BORRADOR DE REGLAMENTO PARA EL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS Y DATOS PERSONALES ASOCIADOS A LA IDENTIDAD DE LAS PERSONAS Y LA PROVISIÓN DEL SERVICIO DE CONSULTA, VERIFICACIÓN Y CERTIFICACIÓN DE IDENTIDAD

La JUNTA CENTRAL ELECTORAL (JCE), institución autónoma de derecho público, con personalidad jurídica, creada y organizada por la Constitución de la República Dominicana y regida por la Ley Orgánica del Régimen Electoral No. 20-23, regularmente constituida en su sede principal, situada en la intersección formada por las avenidas 27 de Febrero y Gregorio Luperón, frente a la "Plaza de la Bandera", en el municipio Santo Domingo Oeste, Provincia Santo Domingo, República Dominicana; integrada por **Román Andrés Jáquez Liranzo**, Presidente; **Dolores Altagracia Fernández Sánchez**, Miembro Titular; **Samir Rafael Chami Isa**, Miembro Titular; **Hirayda Marcelle Fernández Guzmán**, Miembro Titular y; **Rafael Armando Vallejo Santelises**, Miembro Titular; asistidos por **Sonne Beltré Ramírez**, Secretario General, con el voto unánime de sus miembros ha adoptado el siguiente reglamento.

CONSIDERANDO PRIMERO: Que el artículo 8 de la Constitución es función esencial del Estado dominicano *"[…] la protección efectiva de los derechos de la persona, el respeto de su dignidad y la obtención de los medios que le permitan perfeccionarse de forma igualitaria, equitativa y progresiva, dentro de un marco de libertad individual y de justicia social, compatibles con el orden público, el bienestar general y los derechos de todos y todas*".

CONSIDERANDO SEGUNDO: Que la Constitución de la República en su artículo 212, párrafo II, establece que *"serán dependientes de la Junta Central Electoral el Registro Civil y la Cédula de Identidad y Electoral".* Que, asimismo, el referido artículo dispone en su parte in fine, que la Junta Central Electoral *"…tiene facultad reglamentaria en los asuntos de su competencia"*.

CONSIDERANDO TERCERO: Que el artículo 14, numeral 2 de la Ley núm. 20-23, Orgánica del Régimen Electoral, consagra que "*La Junta Central Electoral tiene las siguientes atribuciones: 2) custodiar, mantener y conservar el Registro Civil*".

CONSIDERANDO CUARTO: Que la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, en su artículo 15 dispone que la Junta Central Electoral, encabezada por el Pleno, ejerce la rectoría del Sistema Nacional de Registro del Estado Civil, a cuyo efecto dictará las normas administrativas relativas a su funcionamiento y organización, de conformidad con lo dispuesto en dicha ley.

CONSIDERANDO QUINTO: Que el artículo 16 numeral 4 de la antedicha pieza legislativa, expresa que son atribuciones de la Junta Central Electoral "dictar reglamentos, resoluciones y circulares concernientes al estado civil de las personas".

CONSIDERANDO SEXTO: Que la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, del 18 de enero de 2023, contiene un conjunto de mandatos reglamentarios sobre diferentes aspectos de dicha ley que, debido a su naturaleza y particularidades ameritan ser complementados y desarrollados por la Junta Central Electoral a través de un reglamento de aplicación, tal y como lo preceptúa el artículo 214 de la indicada ley.

CONSIDERANDO SÉPTIMO: Que la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, del 18 de enero de 2023, regula en sus artículos 55 al 61 inclusive, lo concerniente de los datos biométricos de las personas; en ese sentido, el párrafo I del citado artículo 61 de la referida ley dispone que: "*La Junta Central Electoral regulará el acceso a los datos biométricos de las personas asentadas en sus bases de datos para fines de consulta y verificación de identidad".* Que, en ejercicio de las competencias que le atribuyen la Constitución de la República y la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, la Junta Central Electoral elaboró el presente reglamento para regular el tratamiento de datos biométricos de las personas y la provisión del servicio de consulta, verificación y certificación de identidad.

CONSIDERANDO OCTAVO: Que, entre el 22 y el 26 de julio de 2024 se sostuvo una primera ronda de reuniones bilaterales con el Banco Central, la Superintendencia de Bancos, la Asociación de Bancos Múltiples (ABA), el Instituto Dominicano de las Telecomunicaciones (INDOTEL) y la Dirección General de Migración. Una segunda ronda incorporó al Consejo Nacional de Discapacidad (CONADIS). De ese proceso se recibieron ciento treinta y siete (137) comentarios específicos, cuyo tratamiento consta en el informe elaborado por la Oficina Técnica de la Comisión de Tecnología.

CONSIDERANDO NOVENO: Que, la Junta Central Electoral, en cumplimiento a lo dispuesto la Ley núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, del 8 de agosto de 2013, socializó el borrador del presente reglamento con las principales instituciones bancarias y el sector financiero, a los fines de recibir de parte de estos sus opiniones y consideraciones, las cuales fueron recibidas por escrito, siendo dichas entidades las siguientes: 1) El Banco Central de la República Dominicana (Oficio núm. 11774, del 27 de octubre de 2025); 2) La Liga Dominicana de Asociaciones de Ahorros y Préstamos, LIDAAPI (Comunicación núm. 21-2025, del 22 de agosto de 2025); 3) La Superintendencia de Bancos (Comunicación COM-REG-202500199) y; 3) La Asociación de Bancos Múltiples de la República Dominicana, ABA (Matriz de observaciones remitida el 18 de agosto de 2025). De esos cuatro documentos se extrajeron y analizaron un total de ciento treinta (130) recomendaciones específicas, con lo cual este órgano ha dada cumplimiento a lo dispuesto por

CONSIDERANDO DÉCIMO: Que, asimismo y durante el proceso de elaboración del presente reglamento, la Junta Central Electoral, tambien analizó y tomó en consideración el marco jurídico general, previsto, tanto en la Constitución de la República como en los tratados internacionales afines a la materia y todas aquellas leyes que tienen incidencia en el ámbito de regulacion a que se circunscribe el presente reglamento, a los fines de que cada uno de los temas que se tratan en el mismo, cuente con el suficiente y adecuado respaldo jurídico y que permita garantizar una regulacion con todos los estándares de seguridad, trazabilidad e integridad que amerita el tratamiento de datos biométricos de las personas y la provisión del servicio de consulta, verificación y certificación de identidad.

CONSIDERANDO DÉCIMO PRIMERO: Que mediante la sentencia TC/0267/26, del 19 de mayo de 2026, el Tribunal Constitucional confirmó la facultad del Instituto Nacional de Protección de los Derechos del Consumidor (Pro Consumidor) para intervenir, conforme a la Ley núm. 358-05, frente a un tratamiento irregular de datos biométricos realizado por un tercero, estableciendo que no cualquier entidad puede recolectar y procesar dicha categoría de datos. Que dicho precedente confirma la necesidad de que la Junta Central Electoral coordine el ejercicio de sus competencias con las de otros órganos reguladores sectoriales, a fin de evitar conflictos de competencia en el tratamiento de datos biométricos que no se vinculen directamente con el Registro Civil o la cedulación.

VISTA: La Constitución de la República Dominicana, proclamada el 27 de octubre de 2024.

VISTA: La Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948.

VISTO: El Pacto Internacional de Derechos Civiles y Políticos del 16 de diciembre de 1966, ratificado por la República Dominicana en 1978.

VISTA: La Convención Americana de los Derechos Humanos “Pacto de San José” de 1978, ratificada por la República Dominicana el 21 de enero de 1978.

VISTO: El Código Civil Dominicano del 17 de abril de 1884.

VISTA: La Ley núm.126-02, sobre el Comercio Electrónico, Documentos y Firma Digitales, del 4 de septiembre de 2002.

VISTA: La Ley núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002.

VISTA: La Ley núm. 136-03, Código para el Sistema de Protección de Niños, Niñas y Adolescentes del 7 de agosto de 2003.

VISTA: La Ley núm. 200-04 de Libre Acceso a la Información Pública, del 25 de febrero de 2004.

VISTA: La Ley núm. 5-13 sobre Discapacidad, del 16 de enero de 2013.

VISTA: La Ley núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, del 8 de agosto de 2013.

VISTA: La Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, del 15 de diciembre de 2013.

VISTA: La Ley núm. 155-17 contra el Lavado de Activos y el Financiamiento del Terrorismo, del 1 de junio de 2017;

VISTA: La Ley núm. 4-23, Orgánica de los Actos del Estado Civil, del 18 de enero de 2023.

VISTA: La Ley núm. 20-23, Orgánica del Régimen Electoral, del 17 de febrero de 2023.

VISTA: La sentencia núm. TC/0267/26, dictada por el Tribunal Constitucional dominicano en fecha 19 de mayo de 2026.

TÍTULO I

DE LAS DISPOSICIONES FUNDAMENTALES

CAPÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN, DEFINICIONES Y PRINCIPIOS RECTORES

SECCIÓN I

OBJETO Y AMBITO DE APLICACIÓN

Artículo 1. Objeto. El presente reglamento tiene por objeto regular el tratamiento de datos biométricos asociados a la identidad de las personas, así como las condiciones, límites, garantías, procedimientos y responsabilidades aplicables al servicio de consulta, verificación y certificación de identidad provisto por la Junta Central Electoral, conforme a la Constitución de la República, la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, la normativa de protección de datos personales y demás disposiciones legales aplicables. El presente reglamento desarrolla y aplica, en lo que concierne a los datos biométricos bajo custodia de la Junta Central Electoral, la Ley núm. 4-23 y la Ley núm. 172-13, sin crear un régimen general y autónomo de protección de datos personales, materia reservada a la ley conforme a los artículos 44 y 70 de la Constitución.

Párrafo I: Asimismo, establece los derechos de los titulares, las obligaciones de los responsables, encargados y usuarios del servicio, las condiciones de acceso y uso del servicio provisto por la Junta Central Electoral, las reglas sobre consentimiento, conservación, cesión, eliminación, seguridad, trazabilidad, auditoría, supervisión e incumplimiento relacionadas con el tratamiento de datos biométricos y la consulta, verificación o certificación de identidad.

Párrafo II. El servicio de consulta, verificación y certificación de identidad, incluida la identidad digital, firma electrónica e interoperabilidad, regulado por el presente reglamento, forma parte del ecosistema institucional de servicios de identidad de la Junta Central Electoral y se articula con los registros, bases de datos y fuentes oficiales bajo su competencia, incluyendo, cuando corresponda, el Archivo Maestro de Cedulados y demás sistemas institucionales de identidad. Dicho servicio tendrá un régimen especializado por involucrar datos biométricos y datos personales asociados a la identidad, y se sujetará a las condiciones técnicas, jurídicas, tarifarias, de seguridad, trazabilidad, confidencialidad, consentimiento, finalidad,

evaluación, auditoría y control previstas en el presente reglamento, en las resoluciones de la Junta Central Electoral y en los instrumentos aplicables.

Artículo 2. Ámbito de aplicación. Las disposiciones del presente reglamento son aplicables a la recopilación, captura, tratamiento, procesamiento, almacenamiento, conservación, consulta, verificación, certificación, transmisión, cesión, supresión o eliminación de datos biométricos y datos personales asociados a la identidad, cuando dichos tratamientos se encuentren vinculados a las competencias atribuidas a la Junta Central Electoral por la Constitución de la República, la Ley núm. 4-23 y demás normativa aplicable.

Párrafo: También serán aplicables a las entidades públicas o privadas que soliciten, accedan, utilicen o se integren al servicio de consulta, verificación y certificación de identidad provisto por la Junta Central Electoral, así como a los responsables, encargados, usuarios, terceros autorizados y demás personas físicas o jurídicas que intervengan en tratamientos regulados por el presente reglamento.

SECCIÓN II

DE LAS DEFINICIONES

Artículo 3. Definiciones. Además de las definiciones dispuestas en la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, su reglamento de aplicación, la Ley núm. 172-13 sobre Protección Integral de los Datos Personales, y demás normas aplicables, para los fines del presente reglamento se entenderá por:

1) **Algoritmo biométrico:** Secuencia de instrucciones, reglas, operaciones o procedimientos técnicos utilizados por un sistema biométrico para capturar, procesar, extraer, analizar, comparar o evaluar características biométricas, con la finalidad de realizar procesos de identificación, verificación, autenticación o validación biométrica, conforme a los límites establecidos por la ley y el presente reglamento.

2) **Archivo, registro, fichero, base o banco de datos biométricos:** Conjunto organizado de datos biométricos o datos personales asociados a la identidad, contenidos en medios físicos, digitales, electrónicos, automatizados o cualquier otro soporte técnico, que sean objeto de tratamiento o procesamiento, cualquiera que fuere la forma o modalidad de su creación, captura, recopilación, almacenamiento, organización, conservación, consulta, acceso, transmisión, interconexión, supresión o eliminación.

3) **Archivo, registro, fichero, base o banco de datos biométricos bajo competencia de la Junta Central Electoral:** Conjunto organizado de datos biométricos y datos personales asociados a la identidad cuya recopilación, almacenamiento, tratamiento, procesamiento, administración, consulta, verificación o certificación corresponda a la Junta Central Electoral, de conformidad con la Constitución de la República, la Ley núm. 4-23, el presente reglamento y demás disposiciones aplicables.

4) **Autenticación biométrica:** Uso de características biométricas como factor de confirmación o validación de identidad dentro de un proceso de acceso, control, operación, transacción, prestación de servicio o relación directa entre el titular y el responsable del tratamiento. Cuando la autenticación implique consulta, comparación, verificación o certificación contra datos biométricos o datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, deberá realizarse a través del Servicio de Consulta, Verificación y Certificación de Identidad provisto por esta o mediante los mecanismos técnicos autorizados y regulados por la Junta Central Electoral.

5) **Aviso de privacidad:** Documento, comunicación o mecanismo físico, electrónico, digital o tecnológico mediante el cual el responsable del tratamiento informa al titular, de manera previa, clara, sencilla, accesible y comprensible, sobre las condiciones bajo las cuales serán tratados sus datos biométricos o datos personales asociados a la identidad, incluyendo, como mínimo, la identidad del responsable, las finalidades del tratamiento, la base legal aplicable, los datos objeto

de tratamiento, los destinatarios o categorías de destinatarios cuando corresponda, el plazo de conservación, los derechos que asisten al titular, los mecanismos para ejercerlos y las medidas generales de seguridad y confidencialidad aplicables.

6) **Base biométrica paralela, sustitutiva o no autorizada:** Archivo, registro, fichero, base, banco de datos, sistema, plataforma, repositorio, conjunto de plantillas, vectores, patrones, códigos biométricos, muestras biométricas o mecanismos de vinculación creado, mantenido, alimentado, actualizado, explotado o utilizado por una entidad pública o privada, por cuenta propia, dentro de un grupo económico o a favor de terceros, con capacidad de realizar identificación, verificación, autenticación, comparación o tratamiento biométrico autónomo fuera de los límites autorizados por la Ley núm. 4-23, el presente reglamento, las resoluciones de la Junta Central Electoral o las condiciones del servicio provisto por esta.

7) **Biometría:** Disciplina, tecnología o conjunto de métodos que permiten reconocer, identificar, verificar o autenticar a una persona a partir del análisis automatizado o semiautomatizado de características físicas, biológicas, fisiológicas, morfológicas, conductuales o de patrón atribuibles a dicha persona.

8) **Cancelación:** Procedimiento mediante el cual el responsable del tratamiento cesa en el uso activo de datos biométricos o datos personales asociados a la identidad, procediendo, según corresponda, a su bloqueo, restricción, supresión o eliminación segura, conforme a la ley, el presente reglamento y las condiciones aplicables. El bloqueo solo podrá mantenerse de manera excepcional, temporal y limitada cuando exista una obligación legal expresa compatible con la Ley núm. 4-23 o un requerimiento concreto de autoridad competente, exclusivamente para la atención de responsabilidades legales, administrativas o judiciales, sin que ello habilite el uso, consulta, reutilización, comparación biométrica, transferencia, explotación o tratamiento ulterior de los datos biométricos.

9) **Cedente:** Persona física o jurídica, pública o privada, órgano o entidad que comunica, transfiere, revela o pone a disposición datos biométricos o datos personales asociados a la identidad a un cesionario, conforme a los supuestos, condiciones y límites previstos por la ley y el presente reglamento.

10) **Cesión o comunicación de datos:** Tratamiento mediante el cual datos biométricos o datos personales asociados a la identidad son revelados, comunicados, transferidos o puestos a disposición de una persona física o jurídica, pública o privada, distinta del titular, del responsable o del encargado del tratamiento, conforme a la ley y al presente reglamento.

11) **Cesionario:** Persona física o jurídica, pública o privada, órgano o entidad que recibe datos biométricos o datos personales asociados a la identidad como resultado de una cesión o comunicación de datos, quedando sujeto a las obligaciones legales, técnicas, organizativas, de seguridad, confidencialidad y finalidad aplicables.

12) **Certificación de identidad:** Actuación mediante la cual la Junta Central Electoral confirma, acredita o hace constar oficialmente la identidad de una persona, a partir de la validación de datos biométricos, datos documentales y datos personales asociados a la identidad bajo su competencia, conforme a la Ley núm. 4-23, el presente reglamento y las condiciones técnicas y procedimentales establecidas por la Junta Central Electoral.

13) **Consentimiento del titular:** Manifestación de voluntad libre, específica, informada, inequívoca y verificable mediante la cual el titular autoriza el tratamiento de sus datos biométricos o datos personales asociados a la identidad para una o varias finalidades determinadas, salvo los supuestos en que exista habilitación legal expresa conforme a la ley y al presente reglamento.

14) **Consentimiento expreso:** Manifestación clara, afirmativa y verificable de voluntad del titular, otorgada por escrito, medios electrónicos verificables, firma, validación digital, aceptación

expresa u otro mecanismo fehaciente que permita dejar constancia comprobable de su otorgamiento, finalidad, alcance, fecha, medio utilizado e identidad del titular.

15) **Consentimiento tácito:** Manifestación de voluntad que puede inferirse de actos u omisiones del titular. El consentimiento tácito no será válido para el tratamiento de datos biométricos ni para aquellos tratamientos de datos personales asociados a la identidad que, por su naturaleza, finalidad, riesgo o impacto sobre derechos fundamentales, requieran consentimiento expreso, específico, informado, inequívoco y verificable.

16) **Cotejo forense:** Comparación de una muestra o imagen biométrica latente, obtenida lícitamente en el curso de una investigación, contra la base bajo competencia de la Junta Central Electoral, a solicitud de la autoridad competente, cuyo resultado se entrega como constancia sin transferencia del dato del titular.

17) **Credenciales de acceso:** Conjunto de elementos, datos, certificados, claves, perfiles, identificadores, tokens, factores de autenticación o mecanismos de seguridad asignados a una persona, sistema, aplicación o entidad autorizada para acceder a un servicio, plataforma, recurso tecnológico o mecanismo regulado por el presente reglamento.

18) **Datos biométricos:** Datos personales obtenidos a partir de un tratamiento técnico específico relativo a características físicas, biológicas, fisiológicas, morfológicas, conductuales o de patrón de una persona física, que permitan o contribuyan a su identificación, verificación o autenticación de manera única o diferenciada. Los datos biométricos podrán comprender, entre otros, huellas dactilares, rasgos faciales, iris, retina, geometría de la mano, patrones de venas, voz, firma manuscrita, dinámica de tecleo, forma de caminar, cicatrices, marcas, tatuajes u otros rasgos físicos o conductuales utilizados técnicamente para fines de identificación, verificación o autenticación.

19) **Datos personales asociados a la identidad:** Datos que permiten individualizar, identificar, verificar o certificar la identidad de una persona física, cuando sean administrados, tratados, utilizados, verificados, certificados o autorizados por la Junta Central Electoral en el ejercicio de sus competencias constitucionales y legales en materia de Registro Civil, identificación, cedulación y servicios de consulta, verificación o certificación de identidad. Estos datos comprenden, entre otros, datos biométricos, nombres y apellidos, fecha y lugar de nacimiento, sexo, nacionalidad, número único de identidad (NUI), número de cédula de identidad y electoral, fotografía, firma, datos documentales, datos registrales y cualquier otro dato administrado, utilizado o autorizado por la Junta Central Electoral para fines de identidad.

20) **Delegado/a de Protección de Datos:** Persona designada por el responsable o encargado del tratamiento para asesorar, supervisar, coordinar y dar seguimiento al cumplimiento de las obligaciones relativas a la protección de datos personales asociados a la identidad y datos biométricos, así como para servir de punto de contacto con los titulares, la Junta Central Electoral y, cuando corresponda, las autoridades competentes.

21) **Dispositivo de captura biométrica:** Equipo, sensor, lector, cámara, escáner, terminal, aplicación, componente tecnológico o mecanismo utilizado para capturar, registrar, adquirir o convertir una característica biométrica en una muestra biométrica susceptible de tratamiento técnico.

22) **Encargado del tratamiento:** Persona física o jurídica, pública o privada, órgano o entidad que trate datos biométricos o datos personales asociados a la identidad por cuenta del responsable del tratamiento, conforme a sus instrucciones, al contrato o instrumento jurídico correspondiente, a la ley y al presente reglamento.

23) **Entidad usuaria del servicio:** Persona jurídica, pública o privada, órgano o entidad que, previa autorización de la Junta Central Electoral accede o utiliza el Servicio de Consulta, Verificación y Certificación de Identidad, conforme a la Ley núm. 4-23, el presente reglamento, las resoluciones de la Junta Central Electoral y las condiciones contractuales, técnicas y de seguridad aplicables.

24) **Entidades públicas:** El Poder Legislativo del Estado, compuesto por el Congreso Nacional y cualquiera de sus dependencias; el Poder Ejecutivo del Estado y todas las dependencias y entidades de la administración pública; el Poder Judicial del Estado y todos sus órganos; los ayuntamientos; organismos autónomos y descentralizados; órganos constitucionales autónomos; y cualquier otra entidad a la que la Constitución y las leyes le reconozcan naturaleza pública.

25) **Evaluación de impacto:** Proceso sistemático, documentado y previo orientado a identificar, analizar, evaluar y mitigar los riesgos que un tratamiento de datos biométricos o datos personales asociados a la identidad pueda generar sobre los derechos de los titulares, la privacidad, la seguridad, la confidencialidad, la trazabilidad, la integridad de los datos y la competencia institucional de la Junta Central Electoral.

26) **Identificación biométrica:** Proceso técnico mediante el cual se determina o establece la identidad de una persona mediante la comparación uno a muchos (1:N) de sus características biométricas con datos biométricos previamente registrados en una base o sistema de referencia. Cuando dicha identificación se realice sobre datos biométricos o datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, deberá sujetarse a la Ley núm. 4-23, al presente reglamento y a las condiciones establecidas por la Junta Central Electoral.

27) **Información pública:** Todo registro, documento, archivo o dato que se encuentre en poder de entidades públicas y que, conforme a la Constitución, la Ley núm. 200-04 sobre Libre Acceso a la Información Pública y demás normativa aplicable, esté sujeto al principio de publicidad. Esta definición no comprende ni habilita el acceso, divulgación o publicidad de datos biométricos, datos personales asociados a la identidad, plantillas, vectores, patrones, códigos biométricos, minucias, mecanismos de vinculación o informaciones protegidas por confidencialidad, reserva legal, seguridad, privacidad o protección de datos personales.

28) **Interfaz de Programación de Aplicaciones (API, por sus siglas en inglés):** Conjunto de reglas, protocolos o mecanismos técnicos mediante los cuales una entidad usuaria autorizada puede interactuar, de forma segura, controlada, trazable y limitada, con los sistemas o servicios provistos por la Junta Central Electoral, conforme a las especificaciones técnicas, condiciones de acceso, finalidades autorizadas y medidas de seguridad aplicables.

29) **Minucias biométricas:** Características distintivas localizadas en una huella dactilar que se utilizan para individualizar y comparar huellas dactilares, tales como bifurcaciones, terminaciones de crestas u otros puntos característicos empleados técnicamente en procesos de identificación, verificación o autenticación biométrica.

30) **Muestra biométrica:** Representación capturada de una característica biométrica de una persona, obtenida mediante un dispositivo, sistema o procedimiento de captura, que puede ser utilizada para extraer, procesar, comparar o verificar datos biométricos.

31) **Muestra biométrica latente.** Rasgo biométrico —dactilar, palmar o facial— recolectado de una superficie, objeto, imagen o registro, no aportado directamente por el titular.

32) **Persona identificable:** Toda persona física identificada o identificable cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural, social, biométrica, documental o registral.

33) **Plantilla biométrica:** Representación técnica, matemática, digital o codificada derivada de una muestra biométrica, generada mediante procesamiento técnico o algorítmico, que permite comparar, verificar, identificar o autenticar a una persona, sin que necesariamente reproduzca la muestra biométrica original.

34) **Procedimiento de disociación:** Todo tratamiento técnico aplicado a datos biométricos o datos personales asociados a la identidad mediante el cual la información obtenida no pueda asociarse

directamente a una persona determinada o determinable sin el uso de información adicional, medidas técnicas o claves de vinculación separadas. La disociación podrá comprender técnicas de codificación, seudonimización, separación lógica o física de datos, u otros mecanismos de seguridad que reduzcan el riesgo de identificación, sin perjuicio de las obligaciones de confidencialidad, seguridad y control aplicables.

35) **Registro o constancia de consulta:** Registro, evidencia o constancia generada como resultado del uso autorizado del Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral, que podrá contener información limitada sobre la operación realizada, tales como fecha, hora, entidad usuaria, finalidad autorizada, tipo de consulta, identificador transaccional, respuesta o resultado permitido, sin incluir muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que permitan tratamiento biométrico autónomo.

36) **Responsable del tratamiento de datos biométricos:** Persona física o jurídica, organismo público o entidad privada que, conforme a la ley, el presente reglamento y, cuando corresponda, la autorización de la Junta Central Electoral determina los fines, medios, alcance y condiciones del tratamiento de datos biométricos o datos personales asociados a la identidad.

37) **Resultado de verificación o certificación:** Respuesta, validación, constancia o información generada por el Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral, limitada a confirmar, rechazar o informar el resultado autorizado de una consulta, verificación o certificación de identidad, sin que ello implique transferencia, cesión, entrega, réplica o almacenamiento de datos biométricos, muestras, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación.

