BORRADOR DEL REGLAMENTO DE BIOMETRÍA Y DE SERVICIOS DE CONSULTA DE LA IDENTIDAD DE LAS PERSONAS

CONTENIDO

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

La **Junta Central Electoral**, 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 Luperón, Zona Industrial de Herrera, frente a la "*Plaza de la Bandera*", en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana; integrada por los magistrados, **Román Andrés Jáquez Liranzo,** Presidente; **Rafael Armando Vallejo Santelises**, Miembro Titular; **Dolores Altagracia Fernández Sánchez**, Miembro Titular; **Patricia Lorenzo Paniagua**, Miembro Titular y; **Samir Rafael Chami Isa**, Miembro Titular, asistidos por **Sonne Beltré Ramírez**, Secretario General.

VISTOS

VISTA: La Constitución vigente de la República Dominicana.

VISTA: La Ley General de Libre Acceso a la Información Pública núm. 200-04, del 28 de julio del año 2004.

VISTA: La Ley General de Archivos de la República Dominicana núm. 481-08, del 11 de diciembre del año 2008.

VISTA: La Ley núm. 172-13, del 12 de noviembre de 2013, sobre Protección Integral de datos biométricos asentados en archivos, registros públicos, banco de datos y otros medios técnicos.

VISTA: Ley General de Migración núm. 285-04, de fecha 15 de agosto de 2004.

VISTA: La Ley Orgánica de los Actos del Estado Civil, núm. 4-23, de fecha 20 de enero de 2023.

Vista: La Ley 126-02 Sobre comercio electrónico, documentos y firmas digitales, de 4 de septiembre de 2002.

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

VISTO: El Reglamento para acceder a los servicios de: I. "Consulta del Archivo Maestro de Cedulados" y II.- "Validación Biométrica de Identidad", y fija las tasas de cada Servicio, emitido por la Junta Central Electoral el 6 de agosto de 2020.

CONSIDERANDOS

CONSIDERANDO: Que el artículo 8 de la Constitución de la República establece como la finalidad principal del Estado "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".

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

CONSIDERANDO: Que la Constitución de la República, en su artículo 44, sobre el derecho a la intimidad y el honor personal, establece que "[t]oda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley".

CONSIDERANDO: Que en atención a las disposiciones del artículo 72 de la Norma Fundamental "[t]oda persona privada de su libertad o amenazada de serlo, de manera ilegal, arbitraria o irrazonable, tiene derecho a una acción de hábeas corpus ante un juez o tribunal competente, por sí misma o por quien actúe en su nombre, de conformidad con la ley, para que conozca y decida, de forma sencilla, efectiva, rápida y sumaria, la legalidad de la privación o amenaza de su libertad".

CONSIDERANDO: Que el artículo 74 de la Constitución de la República dispone que "[l]os poderes públicos interpretan y aplican las normas relativas a los derechos fundamentales y sus garantías, en el sentido más favorable a la persona titular de los mismos y, en caso de conflicto entre derechos fundamentales, procurarán armonizar los bienes e intereses protegidos por esta Constitución".

CONSIDERANDO: Que el Articulo 212 de la Constitución de la República define "[l]a Junta Central Electoral como un órgano autónomo con personalidad jurídica e independencia técnica, administrativa, presupuestaria y financiera, cuya finalidad principal es organizar y dirigir las asambleas electorales para la celebración de elecciones y de mecanismos de participación popular establecidos por la presente Constitución y las leyes. Tiene facultad reglamentaria en los asuntos de su competencia".

CONSIDERANDO: Que el párrafo II del artículo 212 de la Constitución, establece que: "serán dependientes de la Junta Central Electoral el Registro Civil y la Cédula de Identidad y Electoral".

CONSIDERANDO: Que en los numerales 2 y 3 del artículo 14 de la Ley Orgánica de Régimen Electoral núm. 20-23 de fecha diecisiete (17) de febrero de dos mil veintitrés (2023), establecen como atribuciones de la Junta Central Electoral "[c]ustodiar, mantener y conservar el Registro Civil" y "[c]ustodiar, mantener y conservar la Cédula de Identidad;

CONSIDERANDO: Que la República Dominicana es signataria de la Convención de las Naciones Unidas contra la Corrupción y, como tal, a los fines de combatir la corrupción se comprometió a instaurar los "procedimientos o reglamentaciones que permitan al público en general obtener, cuando proceda, información sobre la organización, el funcionamiento y los procesos de adopción de decisiones de su administración pública y, con el debido respeto a la protección de la intimidad y de los datos biométricos, sobre las decisiones y actos jurídicos que incumban al público";

CONSIDERANDO: Que la Ley General de Libre Acceso a la Información Pública núm. 200-04 del 28 de julio 2004, establece en sus artículos 18,19 y 20: "Limitación al acceso en razón de intereses privados preponderantes", los "casos especiales en que se obtiene el consentimiento de la persona o la entidad con derecho a reservas de sus informaciones y datos", así como "la entrega de información y datos entre órganos de la administración", cuyos fondos dependan total o parciamente del Estado.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

CONSIDERANDO: Que la Ley núm. 172-13, sobre protección integral de datos biométricos asentados en archivos, registros públicos, banco de datos y otros medios técnicos, establece en su "Considerando Séptimo: Que, en la República Dominicana, en los últimos tiempos, se han incrementado los delitos y los crímenes concernientes a la usurpación o el robo de la identidad de las personas físicas, causándoles daños económicos considerables. En consecuencia, se hace imperativo regular legalmente para que en los registros públicos y privados se utilicen técnicas de identificación que dificulten o imposibiliten el robo de las identidades de las personas físicas al momento de contratar bienes y servicios ante los organismos públicos, las empresas públicas y las empresas privadas en el territorio dominicano".

CONSIDERANDO: Que en atención al mandato Constitucional "la familia, la sociedad y el Estado, harán primar el interés superior del niño, niña y adolescente". Sobre este particular se reconoció, mediante la Ley núm. 135-06 la protección al derecho a la intimidad y a la imagen de los niños, niñas y adolescentes indicando que estos "tienen derecho al honor, reputación e imagen personal, a la vida privada e intimidad personal y de la vida familiar" por lo que "[e]stos derechos no pueden ser objeto de injerencias arbitrarias o ilegales del Estado, personas físicas o morales". Asimismo, "[s]e prohíbe disponer o divulgar, a través de cualquier medio, la imagen y datos de los niños, niñas y adolescentes en forma que puedan afectar su desarrollo físico, moral, psicológico e intelectual, su honor y su reputación, o que constituyan injerencias arbitrarias o ilegales en su vida privada e intimidad familiar o que puedan estigmatizar su conducta o comportamiento".

CONSIDERANDO: A que el Tribunal Constitucional, mediante su sentencia TC/0062/13, del 17 de abril de 2013, sentó un principio al decidir qué: "10.10. En la especie, el recurrente no sólo se ha limitado a solicitar la nómina de los empleados, sino también el número de cédula de identidad y electoral, información que es de carácter personal y que, además, no aporta nada en lo que respecta a la transparencia y al control de la corrupción en la administración pública, aspectos que constituyen los objetivos de la Ley No. 200-04, sobre Libre Acceso a la Información Pública. En este sentido, las instituciones públicas no están obligadas ni tienen el derecho a divulgar dicho dato".

CONSIDERANDO: Que a pesar de ésta ser una acción dirigida contra los empleados y funcionarios de la Junta Central Electoral, los fundamentos de la decisión irradian a todos los usuarios y usuarias de los servicios de la institución, que debe velar por la protección de su información, y salvaguardar el derecho protegido el artículo 44 de la Constitución;

CONSIDERANDO: Que atendiendo a la necesidad y/o requerimiento de un número considerable de entidades, de validar la identidad de personas que acceden a sus servicios particulares, la Junta Central Electoral, desde hace varios años, ha facilitado a instituciones públicas y privadas, inicialmente la entrega de archivos electrónicos con datos de cedulados, y a partir del 23 de julio 2013 lo sustituyó por la consulta en línea, formulada en el "Reglamento Que Establece El Procedimiento Para Acceder A La Consulta Avanzada Del Maestro De Cedulados Y fija Las Tasas Del Servicio", el cual quedó derogado con la aprobación y entrada en vigencia del "Reglamento para acceder a los servicios de: I. Consulta del Archivo Maestro de Cedulados y II.-Validación Biométrica de Identidad, y fija las tasas de cada Servicio".

CONSIDERANDO: Que el artículo 55 de la Ley Orgánica de los Actos del Estado Civil, núm. 4-23 ha dispuesto como responsabilidad de la Junta Central Electoral la recopilación, tratamiento y procesamiento de los datos biométricos, "con el propósito de autenticar y certificar la identidad de las personas".

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

CONSIDERANDO: Que por aplicación del artículo 2 y el párrafo del artículo 55 de la mencionada Ley núm. 4-23, —así como el artículo 212 de la Constitución— a la Junta Central Electoral se le ha otorgado la potestad reglamentaria para normar la aplicación de la referida pieza legislativa, en lo relativo a la "recopilación, tratamiento, procesamiento y uso" de los datos biométricos en todo el territorio nacional, las dependencias de la Junta Central Electoral en el exterior y las oficinas consulares.

CONSIDERANDO: Que, como consecuencia de la aplicación del "Reglamento para acceder a los servicios de: I. Consulta del Archivo Maestro de Cedulados y II.-Validación Biométrica de Identidad, y fija las tasas de cada Servicio", desde el 6 de agosto de 2020, la Junta Central Electoral cuenta con personal calificado y la tecnología, necesarios para ofrecer e implementar el servicio de "validación biométrica de identidad", la cual consiste en dar validez de las huellas dactilares que aporten, como resultado de un procedimiento de comparación con la base de datos biométricas archivados en la Junta Central Electoral.

CONSIDERANDO: Que estos servicios de consulta y verificación generan para la Junta Central Electoral costos operativos, que van desde el uso de personal calificado, el acceso a la base de datos, la protección de las aplicaciones, la compra de licencias internacionales, así como la preparación necesaria en equipos y aplicaciones informáticas, para tener capacidad de recibir y responder oportunamente la demanda simultánea de altos volúmenes de consultas por parte las personas usuarias de los servicios.

Por tanto, la Junta Central Electoral, en uso de sus atribuciones constitucionales, legales y reglamentarias, dicta el presente Reglamento.

CAPÍTULO 1. DE LAS DISPOSICIONES FUNDAMENTALES, DEFINICIONES, PRINCIPIOS RECTORES, DERECHOS Y DEBERES

Sección I. De las disposiciones fundamentales

Artículo 1.- Objeto. Este reglamento tiene por objeto establecer los procedimientos y especificaciones requeridas para la recopilación, tratamiento, procesamiento y uso de la biometría; así como de los servicios de consulta y autenticación de la identidad de las personas por los entes públicos y los particulares, en atención a las disposiciones de la Ley Orgánica de los Actos del Estado Civil, núm. 04-23.

Artículo 2.- Ámbito de Aplicación. Este reglamento se aplica en todo el territorio nacional, las dependencias de la Junta Central Electoral en el exterior y las oficinas consulares a que se refiere la Ley Orgánica de los Actos del Estado Civil, núm. 04-23.

Artículo 3.- Interpretación. Las disposiciones del presente reglamento deben ser interpretadas en el sentido más favorable a la persona titular de los datos biométricos y con estricto apego al principio de juridicidad. En caso de

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

conflicto entre los derechos fundamentales del o la titular de los datos biométricos y un particular se procurará armonizar los bienes e intereses protegidos por el ordenamiento jurídico.

