XVI. Relación con el Régimen Ético y Disciplinario

Artículo 65. **Integración normativa.** La presente Política forma parte del sistema institucional de gobernanza ética de ATRIRD y deberá interpretarse armónicamente con los Estatutos Sociales, el Código de Ética y el Reglamento Disciplinario.

Artículo 66. **Consecuencias disciplinarias.** El incumplimiento de esta Política solo podrá producir consecuencias disciplinarias cuando la conducta constituya una infracción conforme a los Estatutos, el Código de Ética, el Reglamento Disciplinario u otra norma válidamente vinculante. Esta Política no podrá crear retroactivamente infracciones, sanciones o competencias disciplinarias.

XVII. Disposiciones Finales

Artículo 67. **Interpretación conforme.** La presente Política deberá interpretarse de manera compatible con la Constitución y la legislación dominicana aplicable, los Estatutos Sociales de ATRIRD y los derechos y obligaciones profesionales correspondientes.

Artículo 68. **Protocolos de implementación.** ATRIRD podrá adoptar protocolos administrativos sobre clasificación, retención, control de acceso, gestión de usuarios, proveedores, nube, copias de seguridad, incidentes, anonimización y demás materias necesarias para implementar esta Política. Estos protocolos no podrán modificar los Estatutos, ampliar competencias institucionales ni crear infracciones o sanciones.

Artículo 69. **Revisión periódica.** La Política será revisada periódicamente para considerar cambios legales, tecnológicos, institucionales y de riesgos, procurando mantener controles proporcionales a la naturaleza y capacidad de ATRIRD.

Artículo 70. **Entrada en vigor.** La presente Política entrará en vigor en la fecha y mediante el mecanismo de aprobación que corresponda conforme a los Estatutos Sociales de ATRIRD. Su implementación podrá realizarse progresivamente, sin perjuicio del cumplimiento inmediato de las obligaciones legales y estatutarias aplicables.

Título III

POLÍTICA INSTITUCIONAL DE USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL Y HERRAMIENTAS DIGITALES

Coordinada con la Política de Protección, Gobernanza y Uso Ético de la Información y Seguridad

Preámbulo

La Asociación Tributaria de la República Dominicana, Inc. (ATRIRD) reconoce que la inteligencia artificial, los sistemas automatizados, las plataformas digitales, los servicios en la nube y otras tecnologías emergentes constituyen herramientas de creciente importancia para la investigación, educación, administración institucional y ejercicio profesional en materia tributaria.

Su utilización puede contribuir significativamente a la eficiencia, productividad, acceso al conocimiento, análisis de información y mejoramiento de los servicios profesionales. Sin embargo, también puede generar riesgos relacionados con la exactitud de la información, confidencialidad, protección de datos, secreto profesional, propiedad intelectual, discriminación algorítmica, ciberseguridad, dependencia tecnológica, transparencia y atribución de responsabilidades.

En consecuencia, ATRIRD adopta la presente Política Institucional de Uso Responsable de Inteligencia Artificial y Herramientas Digitales, coordinada con su Política de Protección, Gobernanza y Uso Ético de la Información, su Código de Ética, su Reglamento Disciplinario y las demás normas institucionales aplicables.

La Política se fundamenta en el principio de que la tecnología constituye un instrumento de apoyo y no un sustituto del juicio, la responsabilidad ni la independencia profesional.

I. Objeto y Finalidad

Artículo 71. **Objeto.** La presente Política tiene por objeto establecer principios, responsabilidades y criterios institucionales para la selección, acceso, utilización, supervisión y control de sistemas de inteligencia artificial y demás herramientas digitales utilizadas en actividades institucionales de ATRIRD.

Asimismo, procura proporcionar criterios de conducta responsable que puedan orientar a sus miembros cuando utilicen estas tecnologías en actividades relacionadas con el ejercicio profesional tributario, sin pretender sustituir las obligaciones legales, contractuales, deontológicas o profesionales que correspondan individualmente a cada usuario.

Artículo 72. **Finalidades.** La Política persigue promover el aprovechamiento responsable de la innovación tecnológica; proteger la confidencialidad y seguridad de la información; preservar el juicio y responsabilidad profesional; reducir riesgos derivados de información incorrecta, incompleta, desactualizada o artificialmente generada; prevenir usos discriminatorios, fraudulentos, engañosos o contrarios a derecho; establecer mecanismos de supervisión humana; fortalecer la transparencia y trazabilidad cuando resulten necesarias; proteger los derechos de ATRIRD, sus miembros y terceros; fomentar competencias digitales y formación continua; e integrar la gobernanza tecnológica dentro del sistema general de gobernanza ética de ATRIRD.

II. Ámbito de Aplicación

Artículo 73. Ámbito institucional. Esta Política será aplicable a los órganos, funcionarios, empleados, colaboradores, comisiones, comités y demás personas que utilicen herramientas tecnológicas por cuenta de ATRIRD o tengan acceso autorizado a sus sistemas o información.

Respecto de los miembros de ATRIRD en el ejercicio independiente de sus profesiones, las disposiciones de esta Política tendrán el alcance que resulte de los Estatutos, el Código de Ética y las demás normas que válidamente les resulten vinculantes.

Artículo 74. Tecnologías comprendidas. Quedan comprendidos, entre otros, los sistemas de inteligencia artificial generativa, asistentes digitales, modelos de lenguaje, herramientas de análisis automatizado, sistemas de traducción y transcripción, plataformas colaborativas, almacenamiento y procesamiento en la nube, herramientas de análisis documental, sistemas de automatización, aplicaciones de análisis de datos, herramientas de ciberseguridad, sistemas de apoyo a decisiones y demás tecnologías digitales que procesen información institucional o profesional.

La Política se aplicará atendiendo al riesgo y no exclusivamente a la denominación comercial o clasificación tecnológica de la herramienta.

III. Principios Rectores

Artículo 75. Supervisión humana. Las decisiones que puedan producir consecuencias jurídicas, tributarias, disciplinarias, profesionales o institucionales relevantes deberán permanecer sujetas a supervisión humana efectiva. Ningún resultado generado automáticamente deberá considerarse correcto por el solo hecho de haber sido producido por un sistema tecnológico.