38) **Servicio de Consulta, Verificación y Certificación de Identidad:** Servicio prestado por la Junta Central Electoral que permite consultar, verificar o certificar la identidad de una persona mediante la validación de datos biométricos y datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, a través de mecanismos técnicos, operativos, digitales, contractuales o de interoperabilidad autorizados, regulados y supervisados por esta.

39) **Seudonimización:** Tratamiento técnico mediante el cual los datos biométricos o datos personales asociados a la identidad dejan de poder atribuirse directamente a una persona específica sin utilizar información adicional, siempre que dicha información adicional se conserve separada y sujeta a medidas técnicas y organizativas destinadas a impedir la identificación no autorizada del titular.

40) **Sistema biométrico:** Sistema, plataforma, aplicación, infraestructura, conjunto de dispositivos o solución tecnológica destinada a capturar, procesar, almacenar, comparar, identificar, verificar, autenticar o gestionar datos biométricos o datos personales asociados a la identidad.

41) **Tercero:** Persona física o jurídica, pública o privada, órgano o entidad distinta del titular, del responsable del tratamiento, del encargado del tratamiento o de la Junta Central Electoral, según corresponda, que intervenga o pueda intervenir en una comunicación, cesión, acceso, prestación, subcontratación o tratamiento de datos biométricos o datos personales asociados a la identidad.

42) **Titular de los datos biométricos:** Persona física identificada o identificable a quien corresponden, pertenecen o se refieren los datos biométricos o datos personales asociados a la identidad objeto de tratamiento.

43) **Tratamiento biométrico autónomo:** Capacidad técnica, operativa o funcional de recopilar, almacenar, conservar, procesar, comparar, consultar, verificar, autenticar, identificar, reutilizar o explotar datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación sin depender del Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral o fuera de las condiciones autorizadas por esta.

44) **Tratamiento de datos biométricos:** Cualquier operación o conjunto de operaciones, automatizadas o no, realizadas sobre datos biométricos o datos personales asociados a la identidad, tales como recopilación, captura, registro, organización, estructuración, conservación, almacenamiento, adaptación, modificación, extracción, consulta, cotejo, comparación, uso, comunicación, transmisión, cesión, interconexión, limitación, bloqueo, supresión, eliminación o destrucción.

45) **Usuario autorizado:** Persona física, perfil técnico, funcionario, empleado, agente, representante, sistema, aplicación o componente tecnológico habilitado por una entidad usuaria o por la Junta Central Electoral para acceder, operar o interactuar con un sistema, servicio, plataforma o mecanismo regulado por el presente reglamento, conforme a permisos, roles, credenciales, condiciones y límites previamente establecidos.

46) **Vector, patrón, código biométrico o mecanismo de vinculación:** Representación técnica, matemática, alfanumérica, codificada, cifrada, seudonimizada o estructurada derivada de datos biométricos o datos personales asociados a la identidad, que permita o facilite la comparación, vinculación, verificación, autenticación, identificación o tratamiento biométrico de una persona.

47) **Verificación biométrica:** Proceso técnico mediante el cual se confirma que una persona es quien afirma ser, a partir de la comparación uno a uno (1:1) entre sus características biométricas presentadas y los datos biométricos previamente registrados o asociados a su identidad. Cuando la verificación tenga efectos frente a terceros o se realice contra datos biométricos o datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, deberá realizarse mediante el servicio provisto por esta o por los mecanismos autorizados y regulados por la Junta Central Electoral.

Párrafo. Las definiciones previstas en la Ley núm. 172-13 sobre Protección Integral de los Datos Personales asentados en archivos, registros públicos, bancos de datos y otros medios técnicos serán supletorias para este reglamento, en la medida en que resulten compatibles y aplicables al tratamiento de datos biométricos y datos personales asociados a la identidad.

SECCIÓN III

DE LOS PRINCIPIOS RECTORES

Artículo 4. Principios rectores. Además de los principios rectores contenidos en el Reglamento de Aplicación de la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, las actuaciones, decisiones, tratamientos, servicios, mecanismos de consulta, verificación y certificación de identidad, y demás operaciones reguladas por el presente reglamento respecto de datos biométricos y datos personales asociados a la identidad bajo competencia de la Junta Central Electoral se regirán por los principios siguientes:

1) **Principio de juridicidad.** El tratamiento de los datos biométricos y de los datos personales asociados a la identidad deberá realizarse conforme a las facultades y atribuciones conferidas por la Constitución, la ley, el presente reglamento y las demás normas aplicables, en armonía con el ordenamiento jurídico.

2) Principio de calidad. Los datos biométricos y los datos personales asociados a la identidad deberán ser adecuados, pertinentes, precisos, correctos y proporcionales al ámbito y finalidad para los que fueron obtenidos, y mantenerse actualizados cuando ello resulte necesario.

3) Principio de minimización. Solo deberán recopilarse, procesarse, consultarse, conservarse o almacenarse los datos biométricos y los datos personales asociados a la identidad que sean adecuados, pertinentes y limitados a lo estrictamente necesario para la finalidad legítima perseguida.

4) Principio de seguridad. El tratamiento de los datos biométricos y de los datos personales asociados a la identidad deberá contar con medidas técnicas, organizativas, administrativas y jurídicas razonables y adecuadas —incluyendo, de manera enunciativa y no limitativa, cifrado, control de acceso, gestión de identidad, trazabilidad, segregación de funciones, monitoreo y auditoría que los protejan contra el acceso no autorizado o ilícito y contra su pérdida, divulgación, alteración, destrucción, daño accidental, uso indebido o tratamiento no autorizado.

5) Principio de transparencia. Al titular deberá proporcionársele información clara, previa, accesible y comprensible sobre la forma en que se tratarán, utilizarán y protegerán sus datos biométricos y datos personales asociados a la identidad, así como sobre sus derechos, el carácter obligatorio o facultativo de proporcionarlos, las consecuencias de hacerlo o no, la finalidad del tratamiento y los mecanismos para ejercer sus derechos, salvo disposición legal expresa en contrario.

6) Principio de consentimiento explícito. El tratamiento de los datos biométricos y de los datos personales asociados a la identidad deberá realizarse con el consentimiento libre, expreso, informado, específico, verificable e inequívoco del titular, salvo disposición legal expresa compatible con la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

7) Principio de tratamiento leal. Los datos biométricos y los datos personales asociados a la identidad solo podrán recolectarse, usarse, almacenarse, modificarse, consultarse, transmitirse, cotejarse, limitarse, suprimirse o destruirse por medios lícitos, leales, transparentes y compatibles con la finalidad autorizada.

8) Principio de confidencialidad. Toda persona que intervenga en cualquier fase del tratamiento de los datos biométricos y de los datos personales asociados a la identidad deberá guardar secreto y confidencialidad respecto de estos. Esta obligación subsistirá aun después de finalizada la relación que dio origen al tratamiento.

9) Principio de información, acceso y corrección. El titular tendrá derecho a recibir información sobre el tratamiento de sus datos biométricos y datos personales asociados a la identidad, acceder a estos y solicitar su corrección, rectificación o actualización cuando resulten inexactos, incompletos o desactualizados. Estas solicitudes deberán ser atendidas de manera oportuna por los responsables del tratamiento, sin perjuicio de los demás derechos reconocidos por la ley y el presente reglamento.

10) Principio de retención limitada. Los datos biométricos y los datos personales asociados a la identidad deberán mantenerse únicamente durante el tiempo necesario, proporcional y legítimo para cumplir la finalidad específica para la cual fueron recolectados, tratados o consultados, conforme al consentimiento otorgado por el titular, la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento. Cumplida dicha finalidad, vencido o retirado el consentimiento, o desaparecida la causa que justificó su tratamiento, deberán ser suprimidos o eliminados de forma segura, salvo disposición legal expresa compatible con la Ley núm. 4-23 o requerimiento concreto de autoridad competente.

11) Principio de responsabilidad. En todo tratamiento de datos biométricos y datos personales asociados a la identidad, el responsable o encargado deberá adoptar medidas efectivas para demostrar el cumplimiento de la ley y del presente reglamento, incluyendo políticas, procedimientos, controles, programas de capacitación, mecanismos de supervisión, gestión de riesgos, atención de reclamaciones, auditoría, trazabilidad y protección de datos desde el diseño y por defecto.

12) Principio de finalidad legítima. El tratamiento de los datos biométricos y de los datos personales asociados a la identidad deberá realizarse para fines específicos, explícitos, legítimos e informados al titular, y no podrán ser tratados ulteriormente para fines incompatibles, distintos o no autorizados. La invocación de una relación contractual, una obligación legal, una finalidad de

interés público, la prevención de fraude, la continuidad operativa, la gestión de riesgos o el cumplimiento normativo no eximirá al responsable de demostrar la necesidad, proporcionalidad, juridicidad y compatibilidad del tratamiento con la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

13) Principio de exactitud de los datos. Los datos biométricos y los datos personales asociados a la identidad deberán ser exactos y mantenerse debidamente actualizados. Deberán adoptarse las medidas necesarias para rectificar, actualizar, limitar o suprimir, sin dilación indebida, los datos que resulten inexactos, incompletos o desactualizados en relación con la finalidad para la que se utilizan.

14) Principio de integridad de la información. La información capturada, almacenada, consultada, procesada o transmitida por cualquier sistema, dispositivo o canal de comunicación no deberá ser accedida, alterada, manipulada, degradada o destruida por terceros no autorizados, garantizándose su integridad en todo momento.

15) Principio de disponibilidad de la información. La información deberá estar disponible para las personas, sistemas o entidades autorizadas cuando sea necesario para el cumplimiento de la finalidad legítima y autorizada, y deberá poder recuperarse ante incidentes que ocasionen pérdida, corrupción, indisponibilidad o afectación del servicio, conforme a las medidas de continuidad, respaldo y seguridad aplicables.

16) Principio de autenticidad de la información. Deberá garantizarse la veracidad de la autoría, origen, integridad y trazabilidad de la información. La información contenida en la documentación oficial es auténtica y resultado del proceso registral correspondiente; su ingreso, modificación, consulta o transmisión en equipos, sistemas o plataformas deberá realizarse únicamente por personas, sistemas o mecanismos autorizados.

17) Principio de privacidad por diseño y por defecto. Las medidas de protección de los datos biométricos y de los datos personales asociados a la identidad deberán integrarse desde la etapa de diseño, planificación, desarrollo, adquisición, implementación y operación de todo sistema, producto, servicio, plataforma o mecanismo que implique su tratamiento, garantizando su protección desde el inicio y por defecto.

18) Principio de soberanía de los datos. En virtud del cual la información generada dentro de un territorio se regirá por las leyes y demás normativas de ese país, sin importar donde se almacene o se procese.

Párrafo: Principios supletorios. Los principios previstos en la Ley núm. 4-23, Orgánica de los Actos del Estado Civil; en la Ley núm. 107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo; en la normativa de protección de datos personales; y en las demás disposiciones compatibles con el presente reglamento, serán de aplicación supletoria y complementaria a la recopilación, tratamiento, procesamiento, uso, consulta, verificación y certificación de identidad mediante datos biométricos, por las entidades públicas y privadas, según corresponda.

CAPÍTULO II

COMPETENCIA, DEBER DE CERTIFICACIÓN Y REGLAS DE INTERPRETACIÓN

Artículo 5. Competencia de la Junta Central Electoral. En concordancia con la obligación constitucional de regir el Registro Civil, la Cédula de Identidad y la Cédula de Identidad y Electoral, la Junta Central Electoral es el órgano público competente para el tratamiento de los datos biométricos y datos personales asociados a la identidad bajo su administración, con el propósito de garantizar la individualización, verificación y certificación de la identidad de las personas.

Párrafo I. La provisión a terceros del servicio de consulta, verificación y certificación de la identidad de las personas a partir de datos biométricos y datos personales asociados a la identidad es competencia

exclusiva de la Junta Central Electoral, conforme a los artículos 55, 58, 60 y 61 de la Ley núm. 4-23, Orgánica de los Actos del Estado Civil. Ninguna otra entidad, pública o privada, podrá ofrecer o prestar dicho servicio, ni atribuir a sus propios tratamientos efectos de certificación de la identidad.

Párrafo II. La competencia de la Junta Central Electoral comprende el tratamiento de los datos biométricos de las personas inscritas en el Registro Civil y de las titulares de los documentos de identidad que ella expide, a saber: la Cédula de Identidad y Electoral; la Cédula de Identidad en sus modalidades para menores de edad y para miembros de las Fuerzas Armadas y de la Policía Nacional; y la Cédula de Identidad para Extranjeros de los residentes legales.

Párrafo III. Quedan fuera del ámbito material del servicio de consulta, verificación y certificación de identidad provisto por la Junta Central Electoral los tratamientos de datos biométricos de personas extranjeras no residentes en la República Dominicana, así como aquellos tratamientos biométricos realizados para fines distintos a la verificación o certificación de identidad bajo competencia de la Junta Central Electoral. Dichos tratamientos se regirán por la legislación especial que les resulte aplicable y por la Ley núm. 172-13 sobre Protección de Datos Personales, sin perjuicio de que deban observar el presente reglamento cuando se vinculen con datos, documentos, registros, servicios, mecanismos de consulta o competencias atribuidas a la Junta Central Electoral.

Artículo 6. Deber de certificación. Todas las instituciones públicas o privadas que, amparadas en una ley, que remita expresamente al servicio provisto por la Junta Central Electoral, requieran verificar o certificar la identidad de las personas mediante datos biométricos deberán hacerlo a través del servicio de consulta, verificación y certificación de identidad provisto por la Junta Central Electoral. Fuera de dicho supuesto, este artículo no restringe el ejercicio de las competencias que correspondan a otros órganos reguladores sectoriales conforme a sus leyes especiales.

Párrafo I. La Junta Central Electoral regulará el acceso a los datos biométricos de las personas asentadas en sus bases de datos para fines de consulta, verificación y certificación de identidad.

Párrafo II. La Junta Central Electoral desarrollará políticas institucionales de acceso, uso, manejo y protección de datos biométricos que garanticen el respeto al derecho a la intimidad, la privacidad, la protección de datos personales, la seguridad y la confidencialidad de las personas.

Párrafo III. La consulta de datos biométricos para fines de verificación y certificación de identidad deberá realizarse respetando el derecho a la intimidad de las personas, la normativa de protección de datos personales, el presente reglamento y las demás leyes sobre la materia.

Párrafo IV. El deber de certificación previsto en este artículo no será exigible:

a) cuando las entidades públicas o privadas utilicen características biométricas únicamente como factor de autenticación para controlar el acceso de una persona a sus instalaciones, propios sistemas, productos o servicios, mediante la comparación de la muestra biométrica con los datos que esa misma persona haya registrado previamente ante la entidad para ese fin; ni

b) cuando el tratamiento recaiga sobre datos biométricos no comprendidos en la competencia de la Junta Central Electoral, conforme al Párrafo III del artículo 3 del presente reglamento.

Párrafo V. En ningún caso la autenticación a que se refiere el literal a) constituye ni produce los efectos de la verificación o la certificación de la identidad, las cuales corresponden de manera exclusiva a la Junta Central Electoral.

Párrafo VI. La Junta Central Electoral establecerá las normas complementarias que sean necesarias para la utilización de la biometría por parte de empresas e instituciones respecto a los controles de acceso y asistencia de sus empleados. Dichas empresas e instituciones deberán, además observar y cumplir lo dispuesto en el presente reglamento.

Artículo 7. Regla de interpretación. Las disposiciones del presente reglamento deberán interpretarse de conformidad con la Constitución de la República, la Ley núm. 4-23, Orgánica de los Actos del Estado Civil, la normativa de protección de datos personales, los principios de juridicidad, finalidad legítima, proporcionalidad, minimización, seguridad, confidencialidad, trazabilidad, responsabilidad y protección reforzada de los datos biométricos.

Párrafo I. Ninguna disposición del presente reglamento podrá interpretarse como autorización general para que entidades públicas o privadas creen, mantengan, alimenten, actualicen, interconecten, exploten, cedan, comuniquen, reutilicen o conserven bases de datos biométricos, bases de datos personales asociados a la identidad, repositorios, registros, sistemas, plataformas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que, por su objeto o efecto, sustituyan, repliquen, desplacen o funcionen como infraestructura paralela o sustitutiva de los registros, bases de datos, servicios o competencias atribuidas a la Junta Central Electoral en materia de identidad, Registro Civil, cedulación, consulta, verificación o certificación de identidad.

Párrafo II. Las obligaciones legales, reglamentarias, contractuales, sectoriales, operativas, probatorias, de continuidad de negocio, gestión de riesgos, prevención de fraude o cumplimiento normativo no se interpretarán, por sí solas, como autorización para conservar, reutilizar, interconectar, explotar o tratar datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que permitan realizar identificación, verificación, autenticación, comparación o tratamiento biométrico autónomo, salvo disposición legal expresa compatible con la Ley núm. 4-23 o requerimiento concreto de autoridad competente.

Párrafo III. La coordinación con órganos reguladores o supervisores sectoriales podrá realizarse cuando corresponda, pero no constituirá condición previa, requisito de validez ni vía exclusiva para el ejercicio de las atribuciones de la Junta Central Electoral en materia de datos biométricos, servicio de consulta, verificación y certificación de identidad, auditoría, supervisión, trazabilidad, seguridad o cumplimiento del presente reglamento.

TÍTULO II

DERECHOS Y CONSENTIMIENTO DE LAS PERSONAS EN EL TRATAMIENTO DE DATOS BIOMÉTRICOS Y DATOS PERSONALES ASOCIADOS A LA IDENTIDAD

CAPÍTULO I

DE LOS DERECHOS DE LAS PERSONAS EN EL TRATAMIENTO DE SUS DATOS

Artículo 8. Ejercicio de los derechos. El ejercicio de cualquiera de los derechos de las personas en relación con el tratamiento de sus datos biométricos y datos personales asociados a la identidad, incluidos el acceso, la rectificación, la cancelación, la oposición y la limitación del tratamiento, no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquiera de estos derechos.

Artículo 9. Accesibilidad y ajustes razonables. Los responsables del tratamiento, encargados y entidades usuarias deberán garantizar que el tratamiento de datos biométricos o datos personales asociados a la identidad, el uso del Servicio de Consulta, Verificación y Certificación de Identidad y el ejercicio de los derechos previstos en el presente reglamento sean accesibles para las personas con discapacidad, en condiciones de igualdad, no discriminación y dignidad.

Párrafo I. Cuando una persona con discapacidad enfrente barreras para la captura, verificación, autenticación, consulta, certificación o ejercicio de sus derechos, el responsable del tratamiento o la entidad usuaria deberá adoptar ajustes razonables, mecanismos alternativos, asistencia accesible, formatos comprensibles, canales adecuados o procedimientos equivalentes que permitan la prestación del servicio o el ejercicio del derecho sin imponer cargas desproporcionadas.

Párrafo II. La imposibilidad técnica, física, sensorial, cognitiva o funcional de capturar o utilizar una modalidad biométrica específica no podrá ser utilizada, por sí sola, como causa de exclusión, denegación

injustificada de servicios, trato discriminatorio o afectación del ejercicio de derechos, debiendo evaluarse alternativas razonables conforme a la finalidad, seguridad, proporcionalidad y normativa aplicable.

Párrafo III. La Junta Central Electoral podrá establecer, mediante instructivos, protocolos o lineamientos técnicos, criterios de accesibilidad, atención preferente, mecanismos alternativos de verificación y ajustes razonables aplicables al servicio provisto por esta y a las entidades usuarias.

Artículo 10. Derecho de acceso. El titular tiene derecho a obtener del responsable del tratamiento confirmación sobre si sus datos biométricos o datos personales asociados a la identidad están siendo tratados, así como acceso a dichos datos y a la información relativa a las condiciones y generalidades del tratamiento. El titular tendrá derecho a conocer, al menos, la siguiente información:

a) Los fines del tratamiento;
b) Las categorías de datos biométricos o datos personales asociados a la identidad objeto de tratamiento;
c) El origen de los datos, cuando no hayan sido obtenidos directamente del titular;
d) Los destinatarios o las categorías de destinatarios a los que se hayan comunicado o serán comunicados los datos biométricos o datos personales asociados a la identidad, cuando corresponda;
e) El plazo previsto de conservación de los datos o, de no ser posible, los criterios utilizados para determinar dicho plazo;
f) La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de los datos biométricos o datos personales asociados a la identidad, así como a oponerse a dicho tratamiento, conforme a la ley y al presente reglamento;
g) La constancia de la consulta, verificación o certificación de identidad realizada mediante el Servicio de Consulta, Verificación y Certificación de Identidad, cuando dicho servicio haya sido utilizado, en los términos establecidos por la Junta Central Electoral.

Párrafo I. La obligación de acceso se dará por cumplida cuando el responsable del tratamiento ponga a disposición del titular, en formato legible, comprensible y seguro, el detalle de los datos biométricos o datos personales asociados a su identidad que sean objeto de tratamiento, así como la información relativa a las condiciones, finalidades y generalidades de dicho tratamiento.

Párrafo II. Cuando los datos biométricos o datos personales asociados a la identidad comprendan elementos técnicos derivados del procesamiento biométrico, tales como plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación, su entrega podrá limitarse cuando la divulgación comprometa la seguridad, integridad o confidencialidad del sistema, incremente el riesgo de suplantación, reutilización indebida o afecte derechos de terceros. En tales casos, deberá proporcionarse al titular información equivalente, suficiente, legible y comprensible que le permita verificar la licitud del tratamiento.

Párrafo III. Cuando el titular solicite constancia de una consulta, verificación o certificación de identidad realizada mediante el Servicio de Consulta, Verificación y Certificación de Identidad, el responsable del tratamiento deberá suministrar, dentro de un plazo razonable y por medios físicos o electrónicos seguros, la constancia o resultado disponible de dicha consulta, conforme a las condiciones establecidas por la Junta Central Electoral.

Párrafo IV. Los datos biométricos y los datos personales asociados a la identidad no constituyen información pública por el solo hecho de encontrarse en poder de una entidad pública, y estarán sujetos a las restricciones, reservas, medidas de confidencialidad y protección previstas en la Constitución, la Ley núm. 4-23, la normativa de protección de datos personales, la Ley núm. 200-04 y el presente reglamento.

Artículo 11. Derecho de rectificación. El titular podrá solicitar la corrección o rectificación de sus datos biométricos o datos personales asociados a la identidad que resulten ser inexactos, incompletos, desactualizados o erróneos, conforme a la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

Párrafo I. Cuando la solicitud se refiera a datos biométricos o datos personales asociados a la identidad administrados, verificados o certificados por la Junta Central Electoral, y la corrección sea de carácter administrativo conforme a la Ley núm. 4-23, deberá ser presentada o canalizada ante la Junta Central Electoral, conforme a los procedimientos establecidos para tales fines.

Párrafo II. Cuando la solicitud implique una rectificación de carácter jurisdiccional, por no encontrarse comprendida dentro de los supuestos de corrección administrativa previstos en la Ley núm. 4-23, por tener carácter contencioso, afectar derechos adquiridos o de terceros, modificar sustancialmente el contenido de un acta del Estado Civil, o haber sido rechazada en sede administrativa, el titular deberá ejercerla ante el Tribunal Superior Electoral, conforme al procedimiento legal aplicable.

Párrafo III. Cuando la inexactitud, inconsistencia o error se encuentre en registros, expedientes, sistemas o bases de datos internas de una entidad usuaria del servicio o de un responsable del tratamiento distinto de la Junta Central Electoral, y no corresponda a una inconsistencia en los datos oficiales administrados, verificados o certificados por esta, dicha entidad usuaria o responsable deberá tramitar y resolver la corrección en sus propios registros, sin remitir indebidamente al titular a la Junta Central Electoral.

Párrafo IV. Cuando la solicitud sea presentada ante una entidad pública o privada usuaria del servicio, o ante un responsable del tratamiento distinto de la Junta Central Electoral, este deberá verificar si la corrección o rectificación solicitada corresponde a datos oficiales administrados por la Junta Central Electoral, a una rectificación jurisdiccional o a datos internos bajo su propia responsabilidad. En el primer caso, deberá orientar al titular sobre el procedimiento administrativo correspondiente ante la Junta Central Electoral; en el segundo, sobre la vía jurisdiccional ante el Tribunal Superior Electoral; y, en el tercero, deberá corregir sus registros internos conforme a la ley y al presente reglamento.

Párrafo V. La solicitud de rectificación deberá presentarse por escrito o por medios electrónicos verificables, indicando los datos biométricos o datos personales asociados a la identidad respecto de los cuales se requiere la corrección, la modificación solicitada y la documentación que sustente su procedencia. El responsable del tratamiento deberá ofrecer mecanismos accesibles, seguros y verificables que faciliten el ejercicio de este derecho en beneficio del titular.

Artículo 12. Derecho de cancelación o supresión. El titular podrá solicitar al responsable del tratamiento la cancelación o supresión de sus datos biométricos o datos personales asociados a la identidad cuando estos ya no sean necesarios para las finalidades que justificaron su tratamiento, cuando haya retirado su consentimiento, cuando los datos hayan sido tratados ilícitamente o cuando proceda conforme a la ley y al presente reglamento.

Párrafo I. La cancelación o supresión podrá proceder respecto de la totalidad de los datos biométricos o datos personales asociados a la identidad del titular o solo de una parte de ellos, según corresponda a la finalidad del tratamiento, la naturaleza de los datos y la procedencia de la solicitud.

Párrafo II. No procederá la cancelación o supresión cuando la conservación temporal de determinados datos resulte necesaria por disposición legal expresa compatible con la Ley núm. 4-23 o por requerimiento concreto de autoridad competente, exclusivamente para la atención de responsabilidades legales, administrativas o judiciales. En tales casos, los datos deberán conservarse bajo medidas efectivas de restricción, seguridad, trazabilidad y control, sin que puedan ser objeto de uso, consulta, comparación biométrica, reutilización, transferencia, explotación o tratamiento ulterior distinto al fin legal que justificó su conservación.

Párrafo III. Las obligaciones legales o reglamentarias de conservación de documentación, registros, evidencias transaccionales o soportes de operaciones no se interpretarán como autorización para conservar datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos o mecanismos de vinculación, salvo disposición legal expresa compatible con la Ley núm. 4-23.

Párrafo IV. El responsable del tratamiento deberá resolver la solicitud de cancelación o supresión y comunicar al titular la decisión adoptada dentro de un plazo máximo de quince (15) días laborables, contado a partir de la recepción de la solicitud. Cuando la complejidad de la solicitud, la necesidad de

verificar identidad, la existencia de terceros involucrados o la revisión de una base legal de conservación lo justifique, dicho plazo podrá ser prorrogado por una sola vez por hasta quince (15) días laborables adicionales, debiendo informarse al titular de manera motivada antes del vencimiento del plazo inicial.