Artículo 4.- Titular de los datos biométricos. Es la persona física que se le reconoce el derecho de gozo, disposición y uso de las informaciones medibles generadas de sus características físicas, fisiológicas, de comportamiento o rasgos atribuibles exclusivamente a su persona.

Artículo 5.- Responsable del tratamiento de los datos biométricos. Persona física o jurídica que se le reconoce el derecho de recolección, uso, almacenamiento, modificación, consulta, transmisión, cotejo, limitación o destrucción de los datos biométricos, con o sin el consentimiento del o la titular y en estricto apego al principio de juridicidad.

Artículo 6. Responsabilidad de la Junta Central Electoral. En concordancia con la obligación Constitucional de regir el Registro Civil y la Cédula de Identidad y Electoral, la Junta Central Electoral es el custodio de la identidad dominicana, y por ende el ente público encargado del tratamiento de los datos biométricos en el Estado dominicano, con el propósito de autenticar y certificar la identidad de las personas.

Artículo 7. **Deber de certificación.** Todas las instituciones públicas que, amparadas en una ley, traten datos biométricos deberán certificar y autenticar la identidad de las personas, a través del servicio de consulta, certificación y autenticación de la identidad provistos por la Junta Central Electoral.

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 y verificación de identidad.

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

Párrafo III.- La consulta de datos biométricos para fines de verificación de identidad deberá realizarse respetando el derecho a la intimidad de las personas, consagrado en este reglamento y las leyes sobre la materia.

Sección II. De las definiciones

Artículo 8.- Definiciones. En reconociendo de la aplicación directa de las definiciones dispuestas en el artículo 3 de la Ley Orgánica de los Actos del Estado Civil, núm. 4-23, para los fines de este reglamento, también se reconocen las siguientes:

1) **Algoritmo biométrico:** Secuencia de instrucciones que le dicen a un sistema biométrico cómo resolver un problema particular. Un algoritmo biométrico tiene número finito de pasos y normalmente lo utiliza el programa del sistema biométrico para decidir si los datos de la muestra biométrica y una referencia biométrica coinciden.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

2) **API:** (Application Programming Interface), Interfaz de Programación de Aplicaciones. Las APIs son un conjunto de funciones utilizadas por los programadores para establecer comunicación entre el software y los dispositivos hardware.

3) **Archivo, registro, ficheros, base o banco de datos biométricos:** Conjunto organizado de datos de carácter personal relativo a la biometría de las personas, que sean objeto de tratamiento o procesamiento, automatizado o no, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Los mismos serán de responsabilidad privada o de titularidad pública

4) **Archivos de datos de responsabilidad pública:** Son aquellos archivos de datos biométricos de los que sean responsables los órganos de la administración pública, así como las entidades u organismos vinculados o dependientes de la misma y las entidades autónomas y descentralizadas del Estado.

5) **Autenticación biométrica:** La autenticación biométrica es un nivel más avanzado y seguro de verificación. Implica comparar los datos biométricos de una persona con los datos almacenados en una base de datos centralizada o un sistema externo (1 a 1) para verificar su identidad de manera más rigurosa. La autenticación se utiliza comúnmente en transacciones financieras, sistemas de seguridad de alto nivel y acceso a información confidencial.

6) **Biometría:** Uso automatizado de características fisiológicas o de conductas para determinar o verificar la identidad de las personas. La biometría fisiológica está basada en datos de la medición directa de algún rasgo del cuerpo humano, sea el iris, la cara o la impresión dactilar. Por biometría conductual se entenderá la relacionada a datos de la medición directa de algún rasgo conductual, de hábitos de uso o comportamiento de una persona.

7) **Cancelación:** Procedimiento en virtud del cual el responsable del tratamiento cesa en el uso de los datos biométricos a partir de un bloqueo de los mismos y su posterior supresión.

8) **Cedente:** Es la persona física o jurídica que una vez recopilados proporciona los datos biométricos del titular a un cesionario.

9) **Cesión o comunicación de datos:** Tratamiento de datos que supone la revelación de los datos biométricos a una persona distinta del o la titular.

10) **Cesionario:** Persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos biométricos.

11) **Certificar**: Asegurar, afirmar, dar por cierto algo. En el uso de sistemas biométricos, "certificar" se refiere al proceso de confirmar, asegurar o verificar la identidad de un individuo a través de datos biométricos provistos por la persona o una entidad.

12) **Consentimiento del o la titular:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el/la titular consiente el tratamiento de datos biométricos que le conciernen.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

13) **Consentimiento expreso:** Se presenta cuando la voluntad del o la titular se manifiesta verbalmente, por escrito, por medios electrónicos, signos inequívocos o por cualquier otra tecnología aceptada y que quede registro de este.

14) **Credenciales:** Conjunto de datos que incluye la identificación y prueba de identificación que se utiliza para obtener acceso a recursos locales y de red; es decir, el conjunto de elementos que utiliza un objeto principal para probar su identidad.

15) **Datos biométricos:** Son propiedades físicas, fisiológicas, de comportamiento o rasgos de la persona, atribuibles a una sola persona y que son medibles; dichos datos son obtenidos a partir de un proceso biométrico, el cual comprende observaciones preliminares, muestras biométricas, modelos, planillas y valoraciones o comparaciones. Los datos biométricos son empleados para describir la información recolectada durante un enrolamiento, verificación o identificación de procesos.

16) **Datos de carácter personal o datos personales:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

17) **Dispositivo de captura biométrica:** Dispositivo que recoge una señal de una característica biométrica y la convierte en una muestra biométrica capturada.

18) **Dominio de internet:** Es la máxima subdivisión de un nombre de dominio en una dirección de red, que identifica el tipo de entidad propietaria de la dirección.

19) **Responsable o encargado del tratamiento:** La persona física o jurídica, pública o privada, que realice el tratamiento de los datos biométricos por cuenta del o la responsable del tratamiento.

20) **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 las que la Constitución y las leyes le reconozcan su naturaleza pública.

21) **Evaluación de Impacto:** Es un proceso sistemático y proactivo para identificar, analizar y abordar los riesgos y efectos potenciales en la privacidad y protección de datos personales que podrían derivarse de un proyecto, iniciativa, producto, servicio o actividad específica, antes de su implementación.

22) **Firma digital:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y el texto del mensaje y que el mensaje inicial no ha sido modificado después de efectuada la transmisión.

23) **Identidad:** Es el conjunto de datos en virtud de los cuales se establece que una persona es verdaderamente la que se dice o la que se presume que es.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

24) **Identificación biométrica:** La identificación biométrica se refiere al proceso de reconocimiento de una persona mediante el uso de características biométricas únicas, como huellas dactilares, iris, rostro, voz, entre otros. El objetivo de la identificación es determinar la identidad de una persona dentro de un conjunto de posibles candidatos (1 a N).

25) **Identificador (ID):** Nombre formado por caracteres alfanuméricos que permite identificar un fichero o cualquier parte de un programa.

26) **Información pública:** Todo registro, archivo o cualquier dato que se recopile, mantenga, procese o se encuentre en poder de las entidades públicas a las que se refiere esta ley. Asimismo, toda información que en virtud de la Constitución de la República Dominicana garantice el principio de publicidad de los actos de los Poderes del Estado y el derecho de acceso a la información pública, establecido en la Ley General de Libre Acceso a la Información Pública núm. 200-04, de fecha 28 de julio de 2004.

27) **Limitación**: Cuando el tratamiento se haya limitado, dichos datos biométricos solo podrán ser objeto de tratamiento, con excepción de su almacenamiento, con el consentimiento del o la titular o para la formulación, el ejercicio o la defensa de reclamaciones, o para la protección de los derechos de otra persona física o jurídica o por razones de importante interés público del Estado.

28) **Línea VPN (Virtual Private Network), Red Privada Virtual**: Extensión de una red privada que abarca vínculos encapsulados, cifrados y autenticados en redes públicas o compartidas. Las conexiones VPN pueden proporcionar acceso remoto y conexiones enrutadas o redes privadas a través de Internet.

29) **lnternet Protocol (IP):** Es un protocolo enrutable responsable del direccionamiento IP y de la fragmentación y ensamblado de los paquetes, no confiables y sin conexión.

30) **Minucias:** Son características distintivas localizadas en una huella dactilar que se utilizan para individualizar y comparar huellas dactilares. Los detalles incluidos en las minucias incluyen las bifurcaciones y las terminaciones de las crestas en un patrón de huella digital. Las minucias ocurren en puntos donde una cresta de la huella dactilar se desvía de un flujo ininterrumpido, y pueden manifestarse como puntos finales (terminaciones), bifurcaciones o tipos compuestos más complejos.

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

32) **Procedimiento de disociación:** Todo tratamiento de datos biométricos de manera que la información obtenida no pueda asociarse a persona determinada o determinable, mediante el uso de técnicas de codificación, de modo que no permita identificar a la persona física ante terceros.

33) **Registro de datos:** Es la modalidad de asiento a través de la cual acceden al Registro Civil los hechos y actos relativos al estado civil de las personas y aquellos otros determinados por esta ley.

34) **Seudonimización:** Es un proceso de protección de datos personales que consiste en reemplazar o modificar ciertos identificadores en un conjunto de datos para que la información ya no pueda asociarse directamente

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

con una persona en particular sin la necesidad de información adicional. El objetivo principal de la seudonimización es reducir el riesgo de exposición y proteger la privacidad de las/los individuos cuyos datos están siendo procesados.

35) **Sistema biométrico:** Sistema desarrollado para el reconocimiento automatizado de individuos basado en sus características fisiológicas o de conducta.

36) **Tercero:** Persona física o jurídica, pública o privada, u órgano administrativo distinto del o la titular o del/la responsable del tratamiento de los datos biométricos.

37) **Titular de los datos biométricos:** Se refiere a la persona física a quien pertenecen los datos biométricos. Es la/el individuo sobre quien se recopilan y procesan los datos biométricos para su identificación y autenticación.

38) **Cesión internacional de datos:** Tratamiento de datos que supone una transmisión de estos fuera del territorio de la República Dominicana, sin importar el soporte, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del o la responsable del archivo de datos biométricos establecido en territorio dominicano.

39) **Tratamiento de datos biométricos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permiten la recolección, conservación, ordenamiento, almacenamiento, modificación, relación, evaluación, bloqueo, destrucción y, en general, el procesamiento de datos biométricos, así como también su cesión a través de terceros.

40) **Usuario:** Persona que utiliza un equipo, el cual tiene acceso a los programas y archivos del equipo, así como a los programas y archivos que se encuentran en la red (en función de las restricciones de cuenta determinadas por el administrador de la red).

41) **Usuarios y usuarias del servicio:** La persona física o jurídica, pública o privada, que utiliza el servicio de consulta, certificación y autenticación biométrica provisto por la Junta Central Electoral.

42) **Validación de datos:** Verificar, controlar o filtrar cada una de las entradas de datos que provienen desde el exterior del sistema.

43) **Verificación biométrica:** La verificación biométrica implica la comparación de los datos biométricos de una persona con sus propios datos almacenados en un sistema, dispositivo físico o en una tarjeta de identificación. El objetivo de la verificación es confirmar que la persona que presenta los datos biométricos es la misma que está registrada en el sistema (1 a 1).

Párrafo. Las definiciones dadas en la Ley núm. 172-13 sobre Protección integral de los datos personales asentados en archivos, registros públicos, banco de datos y otros medios técnicos, son supletorias para este reglamento en la medida que son aplicables a los datos biométricos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Sección III. De principios para el tratamiento de datos biométricos

Artículo 9.- Principios rectores. En el marco del respeto al ordenamiento jurídico y armonía a los principios supletorios dispuestos en el artículo siguiente, se reconocen los siguientes principios:

1) **Principio de juridicidad:** El/la responsable del tratamiento de los datos biométricos debe llevar el tratamiento de los datos conforme y en base a las facultades y atribuciones que la ley y este reglamento le confieren y en armonía con el ordenamiento jurídico.