Artículo 76. Responsabilidad humana. La utilización de inteligencia artificial no trasladará a la herramienta, a su proveedor ni al sistema automatizado la responsabilidad profesional o institucional correspondiente al usuario. Quien utilice una herramienta tecnológica será responsable, dentro del ámbito que jurídicamente le corresponda, de verificar razonablemente los resultados antes de utilizarlos como fundamento de una actuación profesional o institucional.

Artículo 77. Exactitud y verificación. La información producida mediante inteligencia artificial deberá ser sometida al grado de verificación razonablemente exigible según su finalidad, importancia y riesgo.

En materias jurídicas y tributarias deberán comprobarse particularmente la existencia, vigencia, texto y aplicabilidad de leyes, reglamentos, normas generales, jurisprudencia, resoluciones, tratados, doctrina administrativa y demás fuentes jurídicas citadas por sistemas de inteligencia artificial.

No deberán incorporarse a informes, opiniones, escritos, investigaciones o documentos profesionales citas jurídicas generadas mediante inteligencia artificial cuya existencia y contenido no hayan sido razonablemente verificados.

Artículo 78. Proporcionalidad basada en riesgos. Las medidas de control deberán ser proporcionales al riesgo de cada utilización. El uso de una herramienta para corrección gramatical, por ejemplo, no necesariamente requerirá los mismos controles que su utilización

para analizar información confidencial de un contribuyente o elaborar una opinión tributaria destinada a producir efectos jurídicos.

IV. Información, Confidencialidad y Seguridad

Artículo 79. **Coordinación normativa.** Esta Política deberá interpretarse conjuntamente con la Política de Protección, Gobernanza y Uso Ético de la Información y con las normas institucionales de seguridad de ATRIRD.

En caso de utilización de inteligencia artificial sobre información institucional, deberán aplicarse simultáneamente las reglas relativas a clasificación de información, acceso, almacenamiento, conservación, transmisión, terceros, incidentes, eliminación y demás controles establecidos por dichas políticas.

Artículo 80. **Información confidencial.** No deberá introducirse información confidencial, reservada, protegida por secreto profesional o perteneciente a terceros en sistemas públicos de inteligencia artificial o herramientas digitales respecto de las cuales no exista seguridad razonable acerca de las condiciones de tratamiento de dicha información.

Antes de utilizar información protegida deberán considerarse, según corresponda, la finalidad del tratamiento, autorización para utilizar la información, condiciones contractuales del proveedor, almacenamiento y localización de los datos, utilización de la información para entrenamiento de modelos, posibilidad de acceso por terceros, período de conservación, mecanismos de eliminación, medidas de seguridad y obligaciones legales y profesionales aplicables.

Artículo 81. **Minimización.** Solo deberá proporcionarse a una herramienta tecnológica la información estrictamente necesaria para alcanzar una finalidad legítima. Cuando resulte posible, deberán utilizarse mecanismos de anonimización, seudonimización, eliminación de identificadores o sustitución de datos reales por información ficticia.

Artículo 82. **Credenciales y accesos.** Queda prohibido introducir contraseñas, claves privadas, credenciales de acceso, códigos de autenticación u otros mecanismos de seguridad en herramientas de inteligencia artificial cuando ello pueda comprometer los sistemas de ATRIRD o de terceros.

V. Uso Profesional en Materia Tributaria

Artículo 83. **Inteligencia artificial como herramienta auxiliar.** La inteligencia artificial podrá utilizarse como herramienta auxiliar para investigación, organización, análisis preliminar, comparación de documentos, generación de borradores, traducción, sistematización y otras actividades compatibles con la legislación y las obligaciones profesionales correspondientes. Su utilización no sustituirá el análisis profesional necesario para determinar la correcta interpretación y aplicación del ordenamiento tributario.

Artículo 84. **Fuentes primarias.** Cuando una conclusión dependa de una norma jurídica o precedente, deberá procurarse su comprobación mediante fuentes primarias u oficiales. Los

resúmenes, respuestas o interpretaciones proporcionados por una herramienta de inteligencia artificial no deberán confundirse con la fuente jurídica original.

Artículo 85. **Información tributaria sensible.** Deberá prestarse especial protección a declaraciones tributarias, estados financieros, identificadores fiscales, expedientes, informaciones patrimoniales, estrategias de defensa, comunicaciones profesionales y demás información cuya divulgación pueda afectar al contribuyente o infringir obligaciones legales o profesionales.

VI. Transparencia y Trazabilidad

Artículo 86. **Transparencia proporcional.** La utilización de inteligencia artificial deberá ser comunicada cuando la naturaleza de la actividad, las expectativas legítimas del destinatario, una obligación contractual o profesional, o la relevancia de la intervención tecnológica hagan razonablemente necesaria dicha información.

No será necesaria una declaración indiscriminada de toda utilización meramente auxiliar que no altere sustancialmente el contenido, autoría intelectual o responsabilidad profesional del trabajo.

Artículo 87. **Autoría y atribución.** Ninguna persona deberá presentar como resultado de una investigación humana realizada personalmente aquello que haya sido generado sustancialmente mediante sistemas automatizados cuando tal representación resulte materialmente engañosa.

La utilización de inteligencia artificial tampoco deberá emplearse para fabricar fuentes, evidencia, credenciales, testimonios, citas, decisiones judiciales o documentos inexistentes.

Artículo 88. **Trazabilidad.** Para usos institucionales de riesgo significativo, ATRIRD podrá establecer mecanismos razonables para documentar la herramienta utilizada, finalidad, categorías de información procesada, verificaciones realizadas, intervención humana y decisión finalmente adoptada.

VII. Usos Prohibidos

Artículo 89. **Prohibiciones.** No podrán utilizarse herramientas de inteligencia artificial o tecnologías digitales institucionales para cometer, facilitar u ocultar actos contrarios a derecho; fabricar o alterar fraudulentamente documentos; suplantar identidades; generar deliberadamente información falsa destinada a engañar; vulnerar sistemas o medidas de seguridad; revelar información confidencial sin autorización o fundamento jurídico; realizar discriminaciones ilícitas; acosar, intimidar o perjudicar ilegítimamente a terceros; eludir deliberadamente controles institucionales; atribuir a ATRIRD opiniones o decisiones no autorizadas; o realizar cualquier otra actividad incompatible con el Código de Ética o la legislación aplicable.

