DIPUTADA KAROL JARED GONZALEZ MARQUEZ
PRESIDENTA DE LA MESA DIRECTIVA DE
LA LXVI LEGISLATURA DEL CONGRESO
DEL ESTADO DE GUANAJUATO.
P R E S E N T E.

DIPUTADA RUTH NOEMÍ TISCAREÑO AGOITIA proponente y quienes suscriben Diputada y Diputado integrantes de la LXVI Legislatura del H. Congreso del Estado de Guanajuato y del Grupo Parlamentario del Partido Revolucionario Institucional, con fundamento en lo dispuesto en la fracción IV del artículo 56 de la Constitución Política para el Estado de Guanajuato, así como en el artículo 175, fracción II de la Ley Orgánica del Poder Legislativo del Estado de Guanajuato, someto a consideración de esta Legislatura para su aprobación, la iniciativa, por la que **SE ADICIONAN LAS FRACCIONES V Y VI AL ARTÍCULO 214-a DEL CÓDIGO PENAL DEL ESTADO DE GUANAJUATO,** conforme a la siguiente:

EXPOSICIÓN DE MOTIVOS

PROBLEMA.

La constante evolución de la tecnología ha puesto a prueba a las diversas legislaciones en el mundo. En México y en Guanajuato, no ha sido la excepción, debido a que el Código Penal de nuestro Estado, en su artículo 214-a contiene el tipo penal de usurpación de identidad, bajo los conceptos tradicionales que regían en el año 2015.

Sin embargo, el derecho humano a la identidad ha tenido una importante evolución jurídica, derivada de la necesidad de reformular su alcance y protección frente a las nuevas formas en que la identidad puede ser recabada, almacenada, utilizada y acreditada.

En este contexto, actualmente se incorpora al derecho a la identidad el concepto de soberanía digital personal, entendido como una dimensión que permite modernizar la protección de la identidad y adecuarla a los avances acelerados de la ciencia y las nuevas tecnologías. En este ámbito adquieren especial relevancia los datos biométricos, particularmente aquellos que son inmutables, es decir, que no pueden ser modificados o que no varían a lo largo de la vida de una persona, como el iris, la palma de la mano, el rostro y el ADN, entre otros.

En la actualidad, las personas proporcionan este tipo de información al realizar trámites o acceder a servicios ante instituciones gubernamentales, centros educativos, empresas públicas y privadas, organismos descentralizados, compañías telefónicas y otras instituciones, con la finalidad de acreditar y verificar de manera cierta su identidad.

No obstante, los beneficios que ofrece el uso de datos biométricos también implican nuevos riesgos para la protección de la identidad. Su disposición, facilitación, comercialización, falsificación o imitación puede realizarse mediante herramientas tecnológicas cada vez más

sofisticadas, entre ellas la Inteligencia Artificial (IA), comprometiendo la identidad de cualquier persona, con independencia de su edad.

La suplantación o usurpación de identidad, además de afectar directamente al titular de los datos, puede constituir una vía para la comisión de otros ilícitos, como el fraude o la extorsión. El riesgo se incrementa cuando los datos biométricos son obtenidos o facilitados indebidamente por quienes, debido a sus funciones, tienen acceso legítimo a ellos y posteriormente los entregan o comercializan para fines ilícitos.

Por ello, desde el Grupo Parlamentario del PRI, creemos necesario que el Código Penal contemple como circunstancias agravantes aquellos supuestos en los que la conducta se cometa aprovechando el acceso, custodia o manejo de datos biométricos de las personas, particularmente cuando exista una vulneración de la confianza depositada en quien tiene bajo su responsabilidad dicha información.

La gravedad de estas conductas no deriva únicamente de la afectación patrimonial o personal que pueda producir la suplantación de identidad, sino también de la naturaleza de los datos comprometidos y del riesgo que su utilización indebida representa para la soberanía digital personal.

La obtención o facilitación ilícita de estos datos puede, mediante actos de corrupción tanto en el sector público como en el privado, permitir que empleados o personas con acceso a sistemas de información los entreguen a cambio de compensaciones económicas, para posteriormente ser comercializados en mercados ilícitos de datos personales y utilizados con fines de extorsión, fraude o suplantación de identidad, incluso mediante herramientas de Inteligencia Artificial.