2) **Principio de calidad:** Se deberá garantizar que los datos biométricos sean precisos, correctos, adecuados y pertinentes al ámbito y finalidad para los que se hubieren obtenido y evitando la recolección de datos innecesarios. Los datos deben actualizarse en el caso de que ello fuere necesario al ámbito y finalidad para los que se hubieren obtenido.

3) **Principio de seguridad:** Se deberán implementar medidas técnicas y organizativas adecuadas para proteger los datos biométricos contra el acceso no autorizado, la divulgación, la alteración o la destrucción. Se deberán tomar medidas de seguridad adecuadas para proteger los datos biométricos, como el cifrado, el control de acceso y la gestión de identidad.

4) **Principio de transparencia sobre el uso de la biometría:** Se deberá proporcionar información clara y comprensible al titular sobre cómo se tratarán, recolectarán, utilizarán y protegerán sus datos biométricos, salvo disposición contraria de la ley. El/la titular deberá ser informado de los derechos sobre sus datos, si está o no obligado a proporcionarlos y las consecuencias de hacerlo o no hacerlo, salvo disposición contraria de la ley.

5) **Principio de consentimiento explícito:** Los usuarios y usuarias y usuarias deben dar su consentimiento expreso e inequívoco para la recolección y procesamiento de sus datos biométricos, salvo disposición contraria de la ley.

6) **Principio de certificación de la información y no traspaso:** Las instituciones que traten datos especialmente protegidos deberán en la medida de lo posible no compartir los datos de manera íntegra, sino certificar los datos que le sean requeridos.

7) **Principio de tratamiento leal:** El/la responsable solo puede recolectar, usar, almacenar, modificar, consultar, transmitir, cotejar, limitar o destruir de los datos biométricos por medios lícitos.

8) **Principio de confidencialidad:** Consiste en la obligación del o la responsable de establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos biométricos guarden secreto respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

9) **Principio de información, acceso y corrección:** Los usuarios y usuarias y usuarias deben tener el derecho de acceder a sus datos biométricos, corregirlos o completarlos si es necesario, y las organizaciones deben

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

responder a estas solicitudes de manera oportuna, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del o la titular.

10) **Principio de retención:** Los datos biométricos solo deben ser retenidos durante el tiempo necesario para cumplir con el propósito específico para el que se recolectaron, y deben ser eliminados de manera segura cuando ya no sean necesarios.

11) **Principio de responsabilidad**: El o la responsable de tratar datos biométricos deberá adoptar los siguientes mecanismos de protección y seguridad en materia de tratamiento de datos biométricos: Destinar recursos autorizados para instrumentar programas y políticas de protección de datos biométricos; poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en la materia; revisar periódicamente las políticas y programas de seguridad de datos biométricos; establecer un sistema de supervisión y vigilancia interna y/o externa, de las políticas de protección de datos biométricos; establecer procedimientos para recibir y responder dudas y quejas de los titulares; diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos biométricos y garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos biométricos, cumplan por defecto con las obligaciones previstas en la Ley y las demás normativa que resulte aplicable en la materia.

12) **Principio de finalidad legítima**: El tratamiento de datos personales debe llevarse a cabo para fines específicos, explícitos y legítimos, y no debe tratarse de manera incompatible con dichos fines. La finalidad legítima en este contexto podría incluir, por ejemplo, el cumplimiento de un contrato, el cumplimiento de una obligación legal, la protección del interés vital del titular de los datos o el ejercicio de funciones de interés público.

13) **Principio de exactitud de los datos**. Este principio se refiere a que los datos han de ser exactos y han de estar debidamente actualizados. Para ello se han de adoptar las medidas necesarias para rectificar o suprimir aquellos datos inexactos en relación con la finalidad para la que van a ser utilizados.

14) **Principio de integridad de la información.** Este principio establece que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación no ha sido manipulada por terceros de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.

15) **Principio de disponibilidad de la información.** Este principio establece que la información estará disponible siempre que sea necesario para las personas autorizadas para accederla y tratarla, y la misma podrá recuperarse en caso de que ocurra un incidente que cause su pérdida o corrupción.

16) **Principio de autenticidad de información.** Este principio garantiza veracidad de autoría de la información. La autenticidad garantiza la veracidad del autor, de quién produjo la información. La información que descansa en la documentación oficial es auténtica y fruto del proceso registral mismo. Su ingreso a los equipos y sistemas solo es realizado por las/los funcionarios designados para esos fines, garantizando así la autenticidad de la información.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

17) **Principio de privacidad por diseño.** Este principio se refiere a que medidas de protección de datos y privacidad deben ser integradas desde la etapa de diseño y planificación de cualquier sistema, producto o servicio que implique el procesamiento de datos personales, garantizando así la protección de la privacidad de los individuos desde el inicio.

Artículo 10. Principios supletorios. Los principios que integra la Ley Orgánica de los Actos del Estado Civil, núm. 04-23, así como los que sean compatibles de la Ley núm. 107-13 sobre los Derechos de las Personas en sus relaciones con la Administración y de procedimiento Administrativo, son de aplicación directa a la recopilación, tratamiento, procesamiento, uso de la biometría y a los servicios de consulta de la identidad de las personas por las entidades públicas y los particulares.

Sección IV. De los derechos de las personas

Artículo 11: Ejercicio de los derechos. El ejercicio de cualquiera de los derechos de los individuos en relación con el tratamiento de sus datos biométricos, incluidos el acceso, la rectificación, la cancelación, la oposición, la limitación del tratamiento y la portabilidad de los datos, no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquiera de estos derechos.

Artículo 12: Derecho de acceso. El/la titular tiene derecho a obtener del o la responsable del tratamiento sus datos biométricos, así como información relativa a las condiciones y generalidades del tratamiento.

Párrafo I. La obligación de acceso se dará por cumplida cuando el/la responsable del tratamiento ponga a disposición del o la titular los datos biométricos en sitio. El/la responsable del tratamiento deberá determinar el periodo durante el cual el/la titular podrá presentarse a consultarlos, mismo que no podrá ser menor a quince días laborables (ley de acceso a la información), o bien, mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el/la titular.

Artículo 13: Derecho de rectificación. El/la titular podrá solicitar en todo momento al responsable del tratamiento que rectifique sus datos biométricos que resulten ser inexactos o incompletos.

Párrafo. La solicitud de rectificación deberá indicar a qué datos biométricos se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado. El/la responsable deberá ofrecer mecanismos que faciliten el ejercicio de este derecho en beneficio del o la titular.

Artículo 14: Derecho de cancelación. El/la titular podrá solicitar en todo momento al responsable del tratamiento la cancelación de los datos biométricos cuando considere que los mismos ya no sean necesarios para los fines para los que fueron recopilados, si ha retirado su consentimiento, si se oponen al tratamiento o si los datos han sido tratados ilegalmente.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo. La cancelación podrá proceder respecto de la totalidad de los datos biométricos del o la titular o sólo parte de ellos.

Artículo 15: Derecho a la limitación del tratamiento. El/la titular tendrá derecho a obtener del o la responsable del tratamiento la limitación del tratamiento de los datos biométricos cuando se cumpla alguna de las condiciones siguientes:

a) El/la titular impugne la precisión de los datos biométricos, en un plazo que permita al responsable verificar que son exactos y que están completos;

b) El tratamiento sea ilícito y el/la titular se oponga a la supresión de los datos biométricos y solicite en su lugar la limitación de su uso;

c) El/la responsable del tratamiento ya no necesite los datos biométricos para los fines del tratamiento, pero el/la titular los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

Párrafo. En los archivos automatizados, la limitación del tratamiento deberá realizarse, en principio, por medios técnicos. El hecho de que los datos biométricos están limitados se indicará en el sistema de tal modo que quede claro que no se pueden utilizar.

Artículo 16: Derecho de oposición. El/la titular podrá, en todo momento, oponerse al tratamiento de sus datos biométricos o exigir que se cese en el mismo cuando exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o requiera manifestar su oposición para el tratamiento de sus datos biométricos a fin de que no se lleve a cabo el tratamiento para fines específicos.

Párrafo I. No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable del tratamiento.

Artículo 17. Derecho a la portabilidad de los datos. El/la titular tendrá derecho a recibir los datos biométricos que le incumban, que haya facilitado al responsable del tratamiento, en un formato estructurado, comúnmente utilizado y legible y a transmitir eso datos a una tercera persona sin obstáculos por parte de la organización que los proporcionó, cuando el tratamiento se efectúe por medios automatizados.

Párrafo. El derecho a la portabilidad no podrá ser exigido en los casos en que el tratamiento de los datos biométricos sea necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas a la persona responsable del tratamiento.

Sección V. De la definición y roles del o la responsable del tratamiento de datos biométricos

Artículo 18. Definición del 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 en conjunto con otros, determina los fines y medios del tratamiento de datos biométricos. Este responsable asume la

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

responsabilidad y cumple con las obligaciones establecidas en el presente reglamento y en la normativa vigente en materia de protección de datos.

Artículo 19. Roles del responsable del tratamiento de los datos biométricos. Dentro de los roles del responsable del tratamiento de datos biométricos, se encuentran:

a) Establecer y mantener políticas y procedimientos claros y actualizados para el manejo adecuado de los datos biométricos. Esto incluye la creación de directrices para la recolección, almacenamiento, uso, cesión y eliminación segura de los datos.

b) Asegurar el cumplimiento de todas las disposiciones legales y normativas aplicables en materia de tratamiento y protección de datos biométricos, incluyendo el presente reglamento y cualquier otra normativa pertinente.

c) Designar un delegado o delegada de protección de datos personales, el cual deberá contar con la capacidad y competencias necesarias para garantizar el cumplimiento de las obligaciones establecidas en el reglamento.

d) Gestionar y salvaguardar de forma segura los datos biométricos recolectados, garantizando su confidencialidad, integridad y disponibilidad.

e) Implementar medidas de seguridad técnicas y organizativas apropiadas para prevenir el acceso no autorizado, el uso indebido, la alteración, la divulgación o la destrucción no autorizada de los datos biométricos. Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando estas contemplen una protección mayor para él o la titular que la dispuesta en el presente reglamento.

f) Obtener el consentimiento válido y explícito de los titulares de los datos biométricos, asegurando que se informe de manera clara y transparente sobre los fines del tratamiento, los derechos del titular y la duración del almacenamiento de los datos. Asimismo, deberá garantizar el ejercicio de los derechos de los titulares, como el acceso, rectificación, supresión, limitación y oposición al tratamiento de sus datos biométricos.

g) Llevar a cabo evaluaciones de impacto en la protección de datos, especialmente cuando el tratamiento de los datos biométricos pueda entrañar un alto riesgo para los derechos y libertades de los titulares. Estas evaluaciones permitirán identificar y abordar los riesgos asociados al tratamiento de los datos biométricos.

h) En caso de producirse un incidente de seguridad o una violación de datos biométricos, notificar de manera inmediata a la Junta Central Electoral, así como a los titulares de los datos afectados, adoptando las medidas necesarias para mitigar los efectos del incidente.

i) Colaborar de manera activa y cooperativa con la Junta Central Electoral, proporcionando la información requerida y facilitando cualquier acción necesaria para garantizar el cumplimiento de las disposiciones legales en materia de protección de datos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

j) Mantener un registro de las actividades de tratamiento realizadas que incluya, al menos, la siguiente información:

1. Los fines del tratamiento de los datos biométricos.
2. Las categorías de datos biométricos tratados.
3. Los destinatarios o categorías de destinatarios a los que se comunican los datos biométricos.
4. Las cesiones internacionales de datos biométricos, en caso de que existan.
5. Los plazos de conservación de los datos biométricos.
6. Las medidas de seguridad implementadas para proteger los datos biométricos.
7. Cualquier otra información requerida por la normativa aplicable.