VIII. Propiedad Intelectual

Artículo 90. **Respeto de derechos.** La utilización de herramientas digitales deberá respetar los derechos de autor, propiedad intelectual, licencias, condiciones de utilización y demás derechos legítimos de terceros.

Antes de publicar o utilizar institucionalmente contenidos generados o modificados mediante inteligencia artificial deberá evaluarse, cuando resulte material, su procedencia, condiciones de utilización y posible afectación de derechos de terceros.

IX. ADQUISICIÓN Y UTILIZACIÓN DE SISTEMAS POR ATRIRD

Artículo 91. **Evaluación previa.** Antes de adoptar institucionalmente una herramienta que procese información sensible o intervenga en procesos relevantes, ATRIRD procurará evaluar proporcionalmente su seguridad, privacidad, condiciones contractuales, confiabilidad, mecanismos de acceso, tratamiento de información, continuidad del servicio, dependencia del proveedor, posibilidad de recuperación y eliminación de datos y riesgos reputacionales o regulatorios.

Artículo 92. **Proveedores tecnológicos.** Los proveedores que tengan acceso a información institucional deberán estar sujetos, cuando resulte procedente, a obligaciones contractuales adecuadas de confidencialidad, seguridad, tratamiento de información, gestión de incidentes y terminación de servicios.

X. Inteligencia Artificial y Procedimientos Disciplinarios

Artículo 93. **Uso auxiliar.** La inteligencia artificial podrá utilizarse para tareas administrativas auxiliares relacionadas con la organización, búsqueda, clasificación o sistematización de información en procedimientos disciplinarios, siempre que se preserve la confidencialidad y se observen los controles institucionales aplicables.

Artículo 94. **Prohibición de decisión automatizada.** Ninguna determinación sobre admisibilidad, responsabilidad disciplinaria, valoración definitiva de pruebas, graduación de sanciones o resolución de recursos podrá ser delegada exclusivamente en un sistema de inteligencia artificial.

La decisión deberá corresponder al órgano humano competente conforme a los Estatutos y al Reglamento Disciplinario.

Artículo 95. **Verificación de resultados.** Todo resultado tecnológico utilizado en un procedimiento disciplinario deberá ser susceptible de revisión humana y, cuando sea material para una decisión, deberá poder ser razonablemente explicado, contrastado y controvertido por la persona afectada.

XI. Formación y Cultura Digital

Artículo 96. **Educación continua.** ATRIRD promoverá programas razonables de educación profesional continua sobre inteligencia artificial, protección de información, ciberseguridad, riesgos tecnológicos, ética digital, verificación de fuentes y utilización responsable de herramientas emergentes.

Artículo 97. **Competencia digital.** Quienes utilicen herramientas tecnológicas institucionales deberán procurar comprender razonablemente sus capacidades, limitaciones y riesgos, particularmente cuando sus resultados puedan afectar derechos, obligaciones o decisiones profesionales.

XII. Incidentes, Errores y Respuesta

Artículo 88. **Incidentes tecnológicos.** Toda pérdida, acceso no autorizado, divulgación indebida, alteración, compromiso de credenciales o incidente tecnológico que pueda afectar información de ATRIRD deberá comunicarse oportunamente conforme al protocolo institucional de seguridad e incidentes.

Artículo 99. **Corrección.** Cuando se detecte que información materialmente incorrecta generada mediante inteligencia artificial ha sido utilizada o divulgada institucionalmente, deberán adoptarse medidas razonables y oportunas para corregirla y limitar sus posibles consecuencias.

XIII. Gobernanza y Responsabilidades

Artículo 100. Responsabilidad institucional. La Junta Directiva, dentro de las competencias que le atribuyan los Estatutos, promoverá la implementación de esta Política y podrá establecer mecanismos administrativos para la gestión de riesgos tecnológicos.

Ninguna disposición de esta Política podrá interpretarse como modificación de las competencias estatutarias de los órganos de ATRIRD.

Artículo 101. Evaluación periódica. La Política será revisada periódicamente atendiendo a la evolución tecnológica, cambios en los riesgos, experiencia institucional, legislación dominicana aplicable y buenas prácticas nacionales e internacionales pertinentes.

XIV. Relación con el Régimen Ético y Disciplinario

Artículo 102. **Integración normativa.** La presente Política forma parte del sistema de gobernanza ética de ATRIRD y deberá interpretarse armónicamente con los Estatutos Sociales, el Código de Ética, el Reglamento Disciplinario, la Política de Protección, Gobernanza y Uso Ético de la Información, la Política Institucional de Sostenibilidad y ESG y las demás disposiciones internas aplicables.

Artículo 103. **Consecuencias disciplinarias.** El incumplimiento de esta Política únicamente podrá producir consecuencias disciplinarias cuando la conducta constituya una infracción

conforme a los Estatutos, el Código de Ética, el Reglamento Disciplinario u otra norma válidamente vinculante.

Esta Política no podrá utilizarse por sí sola para crear retroactivamente infracciones, sanciones o competencias disciplinarias.

XV. Interpretación y Salvaguardas

Artículo 104. **Interpretación conforme.** La Política deberá interpretarse de manera compatible con la Constitución y la legislación dominicana aplicable, los Estatutos Sociales de ATRIRD y los derechos y obligaciones profesionales correspondientes.

Artículo 105. **Neutralidad tecnológica.** Las obligaciones y salvaguardas establecidas en esta Política se aplicarán atendiendo a la función, riesgo y tratamiento de información realizado por una tecnología, independientemente de su marca, proveedor o denominación comercial.

Artículo 106. **Innovación responsable.** Ninguna disposición deberá interpretarse como prohibición general de la innovación tecnológica. ATRIRD procurará favorecer la utilización responsable de tecnologías que contribuyan al cumplimiento de sus fines, siempre que sus beneficios sean razonablemente compatibles con los riesgos y controles aplicables.

XVI. Disposiciones Finales

Artículo 107. **Protocolos de implementación.** ATRIRD podrá adoptar protocolos operativos sobre clasificación de herramientas por nivel de riesgo, herramientas institucionalmente autorizadas, tratamiento de información confidencial, evaluación de proveedores, gestión de incidentes, conservación de registros, inteligencia artificial generativa y demás materias necesarias para la implementación de esta Política.