En consecuencia, los supuestos que se proponen incorporar como agravantes responden a la especial gravedad que adquiere el delito cuando se vulnera la confianza derivada del acceso legítimo a datos biométricos, así como al riesgo que su disposición indebida representa para la identidad y la seguridad de las personas. Se trata, por tanto, de fortalecer la protección penal frente a conductas que, por los medios empleados, la naturaleza de los datos afectados o la calidad de quien interviene en su obtención o facilitación, producen una lesión particularmente grave a los derechos de sus titulares.

JUSTIFICACIÓN.

La identidad como acto jurídico.

El registro de nacimiento es el acto jurídico a través del cual el Estado cumple con la obligación de garantizar a todas las personas el derecho a la identidad, al nombre y a su filiación familiar, cultural y nacional.

A través de este acto, se garantiza a una persona el reconocimiento administrativo de su existencia y personalidad jurídica.

La importancia del registro de nacimiento y del derecho a la identidad, principalmente entre la población infantil, de acuerdo con el Comité de Derechos Humanos, estriba en sus funciones como medida de protección frente a crímenes que pudieran comprometer su integridad, así como servir de acceso a otros derechos que se relacionan con el desarrollo integral y la garantía de disfrute de condiciones de vida digna para niños y niñas o cualquier persona adulta.

El derecho a la identidad, como concepto.

El derecho a la identidad de una persona es el conjunto de rasgos, datos biológicos, culturales y jurídicos (nombre, género, nacionalidad y filiación) que permiten individualizarla en la sociedad, garantizando su dignidad y su derecho a autodeterminar su propio proyecto de vida.

Enfoques Teóricos:

- **Identidad Jurídica:** Referente a los atributos de la personalidad (nombre, estado civil, nacionalidad) que el Estado reconoce para otorgar capacidad de goce y ejercicio.

- **Identidad Ontológica y Personal:** Los elementos psicológicos, sociales y biológicos que hacen a una persona única. Incluye el libre desarrollo de la personalidad y la identidad de género.

La Suprema Corte de Justicia de la Nación (SCJN) ha establecido tradicionalmente que el derecho a la identidad está íntimamente ligado a la dignidad humana y abarca diversas vertientes:

- **Derecho al Origen Biológico:** La Primera Sala sostiene que conocer el origen biológico es de gran trascendencia jurídica y psicológica. Conocer a los padres biológicos contribuye al adecuado desarrollo de la personalidad.

- **Derecho a la Identidad Personal y Sexual:** La Corte reconoce que la identidad personal es el derecho de todo individuo a ser uno mismo, comprendiendo la identidad de género. El Estado debe garantizar la autodeterminación y el reconocimiento de cómo una persona se asume.

- **Derecho Humano al Nombre:** Considerado un elemento determinante de la identidad. Fija la identidad en las relaciones sociales y ante el Estado, siendo una derivación integral de la expresión de la individualidad.

La identidad en general es pues, la necesidad y la capacidad que tiene una persona de encontrar lazos psicológicos, sociales, culturales y grupos humanos como familia, una sociedad y una nación.

De igual forma, constituye la capacidad de encontrar su propio lugar en todos los aspectos mencionados en sí mismo e involucrarlos en su desarrollo personal.

Ante esto, el derecho a la identidad establece y regula la necesidad de identificación de una persona frente al Estado, que lo individualiza, reconoce y protege en su derecho subjetivo. Esto es inherente a los aspectos que involucran la identidad como el nombre y la nacionalidad, así como el derecho a la personalidad jurídica.

Por eso, el derecho a la personalidad jurídica que permite que cada individuo tenga plena capacidad de ser sujeto de derechos y obligaciones. El hecho de que a la persona se le reconozca esta capacidad para exigir que se respete y garanticen sus derechos, tiene una clara vinculación con el derecho a la identidad personal, pues la persona actúa en nombre propio y con el carácter único en la sociedad y para el ordenamiento jurídico.

En consecuencia, el derecho a la personalidad jurídica implica el reconocimiento a la capacidad o habilidad jurídica de las personas o entidades para que puedan actuar en esa calidad ante los órganos del Estado. Este derecho como todos los derechos humanos tiene carácter interdependiente con el resto de los derechos humanos de las personas.

El derecho a la identidad en el ámbito internacional.