Artículo 13. Derecho a la limitación del tratamiento. El titular tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos biométricos o datos personales asociados a la identidad cuando se cumpla alguna de las condiciones siguientes:

a) El titular impugne la precisión o exactitud de los datos biométricos o datos personales asociados a la identidad, durante un plazo que permita al responsable verificar que son exactos, completos y actualizados;
b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos, solicitando en su lugar la limitación de su uso;
c) El responsable ya no necesite los datos para los fines del tratamiento, pero el titular los requiera para la formulación, ejercicio o defensa de reclamaciones, siempre que ello no implique uso, consulta, comparación biométrica, reutilización, transferencia, explotación o tratamiento ulterior no autorizado;
d) El titular se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos acreditados por el responsable prevalecen conforme a la ley y al presente reglamento.

Párrafo. En los archivos, registros, sistemas o bases de datos automatizadas, la limitación del tratamiento deberá realizarse, en principio, por medios técnicos. El hecho de que los datos biométricos o datos personales asociados a la identidad están limitados deberá indicarse en el sistema de tal modo que quede claro que no pueden utilizarse fuera de las condiciones que justifican dicha limitación.

Artículo 14. Derecho de oposición. El titular podrá oponerse, en todo momento, al tratamiento de sus datos biométricos o datos personales asociados a la identidad, o solicitar el cese de dicho tratamiento para finalidades específicas, cuando exista una causa legítima vinculada a su situación particular, aun cuando el tratamiento sea lícito.
Párrafo I. El responsable del tratamiento deberá cesar el tratamiento objeto de oposición, salvo que acredite motivos legítimos, necesarios y proporcionales que, conforme a una disposición legal expresa y compatible con la Ley núm. 4-23, prevalezcan sobre los intereses, derechos y libertades del titular, o cuando el tratamiento resulte estrictamente necesario para la formulación, ejercicio o defensa de reclamaciones directamente relacionadas con este.

Párrafo II. Las obligaciones legales o reglamentarias de conservación de documentación, registros, evidencias transaccionales, soportes de operaciones o expedientes de cumplimiento no se interpretarán, por sí solas, como motivos suficientes para mantener el tratamiento activo de datos biométricos, ni para conservar muestras biométricas, plantillas, vectores, patrones, códigos biométricos o mecanismos de vinculación fuera de los supuestos permitidos por la Ley núm. 4-23.

Párrafo III. El ejercicio del derecho de oposición no implicará, por sí solo, la cancelación o supresión de los datos biométricos o datos personales asociados a la identidad, la cual se regirá por las disposiciones específicas previstas en el presente reglamento.

Artículo 15. Reclamaciones y denuncias ante la Junta Central Electoral. Sin perjuicio de los canales que deba habilitar el responsable del tratamiento, el titular podrá presentar ante la Junta Central Electoral reclamaciones o denuncias relacionadas con tratamientos de datos biométricos o datos personales asociados a la identidad comprendidos dentro del ámbito de aplicación del presente reglamento, el uso del Servicio de Consulta, Verificación y Certificación de Identidad, la conservación de resultados o constancias, la negativa injustificada de derechos, incidentes de seguridad, tratamientos no autorizados o presuntas infracciones al presente reglamento.

Párrafo I. La Junta Central Electoral habilitará canales físicos, electrónicos o digitales accesibles para la recepción de reclamaciones y denuncias, y establecerá mediante instructivo los requisitos mínimos, procedimiento, plazos de respuesta, medios de seguimiento y medidas aplicables.

Párrafo II. Cuando la reclamación o denuncia resulte admisible, la Junta Central Electoral podrá requerir información al responsable, encargado, entidad usuaria o tercero involucrado; ordenar medidas preventivas o correctivas; requerir la atención del derecho reclamado; disponer auditorías, revisiones o verificaciones; suspender o limitar el acceso al servicio cuando corresponda; o remitir el caso a la autoridad competente.

Párrafo III. La presentación de una reclamación o denuncia ante la Junta Central Electoral no impedirá al titular ejercer las acciones administrativas, civiles, penales, contractuales o de cualquier otra naturaleza que correspondan conforme al ordenamiento jurídico.

Párrafo IV. Cuando de la reclamación o denuncia se deriven daños, perjuicios o afectaciones al titular, la Junta Central Electoral podrá dejar constancia de los hallazgos, requerir medidas de corrección o mitigación y orientar al titular sobre las vías legales disponibles, sin perjuicio de las responsabilidades que correspondan al responsable, encargado, entidad usuaria o tercero conforme a la normativa aplicable.

CAPÍTULO II

DE LAS OBLIGACIONES Y RESPONSABILIDADES DEL RESPONSABLE DEL TRATAMIENTO DE DATOS BIOMÉTRICOS

Artículo 16. Responsable del tratamiento de datos biométricos. El responsable del tratamiento de datos biométricos es la persona física o jurídica, organismo público o entidad privada que, solo o conjuntamente con otros, determina los fines, medios, alcance y condiciones del tratamiento de datos biométricos o datos personales asociados a la identidad, conforme a la ley, el presente reglamento y, cuando corresponda, la autorización de la Junta Central Electoral.

Párrafo. El responsable del tratamiento asumirá las obligaciones previstas en el presente reglamento, en la normativa de protección de datos personales, en las condiciones técnicas y contractuales aplicables, y en las resoluciones, autorizaciones o disposiciones que dicte la Junta Central Electoral dentro del ámbito de sus competencias.

Artículo 17. Obligaciones del responsable del tratamiento de datos biométricos. El responsable del tratamiento de datos biométricos deberá cumplir, como mínimo, con las obligaciones siguientes:

a) Establecer, mantener y actualizar políticas, procedimientos, controles y directrices para la recolección, captura, almacenamiento, uso, consulta, transmisión, conservación, limitación, supresión y eliminación segura de los datos biométricos y datos personales asociados a la identidad.
b) Asegurar el cumplimiento de la Ley núm. 4-23, la normativa de protección de datos personales, el presente reglamento, las resoluciones de la Junta Central Electoral y cualquier otra disposición legal o técnica aplicable al tratamiento realizado.
c) Designar, cuando corresponda, un delegado de protección de datos con capacidad, conocimientos técnicos y competencias suficientes para dar seguimiento al cumplimiento de las obligaciones previstas en la ley y el presente reglamento.
d) Gestionar y salvaguardar de forma segura los datos biométricos y datos personales asociados a la identidad, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
e) Implementar medidas de seguridad técnicas, organizativas, jurídicas y administrativas apropiadas para prevenir el acceso no autorizado, el uso indebido, la alteración, divulgación, pérdida, destrucción, explotación, reutilización o tratamiento no autorizado de los datos biométricos.
f) Obtener el consentimiento expreso, informado, específico, inequívoco y verificable del titular cuando este sea requerido, y garantizar que el titular reciba información clara y transparente sobre las finalidades del tratamiento, los datos objeto de tratamiento, el plazo de conservación, sus derechos y los mecanismos para ejercerlos.
g) Garantizar el ejercicio efectivo de los derechos de los titulares, incluyendo acceso, rectificación, cancelación, supresión, limitación y oposición, conforme a la ley y el presente reglamento.

h) Realizar evaluaciones de impacto cuando el tratamiento de datos biométricos pueda entrañar alto riesgo para los derechos de los titulares, para la seguridad de los sistemas, para la confidencialidad de la información o para la competencia institucional de la Junta Central Electoral.
i) Notificar a la Junta Central Electoral y, cuando corresponda, a los titulares afectados, los incidentes de seguridad o violaciones de datos biométricos, conforme a los plazos, condiciones y procedimientos establecidos en el presente reglamento.
j) Colaborar de manera activa, directa y oportuna con la Junta Central Electoral, proporcionando la información requerida y facilitando las acciones necesarias para verificar el cumplimiento de la ley, del presente reglamento y de las condiciones aplicables al servicio de consulta, verificación y certificación de identidad.
k) Mantener un registro actualizado de las actividades de tratamiento realizadas, que incluya, como mínimo, los fines del tratamiento, las categorías de datos tratados, los destinatarios o categorías de destinatarios, los plazos de conservación, las medidas de seguridad implementadas, las bases legales aplicables, las evaluaciones de impacto realizadas cuando correspondan y cualquier otra información exigida por la normativa aplicable.

Párrafo. Las disposiciones sectoriales que resulten aplicables al responsable del tratamiento podrán establecer medidas adicionales o más estrictas de protección, seguridad, gobernanza, auditoría o gestión de riesgos, siempre que no reduzcan, sustituyan, condicionen ni limiten las competencias de la Junta Central Electoral ni las obligaciones previstas en el presente reglamento.

Artículo 18. Responsabilidad del responsable del tratamiento de datos biométricos. El responsable del tratamiento de datos biométricos asumirá la responsabilidad de garantizar el cumplimiento de las disposiciones establecidas en la ley, el presente reglamento, las autorizaciones, condiciones técnicas, contractuales y de seguridad aplicables.

Párrafo I. El responsable deberá poder demostrar, mediante evidencias documentales, técnicas, operativas y trazables, el cumplimiento de sus obligaciones en materia de consentimiento, finalidad, minimización, seguridad, confidencialidad, retención limitada, atención de derechos, evaluación de impacto, gestión de incidentes y eliminación segura.

Párrafo II. El incumplimiento de las obligaciones previstas en el presente reglamento dará lugar a las medidas, responsabilidades, restricciones, suspensiones, revocaciones, acciones legales o consecuencias que correspondan conforme a la Ley núm. 4-23, la normativa aplicable, los contratos suscritos y las resoluciones de la Junta Central Electoral.

Artículo 19. Subcontratación de servicios. Cuando el responsable del tratamiento subcontrate a terceros para la realización de actividades vinculadas al tratamiento de datos biométricos o datos personales asociados a la identidad, deberá asegurarse de que dichos terceros ofrezcan garantías suficientes para implementar medidas técnicas, organizativas, jurídicas y de seguridad apropiadas, conforme a la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

Párrafo I. La subcontratación deberá constar en contrato, convenio, orden de servicio, acuerdo de tratamiento de datos u otro instrumento jurídico equivalente, en el cual se establezcan, como mínimo, el objeto, duración, finalidad, alcance, instrucciones documentadas, medidas de seguridad, obligaciones de confidencialidad, prohibición de uso para fines propios, reglas de conservación, devolución o eliminación segura, régimen de auditoría, gestión de incidentes y responsabilidad del tercero subcontratado.

Párrafo II. La intervención de terceros subcontratados deberá ser informada al titular de los datos, de forma clara y comprensible, en el aviso de privacidad, consentimiento, contrato, formulario o mecanismo equivalente, indicando la finalidad de dicha intervención y las garantías aplicables, conforme a los principios de transparencia, finalidad y consentimiento informado.

Párrafo III. La subcontratación no constituirá cesión, transferencia ni autorización para que el tercero subcontratado trate datos biométricos o datos personales asociados a la identidad para fines propios, ni para que conserve, reutilice, comunique, explote o realice tratamientos ulteriores fuera de las instrucciones documentadas del responsable, la ley y el presente reglamento.

Párrafo IV. Cuando la subcontratación involucre el servicio de consulta, verificación y certificación de identidad provisto por la Junta Central Electoral, datos biométricos bajo competencia de esta, mecanismos de integración, interoperabilidad, credenciales, interfaces, resultados de verificación o constancias de consulta, deberá sujetarse a las condiciones técnicas, contractuales y de seguridad establecidas por la Junta Central Electoral.

Párrafo V. El responsable del tratamiento conservará la responsabilidad frente al titular, frente a la Junta Central Electoral y frente a las autoridades competentes por los incumplimientos del tercero subcontratado, sin perjuicio de las acciones de repetición, reclamación contractual o responsabilidad que correspondan contra dicho tercero.

Artículo 20. Deber de actualización y formación. El responsable del tratamiento de datos biométricos deberá mantenerse actualizado sobre los avances tecnológicos, riesgos emergentes, buenas prácticas, estándares de seguridad y novedades normativas relacionadas con la protección de datos biométricos y datos personales asociados a la identidad.

Párrafo. El responsable deberá proporcionar formación adecuada, periódica y verificable al personal que participe en la captura, tratamiento, consulta, verificación, certificación, conservación, transmisión, supresión o eliminación de datos biométricos, asegurando que dicho personal conozca sus obligaciones de confidencialidad, seguridad, finalidad, minimización, trazabilidad y protección de los derechos de los titulares.

Artículo 21. Evaluación y revisión periódica. El responsable del tratamiento de datos biométricos deberá realizar evaluaciones y revisiones periódicas de las medidas técnicas, organizativas, jurídicas, administrativas y de seguridad implementadas, con el objetivo de garantizar la eficacia, adecuación, proporcionalidad y conformidad del tratamiento con la ley, el presente reglamento y las condiciones establecidas por la Junta Central Electoral.

Párrafo. Cuando se detecten deficiencias, vulnerabilidades, desviaciones, riesgos o incumplimientos, el responsable deberá adoptar oportunamente las medidas correctivas, preventivas y de mitigación necesarias, dejando constancia verificable de las acciones implementadas.

Artículo 22. Confidencialidad y no divulgación. El responsable del tratamiento de datos biométricos, sus encargados, subcontratados, representantes, funcionarios, empleados, dependientes y cualquier persona que intervenga en el tratamiento deberán mantener la confidencialidad de los datos biométricos y datos personales asociados a la identidad a los que tengan acceso en el ejercicio de sus funciones.

Párrafo I. Los datos biométricos y datos personales asociados a la identidad no podrán ser divulgados, transferidos, consultados, comunicados, reutilizados, explotados ni utilizados para fines distintos a los establecidos en la ley, el presente reglamento, la autorización correspondiente, el consentimiento otorgado cuando aplique o las condiciones del servicio provisto por la Junta Central Electoral.

Párrafo II. La obligación de confidencialidad subsistirá aun después de finalizada la relación laboral, contractual, institucional, comercial o de servicios que dio lugar al acceso o tratamiento de los datos.

Artículo 23. Registro de incidentes de seguridad. El responsable del tratamiento deberá documentar, registrar y gestionar todo incidente de seguridad o violación que comprometa o pueda comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de los datos biométricos, datos personales asociados a la identidad, sistemas, servicios o mecanismos utilizados para su tratamiento, consulta, verificación o certificación.

Párrafo I. Cuando el incidente comprometa o pueda comprometer datos biométricos, datos personales asociados a la identidad, el servicio de consulta, verificación y certificación de identidad, o cualquier mecanismo autorizado o regulado por la Junta Central Electoral, el responsable del tratamiento deberá notificarlo a la Junta Central Electoral en un plazo no mayor de setenta y dos (72) horas contadas a partir del momento en que tenga conocimiento del hecho, sin perjuicio de las notificaciones que correspondan

al Centro Sectorial de Respuesta a Incidentes (CSIRT), al CSIRT-RD del Centro Nacional de Ciberseguridad, al ente regulador sectorial competente o a cualquier otra autoridad legalmente habilitada.

Párrafo II. Cuando el incidente pueda generar un alto riesgo para los derechos del titular, el responsable del tratamiento deberá notificarlo también al titular afectado, en lenguaje claro y comprensible, indicando la naturaleza del incidente, los datos comprometidos o potencialmente comprometidos, las posibles consecuencias, las medidas adoptadas o recomendadas para mitigar sus efectos y los canales habilitados para obtener información adicional.

Párrafo III. La notificación a un ente regulador sectorial, CSIRT sectorial o al CSIRT-RD no sustituirá la obligación de notificar directamente a la Junta Central Electoral cuando el incidente involucre datos personales asociados a la identidad, datos biométricos, servicios de consulta, verificación o certificación de identidad, o cualquier mecanismo autorizado o regulado por la Junta Central Electoral.

Párrafo IV. La notificación deberá contener, al menos, la descripción del incidente, su fecha y hora de ocurrencia o detección, su naturaleza, alcance, sistemas o servicios afectados, categorías de datos comprometidos o potencialmente comprometidos, número aproximado de titulares afectados cuando sea posible determinarlo, medidas de contención y mitigación adoptadas, acciones correctivas y preventivas, así como los datos de contacto del responsable o del delegado de protección de datos.

Párrafo V. El responsable del tratamiento deberá mantener un registro actualizado de los incidentes de seguridad y violaciones ocurridas, incluyendo las circunstancias del hecho, sus efectos, las medidas adoptadas y las comunicaciones realizadas a la Junta Central Electoral, titulares afectados, autoridades competentes, CSIRT sectorial o CSIRT-RD, según corresponda.

Párrafo VI. La información comunicada a la Junta Central Electoral con ocasión de un incidente de seguridad o violación de datos tendrá carácter reservado o confidencial cuando por su naturaleza pueda comprometer la seguridad de los sistemas, investigaciones en curso, secretos protegidos, continuidad operativa, estabilidad del servicio, reputación institucional o derechos de los titulares. Dicha información solo podrá ser utilizada por la Junta Central Electoral para fines de supervisión, coordinación, mitigación, trazabilidad, protección de los titulares y cumplimiento de sus competencias legales, observando los principios de confidencialidad, necesidad, proporcionalidad y minimización.

Artículo 24. Designación de un delegado de protección de datos. El responsable del tratamiento comprendido dentro del ámbito de aplicación del presente reglamento deberá designar un delegado de protección de datos cuando el tratamiento, por su naturaleza, alcance, finalidad, volumen, modalidad, nivel de riesgo o vinculación con el Servicio de Consulta, Verificación y Certificación de Identidad, requiera supervisión especializada para garantizar el cumplimiento de la ley, el presente reglamento y las políticas de protección de datos aplicables.

Párrafo I. La designación del delegado de protección de datos será obligatoria, como mínimo, para las entidades usuarias del Servicio de Consulta, Verificación y Certificación de Identidad; para responsables o encargados que realicen tratamiento sistemático, recurrente, masivo, interoperable o de alto impacto de datos biométricos o datos personales asociados a la identidad; y para aquellos tratamientos que, por su finalidad, tecnología, volumen, riesgos o afectación potencial de derechos, requieran supervisión especializada.

Párrafo II. El delegado de protección de datos deberá ser seleccionado en atención a su experiencia, conocimientos técnicos y competencias en protección de datos personales, seguridad de la información, gestión de riesgos, cumplimiento normativo, privacidad, trazabilidad y tratamiento de datos biométricos.

Párrafo III. El delegado de protección de datos deberá contar con acceso a la información necesaria y autonomía funcional suficiente para emitir recomendaciones, advertir riesgos, requerir medidas correctivas internas y dar seguimiento al cumplimiento de las obligaciones previstas en la ley y el presente reglamento, sin perjuicio de la responsabilidad que corresponde al responsable del tratamiento.

Párrafo IV. El delegado de protección de datos servirá como punto de contacto especializado para la Junta Central Electoral, las autoridades competentes y, cuando corresponda, para los titulares, en asuntos relacionados con el ejercicio de sus derechos, incidentes de seguridad, reclamaciones, consultas complejas o situaciones que requieran supervisión especializada, sin perjuicio de los canales ordinarios que el responsable del tratamiento deberá habilitar para la atención de los titulares.

Párrafo V. El delegado de protección de datos podrá ser interno o externo. Cuando sea externo o subcontratado, su designación deberá constar en contrato o instrumento jurídico escrito que asegure su competencia técnica, disponibilidad efectiva, confidencialidad, independencia funcional, ausencia de conflicto de interés y cumplimiento de las obligaciones previstas en la ley, el presente reglamento y las condiciones establecidas por la Junta Central Electoral. La designación de un delegado externo no eximirá al responsable o encargado del tratamiento de las responsabilidades que le correspondan.

Artículo 25. Delegado/a de Protección de Datos de la Junta Central Electoral. La Junta Central Electoral contará con un delegado/a de protección de datos personales y biométricos, integrado funcionalmente a la estructura de la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad, responsable de dar seguimiento, coordinar y supervisar internamente el cumplimiento de las políticas, medidas y obligaciones de protección de datos personales asociados a la identidad y datos biométricos en los tratamientos, sistemas, servicios y mecanismos bajo competencia de la Junta Central Electoral.

Párrafo I. El delegado/a de protección de datos personales y biométricos actuará como instancia técnica de apoyo, seguimiento y control preventivo dentro de la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad, sin perjuicio de la coordinación funcional que deba mantener en la Dirección Nacional de Cedulación y con la Dirección Nacional de Registro Civil, la Dirección de Registro Electoral, la Dirección Nacional de Informática, la Consultoría Jurídica, las áreas de seguridad de la información, auditoría, planificación y demás dependencias vinculadas al tratamiento de datos biométricos o datos personales asociados a la identidad.

Párrafo II. El delegado/a de protección de datos personales y biométricos deberá contar con autoridad funcional suficiente para requerir información, revisar tratamientos, emitir recomendaciones, advertir riesgos, proponer medidas correctivas, dar seguimiento a incidentes, apoyar evaluaciones de impacto y elevar informes a la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad, a la Dirección Nacional de Cedulación, a la Presidencia de la Junta Central Electoral, al Pleno o a la instancia institucional competente, cuando la naturaleza, gravedad o impacto del asunto lo requiera.

Párrafo III. La integración funcional del delegado/a dentro de la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad no limitará su capacidad de emitir criterios técnicos, advertencias o recomendaciones en materia de protección de datos personales asociados a la identidad y datos biométricos, ni podrá impedir su acceso a la información necesaria para el cumplimiento de sus funciones, conforme a los principios de confidencialidad, necesidad, proporcionalidad, seguridad y trazabilidad.

Párrafo IV. El delegado/a de protección de datos personales y biométricos servirá como punto de contacto institucional para la coordinación con los delegados de protección de datos de las entidades usuarias del servicio, responsables, encargados, autoridades competentes y, cuando corresponda, con los titulares, en asuntos relacionados con el ejercicio de derechos, incidentes de seguridad, reclamaciones, consultas complejas, evaluaciones de impacto o situaciones que requieran supervisión especializada, dentro del ámbito de aplicación del presente reglamento.

Artículo 26. Cooperación entre delegados de protección de datos. Los delegados de protección de datos de las instituciones responsables, encargadas o usuarias del servicio que traten datos biométricos o datos personales asociados a la identidad deberán cooperar con el delegado de protección de datos de la Junta Central Electoral, a fin de asegurar la implementación, seguimiento y cumplimiento de las políticas, medidas y obligaciones de protección de datos previstas en la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

Párrafo I. En el caso de entidades sujetas a supervisión sectorial, la coordinación con su órgano regulador o supervisor competente podrá realizarse conforme a las normas aplicables a dicho sector, sin que ello sustituya la obligación de cooperación directa con la Junta Central Electoral cuando el asunto involucre datos personales asociados a la identidad, datos biométricos, el Servicio de Consulta, Verificación y Certificación de Identidad o cualquier mecanismo de verificación o certificación de identidad regulado por la Junta Central Electoral.

Párrafo II. La cooperación entre delegados de protección de datos deberá realizarse bajo los principios de confidencialidad, necesidad, proporcionalidad, seguridad, trazabilidad y minimización de la información compartida, limitándose a los fines de cumplimiento, supervisión, gestión de riesgos, atención de incidentes, ejercicio de derechos de los titulares y protección de los datos personales asociados a la identidad.

CAPÍTULO III

DEL AVISO DE PRIVACIDAD, DEL CONSENTIMIENTO Y SUS CARACTERÍSTICAS

SECCIÓN I

DEL AVISO DE PRIVACIDAD

Artículo 27. Aviso de privacidad. Previo a la obtención, recopilación, captura o tratamiento de datos biométricos o datos personales asociados a la identidad, el responsable del tratamiento deberá poner a disposición del titular el aviso de privacidad, de forma clara, sencilla, accesible y comprensible, en formato físico, electrónico, digital o mediante cualquier otra tecnología que permita su consulta, conservación y verificación.

Párrafo I. El aviso de privacidad deberá contener, como mínimo, la información siguiente:

a) La identidad, domicilio y datos de contacto del responsable del tratamiento;
b) Las categorías de datos biométricos o datos personales asociados a la identidad que serán tratados;
c) Las finalidades específicas del tratamiento;
d) La base legal o fundamento que habilita el tratamiento;
e) Los destinatarios o categorías de destinatarios a quienes podrán comunicarse los datos, cuando corresponda;
f) El plazo de conservación de los datos o los criterios utilizados para determinarlo;
g) Los derechos que asisten al titular y los mecanismos para ejercerlos;
h) Los canales de atención, consulta o reclamación disponible para el titular;
i) La existencia de encargados, terceros subcontratados o entidades usuarias que intervengan en el tratamiento, cuando corresponda;
j) Las medidas generales de seguridad, confidencialidad y trazabilidad aplicables, sin revelar información que pueda comprometer la seguridad de los sistemas, servicios, mecanismos de consulta, verificación o certificación de identidad.

Párrafo II. Cuando los datos biométricos sean obtenidos directamente del titular, el aviso de privacidad deberá ser puesto a su disposición antes de la captura, recopilación o tratamiento de dichos datos, y deberá incluir un mecanismo que permita al titular manifestar su negativa respecto de tratamientos que no sean necesarios para la finalidad principal, la relación jurídica correspondiente, el servicio solicitado o una obligación legal expresa aplicable.

Párrafo III. Cuando la obtención de los datos biométricos se realice por medios remotos, digitales, electrónicos, ópticos, automatizados o no presenciales, el responsable del tratamiento deberá garantizar que el aviso de privacidad sea accesible antes de la captura o envío de los datos, y que quede constancia verificable de su puesta a disposición y, cuando corresponda, del consentimiento otorgado por el titular.

Párrafo IV. La puesta a disposición del aviso de privacidad no exime al responsable del tratamiento de obtener el consentimiento expreso, informado, específico, inequívoco y verificable del titular cuando este sea requerido conforme a la ley y al presente reglamento.