Estos protocolos no podrán modificar los Estatutos, crear nuevas infracciones o sanciones ni ampliar competencias institucionales.

Artículo 108. **Entrada en vigor.** La presente Política entrará en vigor en la fecha y mediante el mecanismo de aprobación que corresponda conforme a los Estatutos Sociales de ATRIRD. Su implementación podrá realizarse progresivamente atendiendo a la naturaleza de los riesgos, prioridades institucionales y recursos disponibles, sin perjuicio del cumplimiento inmediato de las obligaciones legales y estatutarias aplicables.

Ninguna actuación de contención, recuperación, conservación o eliminación podrá alterar, ocultar, destruir o hacer desaparecer documentos, registros, archivos, metadatos, evidencias u otros elementos que razonablemente puedan estar relacionados con una investigación penal o administrativa vigente o previsible

Título IV

PROGRAMA INSTITUCIONAL DE CUMPLIMIENTO NORMATIVO Y PREVENCIÓN DE RIESGOS PENALES

*Instrumento articulador del Código de Ética, el Reglamento Disciplinario y las Políticas y
Procedimientos Institucionales*

PREÁMBULO

La Asociación Tributaria de la República Dominicana, Inc. (ATRIRD), en atención a su naturaleza de asociación sin fines de lucro, sus fines estatutarios y su compromiso con la integridad profesional, adopta el presente Programa Institucional de Cumplimiento Normativo y Prevención de Riesgos Penales como instrumento para organizar, coordinar y demostrar las medidas razonables destinadas a prevenir, detectar, comunicar, investigar internamente y corregir conductas que puedan comprometer a la institución o a las personas vinculadas con ella.

El Programa articula, sin sustituirlos, el Código de Ética y Normas de Conducta Profesional 2026, el Reglamento Disciplinario y su Protocolo Operativo 2026, y las Políticas y Procedimientos Institucionales 2026. Su aplicación respetará la Constitución, los tratados internacionales vinculantes, los Estatutos Sociales y la legislación imperativa de la República Dominicana.

Se toma especialmente en consideración la Ley núm. 74-25, Orgánica que instituye el Código Penal de la República Dominicana, modificada por la Ley núm. 44-26, particularmente sus disposiciones sobre responsabilidad penal de las personas jurídicas, programas de cumplimiento, prevención de riesgos, controles, formación, canales de denuncia, protección contra represalias, investigación y trazabilidad documental.

I. DISPOSICIONES GENERALES

Artículo 109. **Objeto.** El presente Programa establece el marco institucional para identificar, prevenir, gestionar y reducir razonablemente los riesgos de comisión de infracciones penales vinculadas con las actividades, órganos, representantes, empleados, miembros, contratistas, voluntarios y terceros relacionados con ATRIRD, dentro del ámbito jurídico que corresponda a cada persona.

Artículo 110. **Naturaleza.** El Programa es preventivo, organizativo y de cumplimiento. No constituye una declaración de que ATRIRD sea una entidad regulada de naturaleza distinta a la que legalmente le corresponde, ni atribuye a sus órganos potestades de investigación penal, coerción, persecución o sanción pública.

Artículo 111. **Finalidades.** El Programa procura fortalecer una cultura de legalidad; prevenir infracciones; proteger a ATRIRD, sus miembros y terceros; facilitar la detección temprana de riesgos; asegurar respuestas documentadas y proporcionales; preservar evidencias; promover la mejora continua; y demostrar el cumplimiento razonable de los deberes institucionales de dirección, control y supervisión.

Artículo 112. **Ámbito de aplicación.** El Programa será aplicable a los órganos de gobierno, directivos, miembros, Consultores Tributarios Certificados, candidatos a certificación, empleados, integrantes de comités, contratistas, proveedores, voluntarios y demás personas que actúen en nombre de ATRIRD o tengan acceso autorizado a recursos, información o sistemas institucionales, en la medida compatible con sus Estatutos, contrato, función o aceptación válida.

Artículo 113. **Principios rectores.** La aplicación se regirá por legalidad, buena fe, proporcionalidad, razonabilidad, diligencia, confidencialidad, independencia, presunción de no responsabilidad, debido proceso, no discriminación, protección de denunciantes, necesidad de acceso, minimización de datos, trazabilidad, mejora continua y respeto del secreto profesional.

Artículo 114. **Jerarquía y salvaguarda.** En caso de conflicto prevalecerán la Constitución, los tratados vinculantes, la legislación imperativa y los Estatutos Sociales. Este Programa no creará infracciones, sanciones ni competencias no autorizadas. Las referencias internacionales tendrán carácter orientador, salvo incorporación válida por una fuente vinculante.

II. GOBERNANZA DEL PROGRAMA

Artículo 115. **Responsabilidad de la Junta Directiva.** Dentro de sus competencias estatutarias, la Junta Directiva aprobará el Programa, promoverá los recursos razonablemente necesarios, recibirá informes periódicos, vigilará su implementación y dispondrá su actualización. Esta función no altera las competencias de la Asamblea General, del Comité Disciplinario ni de otros órganos.

Artículo 116. **Responsable de cumplimiento.** La Junta Directiva designará una persona u órgano responsable de coordinar el Programa, con acceso razonable a la información y autonomía funcional suficiente para elevar alertas y recomendaciones. En atención al tamaño y naturaleza de ATRIRD, esta función podrá ser asumida por el órgano de administración o por una comisión designada, siempre que se gestionen adecuadamente los conflictos de interés.

Artículo 117. **Independencia y conflictos de interés.** Quien participe en la evaluación de una alerta o investigación deberá declarar cualquier interés personal, profesional, económico o institucional que pueda afectar su imparcialidad y abstenerse cuando corresponda. Las denuncias contra integrantes de la dirección serán canalizadas de forma que estos no controlen su propia evaluación.

Artículo 118. **Informes.** El responsable de cumplimiento presentará al menos anualmente un informe reservado sobre riesgos identificados, actividades de formación, alertas recibidas, estado de investigaciones, medidas correctivas, incidentes relevantes, eficacia de controles y recomendaciones. Los informes utilizarán datos agregados o anonimizados cuando sea posible.

III. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS PENALES

Artículo 119. **Mapa de riesgos.** ATRIRD mantendrá un mapa proporcional de riesgos penales que identifique actividades, procesos, personas expuestas, factores de riesgo, controles existentes, probabilidad, impacto y medidas de tratamiento. El mapa deberá documentarse y revisarse periódicamente.

Artículo 120. **Ámbitos mínimos.** La evaluación comprenderá, cuando resulten pertinentes, corrupción pública y privada; cohecho; tráfico de influencias; fraude y estafa; falsedad documental; utilización indebida de títulos o credenciales; apropiación o uso indebido de recursos; revelación de secretos; afectaciones a la intimidad; uso no consentido de datos; robo de identidad; discriminación; acoso; represalias; obstrucción de investigaciones; ocultamiento o destrucción de evidencias; delitos tecnológicos; lavado de activos; financiamiento del terrorismo; infracciones tributarias y demás riesgos asociados a las actividades institucionales.

Artículo 121. **Metodología proporcional.** Cada riesgo se valorará considerando su posibilidad de ocurrencia, impacto jurídico, económico, reputacional y operativo, exposición de personas, sensibilidad de la información, participación de terceros y eficacia de los controles. La metodología será sencilla, verificable y adecuada a los recursos de ATRIRD.

Artículo 122. **Revisión extraordinaria.** El mapa se revisará cuando se produzcan cambios legislativos, nuevos servicios, modificaciones organizativas, incidentes, hallazgos de auditoría, incorporación de tecnologías, cambios sustanciales de proveedores o cualquier circunstancia que altere materialmente el perfil de riesgo.

IV. CONTROLES PREVENTIVOS

Artículo 123. **Código de conducta.** El Código de Ética constituye la norma primaria de conducta del Programa. Sus deberes serán comunicados de manera clara a las personas alcanzadas y se incorporarán contractualmente cuando deban obligar a empleados, contratistas, proveedores o terceros.

Artículo 124. **Controles financieros y contables.** ATRIRD implementará controles razonables para prevenir pagos, operaciones o beneficios ilícitos. Estos incluirán segregación de funciones cuando sea materialmente posible, autorizaciones conforme a montos y competencias, soportes documentales, conciliaciones, revisión de beneficiarios y proveedores, prohibición de pagos sin justificación, trazabilidad de reembolsos y controles sobre regalos, atenciones, donaciones, patrocinios y conflictos de interés.

Artículo 125. **Contratación y terceros.** Antes de contratar terceros de riesgo material, ATRIRD realizará una evaluación proporcional de identidad, reputación, capacidad, beneficiario final cuando proceda, conflictos de interés, condiciones de confidencialidad, seguridad, tratamiento de datos y exposición a corrupción o fraude. Los contratos incorporarán obligaciones adecuadas de cumplimiento y mecanismos de terminación o remediación.

Artículo 126. **Interacción con autoridades públicas.** Toda gestión ante funcionarios o entidades públicas deberá responder a fines legítimos, quedar razonablemente documentada y respetar la prohibición absoluta de ofrecer, prometer, entregar, solicitar o aceptar ventajas indebidas. Ninguna relación personal o institucional podrá utilizarse para obtener decisiones contrarias a la ley.

Artículo 127. **Información, tecnología e inteligencia artificial.** Se aplicarán las Políticas de Protección, Gobernanza y Uso Ético de la Información, Uso Responsable de Inteligencia Artificial y Respuesta a Incidentes. Queda prohibido utilizar sistemas o herramientas para suplantar identidades, fabricar evidencias, falsificar documentos, vulnerar controles, divulgar secretos o tratar datos sin autorización o fundamento jurídico.

Artículo 128. **Representación y credenciales.** Nadie podrá comprometer a ATRIRD, utilizar su nombre, logo, certificaciones, títulos, sellos o credenciales fuera del alcance autorizado. Los poderes de representación deberán resultar de los Estatutos, una decisión válida o mandato suficiente.

V. FORMACIÓN Y CULTURA DE CUMPLIMIENTO

Artículo 129. **Programa anual de formación.** ATRIRD aprobará un plan anual proporcional que incluya ética, derechos humanos, anticorrupción, prevención del fraude, protección de información, secreto profesional, riesgos tecnológicos, inteligencia artificial, no discriminación, canales de denuncia, preservación de evidencias y consecuencias del incumplimiento.

Artículo 130. **Formación según riesgo.** La formación se adaptará a las funciones. Quienes administren fondos recibirán capacitación sobre controles financieros; quienes manejen información, sobre confidencialidad y datos; quienes interactúen con autoridades, sobre corrupción y tráfico de influencias; y quienes investiguen denuncias, sobre imparcialidad, debido proceso y evidencia.

Artículo 131. **Registro y evaluación.** Se conservará evidencia de convocatorias, contenidos, asistencia, materiales y evaluaciones. La eficacia podrá medirse mediante preguntas de comprobación, ejercicios, indicadores, seguimiento de incidentes y ajustes derivados de hallazgos.

VI. CANALES DE ALERTA Y PROTECCIÓN

Artículo 132. **Canales internos.** ATRIRD habilitará canales accesibles para comunicar, de buena fe, sospechas o hechos que puedan constituir incumplimientos. Podrán incluir correo institucional, formulario electrónico, comunicación escrita, entrega física u otro medio que permita preservar razonablemente la confidencialidad.

Artículo 133. **Denuncias anónimas.** Se admitirá la recepción de denuncias anónimas cuando contengan información concreta y verificable. El anonimato no eliminará la necesidad

de corroboración ni permitirá imponer responsabilidad basándose exclusivamente en afirmaciones no comprobadas.

Artículo 134. **No represalias.** Quedan prohibidas las represalias contra quien comunique de buena fe, aporte información, coopere o participe como testigo. La protección no ampara denuncias deliberadamente falsas, fabricación de pruebas ni actuaciones realizadas con intención manifiesta de perjudicar.

Artículo 135. **Confidencialidad.** La identidad del denunciante, denunciado y participantes será protegida conforme a la necesidad de conocer, el derecho de defensa y la legislación aplicable. No se prometerá confidencialidad absoluta cuando exista obligación legal o requerimiento válido de autoridad competente.