Artículo 20. Responsabilidad del responsable del tratamiento de datos biométricos. El responsable del tratamiento de datos biométricos asume la responsabilidad última de garantizar el cumplimiento de las disposiciones establecidas en el presente reglamento. En caso de incumplimiento de las obligaciones, la persona responsable estará sujeto a las sanciones y responsabilidades legales correspondientes.

Artículo 21. Subcontratación de servicios. En caso de que el responsable del tratamiento de datos biométricos subcontrate a terceros la realización de actividades de tratamiento, deberá asegurarse de que dichos terceros ofrezcan garantías suficientes para implementar medidas técnicas y organizativas apropiadas que cumplan con las disposiciones legales de protección de datos biométricos.

Párrafo. El ente responsable del tratamiento deberá establecer un contrato o acuerdo que regule las condiciones de la subcontratación, incluyendo las obligaciones específicas en materia de protección de datos biométricos y la responsabilidad de los terceros subcontratados.

Artículo 22. Deber de actualización y formación. La persona responsable del tratamiento de datos biométricos deberá mantenerse actualizado sobre los avances tecnológicos y las novedades normativas relacionadas con protección de datos biométricos. Asimismo, deberá proporcionar la formación adecuada a su personal que participe en el tratamiento de datos biométricos, asegurando que cuenten con los conocimientos necesarios para cumplir con las disposiciones legales reglamentarias y proteger la privacidad de los titulares de datos.

Artículo 23. Evaluación y revisión periódica. Quien es responsable del tratamiento de datos biométricos deberá llevar a cabo evaluaciones y revisiones periódicas de las medidas implementadas, con el objetivo de garantizar la eficacia y adecuación del tratamiento de los datos biométricos. En caso de detectar deficiencias o riesgos, el responsable deberá tomar las medidas correctivas necesarias para asegurar el cumplimiento de las disposiciones legales.

Artículo 24. Confidencialidad y no divulgación. El responsable del tratamiento de datos biométricos y su personal deberán mantener la confidencialidad de los datos biométricos a los que tengan acceso en el ejercicio de sus funciones. No podrán divulgar, transferir o utilizar los datos biométricos para fines distintos a los establecidos en el presente reglamento, salvo que exista consentimiento expreso o una disposición legal que lo permita.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Artículo 25. Registro de violaciones de seguridad. El responsable del tratamiento de datos biométricos deberá llevar un registro de las violaciones de seguridad que afecten a los datos biométricos tratados. Este registro deberá incluir la descripción de la violación, las medidas adoptadas para mitigar sus efectos y las acciones tomadas para

Artículo 26. Designación de un delegado de protección de datos. El o la responsable del tratamiento está obligado a designar un delegado (a) de protección de datos (DPD) para supervisar el cumplimiento de las normas y políticas de protección de datos en la organización.

Párrafo: El DPD será seleccionado en base a su experiencia, habilidades y conocimientos en materia de protección de datos personales y legislación aplicable.

Artículo 27.- Del Delegado de Protección de Datos de la Junta Central Electoral: La Junta Central Electoral tendrá un Delegado/Delegada de Protección de Datos el cual estará adscrito a la Dirección de Servicios de Autenticación de la Identidad y será responsable de supervisar el cumplimiento de las políticas y regulaciones en materia de protección de datos personales emitidas tanto por el Congreso Nacional, la Junta Central Electoral como por otros órganos competentes que estén tratando datos biométricos.

Artículo 28. Los DPD de las instituciones responsables del tratamiento de datos biométricos deberán trabajar en cooperación con el Delegado de Protección de la Junta Central Electoral para asegurar la implementación de las políticas de protección de datos personales.

CAPÍTULO 2.- DEL CONSENTIMIENTO, SUS CARACTERISTICAS Y EL AVISO DE PRIVACIDAD

Sección I. Del consentimiento y sus características

Artículo 29.- La obtención del consentimiento tácito o expreso deberá ser:

a) **Libre:** sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del o la titular;

b) **Específica:** referida a una o varias finalidades determinadas que justifiquen el tratamiento;

c) **Informada**: que el/la titular tenga conocimiento del aviso de privacidad previo al uso u almacenamiento a que serán sometidos sus datos biométricos y las consecuencias de otorgar su consentimiento.

d) **Inequívoca:** que no admite duda o equivocación.

Artículo 30.- Cuando el uso se base en el consentimiento de la persona interesada, el/la responsable deberá ser capaz de demostrar que aquel consintió en el uso de sus datos biométricos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Artículo 31.- Si el consentimiento de la persona interesada se da en el contexto de un contrato escrito que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso, y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

Artículo 32.- El/la titular tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

Artículo 33.- Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos biométricos que no son necesarios para la ejecución de dicho contrato.

Artículo 34.- Cuando la entidad responsable pretenda obtener los datos biométricos de forma directa o personalmente de su titular, deberá previamente poner a disposición de éste el aviso de privacidad, el cual debe contener un mecanismo para que, en su caso, el/la titular pueda manifestar su negativa al tratamiento de datos biométricos para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre la entidad responsable y el/la titular.

Párrafo. El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.

Artículo 35.- Cuando la entidad responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos biométricos o personales de manera automática y simultánea al tiempo que el/la titular hace contacto con los mismos, previamente deberá informar al titular sobre el uso de esas tecnologías, que a través de estas se obtienen datos biométricos y la forma en que se podrá requerir la cancelación de sus datos capturados.

Artículo 36.- Ninguna entidad privada puede recopilar, capturar, procesar y utilizar los datos biométricos de una persona o de un cliente, a menos que se cumplan las condiciones dispuestas en el artículo 58 de la Ley núm. 04-23.

Artículo 37.- No se requerirá el consentimiento para el tratamiento de los datos biométricos cuando sean cedidos a una tercera persona, cuando la cesión sea realizada para el desarrollo, cumplimiento y control del contrato. En este caso la cesión sólo será legítima en la medida en que se limite a la finalidad que le sirve de causa.

Artículo 38.- Se considerará que el consentimiento expreso se otorgó por escrito cuando el/la titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Artículo 39. Las/los responsables del tratamiento de datos biométricos deberán almacenar la prueba del consentimiento dada por el titular de los datos en un repositorio al cual la Junta Central Electoral podrá tener acceso.

Párrafo. La Junta Central Electoral podrá auditar a las instituciones públicas y privadas, que traten datos biométricos con la finalidad de verificar el cumplimiento de la presente disposición y de las demás establecidas en el presente reglamento.

Artículo 40. Las/los responsables del tratamiento de los datos biométricos deberán renovar el consentimiento anualmente, cumpliendo cada vez con los requisitos establecidos en la ley y el presente reglamento para su recaudación y registro.

Artículo 41. Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en la persona responsable del tratamiento.

Artículo 42: Los mecanismos o procedimientos que las y los responsables del tratamiento de los datos biométricos establezcan para atender las solicitudes de revocación del consentimiento no podrán exceder el plazo de 15 días laborables.

Artículo 43: Cuando el/la titular solicite la confirmación del cese del uso o almacenamiento de sus datos biométricos, el responsable del tratamiento deberá responder expresamente a dicha solicitud.

Artículo 44: En caso de que los datos biométricos hubiesen sido cedidos a un tercero con anterioridad a la fecha de revocación del consentimiento al responsable, este último deberá garantizar la cancelación de los datos biométricos tratados por el tercero.

Artículo 45. En caso de negativa de cancelar los datos biométricos tratados por un responsable o un cesionario en razón de la revocación del consentimiento.

Sección II. Del aviso de Privacidad

Artículo 46. Para la difusión de los avisos de privacidad, el/la responsable del tratamiento de los datos biométricos podrán valerse de formatos físicos, electrónicos o cualquier otra tecnología, siempre que garantice las disposiciones sobre el consentimiento y su procedimiento de obtención.

Artículo 49. Cuando los datos biométricos sean obtenidos directamente del o la titular, el/la responsable deberá proporcionar de manera inmediata al menos la siguiente información:

a) La identidad y domicilio del o la responsable del tratamiento;
b) Las finalidades del tratamiento;
c) Los mecanismos que las entidades responsables deben de ofrecer para que el/la titular conozca el aviso de privacidad, de conformidad con el presente reglamento; y
d) Los cesionarios que tratarán sus datos biométricos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo I. La divulgación inmediata de la información antes señalada no exime al responsable de la obligación de proveer los mecanismos para que él o la titular conozca el contenido del aviso de privacidad, de conformidad con el artículo 26 del presente Reglamento.

Artículo 50. Cuando los datos biométricos sean obtenidos de manera indirecta del o la titular, la entidad responsable del tratamiento de los datos biométricos deberá observar lo siguiente para la puesta a disposición del aviso de privacidad:

a) Cuando los datos biométricos sean tratados para una finalidad prevista en una cesión consentida o se hayan obtenido de una fuente de acceso público, el aviso de privacidad se deberá dar a conocer en el primer contacto que se tenga con él o la titular, o

b) Cuando el responsable del tratamiento pretenda utilizar los datos para una finalidad distinta a la consentida, es decir, vaya a tener lugar un cambio de finalidad, se debe recabar el consentimiento del titular de los datos y en el aviso de privacidad deberá darse a conocer previo el aprovechamiento de estos.

CAPÍTULO 3.- DEL TRATAMIENTO DE LOS DATOS BIOMÉTRICOS

Sección I. De los usos y finalidades del uso de los datos biométricos

Artículo 51.- El responsable del tratamiento de los datos biométricos podrá utilizar dichos datos para los siguientes usos y finalidades:

a) **Identificación biométrica:** Se realizará la identificación de una persona desconocida mediante la comparación de sus datos biométricos con una base de datos de referencia compuesta por un conjunto amplio de datos biométricos. Esta comparación puede realizarse en un enfoque 1 a N, es decir, comparando los datos biométricos con múltiples registros de la base de datos para encontrar una coincidencia.

b) **Verificación de identidad:** Los datos biométricos serán utilizados para verificar si una persona es quien afirma ser. Esta verificación se realizará comparando los datos biométricos proporcionados por la persona en el momento con los datos almacenados en una base de datos previamente establecida para tal fin. En este caso, la comparación se realiza en un enfoque 1 a 1, es decir, comparando los datos biométricos con un único registro de la base de datos para validar la identidad afirmada.

c) **Autenticación de identidad:** Se utilizarán los datos biométricos de una persona para verificar y confirmar de manera inequívoca su identidad. Esto implica comparar los datos biométricos de la persona con los datos previamente almacenados y autenticados en una base de datos. Al igual que en la verificación de identidad, esta comparación se realiza en un enfoque 1 a 1 para asegurar la autenticidad de la identidad afirmada.

d) **Control de acceso y asistencia:** Los datos biométricos podrán utilizarse para controlar el acceso a las instalaciones físicas, sistemas de información y equipos tecnológicos, y registrar la asistencia de

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

empleados, clientes y relacionados. Esto se llevará a cabo mediante el escaneo de huellas dactilares o reconocimiento facial.

e) **Seguridad nacional:** Los datos biométricos se utilizarán en aplicaciones de seguridad nacional, como el control de fronteras, la identificación de individuos de interés para la seguridad del país, la prevención de actividades terroristas y la protección de infraestructuras críticas.

f) **Prevención de fraudes:** Se utilizarán los datos biométricos para prevenir fraudes al verificar la identidad de una persona en transacciones financieras, registro de votantes y emisión de documentos oficiales como pasaportes o licencias de conducir.

g) **Investigación forense:** Los datos biométricos se utilizarán en investigaciones forenses para identificar a posibles sospechosos, mediante comparaciones con muestras recolectadas en la escena del crimen.

h) **Cumplimiento de obligaciones legales y reglamentarias:** Para cumplir con las obligaciones legales y reglamentarias impuestas a las entidades públicas y privadas en relación con la identificación y verificación de la identidad de las personas.