SECCIÓN II

DEL CONSENTIMIENTO Y SUS CARACTERÍSTICAS

Artículo 28. Características del consentimiento. La obtención del consentimiento para el tratamiento de datos biométricos o datos personales asociados a la identidad deberá cumplir con las características siguientes:

a) **Expreso:** que resulte de una manifestación clara de voluntad del titular, otorgada por escrito, medios electrónicos verificables, firma, validación digital, aceptación expresa u otro mecanismo fehaciente;
b) **Libre:** que sea otorgado sin que medie error, mala fe, violencia, dolo, coacción, condicionamiento indebido o cualquier otra circunstancia que pueda afectar la manifestación de voluntad del titular;
c) **Específico:** que esté referido a una o varias finalidades determinadas, explícitas y legítimas que justifiquen el tratamiento;
d) **Informado:** que el titular haya tenido conocimiento, previo al tratamiento, del aviso de privacidad, de las finalidades del tratamiento, de los datos biométricos o datos personales asociados a la identidad que serán tratados, de las consecuencias de otorgar o negar su consentimiento, de los derechos que le asisten y de los mecanismos para ejercerlos;
e) **Inequívoco:** que resulte de una manifestación clara de voluntad del titular, sin admitir duda razonable sobre su autorización;
f) **Verificable:** que permita dejar constancia suficiente, trazable y comprobable de su otorgamiento, por escrito, medios electrónicos verificables, firma, validación digital, aceptación expresa u otro mecanismo fehaciente.

Párrafo. El consentimiento tácito no será válido para el tratamiento de datos biométricos ni para aquellos tratamientos de datos personales asociados a la identidad que, por su naturaleza, finalidad, nivel de riesgo o impacto sobre derechos fundamentales, requieran consentimiento expreso, específico, informado, inequívoco y verificable.

Artículo 29. Demostración de obtención del consentimiento. Cuando el tratamiento de datos biométricos o datos personales asociados a la identidad se base en el consentimiento del titular, el responsable del tratamiento deberá ser capaz de demostrar que dicho consentimiento fue otorgado conforme a las condiciones previstas en la ley y el presente reglamento.

Párrafo. La demostración del consentimiento deberá permitir verificar, como mínimo, la identidad del titular, la fecha y hora de otorgamiento, el medio utilizado, la finalidad autorizada, la versión del aviso de privacidad o documento presentado, el alcance del consentimiento y cualquier retiro, modificación o limitación posterior.

Artículo 30. Consentimiento en el contexto de un contrato. Cuando el consentimiento del titular se otorgue en el contexto de un contrato escrito, físico o electrónico, que también se refiera a otros asuntos, la solicitud de consentimiento deberá presentarse de forma claramente distinguible de las demás estipulaciones, en lenguaje claro, sencillo, inteligible y de fácil acceso.

Párrafo I. No será vinculante ninguna cláusula, declaración, autorización o estipulación contractual que implique infracción de la ley, del presente reglamento o de los derechos del titular.

Párrafo II. La aceptación general de un contrato, términos y condiciones, formulario, solicitud, política interna o documento equivalente no sustituirá el consentimiento expreso, específico, informado, inequívoco y verificable requerido para el tratamiento de datos biométricos, salvo que dicho consentimiento conste de forma separada, clara y comprobable.

Artículo 31. Retiro del consentimiento. El titular tendrá derecho a retirar su consentimiento en cualquier momento, mediante mecanismos accesibles, seguros, verificables y proporcionales a los utilizados para su otorgamiento. El retiro del consentimiento no afectará la licitud del tratamiento realizado con base en

el consentimiento previamente otorgado, siempre que dicho tratamiento haya cumplido con la ley y el presente reglamento.

Párrafo I. A partir del retiro del consentimiento, el responsable del tratamiento deberá cesar el tratamiento de los datos biométricos o datos personales asociados a la identidad para las finalidades respecto de las cuales fue retirado y, cuando no exista otra base legal expresa que justifique su conservación, proceder a su cancelación, supresión o eliminación segura, conforme a la ley y al presente reglamento.

Párrafo II. Cuando, por disposición legal expresa compatible con la Ley núm. 4-23 o por requerimiento concreto de autoridad competente, resulte necesaria la conservación temporal de determinados datos, estos deberán mantenerse bajo medidas efectivas de restricción, seguridad, trazabilidad y control, sin que puedan ser objeto de uso, consulta, comparación biométrica, reutilización, transferencia, explotación o tratamiento ulterior distinto al fin legal que justificó su conservación.

Párrafo III. El responsable del tratamiento deberá dejar constancia verificable del retiro del consentimiento, indicando la fecha, medio utilizado, identidad del solicitante, finalidad afectada y las medidas adoptadas como consecuencia de dicho retiro.

Artículo 32. Evaluación del consentimiento libre. Para evaluar si el consentimiento ha sido otorgado libremente, deberá verificarse si la ejecución de un contrato, la prestación de un servicio o el acceso a un beneficio ha sido condicionado al consentimiento para el tratamiento de datos biométricos o datos personales asociados a la identidad que no resulten necesarios, proporcionales o pertinentes para dicha finalidad.

Párrafo I. Cuando el tratamiento de datos personales asociados a la identidad, especialmente datos biométricos, no sea indispensable para la ejecución del contrato, la prestación del servicio, el cumplimiento de una obligación legal aplicable o la finalidad autorizada, el titular deberá contar con una alternativa razonable que no implique dicho tratamiento, salvo disposición legal expresa en contrario.

Párrafo II. No se considerará libre el consentimiento cuando el titular no disponga de una opción real, razonable y proporcional para rechazar tratamientos biométricos no necesarios, o cuando la negativa produzca consecuencias desproporcionadas, injustificadas o incompatibles con la finalidad principal del servicio o relación jurídica correspondiente.

Artículo 33. Tratamiento de datos biométricos de niños, niñas y adolescentes. El tratamiento de datos biométricos o datos personales asociados a la identidad de niños, niñas y adolescentes comprendido dentro del ámbito de aplicación del presente reglamento deberá realizarse observando el principio del interés superior del niño, niña o adolescente, la protección reforzada de sus derechos, la finalidad específica del tratamiento, la necesidad, proporcionalidad, minimización, seguridad, confidencialidad y retención limitada.

Párrafo I. Los niños, niñas y adolescentes no podrán otorgar por sí mismos el consentimiento jurídicamente habilitante para el tratamiento de sus datos biométricos. Cuando el tratamiento se fundamente en el consentimiento, este deberá ser otorgado por el padre, madre, tutor, guardador o representante legal que corresponda conforme a la ley, sin perjuicio de que el niño, niña o adolescente sea informado de manera clara, sencilla y adecuada a su edad, madurez y capacidad de comprensión sobre el tratamiento de sus datos.

Párrafo II. El tratamiento de datos biométricos de niños, niñas y adolescentes solo será admisible cuando resulte estrictamente necesario para una finalidad legítima, específica e informada, vinculada con la identificación, protección, acceso a servicios, ejercicio de derechos, cumplimiento de una obligación legal o prestación de un servicio autorizado, y no pueda alcanzarse razonablemente mediante medios menos intrusivos.

Párrafo III. Queda prohibido utilizar datos biométricos de niños, niñas y adolescentes para finalidades comerciales, publicitarias, de perfilamiento, fidelización, segmentación, vigilancia indiscriminada,

monitoreo permanente o cualquier otra finalidad incompatible con su interés superior y con la finalidad específica que justificó el tratamiento.

Párrafo IV. Cuando el tratamiento involucre el Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral, la entidad usuaria deberá acreditar la base legal, finalidad, necesidad y proporcionalidad del tratamiento, así como las garantías reforzadas aplicables a niños, niñas y adolescentes.

Artículo 34. Consentimiento otorgado por escrito o medios electrónicos. Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo manifieste mediante documento con firma autógrafa, medios electrónicos verificables, firma electrónica conforme a la Ley núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, validación digital, aceptación expresa u otro mecanismo fehaciente que permita identificar al titular y dejar constancia comprobable de su consentimiento, conforme a la normativa aplicable.

Párrafo. Cuando el consentimiento sea otorgado por medios electrónicos, digitales, remotos o automatizados, el responsable del tratamiento deberá garantizar que el mecanismo utilizado permita comprobar la identidad del titular, la fecha y hora del otorgamiento, el medio empleado, la finalidad autorizada, el alcance del consentimiento, la versión del aviso de privacidad puesto a disposición y cualquier otra información necesaria para demostrar la licitud del tratamiento.

Artículo 35. Prueba, carga de la prueba y conservación del consentimiento. Cuando el tratamiento de datos biométricos o datos personales asociados a la identidad se base en el consentimiento del titular, la carga de demostrar su obtención válida recaerá, en todos los casos, en el responsable del tratamiento.

Párrafo I. La prueba del consentimiento deberá ser suficiente para demostrar que este fue otorgado de manera libre, expresa, específica, informada, inequívoca y verificable, conforme a la ley y al presente reglamento.

Párrafo II. El responsable del tratamiento deberá conservar la prueba del consentimiento otorgado por el titular en un repositorio seguro, trazable y auditable, durante el plazo necesario para demostrar la licitud del tratamiento y atender las obligaciones derivadas de la ley y del presente reglamento.

Párrafo III. La conservación de la prueba del consentimiento no habilita al responsable del tratamiento a conservar datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación más allá del plazo, finalidad o base legal que justificó su tratamiento.

Párrafo IV. La Junta Central Electoral podrá auditar a las instituciones públicas y privadas que realicen tratamientos comprendidos dentro del ámbito de aplicación del presente reglamento, con la finalidad de verificar el cumplimiento de esta disposición y de las demás obligaciones establecidas en el presente reglamento.

Artículo 36. Vigencia del consentimiento. En los tratamientos comprendidos dentro del ámbito de aplicación del presente reglamento, el consentimiento será otorgado por tiempo limitado y para finalidades determinadas. En ningún caso podrá exceder el plazo máximo de dos (2) años, contado a partir de la fecha de su otorgamiento, sin perjuicio de que deba cesar antes cuando desaparezca la finalidad que justificó el tratamiento, sea retirado por el titular o deje de existir una base legal que habilite dicho tratamiento.

Párrafo I. Vencido el plazo del consentimiento, si persiste la finalidad para la cual fue otorgado, el responsable del tratamiento deberá informar al titular y solicitar un nuevo consentimiento expreso, específico, informado, inequívoco y verificable antes de continuar el tratamiento de los datos biométricos o datos personales asociados a la identidad. La falta de otorgamiento del nuevo consentimiento impedirá la continuidad del tratamiento para la finalidad correspondiente, salvo que exista una base legal aplicable que justifique dicho tratamiento conforme a la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

Párrafo II. Si la finalidad para la cual fue otorgado el consentimiento desaparece antes del vencimiento del plazo previsto, el responsable del tratamiento deberá cesar el tratamiento y proceder a la cancelación, supresión o eliminación segura de los datos biométricos o datos personales asociados a la identidad, salvo disposición legal expresa compatible con la Ley núm. 4-23 o requerimiento concreto de autoridad competente que justifique su conservación temporal.

Artículo 37. Solicitudes de retiro del consentimiento y confirmación del cese del tratamiento. El titular de los datos biométricos o datos personales asociados a la identidad podrá solicitar en cualquier momento el retiro del consentimiento previamente otorgado. Los mecanismos o procedimientos establecidos por el responsable del tratamiento para atender dichas solicitudes no podrán exceder el plazo de quince (15) días laborables, contado a partir de la recepción de la solicitud.

Párrafo I. El responsable del tratamiento deberá confirmar al titular, por medios accesibles, seguros y verificables, el cese del tratamiento para las finalidades respecto de las cuales fue retirado el consentimiento, así como las medidas adoptadas como consecuencia de dicho retiro, incluyendo, cuando corresponda, la cancelación, supresión o eliminación segura de los datos biométricos o datos personales asociados a la identidad, conforme a la ley y al presente reglamento.

Párrafo II. Las obligaciones legales o regulatorias de conservación de documentación, registros, evidencias transaccionales, soportes de operaciones o medios de prueba no se interpretarán, por sí solas, como autorización para conservar datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos o mecanismos de vinculación, salvo disposición legal expresa compatible con la Ley núm. 4-23 o requerimiento concreto de autoridad competente que justifique su conservación temporal.

Artículo 38. Datos cedidos a terceros antes del retiro del consentimiento. En caso de que los datos biométricos hubiesen sido cedidos a un tercero con anterioridad al retiro del consentimiento, el responsable del tratamiento deberá comunicar dicho retiro al cesionario y adoptar las medidas razonables, documentadas y verificables para que este proceda, cuando corresponda conforme a la ley y al presente reglamento, a la cancelación, supresión o eliminación segura de los datos tratados.

Párrafo I. Cuando la cesión haya sido autorizada previamente por el titular, el retiro del consentimiento deberá ser comunicado por el responsable del tratamiento a los cesionarios identificados en sus registros, sin perjuicio del derecho del titular de ejercer directamente sus derechos frente a dichos cesionarios.

Párrafo II. La entrega, comunicación o constancia de datos personales asociados a la identidad, cuando proceda conforme a la ley y al presente reglamento, no exime al responsable del tratamiento de informar al titular sobre los destinatarios o cesionarios de los datos, ni de conservar trazabilidad de las comunicaciones realizadas.

Artículo 39. Responsabilidad por negativa injustificada de cancelación o supresión. En caso de negativa injustificada de cancelar, suprimir o eliminar los datos biométricos tratados por un responsable o cesionario como consecuencia del retiro del consentimiento, tanto el responsable del tratamiento como el cesionario responderán conforme al régimen de consecuencias aplicable, sin perjuicio de las responsabilidades administrativas, civiles o penales que correspondan.

CAPÍTULO IV

DEL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS

SECCIÓN I

DE LOS USOS Y FINALIDADES DEL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS

Artículo 40. Usos y finalidades permitidas. Cuando resulte legalmente procedente conforme al alcance de la habilitación legal, autorización, consentimiento o condición aplicable, los datos biométricos solo podrán ser tratados para finalidades específicas, legítimas, informadas, necesarias y proporcionales, de conformidad con la Ley núm. 4-23, la normativa de protección de datos personales, el presente reglamento

y las disposiciones dictadas por la Junta Central Electoral dentro del ámbito de sus competencias. Los usos y finalidades admisibles podrán comprender, según corresponda, los siguientes:

a) **Identificación biométrica.** Proceso mediante el cual se determina la identidad de una persona mediante la comparación de sus características biométricas contra una base de datos de referencia, bajo un enfoque uno a muchos (1:N). Este uso solo será admisible cuando exista habilitación legal expresa, autorización conforme al presente reglamento o competencia legal suficiente para la finalidad específica invocada. Cuando la identificación biométrica se realice para los usos previstos en los literales e) y h), se sujetará además a la autorización allí exigida.

b) **Verificación de identidad.** Proceso mediante el cual se confirma que una persona es quien afirma ser, mediante la comparación uno a uno (1:1) de sus características biométricas con datos biométricos previamente asociados a esa identidad. Cuando la verificación tenga por objeto la consulta, validación o certificación de identidad frente a terceros, o la confirmación de identidad con efectos frente a terceros, deberá realizarse a través del servicio provisto por la Junta Central Electoral o de los mecanismos técnicos de acceso, consulta o interoperabilidad autorizados por esta.

c) **Autenticación biométrica.** Uso de características biométricas como factor de autenticación para permitir o validar el acceso del titular a instalaciones, sistemas, plataformas, servicios o transacciones del propio responsable, dentro de una relación directa con el titular y para una finalidad específica, legítima, informada, necesaria, proporcional y consentida cuando corresponda.

d) **Control de acceso y asistencia.** Uso de datos biométricos para controlar el acceso a instalaciones físicas, sistemas de información, equipos tecnológicos o áreas restringidas, así como para registrar asistencia, únicamente respecto de personas vinculadas directamente con la entidad y conforme a una finalidad específica, legítima, informada, necesaria y proporcional. Este uso deberá observar los principios de minimización, disponibilidad de alternativas cuando corresponda, seguridad, confidencialidad y retención limitada.

e) **Seguridad nacional, control fronterizo y protección de infraestructuras críticas.** Uso de datos biométricos por autoridades legalmente competentes, exclusivamente cuando exista habilitación legal expresa, requerimiento concreto de autoridad competente u orden judicial, según corresponda, y siempre que el tratamiento sea necesario, proporcional, limitado a una finalidad específica, sujeto a trazabilidad, controles de acceso, medidas reforzadas de seguridad y garantías aplicables. Este uso no podrá emplearse para fines genéricos, preventivos o prospectivos indeterminados, ni para vigilancia masiva, indiscriminada o permanente de personas fuera de los supuestos permitidos por la Constitución y la ley. La aplicación de esta disposición por parte de la Junta Central Electoral queda limitada a los datos biométricos bajo su custodia y administración.

f) **Identificación de personas en contextos de salud.** Uso de datos biométricos para la identificación o verificación de identidad de pacientes, usuarios o personas vinculadas a la prestación de servicios de salud, únicamente cuando resulte necesario para garantizar la seguridad del paciente, evitar suplantación de identidad, asegurar la correcta vinculación con expedientes o servicios, cumplir una obligación legal expresa, atender situaciones de emergencia o proteger derechos vitales del titular, y siempre bajo principios de finalidad específica, necesidad, proporcionalidad, minimización, confidencialidad, seguridad reforzada y retención limitada.

g) **Prevención, detección y control de fraudes.** Uso de datos biométricos para prevenir, detectar o controlar fraudes, suplantación de identidad o uso indebido de servicios, siempre que dicho tratamiento sea necesario, proporcional, limitado a la finalidad específica informada y no pueda alcanzarse razonablemente mediante medios menos intrusivos.

h) **Investigación forense o persecución de infracciones.** Uso de datos biométricos en investigaciones forenses, penales, administrativas o de otra naturaleza legalmente habilitada, únicamente por autoridades competentes o por disposición de estas, conforme a la ley, orden

judicial, requerimiento de autoridad competente o actuación sujeta a las garantías aplicables, con sujeción a los principios de necesidad, proporcionalidad, trazabilidad, confidencialidad y limitación de finalidad. En estos casos, la comparación contra las bases bajo competencia de la Junta Central Electoral se realizará a través de su servicio, conforme al Párrafo II de este artículo. La regulación del uso de datos biométricos con fines de investigación forense o persecución penal corresponde a la ley procesal y especial aplicable; el presente reglamento se limita a regular el mecanismo de consulta frente a las bases bajo competencia de la Junta Central Electoral.

i) **Cumplimiento de obligaciones legales y reglamentarias.** Uso de datos biométricos para el cumplimiento de obligaciones legales o reglamentarias expresas, siempre que la obligación invocada sea compatible con la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento, y que el tratamiento resulte estrictamente necesario, proporcional y limitado a la obligación específica que lo justifica.

Párrafo I. Ninguno de los usos previstos en este artículo podrá interpretarse como autorización para que entidades públicas o privadas creen, mantengan, alimenten, actualicen, interconecten, exploten o conserven bases de datos biométricos, bases de datos personales asociados a la identidad, repositorios, registros, sistemas, plataformas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que tengan por objeto o efecto sustituir, replicar, desplazar o funcionar como infraestructura paralela o sustitutiva de los registros, bases de datos, servicios o competencias atribuidas a la Junta Central Electoral en materia de identidad, Registro Civil, cedulación, consulta, verificación o certificación de identidad.

Párrafo II. La evidencia biométrica recolectada por las autoridades competentes en el curso de una investigación forense, penal o legalmente habilitada —incluidas las muestras y las huellas o imágenes latentes obtenidas de personas, objetos, superficies, escenas o registros— constituye una categoría distinta, sujeta a la custodia y al régimen del órgano actuante conforme a la normativa procesal aplicable, y no forma parte ni se integra a las bases de datos bajo competencia de la Junta Central Electoral. Su comparación contra dichas bases se realizará exclusivamente a través del servicio de consulta, verificación e identificación provisto por la Junta Central Electoral, que devolverá el resultado y la constancia correspondiente sin transferir plantillas, vectores, minucias, muestras ni cualquier otra representación del dato biométrico. En ningún caso podrán uno y otro conjunto de datos fusionarse, migrarse o interconectarse.

Artículo 41. Limitaciones en el uso de los datos biométricos. El uso de datos biométricos por parte del responsable del tratamiento estará sujeto a las limitaciones siguientes:

a) **Proporcionalidad.** El tratamiento y uso de datos biométricos solo será admisible cuando resulte necesario y proporcional a la finalidad específica, legítima e informada que lo justifica, y no exista un medio menos intrusivo razonablemente idóneo para alcanzar dicha finalidad.

b) **Minimización de datos.** El responsable del tratamiento deberá limitar la recopilación, captura, uso, consulta, conservación y demás operaciones de tratamiento de los datos biométricos al mínimo estrictamente necesario para cumplir la finalidad específica, legítima e informada que justificó el tratamiento. El mínimo necesario deberá determinarse atendiendo a la naturaleza de la finalidad perseguida, la modalidad del tratamiento, los datos indispensables para su ejecución, el nivel de riesgo y la existencia de medios menos intrusivos para alcanzar dicha finalidad.

c) **Transparencia.** El responsable del tratamiento deberá informar al titular, de manera previa, clara, accesible y comprensible, sobre la recopilación, captura, uso y demás operaciones de tratamiento de sus datos biométricos, las finalidades específicas, la base que habilita el tratamiento, los plazos de conservación, los destinatarios o categorías de destinatarios cuando corresponda, los derechos que le asisten y las medidas generales de seguridad adoptadas, sin revelar información que pueda comprometer la seguridad de los sistemas, servicios o mecanismos utilizados.

d) **Consentimiento y base habilitante.** El tratamiento y uso de los datos biométricos no podrá exceder el alcance del consentimiento otorgado por el titular, de la autorización aplicable o de la disposición legal expresa que habilite el tratamiento, según corresponda.

e) **Finalidad y prohibición de reutilización.** Los datos biométricos no podrán ser utilizados, reutilizados, cedidos, comunicados, interconectados o tratados ulteriormente para finalidades distintas, incompatibles o no informadas, salvo nuevo consentimiento del titular, autorización aplicable o habilitación legal expresa conforme a la ley y al presente reglamento.

f) **Retención limitada.** Los datos biométricos solo podrán conservarse durante el tiempo necesario, proporcional y legítimo para cumplir la finalidad específica que justificó su tratamiento, conforme a las reglas de conservación, supresión y eliminación segura establecidas en el presente reglamento.

g) **Seguridad y trazabilidad.** El uso de datos biométricos deberá realizarse mediante medidas técnicas, organizativas, administrativas y de seguridad que permitan proteger su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, así como prevenir accesos, consultas, modificaciones, reutilizaciones, transferencias o tratamientos no autorizados.

h) **Responsabilidad demostrable.** El responsable del tratamiento deberá poder demostrar el cumplimiento de las limitaciones previstas en este artículo mediante evidencias documentales, técnicas, contractuales, operativas o de auditoría, según corresponda a la naturaleza, finalidad, alcance y riesgo del tratamiento.

i) **Prohibición de comercialización, monetización y uso publicitario.** Los datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias, mecanismos de vinculación, resultados de verificación, constancias de consulta o datos personales asociados a la identidad no podrán ser vendidos, comercializados, arrendados, monetizados, cedidos, explotados, perfilados o utilizados para finalidades publicitarias, mercadológicas, de segmentación comercial, fidelización, prospección, analítica comercial o cualquier otra finalidad incompatible con la finalidad específica que justificó su tratamiento, salvo que una disposición legal expresa establezca lo contrario y resulte compatible con la Ley núm. 4-23 y el presente reglamento.

SECCIÓN II

DE LA RECOLECCIÓN DE LOS DATOS BIOMÉTRICOS Y LAS BASES DE DATOS BIOMÉTRICOS

Artículo 42. Recolección de datos biométricos. La recolección de datos biométricos solo será permitida cuando se cumplan las condiciones siguientes:

a) **Consentimiento o habilitación legal.** El titular deberá haber otorgado su consentimiento expreso, informado, específico, inequívoco y verificable para la recolección de sus datos biométricos por parte del responsable del tratamiento, salvo en los casos en que exista disposición legal expresa, autorización aplicable o condición habilitante conforme a la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

b) **Finalidad legítima y específica.** La recolección deberá responder a una finalidad legítima, específica, informada, necesaria y proporcional, previamente comunicada al titular, sin que puedan recolectarse datos biométricos para finalidades genéricas, indeterminadas, incompatibles o no vinculadas con la finalidad informada.

c) **Necesidad y minimización.** Los datos biométricos recolectados deberán limitarse al mínimo estrictamente necesario para cumplir la finalidad que justifica la recolección, atendiendo a la modalidad del tratamiento, al nivel de riesgo, a los datos indispensables para su ejecución y a la existencia de medios menos intrusivos para alcanzar dicha finalidad.

d) **Aviso de privacidad.** Antes de la captura o recolección de los datos biométricos, el responsable del tratamiento deberá poner a disposición del titular el aviso de privacidad correspondiente, conforme a las condiciones previstas en el presente reglamento.

e) **Garantías de seguridad y trazabilidad.** El responsable del tratamiento deberá implementar medidas técnicas, organizativas y de seguridad adecuadas para proteger los datos biométricos desde el momento de su captura o recolección, garantizando su confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y uso limitado.

f) **Condiciones para el tratamiento posterior.** Cuando los datos biométricos recolectados sean objeto de almacenamiento, conservación, acceso por terceros, subcontratación, cesión, comunicación, interconexión o cualquier tratamiento posterior, deberán existir las garantías jurídicas, contractuales, técnicas y organizativas correspondientes, conforme a la ley, el presente reglamento y las autorizaciones que resulten aplicables.

Párrafo I. La recolección de datos biométricos no podrá realizarse para finalidades preventivas, prospectivas, genéricas o indeterminadas, ni bajo fórmulas amplias que impidan al titular conocer de manera clara la finalidad específica del tratamiento.

Párrafo II. Cuando la recolección de datos biométricos se realice mediante dispositivos, aplicaciones, plataformas, medios remotos, digitales, electrónicos, ópticos, automatizados o no presenciales, el responsable deberá garantizar la seguridad del canal, la autenticidad de la operación, la trazabilidad de la captura, la integridad de los datos y la constancia verificable del consentimiento o de la base habilitante aplicable.

Artículo 43. Bases de datos biométricos. Dentro del ámbito de aplicación del presente reglamento, la creación, almacenamiento, conservación, administración, actualización, interconexión o explotación de bases de datos biométricos por entidades públicas o privadas solo será admisible cuando responda a una finalidad específica, legítima, informada, necesaria y proporcional, y se encuentre amparada en una base legal válida, consentimiento expreso cuando corresponda, autorización aplicable o condición habilitante conforme a la Ley núm. 4-23, la normativa de protección de datos personales, el presente reglamento y las disposiciones dictadas por la Junta Central Electoral dentro del ámbito de sus competencias.