VII. RECEPCIÓN, INVESTIGACIÓN Y RESPUESTA

Artículo 136. **Registro inicial.** Toda alerta recibirá un número de referencia y será registrada con fecha, canal, resumen, documentación, clasificación preliminar, persona responsable y medidas urgentes, preservando la seguridad de la información.

Artículo 137. **Evaluación preliminar.** Se verificará competencia institucional, credibilidad inicial, riesgos para personas o evidencias, conflictos de interés, necesidad de contención, posible obligación de informar y relación con procedimientos públicos. La recepción no equivale a admisión de responsabilidad.

Artículo 138. **Investigación interna.** Las investigaciones serán proporcionales, imparciales, documentadas y limitadas a competencias privadas. ATRIRD no utilizará técnicas reservadas a autoridades públicas ni impondrá deberes de autoincriminación. Se respetarán el secreto profesional, la protección de datos y el derecho de defensa.

Artículo 139. **Preservación de evidencias.** Ninguna actuación de contención, recuperación, conservación o eliminación podrá alterar, ocultar, destruir o hacer desaparecer documentos, registros, archivos, metadatos, evidencias u otros elementos razonablemente relacionados con una investigación vigente o previsible. La custodia deberá mantener autenticidad, integridad, trazabilidad y acceso restringido.

Artículo 140. **Relación con autoridades.** Cuando los hechos puedan constituir infracción penal, ATRIRD limitará su actuación a la evaluación y consecuencias internas. Se preservarán las evidencias y se determinarán jurídicamente las obligaciones de comunicación o cooperación, sin desconocer el secreto profesional, la confidencialidad protegida, el derecho de defensa ni las competencias exclusivas de las autoridades.

Artículo 141. **Medidas correctivas.** Según el caso podrán adoptarse medidas de contención, corrección de controles, recuperación de activos o información, suspensión de accesos, revisión contractual, capacitación, supervisión reforzada, remediación y remisión al órgano disciplinario competente. Las medidas provisionales no presumirán responsabilidad ni podrán exceder las competencias estatutarias.

Artículo 142. **Régimen disciplinario.** Las posibles infracciones éticas o disciplinarias se tramitarán exclusivamente conforme al Reglamento Disciplinario y su Protocolo. El Programa

no crea infracciones ni sanciones nuevas y no permite sancionar por analogía o remisiones genéricas.

VIII. DOCUMENTACIÓN, SEGUIMIENTO Y MEJORA

Artículo 143. **Trazabilidad documental.** ATRIRD conservará evidencia suficiente de la aprobación y ejecución del Programa, mapa de riesgos, controles, capacitaciones, alertas, investigaciones, decisiones, medidas correctivas, revisiones y actualizaciones, durante los plazos legales y administrativos aplicables.

Artículo 144. **Indicadores.** Podrán utilizarse indicadores como porcentaje de personal capacitado, revisiones completadas, alertas recibidas y atendidas, tiempos de respuesta, controles implementados, incidentes recurrentes, acciones correctivas cerradas y revisiones de terceros realizadas. Los indicadores no sustituirán la valoración cualitativa.

Artículo 145. **Evaluación anual.** Al menos una vez al año se evaluará la eficacia del Programa. La evaluación considerará diseño, implementación, resultados, proporcionalidad, recursos, independencia, documentación, cambios normativos y lecciones aprendidas.

Artículo 146. **Actualización.** El Programa será actualizado por el órgano competente cuando cambien la legislación, los Estatutos, las actividades, la estructura, los riesgos o los recursos de ATRIRD. Las modificaciones desfavorables del régimen disciplinario no se aplicarán retroactivamente.

IX. DISPOSICIONES FINALES

Artículo 147. **Responsabilidad individual y de la asociación.** La existencia del Programa no excluye la responsabilidad de las personas físicas ni garantiza por sí sola la exclusión de responsabilidad de ATRIRD. Su eficacia dependerá de la adopción real, aplicación verificable, actualización y supervisión razonable de las medidas.

Artículo 148. **No renuncia de derechos.** La firma de compromisos o constancias no implicará renuncia general a derechos, admisión anticipada de responsabilidad, autorización ilimitada para tratar información ni modificación de relaciones contractuales sin consentimiento válido o fundamento jurídico.

Artículo 149. **Interpretación conforme.** Las disposiciones se interpretarán de manera compatible con la Constitución, los tratados vinculantes, la Ley núm. 74-25 modificada por la Ley núm. 44-26, las leyes especiales vigentes, los Estatutos, el Código de Ética, el Reglamento Disciplinario y las políticas institucionales.

Artículo 150. **Aprobación y vigencia.** El Programa entrará en vigor en la fecha determinada mediante resolución del órgano competente conforme a los Estatutos Sociales. La resolución deberá identificar la versión aprobada, responsables de implementación, período inicial de adecuación y fecha de primera revisión.

Título V

PROCEDIMIENTO INSTITUCIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Incluye Matriz Mínima de Responsabilidades sobre Datos Institucionales

I. Objeto, Principios y Concepto

Artículo 151. **Objeto.** El presente Procedimiento establece las actuaciones mínimas que deberá seguir ATRIRD para identificar, comunicar, registrar, evaluar, contener, investigar, gestionar, recuperar y cerrar incidentes de seguridad de la información, así como para adoptar medidas correctivas y preventivas posteriores.

Su aplicación deberá coordinarse con la Política de Protección, Gobernanza y Uso Ético de la Información, la Política Institucional de Uso Responsable de Inteligencia Artificial y Herramientas Digitales, el Código de Ética, el Reglamento Disciplinario y las demás normas internas aplicables.

Artículo 152. **Principios de actuación.** La respuesta a incidentes se desarrollará conforme a criterios de oportunidad, proporcionalidad, confidencialidad, preservación de evidencia, trazabilidad, mínima divulgación, continuidad institucional, cooperación y mejora continua.

La prioridad será proteger y la información afectadas, contener el incidente, preservar los derechos de ATRIRD y de terceros y restablecer de manera segura las operaciones comprometidas.