Existen diversos Tratados Internacionales de los que el Estado mexicano forma parte que reconocen componentes del derecho a la identidad. Tales como el Pacto Internacional de Derechos Civiles y Políticos (PIDESCP) que desarrolla la Declaración Universal de los Derechos Humanos, en su artículo 24 numerales 1 y 2 establecen que "*todo niño será inscrito inmediatamente después de su nacimiento y deberá tener un nombre" y que "tiene derecho a adquirir una nacionalidad*."

El derecho a la identidad en el ámbito nacional.

En México, desde el año 2014 se reconoce a nivel constitucional, el derecho a la identidad al incorporarlo expresamente en el párrafo décimo primero del artículo 4º de nuestra Carta Magna, que dicta: "*Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento*".

Al respecto, el Pleno de la Suprema Corte de Justicia de la Nación al resolver las acciones de inconstitucionalidad 3/2016,7/2016 y 10/2016 presentadas por la Comisión Nacional de Derechos Humanos, ha señalado que este derecho se puede ejercer de manera gratuita, en cualquier momento, independientemente de la edad de la persona ya que "*se trata de un derecho de carácter universal, en la medida que el texto constitucional no establece ningún límite ni restricción para su titularidad, ni para su goce o ejercicio*."

Elementos tradicionales y alcances del derecho a la identidad.

El derecho a la identidad puede considerarse un derecho en sí mismo y no sólo la suma de derechos, además de ser un presupuesto para el ejercicio de otros derechos.

El derecho a la identidad es la "*el derecho fundamental de contar, desde el nacimiento, con los datos biológicos, registrales y atributos culturales que posibilitan la individualización de la persona como sujeto en la sociedad*."

Entonces se puede afirmar que el derecho a la identidad es la garantía fundamental para individualizar a una persona en concreto dentro de la sociedad y que el Estado protege con la expedición del acta de nacimiento.

El nuevo derecho humanos a proteger los datos biométricos inmutables de las personas.

i) Datos biométricos.

Los datos biométricos son características físicas, fisiológicas o de comportamiento únicas e irrepetibles de una persona que permiten identificarla o verificar su identidad de manera inequívoca. Son considerados información personal altamente sensible y se clasifican principalmente en dos categorías: físicos y conductuales.

ii) Datos biométricos inmutables.

Los datos biométricos son inmutables porque están intrínsecamente ligados a nuestra biología y anatomía física o de comportamiento.

A diferencia de una contraseña alfanumérica o un PIN, que pueden cambiarse si se ven comprometidos, factores como las huellas dactilares, el iris, la geometría facial o la voz no pueden alterarse, menos aún cambiarse o sustituirse de forma natural.

Esta inmutabilidad presenta características fundamentales:

- Origen biológico: Rasgos como el patrón del iris se forman antes del nacimiento y se mantienen estables a lo largo de toda la vida.

- Imposibilidad de reemplazo: Si una contraseña es robada, el usuario crea una nueva; si una base de datos biométrica es filtrada, el individuo no puede "cambiar" su rostro o sus huellas dactilares.

- Riesgo de fraude: Debido a que no se pueden restablecer, el robo de estos datos implica una vulnerabilidad de seguridad permanente para la persona titular.

iii). ¿Qué los constituye?

1. Datos físicos o fisiológicos:

- **Huella dactilar**: Los patrones únicos de crestas y valles en la yema de los dedos.

- **Reconocimiento facial**: Medición de las proporciones del rostro (distancia entre los ojos, forma de la mandíbula, etc.).

- **Escaneo de iris o retina**: Patrones complejos y únicos de los vasos sanguíneos en el fondo del ojo o en la capa de color.

- **Geometría de la mano y huellas palmares**: El tamaño, grosor y longitud de los dedos o las líneas de la palma.

- **ADN:** La información genética que constituye a cada individuo.

2. Datos de comportamiento:

- **Reconocimiento de voz:** Análisis del tono, la frecuencia y la textura acústica al hablar.

- **Dinámica de la firma:** El ritmo, la velocidad, la presión y los trazos al firmar.

- **Patrones de tecleo:** La velocidad y el ritmo con el que una persona escribe en un teclado.

iv). Qué son los datos biométricos.

Los datos biométricos son los datos personales relativos a las características únicas del ser humano, sean físicas, fisiológicas o asociadas al comportamiento, que faciliten y garanticen la identificación de un individuo (persona física), mediante sistemas o procedimientos tecnológicos.