Párrafo I. Dentro del ámbito de aplicación del presente reglamento, la Junta Central Electoral podrá establecer, mediante norma complementaria, instructivo o acto administrativo de alcance general, categorías diferenciadas de tratamiento biométrico, atendiendo al volumen de titulares, finalidad, tecnología utilizada, modalidad de almacenamiento, nivel de riesgo, posibilidad de interconexión, cesión, comunicación o acceso por terceros, prestación de servicios a terceros, tratamiento sistemático o masivo, y demás factores relevantes.

Párrafo II. Requerirán autorización previa de la Junta Central Electoral, dentro del ámbito de aplicación del presente reglamento, aquellos tratamientos biométricos que involucren datos biométricos o datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, el uso del Servicio de Consulta, Verificación y Certificación de Identidad, mecanismos de interoperabilidad autorizados por esta, resultados, constancias o registros derivados del servicio, o cualquier tratamiento que pueda afectar directamente las competencias atribuidas a la Junta Central Electoral en materia de identidad, Registro Civil, cedulación, consulta, verificación o certificación de identidad.

Párrafo III. La autorización prevista en este artículo no podrá interpretarse como habilitación para que entidades públicas o privadas, dentro del ámbito de aplicación del presente reglamento, creen, mantengan, alimenten, actualicen, interconecten, exploten o conserven bases de datos biométricos, bases de datos personales asociados a la identidad, repositorios, registros, sistemas, plataformas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que tengan por objeto o efecto sustituir, replicar, desplazar o funcionar como infraestructura paralela o sustitutiva de los registros, bases de datos, servicios o competencias atribuidas a la Junta Central Electoral en materia de identidad, Registro Civil, cedulación, consulta, verificación o certificación de identidad.

Párrafo IV. Los tratamientos biométricos internos y limitados comprendidos dentro del ámbito de aplicación del presente reglamento, destinados exclusivamente al control de acceso, asistencia o seguridad interna de una entidad, sin cesión, comunicación, interconexión, reutilización, prestación de servicios a terceros, sin identificación biométrica uno a muchos (1:N), tratamiento masivo ni conservación centralizada de gran escala, podrán estar sujetos a un régimen simplificado de registro, declaración responsable o cumplimiento mínimo, conforme a las condiciones que establezca la Junta Central Electoral.

Párrafo V. En ningún caso el régimen simplificado eximirá al responsable del cumplimiento de los principios de consentimiento expreso cuando corresponda, información previa, finalidad específica, minimización, seguridad, confidencialidad, trazabilidad, retención limitada, supresión o eliminación segura, ni de la prohibición de reutilizar, ceder, comunicar, explotar o tratar los datos biométricos para finalidades distintas a las informadas o autorizadas.

SECCIÓN III

DE LA CESIÓN DE LOS DATOS BIOMÉTRICOS

Artículo 44. Cesión de datos biométricos. Solo podrán realizarse cesiones, comunicaciones, transferencias o transmisiones de datos biométricos cuando medie consentimiento expreso, específico, informado, inequívoco y verificable del titular, exista una finalidad legítima, determinada y compatible con la finalidad originalmente informada, y la cesión sea necesaria, proporcional y directamente relacionada con las funciones legítimas del cedente y del cesionario, conforme a la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

Párrafo I. Excepcionalmente, no será necesario el consentimiento del titular únicamente en los supuestos previstos por la Ley núm. 4-23 o por una disposición legal expresa compatible con esta. En tales casos, el cedente deberá dejar constancia expresa, documentada y verificable de la causal legal invocada, de la finalidad de la cesión, de la necesidad de transferir los datos, de los datos estrictamente necesarios objeto de cesión, de los límites aplicables y de las garantías adoptadas para proteger los datos biométricos cedidos.

Párrafo II. Cuando corresponda, el cedente deberá dejar constancia de la autoridad requirente, mandato legal, orden judicial o actuación administrativa que justifique la cesión, salvo las restricciones derivadas de reserva legal, secreto de investigación u orden de autoridad competente.

Párrafo III. Cuando el consentimiento otorgado por el titular al momento de la recolección de los datos no haya considerado la cesión de estos, el cedente deberá informar al titular, antes de que la cesión se produzca, la finalidad a la cual serán destinados los datos, la identidad o categoría del cesionario, el tipo de actividad de este y las garantías aplicables, salvo los supuestos de excepción previstos por la ley.

Párrafo IV. La obligación de información previa prevista en el párrafo anterior no será exigible cuando la cesión se realice en virtud de mandato legal, requerimiento de autoridad competente, orden judicial o actuación sujeta a reserva legal, siempre que la comunicación previa al titular resulte incompatible con la finalidad de la investigación, el cumplimiento de la obligación legal, la eficacia de la actuación requerida o la protección de derechos de terceros.

Párrafo V. El consentimiento otorgado para la cesión de datos biométricos será revocable, conforme a las condiciones, efectos y procedimientos establecidos en el presente reglamento. El retiro del consentimiento no afectará la licitud de la cesión realizada con anterioridad, siempre que esta haya cumplido con la ley y el presente reglamento.

Artículo 45. Obligaciones del cesionario. El cesionario quedará sujeto a las mismas obligaciones legales, reglamentarias, técnicas, organizativas, de seguridad, confidencialidad, trazabilidad, finalidad, retención limitada y eliminación segura aplicables al cedente respecto de los datos biométricos cedidos.

Párrafo I. El cesionario solo podrá tratar los datos biométricos recibidos para la finalidad específica que justificó la cesión, dentro de los límites informados al titular, autorizados por este o habilitados por la ley.

Párrafo II. El cesionario no podrá ceder, comunicar, transferir, reutilizar, interconectar, explotar o tratar ulteriormente los datos biométricos recibidos, ni incorporarlos a bases de datos propias o de terceros, salvo que exista consentimiento expreso del titular, habilitación legal expresa o autorización aplicable conforme a la Ley núm. 4-23, la normativa de protección de datos personales y el presente reglamento.

Párrafo III. La conservación de registros, constancias o evidencias mínimas necesarias para demostrar la licitud de la cesión, la trazabilidad de la operación o el cumplimiento de obligaciones legales o contractuales no constituirá, por sí sola, incorporación a una base biométrica reutilizable, siempre que no incluya muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que permitan tratamiento biométrico autónomo no autorizado.

Párrafo IV. Cualquier requerimiento posterior de los datos biométricos cedidos deberá ser tramitado ante el cedente original o ante la autoridad competente, conforme a la Ley núm. 4-23, la normativa aplicable y el presente reglamento.

Párrafo V. El cedente y el cesionario responderán conforme al régimen de consecuencias aplicable por la inobservancia de las obligaciones previstas en este artículo, sin perjuicio de las responsabilidades que correspondan frente al titular, la Junta Central Electoral y demás autoridades competentes.

Artículo 46. Límites de la cesión de datos biométricos. La cesión, comunicación, transferencia o transmisión de datos biométricos no podrá interpretarse como autorización para crear, mantener, alimentar, actualizar, interconectar, explotar o conservar bases de datos biométricos, bases de datos personales asociados a la identidad, repositorios, registros, sistemas, plataformas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que tengan por objeto o efecto sustituir, replicar, desplazar o funcionar como infraestructura paralela o sustitutiva de los registros, bases de datos, servicios o competencias atribuidas a la Junta Central Electoral en materia de identidad, Registro Civil, cedulación, consulta, verificación o certificación de identidad.

Párrafo. Tampoco podrá utilizarse la cesión de datos biométricos para desarrollar, operar, ofrecer o prestar, por cuenta propia, dentro de un grupo económico o a favor de terceros, servicios de consulta, verificación o certificación de identidad, salvo a través de los mecanismos provistos, autorizados o regulados por la Junta Central Electoral, conforme a la Ley núm. 4-23, el presente reglamento y las condiciones establecidas por esta.

Artículo 47. Prueba de cumplimiento de obligaciones en materia de cesión. Para efectos de demostrar que la cesión, comunicación, transferencia o transmisión de datos biométricos se realizó conforme a la ley y el presente reglamento, la carga de la prueba recaerá, en todos los casos, en el cedente y en el cesionario, según sus respectivas obligaciones.

Párrafo I. El cedente deberá conservar evidencia suficiente, íntegra, segura, trazable y auditable de la base legal o consentimiento que habilitó la cesión, la finalidad, los datos cedidos, la identidad del cesionario, la fecha de la operación, las garantías aplicadas, los límites comunicados y las condiciones bajo las cuales se realizó la cesión.

Párrafo II. El cesionario deberá conservar evidencia suficiente, íntegra, segura, trazable y auditable del tratamiento realizado sobre los datos recibidos, la finalidad aplicada, las medidas de seguridad implementadas, los accesos autorizados, los plazos de conservación, las eliminaciones realizadas cuando correspondan y cualquier comunicación posterior vinculada con dichos datos.

Artículo 48. Registro de la cesión y transmisión de datos biométricos a terceros. El responsable del tratamiento deberá llevar un registro actualizado, íntegro y trazable de todas las cesiones, comunicaciones, transferencias o transmisiones de datos biométricos a terceros. Dicho registro deberá incluir, como mínimo, la identidad del tercero receptor, la fecha de la cesión o transmisión, la finalidad específica, el tipo de datos biométricos cedidos o transmitidos, las garantías contractuales, técnicas y organizativas establecidas, y la constancia del consentimiento expreso, específico, informado, inequívoco y verificable del titular, cuando corresponda.

Párrafo I. Cuando la cesión, comunicación, transferencia o transmisión no se fundamente en el consentimiento del titular, el responsable deberá dejar constancia expresa, documentada y verificable de la causal legal específica que la habilita, así como de la justificación de necesidad, proporcionalidad, finalidad, límites aplicables y compatibilidad con la normativa de protección de datos personales y el presente reglamento.

Párrafo II. La Junta Central Electoral podrá requerir acceso, copia o información relacionada con este registro cuando resulte necesario para verificar el cumplimiento de la Ley núm. 4-23, del presente reglamento y de las resoluciones dictadas por la Junta Central Electoral en materia de datos biométricos, consulta, verificación y certificación de identidad. Dicho requerimiento se realizará observando las garantías del debido proceso, la confidencialidad de la información y los principios de necesidad, proporcionalidad y razonabilidad, sin perjuicio de la coordinación que, cuando corresponda, pueda realizarse con el órgano regulador sectorial competente.

Artículo 49. Transferencias internacionales de datos biométricos y datos personales asociados a la identidad. La transferencia internacional de datos biométricos o datos personales asociados a la identidad comprendidos dentro del ámbito de aplicación del presente reglamento solo podrá realizarse cuando exista habilitación legal expresa, consentimiento expreso del titular cuando corresponda, requerimiento de autoridad competente, convenio o instrumento jurídico válido, y siempre que se garanticen niveles adecuados de protección, seguridad, confidencialidad, trazabilidad, finalidad, minimización y limitación de conservación.

Párrafo I. Cuando la transferencia internacional involucre datos biométricos o datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, resultados del Servicio de Consulta, Verificación y Certificación de Identidad, constancias de consulta, mecanismos de interoperabilidad, credenciales, interfaces o datos derivados del servicio, deberá contar con autorización previa de la Junta Central Electoral o encontrarse amparada en una disposición legal expresa compatible con la Ley núm. 4-23.

Párrafo II. Toda transferencia internacional deberá documentarse mediante contrato, convenio, cláusulas de protección de datos, acuerdo de tratamiento, requerimiento formal de autoridad competente o instrumento equivalente, en el cual se establezcan la finalidad, datos objeto de transferencia, destinatario, país de destino, medidas de seguridad, plazo de conservación, prohibición de reutilización, reglas de eliminación segura, auditoría y responsabilidades aplicables.

Párrafo III. La recepción, validación o tratamiento de datos biométricos de personas extranjeras se regirá por la legislación especial aplicable, los convenios o acuerdos válidos y la normativa de protección de datos personales. Cuando dichos tratamientos se vinculen con datos, documentos, registros, servicios, mecanismos de consulta o competencias atribuidas a la Junta Central Electoral, deberán observar las disposiciones del presente reglamento.

Párrafo IV. En ningún caso la transferencia internacional podrá utilizarse para crear, alimentar, replicar, actualizar o explotar bases biométricas paralelas, sustitutivas o no autorizadas, ni para prestar servicios de consulta, verificación o certificación de identidad fuera de los mecanismos provistos, autorizados o regulados por la Junta Central Electoral.

SECCIÓN IV

DEL ALMACENAMIENTO, CONSERVACIÓN Y ELIMINACIÓN DE LOS DATOS BIOMÉTRICOS

Artículo 50. Almacenamiento seguro de datos biométricos. El responsable del tratamiento deberá garantizar el almacenamiento seguro y protegido de los datos biométricos, conforme a la ley, el presente reglamento, la finalidad autorizada, el nivel de riesgo del tratamiento y las medidas técnicas, organizativas y de seguridad aplicables. El almacenamiento de datos biométricos deberá cumplir, como mínimo, con las condiciones siguientes:

a) **Cifrado.** Los datos biométricos deberán ser almacenados utilizando mecanismos de cifrado adecuados que protejan su confidencialidad, integridad y disponibilidad, conforme al nivel de riesgo del tratamiento y a las mejores prácticas aplicables.

b) **Medidas de seguridad físicas, lógicas y organizativas.** Deberán implementarse medidas apropiadas para prevenir accesos no autorizados, alteraciones, pérdidas, destrucción, divulgación, extracción, reutilización, copia, consulta o tratamiento no autorizado de los datos biométricos almacenados.

c) **Control de acceso y segregación.** El acceso a los datos biométricos almacenados deberá limitarse a personas, perfiles, sistemas o componentes expresamente autorizados, conforme a roles, credenciales, principios de mínimo privilegio, segregación de funciones y mecanismos de autenticación adecuados.

d) **Registro de actividades.** El responsable del tratamiento deberá mantener registros íntegros, trazables y auditables de las actividades relacionadas con el almacenamiento, acceso, consulta, modificación, conservación, supresión o eliminación de los datos biométricos.

e) **Política de retención.** El responsable deberá contar con una política documentada de retención que defina los plazos, criterios, condiciones, responsables, medidas de restricción y procedimientos de eliminación segura de los datos biométricos, conforme a las finalidades específicas para las cuales fueron recopilados o tratados.

Párrafo. Queda prohibido registrar, almacenar o conservar datos biométricos en archivos, registros, repositorios, sistemas, dispositivos o bases de datos que no reúnan las condiciones técnicas, organizativas y de seguridad previstas en el presente reglamento.

Artículo 51. Plazos de conservación de los datos biométricos. Los plazos de conservación de los datos biométricos no deberán exceder aquellos que resulten necesarios, proporcionales y legítimos para el cumplimiento de las finalidades específicas que justificaron su tratamiento, conforme a la Ley núm. 4-23, la normativa de protección de datos personales, el presente reglamento, el aviso de privacidad, el consentimiento otorgado cuando corresponda y la base legal aplicable.

Párrafo I. Una vez cumplida la finalidad del tratamiento, vencido o retirado el consentimiento otorgado por el titular, vencido el plazo autorizado para su almacenamiento o desaparecida la causa que justificó la conservación de los datos biométricos, el responsable del tratamiento deberá proceder a su supresión o eliminación segura, salvo que exista disposición legal expresa compatible con la Ley núm. 4-23 o requerimiento concreto de autoridad competente que justifique su conservación temporal.

Párrafo II. La conservación temporal excepcional deberá limitarse a los datos estrictamente necesarios, por el tiempo indispensable para atender la finalidad legal específica que la justifica, y realizarse mediante medidas efectivas de restricción, separación, seguridad, confidencialidad, trazabilidad y control. Durante dicho período, los datos no podrán ser objeto de uso, consulta, comparación, reutilización, cesión, comunicación, transferencia, explotación o tratamiento ulterior distinto al fin legal específico que justificó su conservación.

Párrafo III. Las obligaciones legales, reglamentarias, contractuales, sectoriales o probatorias de conservación de documentación, expedientes, registros, evidencias transaccionales, constancias de consulta, resultados de verificación, soportes de operaciones o medios de prueba no se interpretarán, por sí solas, como autorización para conservar datos biométricos, muestras biométricas, plantillas, vectores, patrones, imágenes biométricas, códigos biométricos o mecanismos de vinculación que permitan realizar identificación, verificación, autenticación, comparación o tratamiento biométrico autónomo, salvo disposición legal expresa compatible con la Ley núm. 4-23 o requerimiento concreto de autoridad competente que justifique su conservación temporal.

Párrafo IV. La conservación, durante el plazo legal o legítimamente aplicable, de constancias, resultados de verificación, registros de consulta, evidencias de consentimiento, soportes transaccionales o

documentación asociada a una operación no habilita la creación, mantenimiento, explotación, actualización o interconexión de bases de datos biométricos paralelas, sustitutivas o no autorizadas.

Artículo 52. Procedimientos de conservación. El responsable del tratamiento deberá establecer, documentar, implementar y mantener procedimientos para la conservación de los datos biométricos, incluyendo los períodos de conservación, las condiciones de restricción, seguridad, trazabilidad, revisión periódica, acceso limitado y eliminación segura, de conformidad con lo dispuesto en el presente reglamento.

Párrafo I. Los procedimientos de conservación deberán ser revisados periódicamente para verificar que los datos biométricos conservados siguen siendo necesarios, proporcionales y compatibles con la finalidad que justificó su tratamiento.

Párrafo II. Cuando desaparezca la finalidad que justificó la conservación, o cuando venza el plazo aplicable, el responsable deberá activar los procedimientos de supresión o eliminación segura, dejando constancia verificable de las medidas adoptadas.

Artículo 53. Eliminación de datos biométricos. La eliminación de los datos biométricos deberá realizarse conforme a los principios de finalidad, necesidad, proporcionalidad, retención limitada, seguridad, confidencialidad, trazabilidad y responsabilidad. La eliminación deberá cumplir con las condiciones siguientes:

a) **Criterios de eliminación.** Los datos biométricos deberán eliminarse de forma segura cuando hayan dejado de ser necesarios para la finalidad específica para la cual fueron recopilados o tratados, cuando el titular lo solicite y no exista causa legal que justifique su conservación temporal, cuando haya vencido o sido retirado el consentimiento que habilitaba su tratamiento, cuando haya vencido el plazo por el cual fue autorizado su almacenamiento, o cuando proceda conforme a la ley y el presente reglamento.

b) **Procedimientos de eliminación.** El responsable del tratamiento deberá establecer procedimientos adecuados para garantizar la eliminación segura, definitiva, verificable e irreversible de los datos biométricos, de manera que no puedan ser recuperados, reconstruidos, reutilizados o asociados nuevamente al titular.

c) **Registro de eliminaciones.** El responsable del tratamiento deberá llevar un registro actualizado, íntegro y trazable de las eliminaciones realizadas, que incluya, como mínimo, la fecha de eliminación, el motivo que la justificó, los datos o categorías de datos eliminados, el método utilizado y las medidas adoptadas para garantizar la eliminación segura.

d) **Responsabilidad en la eliminación.** El responsable del tratamiento será responsable de garantizar la correcta eliminación de los datos biométricos, así como de demostrar el cumplimiento de esta obligación ante la Junta Central Electoral y demás autoridades competentes, cuando corresponda.

e) **Notificación de la eliminación.** El responsable del tratamiento deberá dejar constancia de la eliminación segura de los datos biométricos y, cuando corresponda, notificar al titular sobre dicha eliminación. Si los datos hubieren sido cedidos, comunicados, transferidos o transmitidos a terceros, el responsable deberá informar la eliminación a los terceros receptores identificados en sus registros, a fin de que adopten las medidas que correspondan conforme a la ley, el presente reglamento y las condiciones bajo las cuales recibieron los datos, salvo impedimento legal, requerimiento de autoridad competente, orden judicial o reserva legal aplicable.

TÍTULO III

CONSULTA, VERIFICACIÓN Y CERTIFICACIÓN DE LA IDENTIDAD DE LAS PERSONAS

CAPÍTULO I

DEL SERVICIO DE CONSULTA, VERIFICACIÓN Y CERTIFICACIÓN DE IDENTIDAD PROVISTO POR LA JUNTA CENTRAL ELECTORAL

SECCIÓN I

DEL ALCANCE, CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO

Artículo 54. Servicio de Consulta, Verificación y Certificación de Identidad. La Junta Central Electoral tiene la competencia exclusiva de proveer a terceros el Servicio de Consulta, Verificación y Certificación de Identidad de las personas, mediante el uso de datos biométricos y datos personales asociados a la identidad bajo su competencia, conforme a la Constitución de la República, la Ley núm. 4-23, el presente reglamento y las disposiciones dictadas por la Junta Central Electoral.

Párrafo I. Ninguna entidad pública o privada podrá prestar, desarrollar, operar, explotar o poner a disposición de terceros, por cuenta propia, dentro de un grupo económico o mediante terceros vinculados, sistemas, plataformas, bases de datos, repositorios o mecanismos propios, alternos o paralelos destinados a consultar, verificar o certificar la identidad de personas mediante datos biométricos o datos personales asociados a la identidad bajo competencia de la Junta Central Electoral, cuando tales mecanismos sustituyan, repliquen o funcionen como alternativa al servicio provisto por esta.

Párrafo II. Las necesidades de continuidad operativa, disponibilidad del servicio o contingencia tecnológica de las entidades usuarias deberán ser atendidas mediante mecanismos coordinados, autorizados o regulados por la Junta Central Electoral, tales como procedimientos de contingencia, canales alternos de consulta, acuerdos de niveles de servicio, constancias de verificación, respuestas firmadas, mecanismos de verificación posterior o medidas equivalentes que no impliquen la creación de bases biométricas paralelas, la conservación de datos biométricos reutilizables ni la prestación privada de servicios de consulta, verificación o certificación de identidad.

Párrafo III. La conservación de registros, constancias, resultados de verificación, evidencias transaccionales o soportes operativos derivados del uso del servicio provisto por la Junta Central Electoral no habilita a las entidades usuarias a conservar datos biométricos, muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que permitan realizar identificación, verificación, autenticación, certificación, comparación o tratamiento biométrico autónomo.

Artículo 55. Datos utilizados para la prestación del servicio. Para la prestación del Servicio de Consulta, Verificación y Certificación de Identidad, la Junta Central Electoral podrá utilizar datos biométricos y datos personales asociados a la identidad bajo su competencia, incluyendo, entre otros, huellas dactilares, fotografía o imagen facial, iris, firma, nombres y apellidos, fecha de nacimiento, lugar de nacimiento, sexo, nacionalidad, número único de identidad, número de cédula de identidad o cédula de identidad y electoral, datos documentales, datos registrales y cualquier otro dato administrado, verificado, certificado o autorizado por la Junta Central Electoral para fines de identidad.

Párrafo I. La utilización de los datos indicados en este artículo deberá realizarse conforme a los principios de finalidad, necesidad, proporcionalidad, minimización, seguridad, confidencialidad, trazabilidad, responsabilidad y protección de los derechos de los titulares.

Párrafo II. La prestación del servicio no implicará, por sí misma, cesión total o parcial de los datos biométricos o datos personales asociados a la identidad administrados por la Junta Central Electoral. Las entidades usuarias solo podrán conservar los registros, constancias, resultados o evidencias expresamente autorizados por la Junta Central Electoral, conforme a las condiciones técnicas, contractuales y de seguridad aplicables.

Párrafo III. La Junta Central Electoral procurará implementar medidas de separación lógica, segregación, segmentación, control de acceso, cifrado, trazabilidad y minimización de vínculos entre los repositorios, sistemas o componentes que contengan datos biométricos y aquellos que contengan datos registrales o documentales del Registro Civil, conforme a su arquitectura institucional, gestión de riesgos, disponibilidad del servicio, continuidad operativa y políticas de seguridad de la información.

Párrafo IV. La separación prevista en el párrafo anterior tendrá por finalidad reducir la superficie de exposición, prevenir accesos no autorizados, limitar consultas indebidas, mitigar riesgos de correlación excesiva, proteger la integridad de los registros y preservar la confidencialidad de los datos biométricos y datos personales asociados a la identidad bajo competencia de la Junta Central Electoral.

Párrafo V. La Junta Central Electoral podrá desarrollar mediante norma técnica, política institucional, instructivo o resolución los criterios de arquitectura, segregación, interoperabilidad, trazabilidad, cifrado, control de accesos, auditoría y gestión de riesgos aplicables a sus sistemas internos y al Servicio de Consulta, Verificación y Certificación de Identidad.

Artículo 56. Características del servicio. El Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral se regirá por los principios establecidos en el presente reglamento y por las características siguientes:

a) **Precisión y fiabilidad.** El servicio deberá procurar altos niveles de precisión, confiabilidad y consistencia en la consulta, verificación o certificación de la identidad de las personas, mediante tecnologías, controles y procesos orientados a minimizar errores de identificación, falsas coincidencias, falsos rechazos y resultados inconsistentes.

b) **Multimodalidad.** El servicio podrá utilizar una o varias modalidades biométricas, tales como huellas dactilares, reconocimiento facial, iris u otras que la Junta Central Electoral determine conforme a sus competencias, capacidades técnicas, evaluación de riesgos y necesidades del servicio.

c) **Escalabilidad y disponibilidad.** El servicio deberá diseñarse y gestionarse con capacidad de escalabilidad, continuidad operativa y disponibilidad adecuada, procurando atender de manera eficiente los volúmenes de consulta autorizados sin comprometer la seguridad, integridad, confidencialidad o confiabilidad del servicio.

d) **Seguridad de los datos.** El servicio deberá contar con medidas técnicas, organizativas y de seguridad que protejan la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos biométricos y datos personales asociados a la identidad utilizados para su prestación.

e) **Interoperabilidad controlada.** La integración del servicio con sistemas de entidades usuarias deberá realizarse mediante mecanismos técnicos, protocolos, interfaces, credenciales, controles y condiciones de seguridad autorizados por la Junta Central Electoral.

f) **Usabilidad y soporte.** El servicio deberá procurar condiciones adecuadas de uso, orientación y soporte para las entidades usuarias autorizadas, a fin de facilitar su correcta integración, operación y cumplimiento de las condiciones establecidas por la Junta Central Electoral.

g) **Mantenimiento y actualización.** La Junta Central Electoral establecerá procesos de mantenimiento, monitoreo, mejora y actualización tecnológica del servicio, conforme a los avances técnicos, necesidades operativas, estándares aplicables, gestión de riesgos y requerimientos normativos.

h) **Control institucional.** La Junta Central Electoral mantendrá el control, custodia y administración de los datos biométricos y datos personales asociados a la identidad bajo su competencia, así como de los mecanismos de acceso, consulta, verificación y certificación de identidad provistos a terceros.