La respuesta técnica a un incidente no tendrá por finalidad determinar responsabilidad disciplinaria. Cuando existan indicios que pudieran justificar una actuación disciplinaria, esa cuestión deberá tramitarse separadamente conforme a los Estatutos, el Código de Ética y el Reglamento Disciplinario.

Artículo 153. **Concepto de incidente de seguridad.** Se considerará incidente cualquier evento confirmado o razonablemente sospechado que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de información o sistemas bajo responsabilidad de ATRIRD.

Comprenderá, entre otros supuestos, acceso no autorizado, pérdida o robo de dispositivos, divulgación accidental, envío de información a destinatarios incorrectos, pérdida de documentos, compromiso de cuentas o contraseñas, malware, phishing, ransomware, alteración o eliminación no autorizada de información, indisponibilidad significativa de sistemas, exposición de información almacenada en la nube y utilización indebida de herramientas de inteligencia artificial.

Artículo 154. **Deber de comunicación inmediata.** Toda persona que conozca o sospeche razonablemente la existencia de un incidente deberá comunicarlo sin demora indebida a través del canal institucional establecido.

No será necesario que la persona determine previamente si efectivamente existe una violación de seguridad. La comunicación de buena fe de un incidente o vulnerabilidad no deberá generar represalias.

II. Información Inicial, Registro y Evaluación

Artículo 155. **Información inicial.** La comunicación procurará identificar, cuando la información esté disponible, qué ocurrió, cuándo fue detectado, sistemas o documentos

posiblemente afectados, personas que pudieran estar involucradas, medidas ya adoptadas y cualquier información que pueda contribuir a la contención.

La falta de alguno de estos datos no deberá retrasar la comunicación.

Artículo 156. **Registro.** Todo incidente relevante deberá recibir un registro que permita documentar cronológicamente las actuaciones realizadas.

El registro deberá contener, proporcionalmente a la gravedad del caso, fecha de detección, naturaleza del incidente, información y sistemas afectados, clasificación preliminar, actuaciones de contención, decisiones adoptadas, comunicaciones realizadas, recuperación, cierre y medidas posteriores.

Artículo 157. **Evaluación inicial.** Recibida la comunicación, deberá efectuarse una evaluación preliminar destinada a determinar qué ocurrió, qué información está comprometida, quiénes pueden resultar afectados, si el incidente continúa activo, cuál puede ser su impacto y qué medidas inmediatas son necesarias.

No deberá retrasarse una medida urgente de contención por el solo propósito de completar la evaluación.

III. Clasificación, Contención y Preservación

Artículo 158. **Clasificación por gravedad.** ATRIRD podrá clasificar los incidentes como bajos, moderados, altos o críticos, considerando la sensibilidad y volumen de la información, número de personas afectadas, posibilidad de daño, alcance del acceso no autorizado, duración, afectación de servicios esenciales, posibilidad de recuperación y consecuencias jurídicas, económicas, profesionales o reputacionales.

La clasificación deberá poder modificarse cuando aparezca nueva información.

Artículo 159. **Contención.** ATRIRD adoptará las medidas razonablemente necesarias para detener o limitar el incidente.

Estas podrán comprender bloqueo temporal de cuentas, cambio de credenciales, revocación de sesiones, aislamiento de equipos, suspensión de accesos, recuperación de documentos, restricciones temporales sobre servicios tecnológicos o cualquier otra medida proporcional.

Las medidas de contención deberán procurar preservar evidencia relevante y evitar destrucciones innecesarias de información.

Artículo 160. **Preservación de evidencia.** Cuando exista posibilidad razonable de investigación técnica, reclamación, procedimiento disciplinario o actuación de una autoridad competente, deberán preservarse los registros y demás elementos relevantes.

La preservación deberá realizarse procurando mantener su integridad, procedencia y trazabilidad. ATRIRD no utilizará mecanismos investigativos reservados legalmente a las autoridades públicas.

La preservación de evidencia no autoriza interceptaciones de comunicaciones, registros, accesos a dispositivos, allanamientos, obtención forzosa de credenciales ni otras medidas reservadas por la Constitución o la ley a autoridades competentes. Cuando la evidencia

pueda ser utilizada en un proceso judicial o administrativo, se procurará documentar su origen, integridad, acceso, conservación y transferencias de custodia de manera razonable, sin pretender sustituir las reglas probatorias que correspondan ante la autoridad competente.

IV. Investigación, análisis e información e incidentes.

Artículo 161. **Investigación y análisis.** Cuando la gravedad lo justifique, se realizará un análisis razonable para determinar la causa, alcance, información comprometida, duración, accesos producidos, vulnerabilidades utilizadas y posibles consecuencias.

Podrá solicitarse asistencia especializada externa cuando ATRIRD no disponga internamente de la capacidad técnica necesaria.

Artículo 162. **Información personal y confidencial.** Cuando el incidente involucre datos personales, información tributaria, financiera, patrimonial, profesional, disciplinaria o protegida por secreto profesional, la evaluación deberá considerar especialmente la naturaleza de la información y las consecuencias potenciales de su divulgación.

La respuesta al incidente no constituye por sí misma autorización para ampliar el acceso a la información comprometida.

V. Incidentes

Artículo 163. **Incidentes relacionados con inteligencia artificial.** Cuando el incidente se origine en la utilización de inteligencia artificial o herramientas digitales, deberá evaluarse particularmente si se introdujo información confidencial en sistemas externos, si la información puede conservarse o reutilizarse por el proveedor, si existe posibilidad de eliminarla, si pudo utilizarse para entrenamiento de modelos y si resulta necesario suspender temporalmente la utilización de la herramienta.

Artículo 164. **Servicios en la nube y proveedores.** Cuando intervenga un proveedor tecnológico, ATRIRD deberá activar los mecanismos contractuales y técnicos disponibles para obtener información, contener el incidente, recuperar datos y determinar su alcance.

El hecho de que el incidente se produzca en infraestructura de un tercero no elimina las responsabilidades de gobernanza que correspondan a ATRIRD.