Artículo 52.- Limitaciones en el uso de los datos biométricos. El uso de datos biométricos por parte del responsable del tratamiento de los datos biométricos estará sujeto a las siguientes limitaciones:

a) **Proporcionalidad:** El tratamiento y uso de datos biométricos sólo será admisible si es necesario y proporcional a la finalidad perseguida, y si no existen alternativas menos intrusivas que puedan alcanzar la misma finalidad de manera efectiva.

b) **Minimización de datos:** Los responsables del tratamiento deberán limitar la recopilación y el uso de datos biométricos al mínimo necesario para cumplir con la finalidad perseguida.

c) **Transparencia:** Los responsables del tratamiento deberán informar a las personas de manera clara y accesible sobre la recopilación y el uso de sus datos biométricos, incluyendo las finalidades específicas y las medidas de seguridad adoptadas.

d) **Consentimiento**: Salvo en los casos en que la ley lo autorice expresamente, el tratamiento y uso de datos biométricos requerirá el consentimiento previo, informado e inequívoco de la persona afectada.

e) **Protección de los derechos de las y los interesados:** Los responsables del tratamiento deberán garantizar que las personas cuyos datos biométricos sean tratados puedan ejercer sus derechos de acceso, rectificación, supresión, limitación del tratamiento portabilidad y oposición, de acuerdo con la legislación aplicable.

Sección II. De la recolección y procesamiento de los datos biométricos

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Artículo 53. Recolección de datos biométricos. La recolección de los datos biométricos solo será permitida si se cumplen las siguientes condiciones:

a) **Consentimiento**: El titular de los datos biométricos ha otorgado su consentimiento expreso, informado e inequívoco para compartir sus datos biométricos con el tercero en cuestión, salvo en los casos en que la ley lo autorice expresamente.

b) **Finalidad legítima:** El tercero tiene una finalidad legítima y específica para acceder a los datos biométricos, que es compatible con las finalidades para las cuales los datos fueron recopilados originalmente.

c) **Garantías contractuales:** Existe un contrato entre la entidad o persona responsable del tratamiento de los datos biométricos y el tercero que establece las condiciones y garantías para el acceso y uso de los datos biométricos, incluyendo medidas de seguridad adecuadas y compromisos para respetar los derechos de los titulares de los datos.

d) **Fundamento legal:** Que la recolección de datos biométricos esté expresamente contemplada y autorizada por una ley aplicable que defina las condiciones y límites bajo los cuales dicha recolección es permitida, garantizando el respeto a los derechos y libertades fundamentales de los titulares de los datos biométricos, así como la protección de su privacidad y seguridad.

Sección III. De la cesión de los datos biométricos

Artículo 54. Cesión de datos biométricos. Solo se realizarán cesión de datos biométricos que sean objeto de tratamiento o vayan a serlo tras su cesión, con el consentimiento del o la titular, que ostenten una finalidad legítima y para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

Párrafo I. El consentimiento para la cesión es revocable.

Párrafo II. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la inobservancia de las mismas ante el organismo de control y el/la titular de los datos de que se trate.

Párrafo III. El cesionario no podrá ceder a terceros los datos biométricos cedidos a este por el cedente.

Artículo 55. Excepciones del consentimiento para la cesión de datos biométricos. Toda cesión de datos biométricos se encuentra sujeta al consentimiento de su titular, salvo las excepciones establecidas en el artículo 57 de la Ley núm. 04-23.

Artículo 56. Prueba de cumplimiento de obligaciones en materia de cesión. Para efectos de demostrar que la cesión se realizó conforme a lo que establece la ley y el presente reglamento la carga de la prueba recaerá, en todos los casos, en el/la responsable que transfiere y en el receptor de los datos biométricos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Artículo 57. Medidas de seguridad. De conformidad con lo establecido en el presente reglamento, el responsable de tratamiento de datos biométricos debe adoptar las medidas de seguridad técnicas y organizativas para garantizar la protección y confidencialidad de los datos, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Párrafo I. Queda prohibido registrar y almacenar datos biométricos en archivos, registros o bancos de datos que no reúnan las condiciones técnicas de integridad y seguridad establecidas en el presente reglamento.

Párrafo II. Los terceros deben de notificar a la organización cedente sobre cualquier incidente de seguridad que afecte los datos biométricos cedidos en un plazo de 7 días calendarios.

Artículo 58.- Del registro de la transmisión de los datos biométricos a terceros. El responsable del tratamiento de los datos biométricos deberá llevar un registro de todas las cesiones y transmisiones de datos biométricos a terceros, que incluya información sobre la identidad del tercero, la finalidad de la transmisión, las garantías contractuales establecidas y, si corresponde, el consentimiento del titular de los datos.

Párrafo. La JCE podrá requerir acceso o copia de este registro si lo considera necesario.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Sección IV. Del almacenamiento y eliminación de los datos biométricos

Artículo 59.- El responsable del tratamiento de datos biométricos deberá garantizar el almacenamiento seguro y protegido de dichos datos, a través del cumplimiento de las siguientes condiciones:

a) **Encriptación:** Los datos biométricos serán almacenados utilizando técnicas de encriptación adecuadas, que protejan su confidencialidad e integridad.

b) **Medidas de seguridad:** Se implementarán las medidas de seguridad físicas y lógicas apropiadas para prevenir accesos no autorizados, alteraciones, pérdidas o destrucción de los datos biométricos almacenados contenidas en este reglamento.

c) **Política de retención:** Se establecerá una política de retención de datos que defina los plazos de conservación de los datos biométricos, de acuerdo con las finalidades para las cuales fueron recopilados y las obligaciones legales aplicables en la legislación y el presente reglamento.

d) **Registro de actividades de tratamiento**: Se deberá mantener registros de todas las actividades de tratamiento relacionadas con el almacenamiento de datos biométricos, incluyendo las medidas de seguridad adoptadas y los accesos realizados.

Artículo 60. Los plazos de conservación de los datos biométricos no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate, lo establecido en este reglamento y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
Párrafo. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable del tratamiento de los datos biométricos deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión.

Artículo 61. El responsable del tratamiento de datos biométricos establecerá y documentará procedimientos para la conservación de los datos biométricos, que incluyan los periodos de conservación de los mismos, de conformidad con el artículo anterior.

Artículo 62. Los datos biométricos sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad.

Párrafo. La finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, con claridad, sin lugar a confusión y de manera objetiva y especifica.

Artículo 63.- Eliminación de datos biométricos. La eliminación de datos biométricos deberá realizarse garantizando su adecuada protección y destrucción cuando ya no sean necesarios.

Artículo 64.- La eliminación de los datos biométricos deberá ser realizada cumpliendo con lo siguiente:

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

a) **Criterios de eliminación:** Los datos biométricos deberán eliminarse cuando ya no sean necesarios para la finalidad para la cual fueron recopilados, o cuando el titular de los datos lo solicite y no exista ninguna obligación legal que impida su eliminación.

b) **Procedimientos de eliminación:** El responsable del tratamiento de datos biométricos deberá establecer procedimientos adecuados para garantizar la eliminación segura y definitiva de los datos biométricos, de manera que no puedan ser recuperados ni reconstruidos.

c) **Registro de eliminaciones**: El responsable del tratamiento de datos biométricos deberá llevar un registro de las eliminaciones realizadas, que incluya información sobre la fecha, el motivo de la eliminación y las medidas adoptadas para garantizar la eliminación segura de los datos.

d) **Responsabilidad en la eliminación**: El responsable del tratamiento de los datos biométricos será responsable de garantizar la correcta eliminación de los datos biométricos y de demostrar dicho cumplimiento ante la autoridad competente.

CAPÍTULO 4.- DEL SERVICIO DE AUTENTICACIÓN BIOMETRICA PROVISTO POR LA JUNTA CENTRAL ELECTORAL

Sección I: Del alcance, características y condiciones del servicio

Artículo 65. Del servicio. El servicio de autenticación de identidad se refiere a la certificación o confirmación de la identidad de una persona física mediante el uso de información biométrica y/o de información personal de identificación.

Artículo 66. La Junta Central Electoral tiene la potestad exclusiva de proveer el servicio autenticación y certificación de la identidad de las personas mediante el uso de los datos biométricos.

Artículo 67. Tipos de datos. Los datos que se pueden utilizar para la prestación del servicio de autenticación de identidad pueden incluir información biométrica, como huellas dactilares, fotos del rostro, iris, voz y/o información personal de identificación, tales como, nombres y apellidos, fecha de nacimiento, número único de identidad (NUI), número de cédula de identidad y electoral y lugar de nacimiento y otros datos que la Junta Central Electoral disponga que permitan la autenticación.

Párrafo I: Los datos biométricos no recolectados por la Junta Central Electoral para fines de autenticación y certificación de la identidad de las personas, podrán ser recolectados y utilizados por los responsables del tratamiento de los datos, respetando los principios para el tratamiento de datos biométricos, los derechos de las personas y siguiendo las directrices establecidas en el presente reglamento.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo II. Los responsables del tratamiento deberán garantizar la confidencialidad, integridad y disponibilidad de los datos, así como adoptar las medidas técnicas y organizativas adecuadas para prevenir el acceso no autorizado, la alteración, divulgación o destrucción de dichos datos.

Párrafo III: Ninguna entidad pública o privada puede ofrecer a terceros el servicio de autenticación y certificación de la identidad de las personas a partir de datos biométricos no recolectados por la Junta Central Electoral.

Artículo 68. Características del servicio. El servicio de autenticación biométrica proporcionado por la Junta Central Electoral se regirá tanto por los principios establecidos en el presente reglamento como por las siguientes características:

a) **Precisión y fiabilidad:** El servicio de autenticación biométrica garantizará una alta precisión y confiabilidad en la verificación de la identidad de los individuos. Se emplearán algoritmos y tecnologías avanzadas para minimizar los errores de identificación y falsas coincidencias.

b) **Multimodalidad:** El servicio de autenticación admitirá múltiples modalidades biométricas, como huellas dactilares y reconocimiento facial en principio, pudiendo incorporar otros datos biométricos en el futuro, con el objetivo de proteger la identidad de las personas y adaptarse a las necesidades del órgano y las entidades que requieren el servicio de autenticación biométrica.

c) **Escalabilidad y alta disponibilidad:** El servicio estará diseñado para ser escalable, permitiendo gestionar grandes volúmenes de datos biométricos y atender un número creciente de usuarios y usuarias sin comprometer su rendimiento y eficiencia. Asimismo, se garantizará una alta disponibilidad del servicio, minimizando los tiempos de inactividad y asegurando su operatividad continua.

d) **Seguridad de datos:** Se implementarán medidas de seguridad robustas para proteger la integridad, confidencialidad y disponibilidad de los datos biométricos. Se utilizarán técnicas de encriptación, almacenamiento seguro y transmisión protegida de los datos biométricos, en cumplimiento con lo establecido en el presente reglamento.

e) **Interoperabilidad:** El servicio será compatible con estándares y protocolos reconocidos a nivel nacional e internacional, facilitando la integración con otros sistemas y bases de datos biométricos existentes en entes autorizados, con el objetivo de promover la interoperabilidad y el intercambio seguro de información biométrica.

f) **Usabilidad:** El servicio se diseñará de manera intuitiva y amigable para los usuarios y usuarias, facilitando la correcta captura y verificación de los datos biométricos. Se brindará la asistencia adecuada a los entes que utilicen el servicio, con el fin de maximizar su correcta utilización.

g) **Mantenimiento y actualización:** Se establecerá un plan de mantenimiento y actualización periódica del sistema que soporta el servicio de autenticación biométrica, con el fin de asegurar su óptimo funcionamiento, mejorar la precisión y adaptarse a los avances tecnológicos y nuevos requerimientos normativos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

h) **No cesión:** El servicio de autenticación biométrica proporcionado por la Junta Central Electoral no implicará la cesión total o parcial de los datos biométricos de las personas a terceros. Los datos biométricos se utilizarán exclusivamente para la identificación, verificación y autenticación de la identidad de las personas en el contexto y los fines autorizados.

i) **Exclusividad y control:** El servicio de autenticación biométrica se proporciona bajo el principio de exclusividad y control. La Junta Central Electoral es la institución con la potestad exclusiva de otorgar el servicio de autenticación biométrica y mantendrá el control y la custodia de los datos biométricos en todo momento, y ejercerá un estricto control sobre el acceso y uso de los datos biométricos, asegurando su confidencialidad y privacidad.