Artículo 57. Condiciones para la utilización del servicio. Para acceder al Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral, las entidades solicitantes deberán cumplir, como mínimo, con las condiciones siguientes:

a) Ser una entidad pública o privada legalmente constituida, debidamente registrada y con capacidad jurídica para celebrar contratos, convenios o acuerdos y asumir las obligaciones establecidas en la ley, el presente reglamento y las condiciones del servicio.

b) Contar con una finalidad clara, legítima, específica, necesaria y proporcional para el uso del servicio, vinculada con sus funciones, actividades, obligaciones legales, relación con los titulares o servicios prestados.

c) Acreditar la base legal, contractual o regulatoria que justifica la solicitud de acceso al servicio, según corresponda a la naturaleza de la entidad, la finalidad invocada y la relación con los titulares.

d) Demostrar la implementación de medidas técnicas, organizativas, administrativas y de seguridad adecuadas para proteger los registros, constancias, resultados de consulta, credenciales de acceso, mecanismos de integración y demás información vinculada al servicio.

e) Designar un punto de contacto técnico y un punto de contacto en materia de protección de datos, cumplimiento o seguridad de la información, responsables de la coordinación con la Junta Central Electoral.

f) Suscribir el contrato, convenio o acuerdo correspondiente con la Junta Central Electoral, en el cual se establecerán las condiciones de acceso, uso, seguridad, trazabilidad, confidencialidad, auditoría, niveles de servicio, responsabilidades, causales de suspensión o terminación y demás obligaciones aplicables.

g) Proporcionar la información y documentación que respalde la veracidad, legitimidad, necesidad y proporcionalidad de las actividades y fines para los cuales se solicita el uso del servicio.

h) Comprometerse a utilizar el servicio exclusivamente para la finalidad autorizada, conforme a las condiciones técnicas, contractuales y de seguridad establecidas por la Junta Central Electoral.

i) Abstenerse de ceder, divulgar, reutilizar, interconectar, explotar, comunicar o tratar ulteriormente los datos biométricos, datos personales asociados a la identidad, resultados, constancias, registros o evidencias derivados del uso del servicio para finalidades distintas a las autorizadas, para prestar servicios de consulta, verificación o certificación de identidad a terceros, o para desarrollar sistemas, mecanismos o capacidades que, por su objeto o efecto, sustituyan, repliquen, desplacen o funcionen como alternativa al Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral, salvo habilitación legal expresa, autorización aplicable o disposición de autoridad competente conforme al marco legal correspondiente.

Párrafo I. El cumplimiento de las condiciones previstas en este artículo será evaluado por la Junta Central Electoral antes de la autorización de acceso al servicio y podrá ser revisado durante toda la vigencia del contrato, convenio o acuerdo correspondiente.

Párrafo II. La conservación de datos biométricos o datos personales asociados a la identidad por parte de las entidades usuarias no constituirá, por sí sola, una infracción al presente reglamento, siempre que se encuentre amparada en consentimiento válido, en una base legal válida, se limite a la finalidad específica informada o autorizada, respete el plazo de conservación aplicable y no tenga por objeto o efecto sustituir, replicar o desplazar el servicio provisto por la Junta Central Electoral.

SECCIÓN II

DEL PROCEDIMIENTO DE SOLICITUD DEL SERVICIO DE CONSULTA, VERIFICACIÓN Y CERTIFICACIÓN DE IDENTIDAD

Artículo 58. Solicitud del servicio. Las entidades interesadas en utilizar el Servicio de Consulta, Verificación y Certificación de Identidad deberán presentar una solicitud por escrito, física o electrónica, ante la Junta Central Electoral.

Párrafo I. La solicitud deberá incluir, como mínimo, información sobre la entidad solicitante, su nombre o razón social, domicilio, representante legal, contacto principal, tipo de servicio solicitado, finalidad del uso, base legal, contractual o regulatoria que justifica la solicitud, volumen estimado de consultas, sistemas o plataformas involucradas y cualquier otra información requerida por la Junta Central Electoral.

Párrafo II. La Junta Central Electoral acusará recibo de la solicitud dentro de un plazo de cinco (5) días hábiles contados a partir de su recepción, sin que dicho acuse implique aceptación, autorización, aprobación o habilitación para el uso del servicio.

Artículo 59. Evaluación de legitimidad, finalidad e idoneidad. La Junta Central Electoral evaluará la legitimidad de la entidad solicitante, la finalidad invocada y la idoneidad jurídica, operativa y funcional de la solicitud, con el fin de verificar que sea compatible con la Ley núm. 4-23, el presente reglamento y las resoluciones dictadas por la Junta Central Electoral.

Párrafo I. La Junta Central Electoral podrá requerir documentos, aclaraciones o evidencias adicionales que respalden la legitimidad de la entidad solicitante, la finalidad del uso del servicio, la base legal, contractual, regulatoria o la relación con los titulares, la necesidad y proporcionalidad de la consulta, el volumen estimado de operaciones, la naturaleza de los datos tratados y las garantías de protección de datos aplicables.

Párrafo II. La evaluación de legitimidad, finalidad e idoneidad deberá realizarse dentro de un plazo de veinte (20) días hábiles contados a partir de la recepción completa de la solicitud. Cuando la Junta Central Electoral requiera información adicional, el plazo quedará suspendido hasta tanto la entidad solicitante complete la documentación o aclaraciones requeridas.

Párrafo III. La Junta Central Electoral podrá rechazar la solicitud cuando la entidad solicitante no acredite legitimidad suficiente, cuando la finalidad invocada sea genérica, indeterminada, desproporcionada, incompatible con la Ley núm. 4-23, con el presente reglamento o con las competencias de la Junta Central Electoral, o cuando el acceso solicitado pueda comprometer los derechos de los titulares, la seguridad del servicio, la integridad de los datos o las condiciones técnicas, operativas o contractuales aplicables.

Artículo 60. Evaluación técnica, operativa y de seguridad. Una vez verificada favorablemente la legitimidad de la entidad solicitante, la finalidad invocada y la idoneidad de la solicitud, la Junta Central Electoral realizará una evaluación de los requisitos técnicos, operativos y de seguridad necesarios para la activación del servicio.

Párrafo I. Esta evaluación podrá incluir la revisión de la infraestructura tecnológica, mecanismos de integración, arquitectura de conexión, medidas de seguridad, confidencialidad, trazabilidad, control de acceso, gestión de credenciales, gestión de incidentes, continuidad operativa, resguardo de registros, constancias o resultados de consulta, pruebas de seguridad, pruebas funcionales, documentación técnica, proveedores involucrados y adecuación a los estándares, especificaciones y condiciones requeridas por la Junta Central Electoral.

Párrafo II. La Junta Central Electoral podrá realizar visitas, inspecciones, pruebas técnicas, pruebas de seguridad, requerimientos de información, entrevistas técnicas o cualquier otro mecanismo razonable de verificación que permita comprobar el cumplimiento de los requisitos establecidos en la ley, el presente reglamento, las resoluciones aplicables y las condiciones técnicas del servicio.

Párrafo III. La evaluación técnica, operativa y de seguridad deberá realizarse dentro de un plazo de treinta (30) días hábiles contados a partir de la conclusión favorable de la evaluación de legitimidad, finalidad e idoneidad y de la recepción completa de la documentación técnica requerida. Dicho plazo podrá ser prorrogado por la Junta Central Electoral, de manera motivada, cuando la complejidad técnica, el volumen de integración, las pruebas requeridas, las condiciones de seguridad o la naturaleza del servicio solicitado así lo justifiquen.

Párrafo IV. La evaluación técnica, operativa y de seguridad no implicará autorización para que la entidad solicitante almacene datos biométricos administrados por la Junta Central Electoral, cree bases biométricas propias a partir del servicio, genere plantillas, vectores, patrones, códigos biométricos o mecanismos de vinculación derivados del servicio, ni preste servicios de consulta, verificación o certificación de identidad a terceros fuera de las condiciones autorizadas por la Junta Central Electoral.

Artículo 61. Decisión sobre la solicitud. Concluidas las evaluaciones correspondientes, la Junta Central Electoral decidirá sobre la aceptación o rechazo de la solicitud de acceso al servicio, atendiendo al cumplimiento de los requisitos legales, técnicos, operativos, de seguridad, finalidad, necesidad, proporcionalidad y protección de los derechos de los titulares.
Párrafo I. La aceptación de la solicitud habilitará la continuación del proceso de formalización contractual, pruebas, adecuación técnica y activación del servicio, conforme a las condiciones establecidas por la Junta Central Electoral.

Párrafo II. El rechazo de la solicitud deberá ser motivado y comunicado a la entidad solicitante, indicando, cuando corresponda, las razones legales, técnicas, operativas, de seguridad, finalidad, proporcionalidad o cumplimiento que lo justifican.

Párrafo III. La entidad solicitante podrá presentar una nueva solicitud cuando hayan sido subsanadas las causas que motivaron el rechazo, salvo que la decisión se fundamente en una incompatibilidad legal, imposibilidad técnica, riesgo no mitigable o finalidad incompatible con el marco aplicable.

Artículo 62. Acuerdo de provisión del servicio. Una vez aceptada la solicitud y completadas satisfactoriamente las evaluaciones correspondientes, se suscribirá el contrato, acuerdo o convenio entre la Junta Central Electoral y la entidad solicitante.

Párrafo. El contrato, acuerdo o convenio deberá establecer los términos y condiciones específicos del uso del servicio, incluyendo las responsabilidades de las partes, finalidad autorizada, condiciones técnicas de acceso, obligaciones de confidencialidad, protección de datos personales asociados a la identidad, seguridad de la información, trazabilidad, gestión de incidentes, auditoría, continuidad operativa, niveles de servicio, obligaciones financieras, causales de suspensión o terminación, régimen de consecuencias y demás condiciones aplicables.

Artículo 63. Pruebas, revisión y adecuación interna. La entidad solicitante contará con un período de pruebas, revisión interna y adecuación de sus sistemas, infraestructura, procesos, controles y mecanismos de integración antes de la activación completa del servicio.

Párrafo I. Durante este período, la entidad solicitante podrá realizar las calibraciones, configuraciones, pruebas, ajustes y adecuaciones necesarias para garantizar la correcta integración y funcionamiento del servicio con sus propios sistemas y procesos, conforme a las especificaciones establecidas por la Junta Central Electoral.

Párrafo II. La Junta Central Electoral podrá brindar orientación y soporte técnico durante el proceso de adecuación, sin que ello implique aprobación definitiva, certificación general de cumplimiento o asunción de responsabilidad sobre los sistemas internos, procesos, bases de datos, controles o componentes tecnológicos de la entidad solicitante.

Párrafo III. Los dispositivos, aplicaciones, interfaces, credenciales, certificados, componentes tecnológicos o mecanismos utilizados para acceder o interactuar con el servicio deberán cumplir con las especificaciones técnicas, de seguridad y trazabilidad requeridas por la Junta Central Electoral.

Párrafo IV. El período de pruebas y adecuación tendrá una duración de hasta treinta (30) días hábiles, prorrogables por causa justificada cuando la naturaleza de la integración, las pruebas de seguridad, el volumen de operaciones, la complejidad técnica o las adecuaciones requeridas así lo ameriten.

Artículo 64. Activación del servicio. Una vez completadas satisfactoriamente las etapas anteriores y suscrito el contrato, acuerdo o convenio correspondiente, la Junta Central Electoral activará el servicio para la entidad solicitante y proporcionará las credenciales, claves, certificados, perfiles de acceso o mecanismos de autenticación necesarios para su uso seguro, trazable y confiable.

Párrafo I. La activación del servicio deberá producirse dentro de un plazo de diez (10) días hábiles contados a partir de la suscripción del contrato, acuerdo o convenio correspondiente y de la conclusión satisfactoria de las pruebas técnicas y de seguridad, salvo que existan causas técnicas, operativas, de seguridad, documentales o contractuales que justifiquen su diferimiento.

Párrafo II. La activación del servicio quedará condicionada al cumplimiento permanente de las obligaciones establecidas en la Ley núm. 4-23, el presente reglamento, las resoluciones de la Junta Central Electoral y el contrato, acuerdo o convenio suscrito. La Junta Central Electoral podrá suspender, limitar o revocar el acceso al servicio cuando se verifique incumplimiento, riesgo para la seguridad, uso no autorizado, desviación de finalidad, incidente de seguridad, afectación a los derechos de los titulares o cualquier otra causa prevista en el marco aplicable.

Artículo 65. Registro institucional de entidades autorizadas. La Junta Central Electoral mantendrá un registro institucional de las entidades públicas y privadas autorizadas para acceder o utilizar el Servicio de Consulta, Verificación y Certificación de Identidad, así como de los tratamientos que requieran autorización previa conforme al presente reglamento.

Párrafo I. La Junta Central Electoral podrá publicar en su portal institucional información general sobre las entidades autorizadas, incluyendo nombre o razón social, tipo de entidad, condición de autorización, finalidad general autorizada, modalidad del servicio, fecha de autorización, estado de vigencia y cualquier otra información que resulte pertinente para fines de transparencia y control social.

Párrafo II. La información publicada no incluirá datos biométricos, datos personales asociados a la identidad, credenciales, especificaciones técnicas sensibles, volúmenes detallados de consulta, configuraciones, información reservada, secretos protegidos, datos de seguridad o cualquier información cuya divulgación pueda comprometer la confidencialidad, seguridad, continuidad o integridad del servicio.

Párrafo III. La Junta Central Electoral podrá establecer mediante resolución, instructivo o norma técnica el contenido, formato, actualización, alcance y excepciones aplicables al registro institucional.

SECCIÓN III

DE LAS OBLIGACIONES DE LAS ENTIDADES USUARIAS DEL SERVICIO DE CONSULTA, VERIFICACIÓN Y CERTIFICACIÓN DE IDENTIDAD

Artículo 66. Obligaciones de las entidades usuarias. Las entidades usuarias del Servicio de Consulta, Verificación y Certificación de Identidad deberán cumplir, durante toda la vigencia de su autorización, contrato, convenio o acuerdo, con las obligaciones siguientes:

a) **Uso limitado a la finalidad autorizada.** Utilizar el servicio exclusivamente para la finalidad específica autorizada por la Junta Central Electoral, conforme a la base legal, contractual, regulatoria o consentimiento aplicable, y dentro de los límites técnicos, operativos y contractuales establecidos.

b) **Protección de la información vinculada al servicio.** Garantizar la protección, confidencialidad, integridad, disponibilidad y trazabilidad de los registros, constancias, resultados de consulta,

credenciales, certificados, claves, interfaces, mecanismos de integración y demás información o componentes vinculados al servicio.

c) **Uso adecuado de dispositivos, sistemas e interfaces.** Utilizar los dispositivos, aplicaciones, interfaces, credenciales, certificados, sistemas y mecanismos de conexión de manera correcta, segura y conforme a las especificaciones, políticas, protocolos, manuales, recomendaciones o instrucciones emitidas por la Junta Central Electoral.

d) **Prohibición de uso no autorizado.** Abstenerse de utilizar, reutilizar, interconectar, explotar, ceder, comunicar o tratar ulteriormente los datos biométricos, datos personales asociados a la identidad, resultados, constancias, registros o evidencias derivados del uso del servicio para finalidades distintas a las autorizadas, para prestar servicios de consulta, verificación o certificación de identidad a terceros, o para desarrollar sistemas, mecanismos o capacidades que, por su objeto o efecto, sustituyan, repliquen, desplacen o funcionen como alternativa al Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral.

e) **Confidencialidad y no divulgación.** Mantener estricta confidencialidad respecto de la información, documentación, especificaciones técnicas, credenciales, resultados, constancias, registros, trazas, mecanismos de integración y demás elementos a los que tenga acceso en virtud del servicio, salvo autorización expresa de la Junta Central Electoral, habilitación legal, requerimiento de autoridad competente u obligación derivada del marco aplicable.

f) **Gestión de accesos.** Limitar el acceso al servicio al personal, perfiles, sistemas o componentes expresamente autorizados, aplicando controles de autenticación, segregación de funciones, mínimo privilegio, trazabilidad, revocación oportuna de accesos y demás medidas requeridas por la Junta Central Electoral.

g) **Notificación de incidentes.** Notificar a la Junta Central Electoral cualquier incidente de seguridad relacionado con el servicio, sus credenciales, interfaces, sistemas de integración, registros, constancias, resultados de consulta, datos personales asociados a la identidad o cualquier componente tecnológico vinculado, conforme a los plazos, contenido mínimo, excepciones, deberes de registro y demás condiciones previstas en el presente reglamento.

h) **Cumplimiento normativo.** Cumplir con la Ley núm. 4-23, el presente reglamento, la normativa de protección de datos personales, las resoluciones dictadas por la Junta Central Electoral, las políticas de seguridad aplicables, el contrato, convenio o acuerdo suscrito y cualquier otra disposición vinculante relacionada con el uso del servicio.

i) **Cumplimiento contractual y obligaciones económicas.** Cumplir íntegramente con las obligaciones establecidas en el contrato, convenio, acuerdo, resolución, tarifario, acto administrativo o instrumento aplicable al uso del servicio, incluyendo las condiciones técnicas, operativas, de seguridad, confidencialidad, auditoría, niveles de servicio, reportes, vigencia, renovación, suspensión, terminación, así como el pago oportuno de las tasas, cargos, tarifas o contraprestaciones que correspondan conforme al régimen aprobado por la Junta Central Electoral.

j) **Colaboración con auditorías y verificaciones.** Colaborar con la Junta Central Electoral en auditorías, revisiones, verificaciones, inspecciones o requerimientos relacionados con el uso del servicio, proporcionando la información, registros, evidencias, trazas de acceso, reportes de seguridad, documentación técnica y demás elementos requeridos, conforme al debido proceso, la confidencialidad de la información y los principios de necesidad, proporcionalidad y razonabilidad.

k) **Actualización de información.** Mantener actualizada ante la Junta Central Electoral la información relativa a representantes autorizados, puntos de contacto, responsables técnicos, responsables de protección de datos o cumplimiento, sistemas integrados, finalidad autorizada, volumen estimado de consultas, cambios relevantes de infraestructura, incidentes, proveedores críticos y cualquier otra información necesaria para la adecuada supervisión del servicio.

l) **Gestión de proveedores y terceros.** Garantizar que cualquier proveedor, subcontratista o tercero que participe en la integración, operación, soporte, mantenimiento o seguridad de los sistemas vinculados al servicio cumpla con las obligaciones de confidencialidad, seguridad, trazabilidad, protección de datos, limitación de finalidad y demás condiciones establecidas por la Junta Central Electoral, sin que dicha participación exima a la entidad usuaria de su responsabilidad.

m) **Conservación de datos recolectados directamente y resultados del servicio.** Conservar los datos biométricos o datos personales asociados a la identidad que la entidad usuaria haya recolectado directamente del titular, así como los registros, constancias, resultados de consulta, evidencias transaccionales o soportes operativos derivados del uso del servicio, conforme a la base legal, consentimiento, autorización, finalidad específica, plazo de conservación y condiciones de seguridad aplicables. La conservación de dichos datos, resultados o evidencias deberá limitarse a la finalidad que la justifica y no podrá utilizarse para prestar servicios de consulta, verificación o certificación de identidad a terceros, ni para desarrollar sistemas, mecanismos o capacidades que, por su objeto o efecto, sustituyan, repliquen, desplacen o funcionen como alternativa al servicio provisto por la Junta Central Electoral.

Párrafo I. La recolección y conservación de datos biométricos o datos personales asociados a la identidad por parte de las entidades usuarias, directamente del titular, no constituirá por sí sola una infracción al presente reglamento, siempre que se encuentre amparada en una base válida, se limite a la finalidad específica informada o autorizada, respete el plazo de conservación aplicable y no tenga por objeto o efecto sustituir, replicar, desplazar o funcionar como alternativa al Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral.

Párrafo II. Cuando se trate de entidades sujetas a regulación o supervisión sectorial, la Junta Central Electoral podrá coordinar con el órgano regulador o supervisor competente las auditorías, verificaciones, requerimientos o medidas que resulten necesarias o convenientes. Dicha coordinación no constituirá condición previa, requisito de validez ni vía exclusiva para el ejercicio de las atribuciones de la Junta Central Electoral respecto del servicio.

Párrafo III. El incumplimiento de las obligaciones previstas en este artículo podrá dar lugar a la suspensión, limitación, revocación o terminación del acceso al servicio, sin perjuicio de las demás consecuencias legales, contractuales, administrativas o regulatorias que correspondan.

SECCIÓN IV

DE LAS MEDIDAS DE SEGURIDAD APLICABLES A LAS ENTIDADES USUARIAS DEL SERVICIO

Artículo 67. Medidas de seguridad. Las entidades usuarias del Servicio de Consulta, Verificación y Certificación de Identidad deberán implementar y mantener medidas técnicas, organizativas, administrativas, físicas y lógicas adecuadas para proteger los datos biométricos y datos personales asociados a la identidad que recolecten directamente de los titulares, así como los registros, constancias, resultados de consulta, credenciales, certificados, interfaces, trazas, componentes tecnológicos y demás información vinculada al uso del servicio. Las medidas de seguridad deberán ser proporcionales a la naturaleza del servicio, la finalidad autorizada, el volumen de consultas, el tipo de datos tratados, los riesgos identificados, la modalidad de integración, los sistemas involucrados y las condiciones establecidas por la Junta Central Electoral. Las entidades usuarias deberán implementar, como mínimo, las medidas siguientes:

a) **Privacidad y seguridad desde el diseño.** Incorporar medidas de protección de datos personales, seguridad de la información, minimización, limitación de finalidad, trazabilidad y control de acceso desde la etapa de diseño, desarrollo, adquisición, configuración o integración de cualquier sistema, aplicación, dispositivo, interfaz o proceso vinculado al servicio.

b) **Cifrado y protección de la información.** Proteger los datos, resultados, constancias, credenciales, trazas, registros y comunicaciones vinculadas al servicio mediante mecanismos de cifrado, protección en tránsito y en reposo, controles criptográficos, canales seguros y demás medidas proporcionales al nivel de riesgo.

c) **Segregación y control de datos.** Mantener separados, cuando corresponda, los datos biométricos, datos personales asociados a la identidad, resultados del servicio, credenciales, registros técnicos y demás componentes sensibles, utilizando identificadores seguros, controles de acceso y mecanismos que reduzcan el riesgo de asociación indebida, reutilización no autorizada o tratamiento incompatible.

d) **Gestión de accesos y privilegios.** Establecer controles de acceso basados en roles, perfiles autorizados, autenticación robusta, mínimo privilegio, segregación de funciones, revisión periódica de permisos, revocación oportuna de accesos y trazabilidad de las operaciones realizadas.

e) **Registro, monitoreo y trazabilidad.** Mantener registros íntegros, seguros y auditables de las operaciones vinculadas al servicio, incluyendo accesos, consultas, respuestas, errores, incidentes, modificaciones, fallos de integración, uso de credenciales y demás eventos relevantes para la seguridad y supervisión del servicio.

f) **Seguridad de sistemas, aplicaciones y redes.** Proteger los sistemas, aplicaciones, redes, interfaces, dispositivos y componentes tecnológicos vinculados al servicio mediante prácticas seguras de desarrollo, gestión de vulnerabilidades, actualización de software, gestión de parches, protección perimetral, monitoreo, detección de intrusiones y controles contra accesos no autorizados.

g) **Seguridad física y protección de dispositivos.** Adoptar medidas de seguridad física para proteger los equipos, servidores, dispositivos de captura, estaciones de trabajo, medios de almacenamiento, centros de datos, áreas restringidas y demás componentes utilizados para acceder, operar o integrarse con el servicio.

h) **Gestión de proveedores y terceros.** Evaluar, controlar y supervisar a los proveedores, subcontratistas o terceros que participen en la integración, operación, soporte, mantenimiento, almacenamiento, seguridad o procesamiento de información vinculada al servicio, garantizando que cumplan las obligaciones de confidencialidad, protección de datos, seguridad, trazabilidad y limitación de finalidad.

i) **Respaldo, continuidad y recuperación.** Implementar mecanismos de respaldo, continuidad operativa, recuperación ante desastres, disponibilidad del servicio interno, gestión de contingencias y restauración segura de los sistemas vinculados al servicio, sin que dichos mecanismos impliquen conservación no autorizada de datos biométricos, creación de bases paralelas o tratamiento biométrico autónomo.

j) **Evaluación de riesgos y pruebas de seguridad.** Realizar evaluaciones periódicas de riesgos, revisiones de seguridad, pruebas de vulnerabilidad, pruebas de penetración o mecanismos equivalentes, conforme a la naturaleza de la integración, el nivel de riesgo, el volumen de operaciones y las condiciones establecidas por la Junta Central Electoral.

k) **Formación y concienciación.** Capacitar al personal autorizado, usuarios internos, administradores, operadores técnicos y terceros vinculados sobre el uso correcto del servicio, protección de datos personales, confidencialidad, seguridad de la información, gestión de incidentes, obligaciones contractuales y consecuencias del uso indebido.

l) **Políticas y procedimientos internos.** Adoptar políticas, procedimientos, manuales, controles internos y registros documentales que permitan demostrar el cumplimiento de las obligaciones de

seguridad, protección de datos, trazabilidad, confidencialidad, gestión de accesos, gestión de incidentes, auditoría y continuidad operativa.

Párrafo I. Las medidas previstas en este artículo constituyen condiciones mínimas. La Junta Central Electoral podrá establecer requisitos adicionales mediante resolución, norma técnica, instructivo, contrato, convenio, acuerdo, anexo de seguridad o cualquier otro instrumento aplicable, atendiendo al nivel de riesgo, modalidad de integración, volumen de consultas, sensibilidad de los datos, criticidad del servicio o evolución tecnológica.

Párrafo II. La implementación de medidas de respaldo, continuidad, recuperación, monitoreo o seguridad no habilitará a las entidades usuarias a conservar datos biométricos administrados por la Junta Central Electoral, generar plantillas, vectores, patrones, códigos biométricos o mecanismos de vinculación derivados del servicio, ni realizar tratamiento biométrico autónomo fuera de las condiciones autorizadas.

Párrafo III. Las entidades usuarias deberán mantener evidencia documental, técnica y operativa suficiente para demostrar el cumplimiento de las medidas de seguridad previstas en este artículo, y ponerla a disposición de la Junta Central Electoral cuando esta lo requiera, conforme al debido proceso, la confidencialidad de la información y los principios de necesidad, proporcionalidad y razonabilidad.