Por ejemplo, son datos biométricos las huellas dactilares o la voz. El cuerpo de una persona posee gran cantidad de datos exclusivos y sensibles. Datos que pueden codificarse y almacenarse para aplicar diversos procesos de identificación.

Para que los sistemas de identificación sean realmente fiables, los datos biométricos empleados deben ser rasgos universales, inalterables y únicos. Esto significa que dichos rasgos estén presentes en todas las personas, pero que en cada una se diferencie de una forma única y, además, no cambien durante toda su vida.

v) Utilidad de los datos biométricos.

En la actualidad, los datos biométricos son ampliamente utilizados en múltiples sectores de la sociedad, como en el sector bancario, el médico, el comercial, el empresarial, etc. Entre sus diferentes usos se encuentran los siguientes:

v.1) Protección de identidad del usuario.

- La biometría tiene un papel clave en la protección de identidad de las personas, para evitar el robo de identidad o el fraude de documentos.

- Gracias a estos datos tan sensibles y a la tecnología se ha implementado la autenticación biométrica de identidad del individuo, de una forma segura y rápida.

- Por ejemplo, las entidades bancarias deben asegurar la protección de la información financiera de sus clientes, ofreciéndoles seguridad y facilidad en sus transacciones. Y con el uso de datos biométricos, los bancos pueden garantizar a sus clientes un acceso seguro a sus servicios.

- Otro ejemplo es el dispositivo móvil con la tecnología para analizar el comportamiento biométrico del usuario, la forma en la que éste interactúa con el equipo, como la rapidez con la que escribe.

v.2) Control de acceso.

Los datos biométricos también pueden emplearse como método de control de acceso a las instalaciones de una empresa, institución o a cualquier área en la que se requiera gran seguridad y solo puedan acceder personas autorizadas. Hoy en día el control de acceso basado en datos biométricos también es muy utilizado para el control de asistencia del empleado, para registrar la entrada y salida de su jornada de trabajo. Incluso en el trabajo remoto. Normalmente, se emplea la huella digital, pero también es muy utilizado el reconocimiento de voz o del iris.

v.3) Control de trámites en general, migratorios o de movilidad.

Otro de los grandes usos de los datos biométricos es en el control de migración a través de los actuales pasaportes biométricos. Este documento cuenta con un chip insertado en su reverso con los datos biométricos del titular (rasgos faciales), además de los datos personales como el nombre, la nacionalidad, el sexo, etc.

Los países han implementado diversos controles fronterizos como cámaras y escáneres para identificar, a través de los datos biométricos y los respectivos registros, a las personas que ingresan en su territorio

vi) Tipo de datos biométricos.

Entre los datos biométricos que más se emplean en los sistemas de identificación de las personas se encuentran las huellas dactilares, la voz, los patrones faciales o la retina.

Para capturar estos rasgos son utilizados, comúnmente, los siguientes métodos de identificación.

vi.1) Reconocimiento facial.

El reconocimiento facial es la identificación automática de un rostro humano, para confirmar la identidad de determinada persona. Se toma como base la imagen o vídeo de su faz que ha sido registrada bajo códigos matemáticos.

vi. 2) Reconocimiento de firma.

Es un tipo de reconocimiento que se realiza en base al análisis de los patrones de los puntos y curvas de la firma de una persona, a través de algoritmos especializados que emplean el cotejo simple, buscando las similitudes entre dos firmas, o la prueba dinámica, en la que se estudia la velocidad y la forma de los trazos.

Pero la **firma biométrica** no debe confundirse con **la firma digital**. Aunque ambas son válidas en la autorización de documentos e identificación de una persona, son firmas que se diferencian en la tecnología que emplean.

La firma biométrica puede registrarse a través de la firma manuscrita sobre dispositivos digitales como una tableta o Smartphone. Y mediante softwares especializados se realiza la captura de ciertos parámetros de los trazos de la firma. Esto facilita la autenticación biométrica en tiempo real.

Mientras que, para firmar digitalmente es necesario que la persona cuente con un dispositivo para la creación de la firma. Como, por ejemplo, con un certificado digital, un documento digital que contiene datos de identificación del firmante.

Los retos del derecho a la protección de la identidad mediante la Soberanía Digital Personal.