Artículo 69. Condiciones para la utilización del servicio. Para acceder al servicio de autenticación biométrica provisto por la Junta Central Electoral, los responsables del tratamiento de los datos biométricos deberán cumplir con los siguientes requisitos:

a) Ser una entidad pública o privada legalmente constituida y debidamente registrada, con capacidad jurídica para celebrar contratos y cumplir con las obligaciones establecidas en este reglamento.

b) Contar con una justificación clara y legítima para el uso del servicio de autenticación biométrica, relacionada con sus actividades y finalidades específicas, y en cumplimiento de la normativa aplicable.

c) Demostrar la implementación de medidas de seguridad adecuadas para proteger los datos biométricos y garantizar su confidencialidad, integridad y disponibilidad, de acuerdo con los estándares y requisitos establecidos en este reglamento, así como los estándares de gestión y transferencia de datos requeridos para la interoperabilidad entre sistemas.

d) Designar a una o un delegado de protección de datos, encargado de supervisar y garantizar el cumplimiento de las disposiciones legales y normativas en materia de protección de datos personales y privacidad.

e) Firmar un contrato o acuerdo con la institución, en el que se establecerán las condiciones, responsabilidades y obligaciones de ambas partes, así como los niveles de requerimientos de seguridad y las medidas de salvaguardia de los datos biométricos.

f) Proporcionar la información y documentación necesaria que respalde la veracidad y legalidad de las actividades y fines para los cuales se utilizará el servicio de autenticación biométrica.

g) Comprometerse a no ceder, ni crear bases de datos a partir del almacenamiento de los datos biométricos y otros datos de identidad de las personas registrados en las bases de datos de la Junta Central Electoral.

Artículo 70. Evaluación previa. La Junta Central Electoral realizará una evaluación de los entes solicitantes para determinar su idoneidad y cumplimiento de los requisitos establecidos. Esta evaluación podrá incluir la revisión de la documentación presentada, visitas de inspección, pruebas de seguridad, entre otros mecanismos que permitan verificar el cumplimiento de los requisitos establecidos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo: La institución se reserva el derecho de aceptar o rechazar las solicitudes de acceso al servicio de autenticación biométrica, basándose en la evaluación realizada y en cumplimiento de la normativa vigente.

Artículo 71. En caso de ser aceptada la solicitud, la Junta Central Electoral proporcionará al ente solicitante las credenciales de acceso y los protocolos de conexión necesarios para utilizar el servicio de autenticación biométrica. Estas credenciales son de carácter personal e intransferible, y su uso deberá restringirse al personal autorizado del ente solicitante.

Sección II: Del procedimiento de solicitud del servicio de autenticación

Artículo 72. Solicitud del servicio. Las entidades interesadas en utilizar el servicio de autenticación biométrica deberán presentar una solicitud por escrito ante la Junta Central Electoral.

Párrafo II: La solicitud deberá incluir información detallada sobre la entidad solicitante, incluyendo su nombre, dirección, representante legal, contacto principal, el tipo de servicio solicitado y la finalidad del uso de este.

Artículo 73. Verificación de legitimidad. La Junta Central Electoral realizará una evaluación de la legitimidad de la entidad solicitante, con el fin de garantizar que cumpla con los requisitos establecidos en el reglamento.

Párrafo. Se podrán solicitar documentos y evidencias adicionales que respalden la legitimidad y el propósito del uso del servicio de autenticación biométrica.

Artículo 74. Evaluación de requisitos. Una vez verificada la legitimidad de la entidad solicitante, la Junta Central Electoral realizará una evaluación de los requisitos técnicos y de seguridad necesarios para la activación del servicio.

Párrafo. Esta evaluación puede incluir la revisión de la infraestructura tecnológica, la capacidad de almacenamiento de datos biométricos, la implementación de medidas de seguridad y la adecuación a los estándares y normativas vigentes.

Artículo 75. Acuerdo de provisión de servicios de consulta biométrica. Una vez completada la evaluación de requisitos, se firmará un contrato de servicio o establecerá un acuerdo entre la Junta Central Electoral y la entidad solicitante.

Párrafo. El contrato de servicio, acuerdo o convenio deberá establecer los términos y condiciones específicos del uso del servicio de autenticación biométrica, incluyendo las responsabilidades de ambas partes, la protección de datos personales, la confidencialidad y las obligaciones financieras.

Artículo 76. Pruebas, revisión y adecuación interna. La entidad solicitante contará con un periodo de revisión interna y adecuación de sus sistemas e infraestructura antes de la activación completa del servicio.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo I. Durante este periodo, la entidad solicitante podrá realizar las calibraciones y ajustes necesarios para garantizar la correcta integración y funcionamiento del sistema de autenticación biométrica con sus propios sistemas y procesos.

Párrafo II. La Junta Central Electoral podrá brindar orientación y soporte técnico durante el proceso de adecuación.

Párrafo III. Los dispositivos biométricos utilizados para la captura y verificación de los datos biométricos deberán cumplir con las especificaciones técnicas requeridas por la Junta Central Electoral.

Artículo 77. Activación del servicio. Una vez completados los pasos anteriores, la Junta Central Electoral activará el servicio de autenticación biométrica para la entidad solicitante y proporcionará las credenciales y claves de acceso necesarias para que la entidad pueda comenzar a utilizar el servicio de manera segura y confiable.

Sección III: De las obligaciones de las entidades usuarias del servicio de autenticación

Artículo 78. Responsabilidades y obligaciones. Las entidades usuarias del servicio tendrán las siguientes responsabilidades y obligaciones en relación con el servicio de autenticación biométrica:

a) **Protección y custodia de los datos biométricos:** Los usuarios y usuarias del servicio deberán garantizar la adecuada protección y custodia de los datos biométricos de los individuos registrados. Está estrictamente prohibido crear bases de datos con informaciones relativas al registro del estado civil de las personas y sus datos biométricos en contravención con lo dispuesto en la Ley No. 4-23.

b) **Uso adecuado de los dispositivos y sistemas**: Los usuarios y usuarias del servicio deberán utilizar los dispositivos biométricos y sistemas de autenticación de manera correcta y conforme a las recomendaciones proporcionadas por la Junta Central Electoral. Se deberán seguir las mejores prácticas de seguridad y privacidad en el manejo de los dispositivos y sistemas, evitando cualquier mal uso o manipulación indebida.

c) **Notificación de incidentes de seguridad:** En caso de que se produzca cualquier incidente de seguridad relacionado con el servicio de autenticación biométrica, las entidades usuarias deberán notificar la Junta Central Electoral en un plazo máximo de 72 horas. Esta notificación deberá incluir detalles sobre el incidente, su naturaleza, las personas afectadas, si las hubiere, las medidas correctivas adoptadas y las acciones preventivas implementadas para evitar futuros incidentes. Si el incidente de seguridad implica un alto riesgo para los derechos y libertades de las y los individuos, los usuarios y usuarias del servicio deben informar a las personas afectadas en un plazo máximo de 1 semana, proporcionando detalles sobre el incidente y las medidas tomadas para abordarlo.

d) **Cumplimiento de las disposiciones legales y normativas:** Los usuarios y usuarias del servicio deberán cumplir con todas las disposiciones legales y normativas aplicables en materia de protección de datos personales, seguridad de la información y cualquier otra regulación relacionada con el uso del servicio de autenticación biométrica.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

e) **Colaboración en auditorías y verificaciones:** Los usuarios y usuarias del servicio deberán colaborar con la Junta Central Electoral en la realización de auditorías y verificaciones periódicas del servicio de autenticación biométrica. Esto incluirá proporcionar la información y los datos solicitados, así como permitir el acceso a sus instalaciones y sistemas relacionados con el servicio.

f) **Confidencialidad y no divulgación.** Los usuarios y usuarias del servicio se comprometen a mantener la confidencialidad de la información y datos a los que tengan acceso en el marco del servicio de autenticación biométrica. Está terminantemente prohibida la divulgación, compartición de dicha información a terceros sin el consentimiento expreso de la Junta Central Electoral y de conformidad con la normativa vigente.

Sección IV: De las medidas de seguridad

Artículo 79. Medidas de seguridad. Las entidades usuarias del servicio de autenticación biométrica deberán adoptar medidas adecuadas para proteger y prevenir cualquier forma de acceso no autorizado a los datos biométricos y garantizar la integridad de estos. Esto incluye la implementación de las siguientes medidas:

1. **Seguridad y protección de datos:**

   a) **Privacidad por diseño.** El responsable de tratamiento de datos biométricos que almacene datos biométricos deberá integrar medidas de protección de datos y privacidad desde la etapa de diseño y planificación de cualquier sistema, producto o servicio que implique el procesamiento de datos biométricos.

   b) **Seudonimización**. Las bases de datos biométricos deberán cumplir con la segregación de datos y la encriptación como medidas mínimas de seudonimización, sin perjuicio de la implementación de otras.

   c) **Encriptación.** Los datos biométricos deben ser encriptados tanto en tránsito como en reposo para garantizar su confidencialidad e integridad.

   d) **Segregación de datos.** La información personal identificable y los datos biométricos de las personas siempre estarán en bases de datos separadas. Se vincularán sólo mediante identificadores únicos y seguros para dificultar la asociación directa entre los datos biométricos y las personas a las que pertenecen.

   e) **Monitoreo y registro del tratamiento de datos biométricos.** El responsable de tratamiento de datos biométricos deberá establecer mecanismos de monitorización y registro de todas las actividades de tratamiento y acceso a los datos biométricos para detectar y prevenir actividades sospechosas o no autorizadas.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

f) **Respaldo y recuperación de datos.** El responsable de tratamiento de datos biométricos deberá implementar soluciones de respaldo y recuperación de datos para garantizar la disponibilidad de los datos biométricos en caso de incidentes de seguridad o fallos del sistema.

g) **Evaluación de riesgos**: El responsable de tratamiento de datos biométricos deberá realizar evaluaciones periódicas de riesgos y pruebas de penetración para identificar y abordar posibles vulnerabilidades en los sistemas de tratamiento de datos biométricos.

h) **Formación y concienciación:** El responsable de tratamiento de datos biométricos deberá capacitar al personal y a los usuarios y usuarias finales sobre la importancia de la protección de datos personales y las políticas y procedimientos de seguridad aplicables.

i) **Políticas y procedimientos internos.** El responsable de tratamiento de datos biométricos deberá establecer políticas y procedimientos internos para garantizar el cumplimiento de las disposiciones de protección de datos y seguridad de este reglamento y la demás legislación y reglamentación en la materia.