SECCIÓN V

DE LAS EVALUACIONES DE IMPACTO

Artículo 68. Evaluación de impacto para el tratamiento de datos biométricos vinculado al servicio. Antes de implementar, modificar sustancialmente o poner en operación sistemas, plataformas, aplicaciones, dispositivos, procesos o mecanismos que impliquen tratamiento de datos biométricos o datos personales asociados a la identidad para el uso del Servicio de Consulta, Verificación y Certificación de Identidad, la entidad usuaria deberá realizar una evaluación de impacto.

Párrafo I. La evaluación de impacto tendrá por objeto identificar, analizar, documentar y mitigar los riesgos que el tratamiento pueda generar para la privacidad, seguridad, integridad, confidencialidad, trazabilidad y derechos de los titulares, así como para la correcta utilización del servicio provisto por la Junta Central Electoral.

Párrafo II. La evaluación de impacto deberá realizarse antes de la activación del servicio, cuando la Junta Central Electoral lo requiera como condición de acceso, y cada vez que se produzcan cambios sustanciales en la finalidad, alcance, tecnología, modalidad de captura, almacenamiento, interconexión, proveedores, flujos de datos, volumen de operaciones, medidas de seguridad o nivel de riesgo del tratamiento.

Párrafo III. La realización de la evaluación de impacto no exime a la entidad usuaria del cumplimiento de las demás obligaciones establecidas en la ley, el presente reglamento, las resoluciones de la Junta Central Electoral, el contrato, convenio o acuerdo correspondiente, ni de las condiciones técnicas y de seguridad aplicables al servicio.

Artículo 69. Contenido mínimo de la evaluación de impacto. La evaluación de impacto deberá contener, como mínimo, los elementos siguientes:

a) **Descripción del tratamiento.** Identificación de los sistemas, plataformas, aplicaciones, dispositivos, procesos, responsables, encargados, proveedores y componentes tecnológicos involucrados en el tratamiento.

b) **Datos tratados.** Identificación de los datos biométricos, datos personales asociados a la identidad, resultados, constancias, registros, evidencias transaccionales o demás información vinculada al servicio que serán tratados, así como su origen, naturaleza, formato y modalidad de captura o conservación.

c) **Finalidad y base habilitante.** Descripción de la finalidad específica del tratamiento, la base legal, contractual, regulatoria, autorización o condición habilitante aplicable, y la relación de necesidad y proporcionalidad entre los datos tratados y la finalidad perseguida.

d) **Procesos y flujos de datos.** Análisis de los flujos de datos durante las etapas de captura, consulta, verificación, respuesta, almacenamiento, acceso, transmisión, conservación, supresión o eliminación, incluyendo cesiones, comunicaciones, interconexiones o intervención de terceros cuando corresponda.

e) **Riesgos para los titulares y para el servicio.** Identificación y valoración de los riesgos para la privacidad, protección de datos personales, derechos de los titulares, confidencialidad, integridad, disponibilidad, trazabilidad, uso indebido del servicio, acceso no autorizado, desviación de finalidad, divulgación indebida, pérdida, alteración, reutilización o tratamiento no autorizado.

f) **Medidas de mitigación.** Identificación de las medidas técnicas, organizativas, administrativas, contractuales, físicas y lógicas destinadas a prevenir, reducir, transferir, controlar o mitigar los riesgos identificados, incluyendo controles de acceso, cifrado, segregación, monitoreo, registro de operaciones, seudonimización, retención limitada, gestión de incidentes, capacitación y auditoría.

g) **Evaluación de necesidad y proporcionalidad.** Análisis de la necesidad del tratamiento biométrico, la proporcionalidad de los datos tratados, la existencia de medios menos intrusivos, los plazos de conservación, los límites de uso y las salvaguardas aplicables.

h) **Impacto en derechos y garantías.** Evaluación de los efectos que el tratamiento pueda generar sobre los derechos y libertades de los titulares, incluyendo privacidad, protección de datos personales, no discriminación, acceso a servicios, debido proceso, transparencia, seguridad y ejercicio de derechos.

i) **Participación de áreas competentes.** Identificación de las áreas internas o partes interesadas consultadas, tales como protección de datos, seguridad de la información, cumplimiento, legal, tecnología, operaciones, auditoría, gestión de riesgos, regulador sectorial cuando corresponda, o expertos en protección de datos, seguridad de la información y biometría.

j) **Conclusiones, plan de acción y seguimiento.** Documentación de los resultados, riesgos residuales, medidas adoptadas, responsables de implementación, plazos, recomendaciones, controles de seguimiento y mecanismos de revisión periódica.

Artículo 70. Frecuencia, actualización y remisión de la evaluación de impacto. Las entidades usuarias deberán actualizar la evaluación de impacto, como mínimo, cada dos (2) años, y antes de implementar modificaciones sustanciales que puedan alterar la finalidad, alcance, tecnología, volumen, modalidad, seguridad, flujos de datos o nivel de riesgo del tratamiento.
Párrafo I. Cuando la evaluación de impacto sea requerida como condición de acceso, continuidad, modificación o ampliación del servicio, sus resultados deberán ser remitidos a la Junta Central Electoral dentro del plazo que esta establezca o, en su defecto, dentro de los treinta (30) días calendario siguientes a su conclusión.

Párrafo II. Cuando la entidad usuaria pretenda implementar modificaciones sustanciales en sistemas, plataformas, aplicaciones, procesos o tecnologías vinculadas al servicio, deberá remitir a la Junta Central Electoral la evaluación de impacto actualizada con una antelación mínima de treinta (30) días calendario a la fecha prevista para su puesta en operación, salvo casos justificados de urgencia, contingencia o seguridad, debidamente documentados.

Párrafo III. La remisión de la evaluación de impacto a la Junta Central Electoral tendrá por finalidad permitir la supervisión, formulación de recomendaciones, requerimiento de medidas de mitigación, actualización de condiciones técnicas o evaluación de continuidad del servicio, sin trasladar a la Junta Central Electoral la responsabilidad que corresponde a la entidad usuaria por el tratamiento que realiza.

Artículo 71. Riesgos significativos o de alto impacto. Cuando la evaluación de impacto identifique riesgos significativos, altos o no mitigados que puedan comprometer la privacidad, seguridad, integridad, confidencialidad, disponibilidad, trazabilidad, derechos de los titulares o correcto uso del servicio, la entidad usuaria deberá informarlo a la Junta Central Electoral dentro de un plazo no mayor de setenta y dos (72) horas contadas a partir de su identificación.

Párrafo I. La comunicación deberá incluir, como mínimo, la descripción del riesgo identificado, sistemas o procesos afectados, datos involucrados, titulares potencialmente impactados, probabilidad y severidad estimada, medidas adoptadas o propuestas, riesgos residuales, responsables de mitigación y cualquier otra información necesaria para que la Junta Central Electoral evalúe las medidas correspondientes dentro del ámbito de sus competencias.

Párrafo II. La Junta Central Electoral podrá requerir aclaraciones, documentación complementaria, medidas adicionales de protección, suspensión temporal de funcionalidades, limitación de consultas, actualización de controles, auditoría extraordinaria o cualquier otra medida proporcional al nivel de riesgo identificado.

Artículo 72. Lineamientos para las evaluaciones de impacto. La Junta Central Electoral podrá establecer, mediante resolución, norma técnica, instructivo, guía, formato, anexo contractual o cualquier otro instrumento aplicable, los lineamientos, criterios, metodología, contenido mínimo, formatos de reporte, indicadores, plazos y condiciones para la realización, actualización y remisión de las evaluaciones de impacto.

Párrafo. Los lineamientos que emita la Junta Central Electoral deberán atender a la naturaleza del tratamiento, el nivel de riesgo, la finalidad autorizada, la modalidad de integración, el volumen de consultas, los datos tratados, la sensibilidad de la información, la tecnología utilizada y las condiciones específicas del servicio.

SECCIÓN VI

DE LA ACTUALIZACIÓN, EL MONITOREO Y LA EVALUACIÓN CONTINUA

Artículo 73. Monitoreo operativo continuo del servicio. La Junta Central Electoral podrá realizar el monitoreo operativo continuo del Servicio de Consulta, Verificación y Certificación de Identidad, con el propósito de verificar su correcto funcionamiento, disponibilidad, seguridad, trazabilidad, calidad, uso autorizado, cumplimiento normativo y adecuación a las condiciones técnicas, operativas y contractuales aplicables.

Párrafo I. El monitoreo operativo continuo podrá comprender, según corresponda, la revisión de indicadores de disponibilidad, desempeño, volumen de consultas, tiempos de respuesta, incidentes, errores, eventos de seguridad, trazas de acceso, uso de credenciales, cumplimiento de finalidades autorizadas, niveles de servicio, reportes de auditoría, medidas correctivas y demás elementos vinculados al servicio.

Párrafo II. La Junta Central Electoral podrá requerir a las entidades usuarias información, registros, evidencias, reportes, indicadores, documentación técnica o aclaraciones necesarias para verificar el uso adecuado del servicio, conforme al debido proceso, la confidencialidad de la información y los principios de necesidad, proporcionalidad y razonabilidad.

Artículo 74. Actualización y mantenimiento de sistemas vinculados al servicio. Las entidades usuarias deberán mantener actualizados, seguros y operativos los sistemas, aplicaciones, dispositivos, interfaces, credenciales, certificados, controles, procesos y demás componentes tecnológicos vinculados al uso del Servicio de Consulta, Verificación y Certificación de Identidad, conforme a las especificaciones técnicas, políticas, protocolos, instrucciones, condiciones contractuales y requerimientos establecidos por la Junta Central Electoral.

Párrafo I. Las entidades usuarias deberán informar oportunamente a la Junta Central Electoral sobre cambios relevantes en su infraestructura, sistemas, proveedores, mecanismos de integración, procesos de

captura, medidas de seguridad, condiciones de operación, volumen de consultas o cualquier otro elemento que pueda afectar la seguridad, disponibilidad, trazabilidad, finalidad autorizada o correcto funcionamiento del servicio.

Párrafo II. La Junta Central Electoral podrá requerir ajustes, actualizaciones, medidas correctivas, pruebas adicionales, revisión de configuraciones, sustitución de credenciales, fortalecimiento de controles o adecuaciones técnicas cuando identifique riesgos, vulnerabilidades, fallos de integración, incumplimientos, cambios tecnológicos o condiciones que puedan afectar el servicio.

Párrafo III. La asistencia técnica, orientación o soporte que la Junta Central Electoral brinde a las entidades usuarias no implicará aprobación general de sus sistemas internos, certificación integral de cumplimiento ni asunción de responsabilidad por los tratamientos de datos biométricos o datos personales asociados a la identidad que dichas entidades realicen bajo su propia responsabilidad.

Artículo 75. Evaluaciones periódicas del servicio. La Junta Central Electoral podrá realizar evaluaciones formales periódicas del Servicio de Consulta, Verificación y Certificación de Identidad, separadas del monitoreo operativo continuo, con el propósito de mejorar sus procesos, fortalecer la seguridad, verificar el cumplimiento de las condiciones autorizadas, identificar riesgos, actualizar controles y asegurar la calidad del servicio.

Párrafo I. Las entidades usuarias deberán colaborar con dichas evaluaciones proporcionando la información, registros, evidencias, indicadores, reportes, trazas, documentación técnica o datos que resulten necesarios y proporcionales para evaluar el funcionamiento, seguridad, uso autorizado, desempeño y cumplimiento del servicio.

Párrafo II. Cuando la información requerida se encuentre sujeta a confidencialidad, secreto profesional, secreto bancario, reserva legal o regulación sectorial, la entidad usuaria deberá informarlo de manera motivada y proponer mecanismos de entrega compatibles con dichas obligaciones, tales como información agregada, anonimizada, disociada, seudonimizada, limitada o bajo condiciones de reserva.

Párrafo III. La invocación de confidencialidad, secreto profesional, secreto bancario, reserva legal, regulación sectorial o deber contractual de reserva no podrá ser utilizada para impedir injustificadamente el monitoreo, evaluación o supervisión del servicio por parte de la Junta Central Electoral, sin perjuicio de la adopción de medidas razonables para proteger la información sensible, reservada o confidencial.

SECCIÓN VII

DE LA SUSPENSIÓN, LIMITACIÓN, CANCELACIÓN, TERMINACIÓN, CIERRE Y REANUDACIÓN DEL SERVICIO

Artículo 76. Causas de suspensión, limitación, cancelación o terminación del servicio. La Junta Central Electoral podrá suspender, limitar, cancelar o dar por terminado el acceso al Servicio de Consulta, Verificación y Certificación de Identidad provisto a una entidad usuaria, cuando se configure cualquiera de las causas siguientes:

a) Incumplimiento de las obligaciones establecidas en la ley, el presente reglamento, las resoluciones de la Junta Central Electoral, el contrato, convenio, acuerdo, autorización o instrumento aplicable al servicio.

b) Incumplimiento de los requisitos técnicos, operativos, de seguridad, confidencialidad, trazabilidad, auditoría, protección de datos o continuidad establecidos para el uso del servicio.

c) Uso indebido, fraudulento, no autorizado, desproporcionado o incompatible con la finalidad autorizada del servicio.

d) Desviación de finalidad, reutilización no autorizada, cesión, comunicación, interconexión, explotación o tratamiento ulterior de datos biométricos, datos personales asociados a la identidad,

resultados, constancias, registros o evidencias derivados del uso del servicio, fuera de las condiciones autorizadas.

e) Prestación, desarrollo, operación, explotación o puesta a disposición de terceros de servicios, sistemas, mecanismos o capacidades de consulta, verificación o certificación de identidad que, por su objeto o efecto, sustituyan, repliquen, desplacen o funcionen como alternativa al servicio provisto por la Junta Central Electoral.

f) Creación, conservación, alimentación, actualización, interconexión, explotación o uso de bases de datos biométricos, bases de datos personales asociados a la identidad, copias no autorizadas, plantillas, vectores, patrones, códigos biométricos, minucias, sistemas, plataformas o mecanismos de vinculación derivados del servicio o de datos administrados por la Junta Central Electoral, que por su objeto o efecto sustituyan, repliquen, desplacen o funcionen como infraestructura paralela o sustitutiva del Servicio de Consulta, Verificación y Certificación de Identidad.

g) Incidente de seguridad, acceso no autorizado, divulgación indebida, pérdida de control de credenciales, afectación a la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad del servicio, o cualquier otro evento que genere riesgo significativo para los datos, titulares o sistemas vinculados.

h) Falta de pago, mora o incumplimiento de las tasas, cargos, tarifas, contraprestaciones u obligaciones económicas aplicables al uso del servicio, conforme al contrato, convenio, acuerdo, resolución, tarifario o instrumento correspondiente.

i) Pérdida de capacidad jurídica, autorización legal, habilitación regulatoria, condición operativa, legitimidad institucional o condición necesaria para utilizar el servicio.

j) Negativa injustificada a colaborar con auditorías, revisiones, verificaciones, inspecciones, requerimientos de información o evaluaciones realizadas por la Junta Central Electoral conforme al marco aplicable.

k) Orden, requerimiento o disposición de autoridad competente que requiera la suspensión, limitación, cancelación o terminación del servicio por razones legales, de seguridad, interés público, investigación, protección de derechos o cumplimiento normativo.

l) Cualquier otra causa prevista en la ley, el presente reglamento olas resoluciones dictadas por la Junta Central Electoral.

Párrafo I. La medida adoptada por la Junta Central Electoral deberá ser proporcional a la gravedad del incumplimiento, riesgo identificado, afectación producida, reincidencia, urgencia, posibilidad de mitigación y demás circunstancias del caso.

Párrafo II. Cuando la naturaleza del riesgo lo permita, la Junta Central Electoral podrá requerir medidas correctivas, planes de remediación, ajustes técnicos, restricciones operativas, reducción de funcionalidades, sustitución de credenciales, auditorías extraordinarias o cualquier otra medida previa o concurrente a la suspensión, limitación, cancelación o terminación del servicio.

Párrafo III. Cuando exista riesgo grave, inminente o no mitigado para la seguridad del servicio, la integridad de los datos, los derechos de los titulares o las competencias de la Junta Central Electoral, esta podrá adoptar medidas inmediatas de suspensión, limitación o bloqueo preventivo, sin perjuicio de la posterior notificación y del procedimiento que corresponda. La notificación posterior deberá producirse dentro de un plazo no mayor de setenta y dos (72) horas contadas a partir de la adopción de la medida, y dará inicio al procedimiento contradictorio previsto en el artículo 94 del presente reglamento

Párrafo IV. Para la calificación de los conceptos de riesgo grave, inminente o no mitigado, desviación de finalidad y uso desproporcionado prescritos en este artículo, la Junta Central Electoral deberá considerar como criterios, la probabilidad de materialización del riesgo, la magnitud del impacto sobre los titulares

o el servicio, la reincidencia de la entidad usuaria y la existencia de medidas de mitigación disponibles, dejando constancia motivada de dicha valoración en el acto.

Artículo 77. Notificación y efectos de la suspensión, limitación, cancelación o terminación. La Junta Central Electoral notificará por escrito a la entidad usuaria la suspensión, limitación, cancelación o terminación del servicio, indicando las causas, alcance, efectos, plazo de cumplimiento, medidas requeridas y, cuando corresponda, las condiciones para su corrección o reanudación.

Párrafo I. La entidad usuaria deberá cesar el uso del servicio en los términos indicados por la Junta Central Electoral, adoptar las medidas necesarias para proteger la información vinculada al servicio, preservar los registros y evidencias requeridos, desactivar accesos internos cuando corresponda y cumplir las instrucciones técnicas, operativas o de seguridad aplicables.

Párrafo II. La suspensión, limitación, cancelación o terminación del servicio no exime a la entidad usuaria del cumplimiento de las obligaciones de confidencialidad, seguridad, protección de datos, trazabilidad, cooperación, auditoría, responsabilidad, pago de obligaciones pendientes, conservación legítima de evidencias o eliminación segura que subsistan conforme a la ley, el presente reglamento, las resoluciones aplicables o el contrato, convenio o acuerdo correspondiente.

Artículo 78. Terminación, cierre y verificación posterior del servicio. En caso de terminación, vencimiento, resolución, cancelación o finalización del contrato, convenio, acuerdo o autorización de acceso al Servicio de Consulta, Verificación y Certificación de Identidad, la Junta Central Electoral podrá realizar auditorías, revisiones, verificaciones o requerimientos posteriores, conforme a la Ley núm. 4-23, el presente reglamento, las resoluciones aplicables y las condiciones contractuales correspondientes.
Estas actuaciones tendrán por objeto verificar el cese efectivo del acceso al servicio, la desactivación de credenciales, certificados, claves, perfiles de acceso, interfaces o mecanismos de integración, así como el cumplimiento de las obligaciones asumidas por la entidad usuaria durante y después de la terminación del servicio.

Párrafo I. Las auditorías, revisiones, verificaciones o requerimientos posteriores podrán comprender la revisión de registros, constancias, resultados de consulta, evidencias transaccionales, trazas de acceso, documentación técnica, configuraciones, mecanismos de integración, gestión de credenciales, registros de incidentes, controles de seguridad y demás elementos vinculados al uso del servicio.

Párrafo II. La entidad usuaria deberá acreditar, cuando corresponda, que no conserva datos biométricos administrados por la Junta Central Electoral, copias no autorizadas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación derivados del servicio, ni sistemas o capacidades que permitan realizar tratamiento biométrico autónomo fuera de las condiciones autorizadas.

Párrafo III. La terminación, vencimiento, resolución, cancelación o finalización del servicio no exime a la entidad usuaria del cumplimiento de las obligaciones de confidencialidad, seguridad, trazabilidad, protección de datos, conservación legítima de evidencias, eliminación segura, cooperación, auditoría y responsabilidad que subsistan conforme a la ley, el presente reglamento, las resoluciones aplicables o el contrato, convenio o acuerdo correspondiente.

Párrafo IV. Cuando se trate de entidades sujetas a regulación o supervisión sectorial, la Junta Central Electoral podrá coordinar con el órgano regulador o supervisor competente la realización de auditorías, revisiones, verificaciones o requerimientos posteriores, cuando resulte necesario o conveniente. Dicha coordinación no constituirá condición previa, requisito de validez ni vía exclusiva para el ejercicio de las atribuciones de la Junta Central Electoral respecto del servicio.

Artículo 79. Reanudación del servicio. La reanudación del servicio estará sujeta a la corrección efectiva de las causas que dieron lugar a la suspensión o limitación, al cumplimiento de las medidas requeridas por la Junta Central Electoral, a la verificación de las condiciones técnicas, operativas, contractuales, económicas y de seguridad aplicables, y a la decisión favorable de la Junta Central Electoral.

Párrafo I. La Junta Central Electoral podrá requerir, antes de la reanudación, evidencias documentales, pruebas técnicas, auditorías, certificaciones, actualización de evaluaciones de impacto, sustitución de credenciales, medidas correctivas, planes de remediación, garantías adicionales o cualquier otra condición proporcional al riesgo identificado.

Párrafo II. La reanudación del servicio no impedirá la aplicación de medidas correctivas, consecuencias contractuales, acciones legales, auditorías posteriores o responsabilidades que correspondan por los hechos que motivaron la suspensión o limitación.

Artículo 80. Acciones, medidas correctivas y consecuencias. La Junta Central Electoral podrá ejercer las acciones legales, contractuales, administrativas o judiciales que correspondan frente a incumplimientos, usos indebidos, daños, perjuicios, riesgos, incidentes o conductas contrarias a la ley, el presente reglamento, las resoluciones aplicables o las condiciones del servicio.

Párrafo I. La Junta Central Electoral podrá requerir medidas correctivas, planes de remediación, auditorías extraordinarias, restricciones de uso, fortalecimiento de controles, sustitución de credenciales, eliminación segura, bloqueo de funcionalidades, limitación de consultas o cualquier otra medida necesaria y proporcional para restablecer el cumplimiento, mitigar riesgos o proteger el servicio.
Párrafo II. Las medidas previstas en este artículo se aplicarán sin perjuicio de las sanciones, penalidades, indemnizaciones, responsabilidades civiles, administrativas, contractuales, penales o regulatorias que correspondan conforme a la normativa aplicable.

Artículo 81. Tasas, cargos y obligaciones económicas del servicio. El Pleno de la Junta Central Electoral, conforme a sus competencias legales y administrativas, establecerá las tasas, cargos, tarifas o contraprestaciones aplicables por la prestación del Servicio de Consulta, Verificación y Certificación de Identidad, tomando en cuenta los costos, gastos, sostenibilidad, operación, mantenimiento, seguridad, disponibilidad, mejora continua y demás elementos vinculados a la prestación del servicio.

Párrafo I. Las tasas, cargos, tarifas o contraprestaciones aplicables podrán ser establecidas, actualizadas o modificadas mediante resolución, tarifario, contrato, convenio, acuerdo, acto administrativo o instrumento correspondiente, conforme al régimen aprobado por la Junta Central Electoral.

Párrafo II. Las entidades usuarias deberán cumplir oportunamente con las obligaciones económicas que correspondan por el uso del servicio. La falta de pago, mora o incumplimiento de dichas obligaciones podrá dar lugar a la suspensión, limitación, cancelación o terminación del servicio, conforme al presente reglamento y al instrumento aplicable.

Artículo 82. Supervisión y control. La Junta Central Electoral podrá llevar a cabo medidas de supervisión y control para verificar el cumplimiento de la ley, el presente reglamento, las resoluciones aplicables, las condiciones del servicio, la protección de los datos biométricos y datos personales asociados a la identidad, la seguridad, trazabilidad, finalidad autorizada y uso adecuado del servicio.

Párrafo. Las medidas de supervisión y control podrán incluir auditorías, inspecciones, revisiones periódicas, requerimientos de información, evaluaciones técnicas, revisión de registros, verificación de trazas, análisis de incidentes, pruebas de seguridad, revisión de cumplimiento contractual y cualquier otro mecanismo razonable y proporcional conforme al marco aplicable.

CAPÍTULO II

DE LA UNIDAD DE COMERCIALIZACIÓN DE LOS SERVICIOS DE IDENTIDAD DIGITAL, FIRMA ELECTRÓNICA E INTEROPERABILIDAD

Artículo 83. Definición, objeto y adscripción. La unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad es una dependencia especializada, adscrita a la Dirección Nacional de Cedulación, responsable de gestionar, coordinar, supervisar y asegurar la calidad, disponibilidad, continuidad, seguridad, trazabilidad y mejora continua de los servicios de consulta, verificación y certificación de identidad digital, firma electrónica e interoperabilidad, provistos por la

Junta Central Electoral a entidades públicas y privadas, mediante datos biométricos y datos personales asociados a la identidad bajo competencia de la Junta Central Electoral.

Párrafo I. La Dirección Nacional de Cedulación será la dependencia encargada de supervisar las tareas diarias de la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad, así como de fiscalizar el cumplimiento de las metas de esta y aplicar las medidas disciplinarias u operativas a su personal y respecto a las decisiones de dicha unidad.

Párrafo II. La adscripción de la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad a la Dirección Nacional de Cedulación se fundamenta en la vinculación operativa de esta última con los procesos de captura, actualización, gestión y administración de datos asociados a la identidad y documentos de identidad emitidos por la Junta Central Electoral, sin perjuicio de las competencias que correspondan a la Dirección Nacional de Registro Civil, la Dirección de Registro Electoral, la Dirección Nacional de Informática, la Consultoría Jurídica y demás áreas institucionales competentes.

Párrafo III. La unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad ejercerá sus funciones con carácter especializado, técnico-operativo y transversal, conforme a la Constitución de la República, la Ley núm. 4-23, el presente reglamento, las resoluciones dictadas por la Junta Central Electoral, las políticas institucionales aplicables, las directrices del Pleno y los lineamientos de la Dirección Nacional de Cedulación, en lo relativo a su adscripción administrativa y coordinación operativa.

Párrafo IV. La adscripción prevista en este artículo no limitará la coordinación directa que la unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad deba mantener con las áreas institucionales que intervengan en la prestación, seguridad, soporte, trazabilidad, contratación, supervisión, auditoría, protección de datos, gestión de riesgos, continuidad y mejora del servicio.

Párrafo V. La unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad deberá contar con la autoridad funcional, capacidades técnicas, jurídicas, operativas, tecnológicas, de seguridad, trazabilidad, gestión de riesgos, supervisión y coordinación institucional necesarias para garantizar la adecuada prestación, control, continuidad y mejora del servicio regulado por el presente reglamento.