El nuevo derecho fundamental vinculado a la protección de datos biométricos frente a las tecnologías emergentes se está consolidando bajo el concepto de Soberanía Digital Personal. Este principio reconoce que, debido al carácter inmutable de la biometría, las personas deben mantener el control absoluto sobre su identidad biológica y digital frente a sistemas automatizados.

Las innovaciones tecnológicas (como la Inteligencia Artificial generativa y la biometría conductual) plantean desafíos sin precedentes que exigen una protección jurídica reforzada, sobre todo de los datos biométricos inmutables de las personas.

Para nadie es desconocido que en la actualidad instituciones gubernamentales, privadas, empresas privadas o descentralizadas o centros escolares solicitan en forma constante a las personas menores de edad o adultas, registrar en sistemas o plataformas tecnológicas su rostro, las huellas dactilares o el iris de sus ojos, como condición para acceso, trámites, autorizaciones o reconfirmación de la certeza sobre la identidad de una persona, y en el caso de las autoridades de gobierno, con el propósito incluso de tener control sobre la ciudadanía.

Incluso, en estos tiempos, por un lado, se está solicitando el registro de la línea telefónica para lo cual se deben proporcionar datos biométricos que, “supuestamente resguardaran” las compañías telefónicas. Lo cual se ve difícil. Por otro, se esta en proceso de la expedición de

la nueva CURP, en cuyo trámite también habrá que proporcionar datos biométricos de los denominados "inmutables", como son el rostro, la huella dactilar y lo más novedoso el iris de los ojos.

Por ello, se debe trabajar desde el ámbito legislativo para ampliar los espectros normativos de protección de las leyes, entre las que se encuentra la ley sustantiva penal, pues hoy en día, sin duda alguna hay altos riesgos en los mecanismos que se implementan en el ámbito público o privado para autenticación biométrica de una persona.

Soberanía digital como derecho emergente.

La soberanía digital en México es un derecho emergente concebido tanto desde la perspectiva de la soberanía tecnológica de la Nación (sobre infraestructuras críticas y ciberespacio) como un derecho humano personal. Este último enfoque busca frenar la imposición de bases de datos biométricas obligatorias (como la CURP biométrica) que vulneran el control de la propia identidad.

Evolución de la Privacidad hacia la Soberanía Digital.

Debido a la implementación masiva de identificadores biométricos (como la CURP biométrica en México), los tribunales han comenzado a redefinir la privacidad. El nuevo paradigma de soberanía digital personal busca garantizar:

- Autonomía sobre el cuerpo y el rostro: Que la persona conserve el control sobre el uso que se le da a su identidad biológica.

- Transparencia radical: Conocer exactamente qué algoritmos o tecnologías procesan y analizan la información sensible.

- Consentimiento informado e inequívoco: Los datos no pueden ser tomados de manera obligatoria para acceder a servicios básicos sin garantías de protección.

Soberanía digital como nuevo derecho humano.

En el contexto legal en junio de 2026, tribunales federales emitieron un criterio judicial que reconoce la soberanía digital personal frente a las medidas que exigen la entrega de datos biométricos.

Se determinó que, como alcance de este nuevo derecho frente a la insuficiencia protectora de los tradicionales Derechos ARCO, este derecho plantea que las personas deben conservar un control real sobre su identidad biológica y digital**.**

Incluso todo ello, está basado en la Tesis del Semanario Judicial, que a la letra señala:

> **"*Registro digital:*** *2032324*
> ***Duodécima Época***
> ***Materia(s):*** *Constitucional, Administrativa*

Tesis: *I.20o.A.56 A (12a.)*
Instancia: *Tribunales Colegiados de Circuito*
Tipo: *Aislada*
Fuente: *Semanario Judicial de la Federación.*
Publicación: *Viernes 26 de junio de 2026 10:32 horas.*

DERECHO HUMANO A LA PRIVACIDAD, EN SU VERTIENTE DE AUTODETERMINACIÓN INFORMATIVA. ES NECESARIO RECONCEPTUALIZARLO COMO SOBERANÍA DIGITAL PERSONAL ANTE LOS NUEVOS DESAFÍOS TÉCNICOS, DILEMAS ÉTICOS Y RETOS JURÍDICOS QUE IMPLICA LA BIOMETRÍA LLEVADA A CABO POR AUTORIDADES.