2. Seguridad de sistemas y redes

a) **Detección de intrusiones y prevención**: El responsable de tratamiento de datos biométricos que almacene datos biométricos deberá implementar sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear y proteger las redes y sistemas que almacenan y procesan datos biométricos de actividades maliciosas y accesos no autorizados.

b) **Seguridad de aplicaciones**: El responsable de tratamiento de datos biométricos deberá garantizar que las aplicaciones que procesan y almacenan datos biométricos estén diseñadas y desarrolladas siguiendo prácticas seguras de codificación y estén protegidas contra vulnerabilidades conocidas y potenciales.

c) **Protección de perímetro**: El responsable de tratamiento de datos biométricos deberá establecer firewalls, Sistemas de Prevención de Fugas de Datos (DLP) y otras tecnologías de protección de perímetro para proteger las redes y sistemas que contienen datos biométricos de accesos no autorizados y ataques externos.

d) **Gestión de parches y actualizaciones**: El responsable de tratamiento de datos biométricos deberá mantener los sistemas y software actualizados con las últimas versiones y parches de seguridad para proteger los datos biométricos de vulnerabilidades conocidas.

3. Seguridad física y control de acceso

a) **Seguridad física**: El responsable de tratamiento de datos biométricos deberá implementar medidas de seguridad física, como el control de acceso a áreas donde se almacenan y procesan datos biométricos, la protección contra incendios, inundaciones y otras amenazas físicas.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

b) **Política de dispositivos y uso de medios extraíbles**: El responsable de tratamiento de datos biométricos deberá establecer políticas y procedimientos para el uso seguro de dispositivos y medios extraíbles que puedan contener datos biométricos para prevenir la pérdida o el robo de información.

4. Auditoría, cumplimiento y continuidad

a) **Auditorías y revisiones de seguridad**: El responsable de tratamiento de datos biométricos deberá realizar auditorías y revisiones de seguridad periódicas para evaluar la eficacia de las medidas de seguridad implementadas y garantizar el cumplimiento de las normas y regulaciones aplicables.

b) **Gestión de proveedores y terceros**: El responsable de tratamiento de datos biométricos deberá establecer políticas y procedimientos para evaluar y monitorear la seguridad de los proveedores y terceros que acceden o procesan datos biométricos para garantizar que cumplan con los requisitos de seguridad y protección de datos aplicables.

c) Planificación de la continuidad del negocio y recuperación ante desastres: La Junta Central Electoral implementará un plan de continuidad del negocio y recuperación ante desastres para garantizar la disponibilidad y recuperación de datos biométricos en caso de interrupciones imprevistas o desastres**.**

Artículo 80.- La Junta Central Electoral contará con un Plan de Continuidad del Negocio y Recuperación ante Desastres (CNRD) donde se contemplen políticas y procedimientos para garantizar la disponibilidad y recuperación de los datos biométricos en caso de interrupciones imprevistas o desastres, protegiendo la confidencialidad, integridad y disponibilidad de la información.

Artículo 81. Terminación del servicio. En caso de finalizar el acuerdo o contrato de servicio entre la Junta Central Electoral y el usuario del servicio de autenticación biométrica, la Junta Central Electoral podrá realizar auditorías y verificaciones posteriores a la terminación del servicio con el propósito de asegurarse de que no se haya realizado ninguna creación de bases de datos a partir de la información de identidad de las personas gestionada por la JCE.

Párrafo. Estas auditorías y verificaciones se llevarán a cabo con el fin de garantizar la integridad y seguridad de los datos personales y prevenir cualquier mal uso o divulgación no autorizada de la información.

Sección V. De las evaluaciones de impacto

Artículo 82.- Evaluación de impacto para el tratamiento de datos biométricos. Antes de implementar un sistema de tratamiento de datos biométricos para utilizar el servicio de autenticación biométrica provisto por la Junta Central Electoral, los responsables del tratamiento deberán llevar a cabo una evaluación de impacto. Esta evaluación tendrá como objetivo identificar y abordar los riesgos asociados al tratamiento de datos biométricos, así como implementar las medidas de protección adecuadas. En la evaluación de impacto se deberán considerar los siguientes aspectos:

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

a) **Identificación de datos biométricos:** Se deberá determinar qué datos biométricos serán tratados, asegurando que exista una justificación legal y necesidad para recopilar dichos datos.

b) **Finalidad y contexto del tratamiento:** Deberá identificarse la finalidad del tratamiento de datos biométricos y cómo se utilizarán dichos datos. Esto incluye identificar las entidades públicas y privadas involucradas, así como cualquier cesión de datos a terceros.

c) **Procesos y flujos de datos:** Se deberán analizar los procesos y flujos de datos dentro del sistema de tratamiento de datos biométricos, considerando las etapas de recopilación, almacenamiento, procesamiento y eliminación de datos.

d) **Evaluación de riesgos:** Se deberán identificar los posibles riesgos para la privacidad y seguridad de los datos biométricos, como el acceso no autorizado, divulgación indebida, alteración o pérdida de datos.

e) **Medidas de mitigación:** Se deberán identificar las medidas técnicas y organizativas adecuadas para mitigar los riesgos identificados, tales como la encriptación, control de acceso, seudonimización y medidas de seguridad física.

f) **Evaluación de impacto en los derechos y libertades:** Deberá analizarse cómo el tratamiento de datos biométricos puede afectar los derechos y libertades fundamentales de las personas, incluyendo el derecho a la privacidad y protección de datos personales.

g) **Consulta y participación de las partes interesadas:** Deberán involucrarse a las partes interesadas pertinentes, como los titulares de datos, empleados, autoridades reguladoras y expertos en protección de datos, en el proceso de evaluación de impacto, con el fin de obtener una visión completa y equilibrada de los riesgos y mitigaciones.

h) **Documentación y seguimiento:** Se deberán documentar los resultados de la evaluación de impacto, incluyendo las conclusiones y recomendaciones, y establecer un proceso de seguimiento para monitorear la efectividad de las medidas de mitigación implementadas y realizar ajustes según sea necesario.

Artículo 83. Frecuencia de las evaluaciones. Las evaluaciones de impacto deberán ser realizadas al menos una vez al año o de manera más frecuente si existen cambios significativos en el sistema de tratamiento de datos biométricos, en las finalidades del tratamiento, en los procesos y flujos de datos, o si se identifican nuevos riesgos o amenazas.

Párrafo I. Los resultados de las evaluaciones de impacto periódicas deberán ser compartidos con la Junta Central Electoral dentro de un plazo no mayor a los 30 días calendario, contados a partir de la conclusión de la referida evaluación de impacto. El objetivo de este reporte es proporcionar a la Junta Central Electoral información actualizada sobre las medidas de protección implementadas, los riesgos identificados y las medidas de mitigación adoptadas, para garantizar la transparencia y supervisión adecuada del tratamiento de datos biométricos en el marco de la provisión del servicio de autenticación biométrica.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo II. En el caso de que, durante la evaluación de impacto, la entidad responsable del tratamiento de datos biométricos y usuaria del servicio de autenticación biométrica identifique riesgos de alto impacto que requieran atención inmediata, deberá informar a la Junta Central Electoral en un plazo no mayor a 72 horas. Esta notificación deberá incluir una descripción detallada de los riesgos identificados, las acciones tomadas o propuestas para mitigarlos, y cualquier otra información relevante que pueda ayudar a la Junta Central Electoral a evaluar y tomar medidas apropiadas.

Párrafo III. La Junta Central Electoral podrá solicitar a los responsables del tratamiento de datos biométricos información adicional, aclaraciones o documentos complementarios relacionados con las evaluaciones de impacto periódicas. Los responsables del tratamiento deberán brindar toda la cooperación necesaria y proporcionar la información solicitada en el plazo establecido por la Junta Central Electoral.
Párrafo IV. En caso de que las evaluaciones de impacto periódicas identifiquen riesgos significativos para la privacidad y seguridad de los datos biométricos, la Junta Central Electoral podrá requerir a los responsables del tratamiento la adopción de medidas adicionales de protección y seguridad, para garantizar el cumplimiento de las disposiciones legales y normativas aplicables.

Párrafo V. La Junta Central Electoral establecerá lineamientos y criterios para la realización de las evaluaciones de impacto periódicas y el reporte de los resultados. Estos lineamientos podrán incluir indicadores de evaluación, formatos de reporte y plazos específicos para el envío de la información requerida.

Artículo 84. Auditorías periódicas. Para garantizar el uso adecuado del servicio de autenticación, la Junta Central Electoral se reserva el derecho de realizar auditorías periódicas (informáticas o de otro orden), con el fin de monitorear el uso y origen de los requerimientos, y el cumplimiento de lo establecido en el presente reglamento.

Sección VI: De la actualización, el monitoreo y la evaluación continua

Artículo 85. Monitoreo y evaluación continua. La Junta Central Electoral llevará a cabo un monitoreo y evaluación continua del servicio de autenticación biométrica provisto a la entidad solicitante, con el objetivo de garantizar su correcto funcionamiento y cumplimiento de los requisitos establecidos.

Artículo 86. Actualización y mantenimiento. La entidad solicitante se compromete a mantener actualizada la infraestructura tecnológica y los dispositivos biométricos utilizados en el servicio de autenticación.

Párrafo. La Junta Central Electoral brindará asistencia técnica y soporte para la resolución de problemas técnicos y actualizaciones necesarias requeridas para el correcto funcionamiento del servicio de autenticación.

Artículo 87. Protección de datos personales. Tanto la Junta Central Electoral como la entidad solicitante se comprometen a cumplir con las disposiciones legales y normativas en materia de protección de datos personales.

Párrafo. Se establecerán medidas de seguridad y procedimientos adecuados para garantizar la confidencialidad, integridad y disponibilidad de los datos biométricos.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Artículo 88. Evaluación periódica del servicio. La Junta Central Electoral realizará evaluaciones periódicas del servicio de autenticación biométrica para garantizar su eficacia y mejorar continuamente los procesos.

Párrafo. La entidad solicitante colaborará en las evaluaciones proporcionando la información y los datos solicitados.

Sección VII: De la suspensión o cancelación del servicio

Artículo 89. Causas de la suspensión o cancelación del servicio de autenticación biométrica. La Junta Central Electoral podrá suspender o cancelar el servicio de autenticación biométrica provisto a una entidad público o privado en los siguientes casos:

a) Incumplimiento de las obligaciones y responsabilidades establecidas en el contrato o acuerdo de acceso al servicio de autenticación biométrica, incluyendo el incumplimiento de los requisitos de seguridad y protección de datos biométricos establecidos en este reglamento.

b) Uso indebido o fraudulento del servicio de autenticación biométrica, incluyendo la utilización de los datos biométricos para fines distintos a los autorizados o permitidos por la normativa aplicable.

c) Pérdida de la capacidad jurídica del ente solicitante para celebrar contratos o ejercer sus actividades comerciales o profesionales de manera legal y ética.

d) Falta de pago o incumplimiento de las obligaciones financieras pactadas en el contrato o acuerdo de acceso al servicio de autenticación biométrica.

e) Violación grave de la privacidad, confidencialidad o derechos de los individuos cuyos datos biométricos son procesados en el servicio de autenticación biométrica, incluyendo la divulgación no autorizada o el acceso no autorizado a dichos datos.

f) Orden o disposición de una autoridad competente que requiera la cancelación del servicio de autenticación biométrica por razones legales, de seguridad nacional o de interés público.