Artículo 84. Funciones de la Unidad de Comercialización de los Servicios de Identidad Digital, Firma Electrónica e Interoperabilidad. La unidad de comercialización de los servicios de identidad digital, firma electrónica e interoperabilidad tendrá, entre otras, las funciones siguientes:

a) **Gestión de contratos, convenios y acuerdos.** Participar en la elaboración, gestión, seguimiento y administración de los contratos, convenios, acuerdos, anexos técnicos, niveles de servicio y demás instrumentos vinculados con la prestación del servicio a entidades públicas y privadas.

b) **Evaluación de solicitudes.** Coordinar, tramitar o apoyar, según corresponda, la evaluación de las solicitudes de acceso al servicio, incluyendo la revisión de finalidad, legitimidad, requisitos técnicos, condiciones de seguridad, documentación de soporte y demás elementos necesarios para su autorización.

c) **Políticas, procedimientos y estándares.** Proponer, desarrollar, implementar y supervisar políticas, procedimientos, manuales, criterios operativos, estándares de calidad, requisitos técnicos y condiciones de seguridad relacionados con la prestación del servicio, en coordinación con las áreas institucionales competentes.

d) **Supervisión operativa y control de cumplimiento.** Supervisar el uso autorizado del servicio, verificar el cumplimiento de las condiciones establecidas por la Junta Central Electoral, dar seguimiento a indicadores, reportes, incidentes, auditorías, evaluaciones, planes de mejora y medidas correctivas vinculadas al servicio.

e) **Coordinación institucional.** Coordinar a través de la Dirección Nacional de Cedulación con las direcciones, departamentos, unidades y órganos internos de la Junta Central Electoral que intervengan en la administración, operación, seguridad, protección de datos, soporte, auditoría, legalidad, contratación, facturación o supervisión del servicio.

f) **Otras funciones.** Ejercer las demás funciones que le sean asignadas por el Pleno de la Junta Central Electoral, la Presidencia, la ley, el presente reglamento, las resoluciones aplicables o los instrumentos institucionales correspondientes.

Artículo 85. Coordinación interna. La Unidad de Comercialización de los Servicios de Identidad Digital, Firma Electrónica e Interoperabilidad, a través de la Dirección Nacional de Cedulación actuará en coordinación con la Dirección Nacional de Informática, la Dirección Nacional de Registro Civil, la Dirección Nacional de Cedulación, la Dirección Nacional de Registro Electoral, la Consultoría Jurídica, la Oficina del Delegado de Protección de Datos, las áreas de seguridad de la información, auditoría, planificación, financiera, administrativa y demás dependencias competentes de la Junta Central Electoral, según la materia de que se trate.

Párrafo. La estructura, funciones y responsabilidades de la Unidad podrán ser modificadas, precisadas o ampliadas por el Pleno de la Junta Central Electoral conforme a las necesidades institucionales, evolución tecnológica, requerimientos operativos y disposiciones legales o reglamentarias aplicables.

CAPÍTULO III

DE LAS EVALUACIONES Y AUDITORÍAS DE CUMPLIMIENTO

Artículo 86. Evaluaciones y auditorías de cumplimiento. La Junta Central Electoral, por medio de las áreas competentes y, cuando corresponda, de la Dirección Nacional de Cedulación, podrá realizar o requerir evaluaciones, auditorías, revisiones, inspecciones o verificaciones de cumplimiento respecto de los tratamientos de datos biométricos, datos personales asociados a la identidad y servicios de consulta, verificación y certificación de identidad comprendidos dentro del ámbito de aplicación del presente reglamento.

Párrafo I. Las evaluaciones y auditorías de cumplimiento tendrán por objeto verificar la observancia de la Ley núm. 4-23, el presente reglamento, las resoluciones dictadas por la Junta Central Electoral, las condiciones técnicas, contractuales y de seguridad aplicables, las finalidades autorizadas, las medidas de protección de datos, la trazabilidad de las operaciones, la gestión de incidentes, la conservación y eliminación de datos, y el cumplimiento de las obligaciones asumidas por los responsables, encargados y entidades usuarias.

Párrafo II. Las evaluaciones y auditorías podrán realizarse de manera periódica, aleatoria, extraordinaria, preventiva, correctiva o como consecuencia de incidentes de seguridad, denuncias, reclamaciones, cambios tecnológicos, modificaciones sustanciales del tratamiento, desviaciones de finalidad, riesgos identificados, incumplimientos contractuales o cualquier circunstancia que pueda afectar la seguridad, privacidad, trazabilidad, finalidad autorizada o derechos de los titulares.

Párrafo III. Las evaluaciones y auditorías deberán realizarse conforme a criterios de necesidad, proporcionalidad, razonabilidad, confidencialidad, debido proceso, gestión de riesgos y protección de la información sensible, reservada o confidencial a la que se tenga acceso durante su ejecución.

Artículo 87. Alcance de las evaluaciones y auditorías. Las evaluaciones y auditorías de cumplimiento podrán comprender, según corresponda, los aspectos siguientes:

a) Finalidad, legitimidad, necesidad y proporcionalidad del tratamiento de datos biométricos o datos personales asociados a la identidad.

b) Base legal, consentimiento, autorización, contrato, convenio, acuerdo o condición habilitante que justifica el tratamiento o el uso del servicio.

c) Cumplimiento de las condiciones de acceso, uso, integración, operación, seguridad, confidencialidad y trazabilidad del servicio.

d) Medidas técnicas, organizativas, administrativas, físicas y lógicas implementadas para proteger los datos, registros, resultados, constancias, credenciales, interfaces, trazas y demás información vinculada.

e) Gestión de accesos, credenciales, perfiles, roles, segregación de funciones, mínimo privilegio y revocación de permisos.

f) Registros de consulta, constancias de verificación, resultados del servicio, evidencias transaccionales, trazas de acceso, logs de operación y mecanismos de auditoría.

g) Procedimientos de conservación, retención, supresión o eliminación segura de datos biométricos, datos personales asociados a la identidad, registros o evidencias, según corresponda.

h) Gestión de incidentes de seguridad, notificaciones, medidas de contención, mitigación, remediación y seguimiento.

i) Evaluaciones de impacto, análisis de riesgos, pruebas de seguridad, auditorías internas, planes de acción y evidencias de cumplimiento.

j) Gestión de proveedores, subcontratistas, terceros tecnológicos, encargados del tratamiento o cualquier actor que intervenga en la operación, integración, soporte o seguridad del servicio.

k) Cumplimiento de las obligaciones económicas, contractuales, operativas y de reporte aplicables al uso del servicio.

l) Cualquier otro aspecto necesario para verificar el cumplimiento de la ley, el presente reglamento, las resoluciones aplicables o las condiciones autorizadas por la Junta Central Electoral.

Artículo 88. Procedimiento para la evaluación o auditoría de cumplimiento. La Junta Central Electoral establecerá el procedimiento aplicable para la realización de evaluaciones y auditorías de cumplimiento, el cual podrá incluir, como mínimo, las etapas siguientes:

a) Definición del alcance, objetivo, período, criterios y metodología de la evaluación o auditoría.

b) Identificación de los riesgos, procesos, sistemas, datos, controles, responsables, encargados, proveedores o entidades usuarias objeto de evaluación.

c) Requerimiento de información, documentación, registros, evidencias, reportes, trazas, políticas, procedimientos, contratos, evaluaciones de impacto, informes técnicos o cualquier otro soporte pertinente.

d) Revisión documental, entrevistas, pruebas técnicas, verificaciones de seguridad, revisión de configuraciones, inspecciones, análisis de registros o cualquier otro mecanismo razonable de evaluación.

e) Identificación de hallazgos, incumplimientos, brechas, riesgos, debilidades, oportunidades de mejora o medidas correctivas necesarias.

f) Elaboración de informe de resultados, recomendaciones, medidas requeridas, plazos de subsanación y responsables de implementación.

g) Seguimiento del plan de acción, verificación de cumplimiento de medidas correctivas y cierre formal de la evaluación o auditoría cuando corresponda.

Párrafo I. La entidad evaluada o auditada deberá colaborar de manera diligente, completa y oportuna con la Junta Central Electoral, proporcionando la información, acceso, explicaciones, evidencias y soportes razonablemente requeridos, sin perjuicio de las medidas de confidencialidad, reserva o protección de información sensible que resulten aplicables.

Párrafo II. Cuando la información requerida se encuentre sujeta a confidencialidad, secreto profesional, secreto bancario, reserva legal, regulación sectorial o deber contractual de reserva, la entidad evaluada deberá informarlo de manera motivada y proponer mecanismos de entrega compatibles con dichas obligaciones, tales como acceso limitado, información agregada, anonimizada, disociada, seudonimizada, restringida, bajo condiciones de reserva o mediante coordinación con el órgano regulador o supervisor competente.

Párrafo III. La invocación de confidencialidad, secreto profesional, secreto bancario, reserva legal, regulación sectorial o deber contractual de reserva no podrá ser utilizada para impedir injustificadamente la evaluación, auditoría, revisión, inspección o verificación de cumplimiento por parte de la Junta Central Electoral.

Artículo 89. Informes, medidas correctivas y seguimiento. Como resultado de las evaluaciones o auditorías de cumplimiento, la Junta Central Electoral podrá emitir informes, recomendaciones, observaciones, requerimientos, medidas correctivas, planes de remediación, plazos de subsanación, restricciones operativas, auditorías de seguimiento o cualquier otra medida proporcional al nivel de riesgo o incumplimiento identificado.
Párrafo I. Las entidades evaluadas o auditadas deberán implementar las medidas requeridas dentro de los plazos establecidos por la Junta Central Electoral y remitir las evidencias de cumplimiento correspondientes.

Párrafo II. El incumplimiento de las medidas correctivas, la negativa injustificada de colaboración, la presentación de información falsa, incompleta o engañosa, o la persistencia de riesgos no mitigados podrá dar lugar, cuando corresponda, a la suspensión, limitación, cancelación o terminación del servicio, sin perjuicio de las sanciones, responsabilidades, acciones legales o consecuencias contractuales que resulten aplicables.

Párrafo III. La Junta Central Electoral podrá realizar auditorías de seguimiento para verificar la implementación efectiva de las medidas correctivas y la mitigación de los riesgos identificados.

CAPÍTULO IV

DE LA ARTICULACIÓN Y COOPERACIÓN INTERINSTITUCIONAL

Artículo 90. Articulación y cooperación interinstitucional. La Junta Central Electoral podrá establecer canales de articulación, cooperación y coordinación con instituciones públicas, órganos constitucionales, entes reguladores o supervisores, autoridades competentes, organismos especializados, entidades técnicas, organismos internacionales y demás actores relevantes, cuando resulte necesario o conveniente para la adecuada aplicación del presente reglamento, la protección de los datos biométricos y datos personales asociados a la identidad, y la prestación segura, eficiente y confiable del Servicio de Consulta, Verificación y Certificación de Identidad.

Párrafo I. La cooperación interinstitucional podrá tener por objeto, entre otros fines, promover la protección de los datos biométricos y datos personales asociados a la identidad, fortalecer la seguridad de la información, facilitar la coordinación técnica u operativa, atender riesgos o incidentes, mejorar la interoperabilidad controlada, apoyar auditorías o verificaciones, armonizar criterios de cumplimiento y promover buenas prácticas en materia de identidad, biometría, protección de datos, seguridad y servicios de verificación o certificación de identidad.

Párrafo II. Cuando se trate de entidades públicas o privadas sujetas a regulación o supervisión sectorial, la Junta Central Electoral podrá coordinar con el órgano regulador o supervisor competente las actuaciones, requerimientos, auditorías, verificaciones, lineamientos, medidas correctivas o acciones de

seguimiento que resulten necesarias o convenientes, sin que dicha coordinación constituya condición previa, requisito de validez, autorización sustitutiva ni vía exclusiva para el ejercicio de las atribuciones de la Junta Central Electoral.

Párrafo III. La cooperación con órganos reguladores o supervisores no podrá interpretarse como renuncia, delegación, limitación o transferencia de las competencias atribuidas a la Junta Central Electoral por la Constitución, la Ley núm. 4-23, el presente reglamento y las disposiciones aplicables en materia de Registro Civil, identificación, cedulación, datos biométricos, consulta, verificación o certificación de identidad.

Párrafo IV. La Junta Central Electoral podrá suscribir convenios, acuerdos, protocolos, mesas técnicas, mecanismos de intercambio de información, guías de actuación o instrumentos de coordinación interinstitucional, siempre que sean compatibles con la Ley núm. 4-23, el presente reglamento, la normativa de protección de datos personales, la seguridad de la información, la confidencialidad de los datos y los derechos de los titulares.

Párrafo V. Cualquier intercambio de información que se realice en el marco de la cooperación interinstitucional deberá limitarse a la finalidad específica que lo justifica, observar los principios de necesidad, proporcionalidad, minimización, seguridad, confidencialidad y trazabilidad, y no podrá implicar cesión, transferencia, interconexión o tratamiento de datos biométricos fuera de los supuestos autorizados por la ley, el presente reglamento o la Junta Central Electoral.

Párrafo VI. La cooperación interinstitucional podrá comprender la elaboración de criterios técnicos, formatos, protocolos, mecanismos de reporte, medidas de gestión de incidentes, esquemas de supervisión coordinada, programas de capacitación, intercambio de buenas prácticas y demás instrumentos que contribuyan al cumplimiento del presente reglamento y a la protección de los titulares.

CAPÍTULO V

DEL INCUMPLIMIENTO, MEDIDAS CORRECTIVAS Y CONSECUENCIAS

Artículo 91. Incumplimiento de obligaciones. Sin perjuicio de las medidas específicas aplicables a la suspensión, limitación, cancelación, terminación, cierre o reanudación del Servicio de Consulta, Verificación y Certificación de Identidad previstas en la Sección VII del Capítulo I del Título III del presente reglamento, constituirá incumplimiento la inobservancia, total o parcial, de las obligaciones, condiciones, límites, prohibiciones, medidas de seguridad, finalidades autorizadas, requisitos técnicos, contractuales, económicos, operativos, de confidencialidad, trazabilidad, protección de datos, conservación, eliminación segura, cooperación, auditoría o reporte establecidos en la Ley núm. 4-23, el presente reglamento, las resoluciones dictadas por la Junta Central Electoral, el contrato, convenio, acuerdo, autorización o instrumento aplicable.

Párrafo I. Cuando la naturaleza del incumplimiento lo permita, la Junta Central Electoral podrá requerir a la entidad usuaria, responsable, encargado o sujeto obligado la adopción de medidas correctivas, planes de remediación, ajustes técnicos, fortalecimiento de controles, actualización documental, eliminación segura, suspensión de funcionalidades, restricción de accesos, capacitación, auditorías extraordinarias o cualquier otra medida necesaria y proporcional para restablecer el cumplimiento.
Párrafo II. La Junta Central Electoral podrá otorgar un plazo razonable para la subsanación del incumplimiento, atendiendo a su gravedad, riesgo, impacto sobre los titulares, afectación al servicio, reincidencia, urgencia, posibilidad de mitigación y demás circunstancias del caso.

Párrafo III. Cuando exista riesgo grave, inminente o no mitigado para la seguridad del servicio, la integridad de los datos, la confidencialidad, trazabilidad, derechos de los titulares o competencias de la Junta Central Electoral, esta podrá adoptar medidas inmediatas de suspensión, limitación, bloqueo preventivo, revocación de credenciales, restricción de funcionalidades o cualquier otra medida proporcional, sin perjuicio del procedimiento posterior que corresponda. Dicho procedimiento posterior se sujetará al plazo y a las garantías previstas en el artículo 94 del presente reglamento, debiendo notificarse a la entidad afectada dentro de un plazo no mayor de setenta y dos (72) horas.

Artículo 92. Incumplimientos relacionados con bases de datos, uso no autorizado o tratamiento autónomo. Constituirá incumplimiento grave que una entidad usuaria, responsable, encargado o tercero cree, mantenga, alimente, actualice, interconecte, replique, explote, ceda, comunique, reutilice o trate indebidamente bases de datos biométricos, bases de datos personales asociados a la identidad, repositorios, registros, sistemas, plataformas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación que, por su objeto o efecto, sustituyan, repliquen, desplacen o funcionen como infraestructura paralela o sustitutiva de los registros, bases de datos, servicios o competencias atribuidas a la Junta Central Electoral en materia de identidad, Registro Civil, cedulación, consulta, verificación o certificación de identidad.

Párrafo I. También constituirá incumplimiento grave la creación, conservación, explotación o utilización de copias no autorizadas, plantillas, vectores, patrones, códigos biométricos, minucias, mecanismos de vinculación, sistemas, plataformas o capacidades derivados del servicio provisto por la Junta Central Electoral, o de datos administrados por esta, que permitan realizar identificación, verificación, certificación, comparación o tratamiento biométrico autónomo fuera de las condiciones autorizadas.

Párrafo II. La conservación de registros de consulta, constancias de verificación, resultados del servicio, evidencias transaccionales, soportes operativos o documentación asociada a una operación no constituirá, por sí sola, incumplimiento del presente reglamento, siempre que se realice conforme a la finalidad autorizada, al plazo aplicable, a las condiciones de seguridad correspondientes y no incluya muestras biométricas, plantillas, vectores, patrones, códigos biométricos, minucias o mecanismos de vinculación derivados del servicio que permitan realizar tratamiento biométrico autónomo no autorizado.

Párrafo III. La recopilación, tratamiento o conservación de datos biométricos o datos personales asociados a la identidad suministrados directamente por el titular, en el marco de una relación contractual, comercial, laboral, regulatoria o de prestación de servicios, no constituirá por sí sola incumplimiento del presente reglamento, siempre que se encuentre amparada en una base válida, se limite a la finalidad específica informada o autorizada, respete el plazo de conservación aplicable y no tenga por objeto o efecto sustituir, replicar, desplazar o funcionar como alternativa al Servicio de Consulta, Verificación y Certificación de Identidad provisto por la Junta Central Electoral.

Párrafo IV. Las necesidades de continuidad operativa, disponibilidad del servicio, gestión de contingencias, cumplimiento regulatorio, gestión de riesgos, prevención de fraude, soporte probatorio o clasificación de una actividad como servicio esencial no habilitarán, por sí solas, la creación, mantenimiento, explotación, actualización o interconexión de bases biométricas paralelas, sustitutivas o no autorizadas, ni la prestación de servicios de consulta, verificación o certificación de identidad a terceros fuera de los mecanismos provistos, autorizados o regulados por la Junta Central Electoral.

Artículo 93. Consecuencias del incumplimiento. Los incumplimientos al presente reglamento podrán dar lugar, según corresponda y conforme a la gravedad, naturaleza, impacto, riesgo, reincidencia y circunstancias del caso, a medidas correctivas, suspensión, limitación, revocación, cancelación o terminación del acceso al servicio, eliminación segura de datos o mecanismos no autorizados, auditorías extraordinarias, restricciones operativas, acciones contractuales, reclamación de daños y perjuicios, puesta en conocimiento de autoridades competentes o aplicación de las sanciones, penalidades y consecuencias previstas en la Ley núm. 4-23 y demás normativa aplicable.

Párrafo I. Las medidas adoptadas deberán ser necesarias, proporcionales y razonables, atendiendo a la protección de los titulares, la seguridad de los datos, la integridad del servicio, la preservación de las competencias de la Junta Central Electoral y el restablecimiento del cumplimiento.

Párrafo II. La aplicación de medidas correctivas o contractuales no impedirá el ejercicio de acciones legales, administrativas, civiles, penales, regulatorias o de cualquier otra naturaleza que correspondan conforme al marco aplicable.

Artículo 94. Notificación, oportunidad de corrección y debido proceso. Salvo en los casos de riesgo grave, inminente o no mitigado, la Junta Central Electoral notificará a la entidad usuaria, responsable,

encargado o sujeto obligado los incumplimientos identificados, las medidas requeridas, los plazos de corrección y las consecuencias aplicables en caso de persistencia o agravamiento del incumplimiento.

Párrafo I. La entidad notificada podrá presentar las explicaciones, evidencias, medidas adoptadas, plan de remediación o descargos que estime pertinentes dentro del plazo otorgado por la Junta Central Electoral.

Párrafo II. La Junta Central Electoral evaluará las informaciones presentadas y podrá confirmar, modificar, ampliar, dejar sin efecto o requerir nuevas medidas, atendiendo a la naturaleza del incumplimiento, nivel de riesgo, medidas de mitigación adoptadas y demás circunstancias relevantes.

Párrafo III. Cuando el incumplimiento genere riesgo grave, inminente o no mitigado para la seguridad del servicio, la confidencialidad, integridad o disponibilidad de los datos, los derechos de los titulares o las competencias de la Junta Central Electoral, esta podrá adoptar medidas preventivas o correctivas inmediatas, sin perjuicio de la notificación posterior y del derecho de la entidad afectada a presentar las explicaciones correspondientes.

Artículo 95. Recursos administrativos. Los actos dictados por la Junta Central Electoral en aplicación del presente reglamento y respecto a los cuales se alegue que afectan desfavorablemente a la entidad usuaria, responsable, encargado o sujeto obligado podrán ser recurridos conforme la Ley 107-13 que regula los derechos y deberes de las personas en sus relaciones con la Administración Pública dominicana y establece el procedimiento administrativo aplicable en el país.

Artículo 96. Responsabilidad posterior y subsistencia de obligaciones. La suspensión, limitación, cancelación, terminación, vencimiento o finalización del servicio, contrato, convenio, acuerdo o autorización no extinguirá las obligaciones de confidencialidad, seguridad, trazabilidad, protección de datos, cooperación, auditoría, conservación legítima de evidencias, eliminación segura, pago de obligaciones pendientes, responsabilidad por incumplimientos anteriores o cualquier otra obligación que, por su naturaleza, deba subsistir conforme a la ley, el presente reglamento o el instrumento aplicable.

TÍTULO IV

DISPOSICIONES FINALES Y TRANSITORIAS

Artículo 97. Entrada en vigor. Dispone que el presente reglamento entrará en vigor a los treinta (30) días calendario, contados a partir de su publicación oficial, sin perjuicio de los plazos especiales de adecuación previstos en las disposiciones transitorias.

Artículo 98. Régimen transitorio de implementación. Las entidades usuarias del Servicio de Consulta, Verificación y Certificación de Identidad, así como los responsables y encargados de tratamientos comprendidos dentro del ámbito de aplicación del presente reglamento, dispondrán de un plazo de noventa (90) días calendario, contado a partir de la entrada en vigor del presente reglamento, para adecuar sus políticas, avisos de privacidad, mecanismos de consentimiento, registros, procedimientos internos, medidas de seguridad, canales de atención, gestión de incidentes y demás obligaciones documentales previstas en este reglamento.

Párrafo I. Cuando la adecuación requiera ajustes tecnológicos, modificación de sistemas, implementación de mecanismos de trazabilidad, segregación, cifrado, interoperabilidad, gestión de credenciales, auditoría, actualización de contratos, convenios o acuerdos, o cualquier otra medida técnica u operativa compleja, la Junta Central Electoral podrá otorgar un plazo adicional de hasta ciento ochenta (180) días calendario, previa solicitud motivada de la entidad interesada y presentación de un plan de adecuación.

Párrafo II. Durante el período transitorio, las entidades deberán abstenerse de iniciar nuevos tratamientos, integraciones, cesiones, interconexiones o usos del servicio que resulten incompatibles con el presente reglamento, y deberán adoptar medidas mínimas de seguridad, confidencialidad, finalidad, trazabilidad y protección de los titulares.

Párrafo III. La Junta Central Electoral podrá emitir instructivos, guías, normas técnicas, formatos, cronogramas o requerimientos específicos para facilitar la implementación progresiva del presente reglamento.

Artículo 99. Articulación normativa con disposiciones anteriores. Las disposiciones del Reglamento de Consulta del Archivo Maestro de Cedulados y Validación Biométrica de Identidad, aprobado por la Junta Central Electoral el seis (6) de agosto de dos mil veinte (2020), así como cualquier otra resolución, norma técnica, instructivo, contrato, convenio, acuerdo o disposición administrativa relacionada con servicios de consulta, validación, verificación o certificación de identidad, continuarán aplicándose en cuanto no sean contrarias al presente reglamento.

Párrafo I. En caso de contradicción entre el presente reglamento y disposiciones administrativas anteriores, prevalecerá el presente reglamento, sin perjuicio de las adecuaciones, actualizaciones o derogaciones expresas que disponga el Pleno de la Junta Central Electoral.

Párrafo II. Las tasas, tarifas, cargos o contraprestaciones previamente aprobadas para servicios de consulta, validación biométrica, verificación o certificación de identidad continuarán vigentes hasta tanto sean modificadas, sustituidas o actualizadas por el Pleno de la Junta Central Electoral mediante el instrumento correspondiente.

Párrafo III. La Junta Central Electoral podrá aprobar una tabla de correspondencia, adecuación o actualización normativa para armonizar los contratos, convenios, acuerdos, anexos técnicos, tarifas, procedimientos y condiciones operativas vigentes con las disposiciones del presente reglamento.

Artículo 100. Protocolos e instructivos. La comisión de tecnología de este órgano, a través de la Oficina Técnica, tendrá a su cargo la elaboración de los protocolos e instructivos que sean necesarios para la aplicación efectiva del presente reglamento y someterlos a la consideración del Pleno de la Junta Central Electoral para su aprobación.

Artículo 101. Facultades del Pleno. El Pleno de la Junta Central Electoral podrá adoptar cualquier otra medida complementaria y que sea necesaria, con ocasión de los procedimientos previstos en el presente reglamento y podrá disponer, en adición a las medidas de seguridad previstas en el mismo, otras acciones en materia de seguridad tecnológica, infraestructuras y aspectos operativos para garantizar la integridad en el tratamiento de los datos biométricos y datos personales asociados a la identidad de las personas y la provisión del servicio de consulta, verificación y certificación de identidad.

Artículo 101. Publicación y difusión del presente reglamento. Ordena que el presente reglamento sea publicado a través de los medios de comunicación institucionales de la Junta Central Electoral, a los fines de que el mismo sea de conocimiento de la población en general.

DADO en el municipio Santo Domingo Oeste, Provincia Santo Domingo, República Dominicana, a los _____ (__) días del mes de _____ del año dos mil veintiséis (2026).

Román Andrés Jáquez Liranzo
Presidente

Dolores Altagracia Fernández Sánchez
Miembro Titular

Samir Rafael Chami Isa
Miembro Titular

Hirayda Marcelle Fernández Guzmán
Miembro Titular

Rafael Armando Vallejo Santelises
Miembro Titular

Sonne Beltré Ramírez
Secretario General