Hechos: Una persona promovió amparo indirecto contra el artículo 91 Bis de la Ley General de Población, adicionado mediante decreto publicado el 16 de julio de 2025, que prevé la creación de la Clave Única de Registro de Población (CURP) biométrica como documento nacional de identidad obligatorio, así como la obtención, el almacenamiento, la administración, la consulta y el uso de datos biométricos para la instauración de una Plataforma Única de Identidad. El Juzgado de Distrito concedió la suspensión provisional solicitada. Contra esa decisión la autoridad responsable interpuso recurso de queja.

Criterio jurídico: Es necesario reconceptualizar el derecho humano a la privacidad, en su vertiente de autodeterminación informativa, como soberanía digital personal ante los desafíos técnicos, dilemas éticos y retos jurídicos de la biometría llevada a cabo por autoridades.

Justificación: El derecho a la autodeterminación informativa, que forma parte de la privacidad, garantiza la protección de la dignidad humana, la autonomía y la libertad en tanto configura una barrera contra el abuso del derecho a la información por particulares y contra invasiones a la intimidad por autoridades que pueden modificar hábitos o preferencias, suprimir conductas democráticamente valiosas, "someter a la ciudadanía" y reducir su participación en la vida política y social del país.

Sin embargo, las amenazas, los riesgos, las vulnerabilidades y las fragilidades que puede ocasionar la indebida solución de los desafíos técnicos, dilemas éticos y retos jurídicos intrínsecos a la biometría llevada a cabo por autoridades y las repercusiones que puede ocasionar el monitoreo biométrico en el libre ejercicio de varios derechos humanos, especialmente en el entorno económico actual que posibilita una vigilancia sin precedentes, son factores que exceden los alcances de la autodeterminación informativa como herramienta analítica y disminuyen su potencial para salvaguardar la intimidad, la vida privada de las personas, su seguridad y su integridad. Lo anterior, porque la explotación de datos biométricos, por su naturaleza única e inmutable, sigue una dinámica tan distinta que exige una protección más amplia, renovada y reforzada que no se agote en la aplicación de disposiciones administrativas vinculadas casi exclusivamente con el ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición) y que, en cambio, articule un control personal o colectivo efectivo sobre la propia identidad (biológica y comportamental) y en todo tipo de espacios (físicos y digitales) a fin de abordar y superar riesgos para los que la privacidad y sus garantías originales no fueron

concebidas. Por lo que ante la biometría y sus impactos negativos es indispensable reconceptualizar la privacidad como un derecho humano emergente a la soberanía digital personal."

Los Retos de las Nuevas Tecnologías

- **Sustitución de identidad por Inteligencia Artificial:** Sistemas de IA pueden simular o generar expresiones, gestos, rostros y voces, permitiendo la apropiación de identidad sin necesidad de contacto físico.

- **Biometría no invasiva:** La captura remota de iris, el reconocimiento de voz o el análisis de patrones de comportamiento (como la forma de caminar o escribir) ocurren a menudo sin el consentimiento explícito del titular.

- **Inmutabilidad de los datos:** A diferencia de una contraseña o un número de tarjeta, si una huella dactilar o el escaneo facial son vulnerados en una base de datos, el daño es permanente e irreparable.

INTELIGENCIA ARTIFICIAL.

Factibilidad de falsear los datos biométricos inmutables de las personas mediante la inteligencia artificial (IA).

Es totalmente posible falsificar y engañar a los sistemas que utilizan datos biométricos. Aunque tus rasgos físicos reales (como las huellas dactilares, el iris o las facciones del rostro) son inmutables y no cambian, la representación digital de estos datos o su captura física sí pueden ser replicadas, clonadas o inyectadas por ciberdelincuentes para suplantar identidades**.**

Métodos actuales de falsificación biométrica.

El fraude biométrico ha evolucionado desde técnicas analógicas simples hasta sofisticados ataques de Inteligencia Artificial:

1. Ataques de presentación física (Spoofing).

Consisten en presentar un objeto falso o una réplica directamente ante el sensor físico del dispositivo:

- Huellas dactilares de silicona: Se clonan las huellas utilizando moldes de látex, silicona o acetato con pegamento. Casos delictivos reales demuestran que técnicas de bajo costo logran burlar lectores comerciales.

- Máscaras 3D y fotografías: Para evadir el reconocimiento facial, los atacantes emplean desde fotos impresas en alta resolución hasta máscaras de resina hiperrealistas que simulan la profundidad del rostro.