Artículo 90. Notificación de la suspensión o cancelación. En caso de suspensión o cancelación del servicio de autenticación biométrica, la Junta Central Electoral notificará por escrito al ente solicitante, especificando las causas y motivos que llevaron a dicha suspensión o cancelación. El ente solicitante tendrá un plazo determinado para cesar el uso del servicio y tomar las medidas necesarias para garantizar la protección de los datos biométricos y su eliminación conforme a la normativa vigente.

Párrafo I. La suspensión o cancelación del servicio de autenticación biométrica no exime al ente solicitante de cumplir con sus obligaciones y responsabilidades derivadas del tratamiento de datos biométricos previamente realizado.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Párrafo II. El ente solicitante deberá adoptar las medidas necesarias para garantizar la protección de los datos biométricos y el cumplimiento de la normativa aplicable.

Artículo 91. Acciones legales. La Junta Central Electoral se reserva el derecho de emprender acciones legales y reclamar los daños y perjuicios ocasionados por el ente solicitante en caso de suspensión o cancelación del servicio por incumplimiento o conducta indebida.

Artículo 92. En caso de existir cláusulas adicionales o disposiciones específicas relacionadas con la suspensión o cancelación del servicio de autenticación biométrica, estas serán detalladas en el contrato o acuerdo de acceso al servicio y tendrán plena validez y efecto.

Artículo 93. Reanudación del servicio. La reanudación del servicio estará sujeta a la satisfacción de las condiciones y requisitos establecidos por la Junta Central Electoral, así como a la corrección de las deficiencias o irregularidades que dieron lugar a la suspensión o cancelación.

Artículo 94. Definición de las tasas. El pleno de la Junta Central Electoral establecerá las tasas a ser cobradas por la prestación del servicio de autenticación de identidad, teniendo en cuenta los costos y gastos en que incurra el prestador del servicio. Las tasas serán fijadas en base a la aprobación del presupuesto anual.

Artículo 95. Supervisión y control. La Junta Central Electoral llevará a cabo medidas de supervisión y control que garanticen el cumplimiento del reglamento y la protección de los datos personales. Esto incluirá la realización de auditorías, inspecciones y revisiones periódicas de la implementación del reglamento.

CAPÍTULO 5.- DE LA DIRECCIÓN DE SERVICIOS DE AUTENTICACIÓN DE LA IDENTIDAD

Artículo 96. Definición y objeto. La Dirección de Servicios de Autenticación de la Identidad es la encargada de gestionar y asegurar la calidad, eficiencia, disponibilidad y seguridad de los servicios de consulta, certificación de la identidad y autenticación biométrica provistos por la Junta Central Electoral a entidades del sector público y privado.

Artículo 97. Alcance de funciones. Dentro de las funciones de la Dirección de Servicios de Autenticación de la Identidad se encuentran las siguientes:

a. **Gestión de acuerdos y contratos de servicios:** La Dirección será responsable de gestionar y administrar los acuerdos y contratos relacionados con los servicios de consulta, certificación de la identidad y autenticación biométrica provisto por la Junta Central Electoral a entidades públicas y privadas. Esto incluirá la gestión, seguimiento y supervisión de dichos acuerdos y contratos, garantizando su cumplimiento y calidad.

b. **Desarrollo, implementación y supervisión de políticas y procedimientos:** La Dirección se encargará de desarrollar, implementar y supervisar las políticas y procedimientos relacionados con los servicios de autenticación de la identidad. Esto incluirá establecer, en coordinación con la Dirección Nacional de

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

Informática, los estándares de seguridad, privacidad y calidad, así como garantizar su aplicación y actualización constante.

c. **Evaluación, recomendación y supervisión de la implementación y funcionamiento de tecnologías biométricas y de autenticación:** La Dirección llevará a cabo la evaluación y recomendación de las tecnologías biométricas y de autenticación utilizadas en los servicios. Asimismo, supervisará su implementación, funcionamiento y mantenimiento, asegurando su eficacia, confiabilidad y cumplimiento de los estándares establecidos.

d. **Soporte técnico y asistencia:** La Dirección proporcionará soporte técnico de primera línea a las entidades usuarias de los servicios de autenticación de la identidad. Esto incluirá brindar asistencia y orientación en el uso de las tecnologías y sistemas, resolver consultas y problemas técnicos, y garantizar una experiencia de usuario satisfactoria.

e. **Gestión y fiscalización de aplicación del reglamento.** La Dirección será responsable de garantizar y fiscalizar el estricto cumplimiento de lo establecido en el presente reglamento. Esto incluirá la supervisión del manejo adecuado de los datos biométricos, la protección de la privacidad y confidencialidad de la información, y el aseguramiento de que todos los procesos y actividades se realicen de acuerdo con las normativas y estándares aplicables. Asimismo, se encargará de llevar a cabo auditorías internas para verificar el cumplimiento de las políticas y procedimientos establecidos, y de coordinar con las entidades pertinentes en caso de identificar incumplimientos o irregularidades.

f. **Auditoría y evaluación de cumplimiento:** La Dirección realizará auditorías, monitoreo y evaluación periódica del cumplimiento de los servicios de autenticación de la identidad. Esto incluirá revisar y analizar los registros, verificar el cumplimiento de los procedimientos establecidos, identificar áreas de mejora y aplicar las medidas correctivas necesarias.

g. **Relaciones externas y colaboración con entidades externas relacionadas con la autenticación de la identidad:** La Dirección establecerá y mantendrá relaciones externas con entidades relacionadas con la autenticación de la identidad, como proveedores de tecnología, organismos reguladores y otros actores relevantes. Asimismo, colaborará con estas entidades en proyectos, intercambio de información y buenas prácticas para promover la mejora continua de los servicios de autenticación.

h. **Protección de datos personales:** Desarrollar e implementar las políticas de protección de datos personales emanadas tanto de la Junta Central Electoral y demás estamentos del estado a través de la Oficina del Delegado de Protección de Datos de la Junta Central Electoral, la cual está subordinada a la Dirección.

i. **Investigación y desarrollo:** La Dirección debería impulsar la investigación y el desarrollo en el campo de la autenticación biométrica, con el objetivo de mejorar constantemente los servicios ofrecidos. Esto implicaría el diseño de nuevos servicios, la exploración de nuevas tecnologías, técnicas de análisis y aplicaciones innovadoras en el ámbito de la autenticación de identidad.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

j. **Cualquier otra función requerida por el Pleno de la Junta Central Electoral:** La Dirección estará sujeta a las directrices y requerimientos establecidos por el Pleno de la Junta Central Electoral. En caso de ser necesario, podrá asumir otras funciones adicionales para cumplir los objetivos de la Dirección y contribuir al adecuado funcionamiento de los servicios de autenticación de la identidad.

Artículo 98. La Dirección de Servicios de Autenticación de la Identidad trabajará en estrecha colaboración con la Dirección de Cedulación, la Dirección de Registro Electoral, la Dirección Nacional de Registro Civil y la Dirección Nacional de Informática para garantizar la integridad y confiabilidad de los datos biométricos, así como la correcta implementación de los procesos de autenticación.

Párrafo I. La Dirección colaborará con entidades externas relevantes y seguirá las mejores prácticas y estándares internacionales en materia de protección de datos personales y autenticación de la identidad.

Artículo 99. La estructura, funciones y responsabilidades descritas en este reglamento podrán ser modificadas o ampliadas por el Pleno de la Junta Central Electoral según las necesidades y disposiciones de la institución, siempre en cumplimiento de las leyes y regulaciones vigentes.

CAPÍTULO 6.- DE LAS EVALUACIONES Y AUDITORÍAS DE CUMPLIMIENTO

Artículo 100. Requisitos para la realización de evaluaciones y auditorías de cumplimiento. La Dirección de Servicios de Autenticación de la Identidad de la Junta Central Electoral realizará periódicamente evaluaciones y auditorías de cumplimiento, teniendo en cuenta los riesgos asociados al tratamiento de los datos biométricos y la provisión del servicio de autenticación de identidad. Asimismo, se deberán realizar evaluaciones y auditorías cuando se produzcan cambios significativos en el tratamiento de los datos biométricos o en las medidas de seguridad implementadas.

Párrafo I. La realización de evaluaciones y auditorías de cumplimiento es obligatoria para garantizar que el responsable del tratamiento de datos biométricos y las entidades usuarias del servicio de autenticación biométrica cumplan con las disposiciones del reglamento.

Párrafo II. Las entidades que utilicen los servicios de autenticación biométrica y certificación de la identidad provistos por la Junta Central Electoral, deberán proveer toda la colaboración e informaciones relevantes relacionadas con el tratamiento de datos biométricos, incluyendo políticas, procedimientos, registros y sistemas de información.

Artículo 101. Procedimiento para la evaluación y auditoría de cumplimiento. La Dirección de Servicios de Autenticación de la Identidad de la Junta Central Electoral establecerá un procedimiento para llevar a cabo las evaluaciones y auditorías de cumplimiento. Este procedimiento incluirá, al menos, lo siguiente:

a) Identificación del alcance de la evaluación y auditoría de cumplimiento.

b) Identificación de los riesgos asociados al tratamiento de los datos biométricos y la provisión del servicio de autenticación de identidad.

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

c) Selección de los controles a evaluar y auditar.

d) Selección del equipo de evaluación y auditoría.

e) Realización de la evaluación y auditoría.

f) Documentación de los resultados y elaboración de un plan de acción para abordar cualquier problema o incumplimiento identificado.

CAPÍTULO 7.- DE LA ARTICULACION Y COOPERACION INTERINSTITUCIONAL

Artículo 102. Cooperación con instituciones del sector público. La Junta Central Electoral establecerá canales de cooperación y coordinación con los entes del sector público que en el cumplimiento de sus funciones requieran del tratamiento de los datos biométricos de las personas y del uso del servicio de autenticación biométrica de la identidad provisto por la Junta Central Electoral.

Párrafo I. La Junta Central Electoral establecerá canales de cooperación y coordinación con los entes reguladores de las entidades del sector privado que para el desarrollo de sus actividades económicas requieran del tratamiento de los datos biométricos y del uso del servicio de autenticación biométrica de la identidad provisto por la Junta Central Electoral.

Párrafo II. Los canales de colaboración y cooperación tendrán por objeto promover una gestión adecuada y responsable de los datos biométricos, garantizando su protección y privacidad. Además de asegurar el cumplimiento de la legislación y normativas que regulan la recopilación, uso y manejo de los datos biométricos.

CAPÍTULO 8.- DE LAS SANCIONES

Artículo 103. Medidas de sanción. En caso de incumplimiento de las responsabilidades y obligaciones establecidas en este reglamento, la Junta Central Electoral podrá aplicar las medidas de sanción correspondientes establecidas en este reglamento, previa notificación y oportunidad de rectificación por parte de la entidad usuaria. Estas medidas pueden incluir la suspensión temporal del servicio, la imposición de multas o la terminación definitiva del acuerdo o contrato de servicio, según la gravedad de la infracción cometida.

Párrafo I. La Junta Central Electoral se reserva el derecho de ejercer acciones legales adicionales en caso de que el incumplimiento de las obligaciones por parte de la entidad usuaria cause daños o perjuicios a los usuarios y usuarias y usuarias del servicio o a terceros. Esto puede incluir la exigencia de indemnización por los daños ocasionados.

a) **Sanciones por incumplimiento:** En caso de que las entidades usuarias creen bases de datos con informaciones relativas al registro del estado civil de las personas y sus datos biométricos en

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do

contravención con lo dispuesto en la Ley No. 4-23, estarán sujetas a las sanciones y penalidades establecidas por las autoridades competentes, de acuerdo con la normativa aplicable.

DISPOSICIONES FINALES

Av. Gregorio Luperón esq. Av. 27 de Febrero, Plaza de la Bandera
Santo Domingo, República Dominicana, Tel. 809-539-5419 • www.jce.gob.do