Párrafo: Ninguna actuación de contención, recuperación, conservación o eliminación podrá alterar, ocultar, destruir o hacer desaparecer documentos, registros, archivos, metadatos, evidencias u otros elementos que razonablemente puedan estar relacionados con una investigación penal o administrativa vigente o previsible

Artículo 165. **Evaluación jurídica.** Cuando la naturaleza del incidente lo justifique, deberá determinarse si existen obligaciones legales o contractuales de comunicar a las personas afectadas; informar a una autoridad competente; preservar determinada información; realizar una denuncia; comunicar a un asegurador; o adoptar alguna otra actuación.

Esta evaluación deberá efectuarse conforme a la legislación vigente al momento del incidente y a las circunstancias particulares del caso.

Las decisiones de notificación deberán documentar su fundamento jurídico y respetar los principios de necesidad, proporcionalidad y mínima divulgación. Cuando exista duda razonable sobre una obligación de reporte o sobre el alcance del secreto profesional, deberá obtenerse evaluación jurídica antes de divulgar información, salvo que una actuación inmediata sea exigida inequívocamente por una norma imperativa.

Artículo 166. **Comunicación a personas afectadas.** Cuando la comunicación resulte jurídicamente obligatoria o sea razonablemente necesaria para que la persona afectada pueda proteger sus derechos, bienes, credenciales o intereses legítimos, ATRIRD deberá efectuarla oportunamente. En los demás casos podrá realizarla después de valorar la naturaleza de la información, el riesgo de daño y las exigencias de confidencialidad aplicables.

La comunicación deberá ser clara y proporcional e indicar, cuando corresponda, la naturaleza del incidente, información posiblemente comprometida, medidas adoptadas y actuaciones razonablemente recomendables.

No deberán realizarse afirmaciones especulativas ni atribuciones prematuras de responsabilidad.

Artículo 167. **Comunicación pública.** La comunicación externa sobre un incidente deberá realizarse únicamente por las personas autorizadas institucionalmente.

Deberá preservarse la exactitud de la información, los derechos de las personas afectadas, la confidencialidad de la investigación y la seguridad de los sistemas.

Artículo 168. **Recuperación.** Una vez controlado el incidente, deberán adoptarse las medidas necesarias para restaurar de forma segura los sistemas, accesos e información afectados.

Antes de restablecer servicios críticos deberá procurarse razonablemente verificar que la vulnerabilidad que originó el incidente haya sido eliminada o suficientemente mitigada.

Artículo 169. **Cierre.** Un incidente podrá cerrarse cuando se hayan completado razonablemente la contención, recuperación y documentación correspondiente y no existan actuaciones inmediatas pendientes.

El cierre deberá quedar documentado.

Artículo 170. **Evaluación posterior.** Los incidentes relevantes deberán ser objeto de una revisión posterior destinada a determinar sus causas y las medidas necesarias para reducir la probabilidad de repetición.

La revisión podrá generar recomendaciones sobre controles de acceso, capacitación, proveedores, contratos, configuración tecnológica, respaldo, inteligencia artificial, clasificación de información o actualización de políticas.

Artículo 171. **No represalias.** Ninguna persona deberá ser objeto de represalias por comunicar de buena fe un incidente, error, vulnerabilidad o riesgo de seguridad.

Esta protección no impedirá evaluar separadamente una conducta deliberada, fraudulenta o gravemente contraria a las obligaciones aplicables mediante los procedimientos correspondientes.

VI. Separación de Funciones

Artículo 172. Separación de funciones. La investigación técnica del incidente deberá mantenerse diferenciada, en la medida razonablemente posible, de cualquier investigación disciplinaria posterior.

La información obtenida técnicamente podrá ser considerada en un procedimiento disciplinario únicamente respetando las garantías establecidas en el Reglamento Disciplinario.

Artículo 173. Matriz Mínima de Responsabilidades sobre Datos Institucionales. La matriz siguiente establece responsabilidades mínimas y deberá aplicarse sin modificar la distribución de competencias prevista en los Estatutos Sociales de ATRIRD. La asignación operativa de una función no confiere por sí sola facultades estatutarias adicionales.

FUNCIÓN		RESPONSABILIDAD MÍNIMA
Junta Directiva	:	Aprobar las políticas generales, determinar el marco de gobernanza y supervisar los riesgos institucionales relevantes dentro de sus competencias estatutarias.
Responsable institucional de información	:	Coordinar la aplicación de la política, clasificación, controles, conservación, incidentes y revisiones periódicas. Su designación no modifica competencias estatutarias.
Propietario funcional de la información	:	Determinar la finalidad institucional, clasificación, necesidad de acceso y período razonable de conservación de la información bajo su responsabilidad.
Custodio tecnológico	:	Implementar controles técnicos, accesos, respaldos, recuperación, seguridad y registros conforme a las instrucciones institucionales autorizadas.
Usuarios autorizados	:	Utilizar la información exclusivamente para fines legítimos, proteger credenciales, respetar la clasificación y comunicar incidentes.
Comité Disciplinario	:	Custodiar y utilizar la información de expedientes disciplinarios dentro de sus competencias, garantizando confidencialidad, acceso restringido y debido proceso.
Terceros y proveedores	:	Utilizar la información únicamente para los fines autorizados, aplicar las medidas de seguridad acordadas, restringir accesos, comunicar incidentes y devolver o eliminar la información conforme a las obligaciones aplicables.
Responsable de respuesta al incidente	:	Coordinar la recepción, registro, evaluación, contención, recuperación, documentación y cierre del incidente, convocando apoyo técnico, jurídico o administrativo cuando resulte necesario.
Asesoría jurídica o función jurídica designada	:	Evaluar, cuando proceda, obligaciones legales o contractuales de comunicación, preservación, cooperación con autoridades, secreto profesional y demás consecuencias jurídicas del incidente.

Comunicaciones institucionales	Gestionar, cuando sea necesario, las comunicaciones públicas o externas autorizadas sobre el incidente, preservando exactitud, confidencialidad y derechos de las personas afectadas.
--------------------------------	---

VII. Disposiciones Finales

Artículo 174. **Cláusula de coordinación y revisión.** Este Procedimiento deberá revisarse periódicamente y siempre que un incidente relevante, cambio tecnológico, modificación normativa o experiencia institucional evidencie la necesidad de ajustar sus controles. Los protocolos técnicos que se adopten para su ejecución no podrán modificar los Estatutos Sociales, crear infracciones o sanciones ni ampliar las competencias de los órganos de ATRIRD.