2. Inyección digital y Deepfakes (Ataques de software).

Son los métodos más peligrosos debido al auge de la Inteligencia Artificial Generativa:

- Ataques de inyección de video: El atacante vulnera el software o el hardware del dispositivo para interceptar la señal de la cámara. En lugar de capturar el entorno real, se "inyectan" datos directamente en el sistema de verificación.

- Deepfakes de rostro y voz: Herramientas de IA generan rostros sintéticos en tiempo real o clonan la voz con total precisión matemática. Estos modelos son capaces de parpadear y gesticular para engañar los flujos digitales de verificación bancaria (*KYC*).

3. Robo y reconstrucción de plantillas.

Pueden robar estos archivos de datos abstractos.

- Utilizan algoritmos inversos para reconstruir o aproximar un mapa biométrico sintético compatible con los lectores.

- Cuando te registras en un sistema institucional, tu característica física no se guarda como una foto, sino como una plantilla matemática cifrada (hash). Si los atacantes vulneran la base de datos central de una organización.

¿Qué es la inteligencia artificial?

La Inteligencia Artificial, en lo sucesivo (IA), al igual que la humana, es un concepto complejo de definir. Aún no existe una definición formal y universalmente aceptada[1].

La Comisión Europea la define como sistemas de software (y posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital:

- Percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados.

- Razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado.

- Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico. También pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas.

- Dicho de otro modo:

[1] Consultable en. Qué es la Inteligencia Artificial | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. Plan de Recuperación, Transformación y Resiliencia. Gobierno de España.

- La inteligencia artificial (IA) es un campo de la informática que se enfoca en crear sistemas que puedan realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción.

- Estos sistemas pueden percibir su entorno, razonar sobre el conocimiento, procesar la información derivada de los datos y tomar decisiones para lograr un objetivo dado.

¿Cómo funciona la IA?

Las Inteligencias artificiales utilizan algoritmos y modelos matemáticos para procesar grandes cantidades de datos y tomar decisiones basadas en patrones y reglas establecidas a través del aprendizaje automático, que es la capacidad de una máquina para aprender de forma autónoma a partir de datos sin ser programada específicamente para hacerlo. De esta manera la IA puede mejorar su precisión y eficiencia con el tiempo

Tipos de inteligencia artificial.[2]

Según la definición de Inteligencia Artificial de la Comisión Europea existen dos tipos de IA:

- Software: asistentes virtuales, software de análisis de imágenes, motores de búsqueda o sistemas de reconocimiento de voz y rostro.

- Inteligencia artificial integrada: robots, drones, vehículos autónomos o el Internet de las Cosas.

Combate a la falsificación de datos biométricos inmutables mediante la Inteligencia artificial.

Para mitigar el riesgo de que la inmutabilidad de tus datos se vuelva en tu contra (ya que una huella robada no se puede cambiar como una contraseña), la industria de la ciberseguridad implementa múltiples capas de protección

- Detección de vitalidad (Liveness Detection): Los sensores modernos analizan texturas, micro-movimientos oculares, flujo sanguíneo, temperatura o conductividad eléctrica para asegurar que la muestra proviene de un tejido vivo y no de una pantalla o molde.

- Biometría multimodal: Obliga al usuario a pasar varios filtros independientes, combinando por ejemplo el escaneo del iris con el mapa vascular de la palma o el reconocimiento de voz.

- Autenticación Multifactor (MFA): Los sistemas seguros nunca dependen únicamente de la biometría. Exigen un factor complementario como un PIN dinámico, un token físico o una clave temporal.

[2] Vid. Consultar en: Que es la IA por IBM.pdf

Delito de Usurpación de Identidad, en el Código Penal del Estado de Guanajuato.

En el estado de Guanajuato, el delito de usurpación de identidad fue incorporado al Código Penal mediante decreto publicado en el Periódico Oficial del Gobierno del Estado el **11 de septiembre de 2015**. Para ello, se adicionó el **Título Sexto**, con un **Capítulo Único**, dentro del cual se incorporó el **artículo 214-a**, cuyo texto dispone:

> *"**TÍTULO SEXTO***
> ***DE LOS DELITOS CONTRA LA IDENTIDAD DE LAS PERSONAS***
>
> ***CAPÍTULO ÚNICO***
>
> ***Artículo 214-a.-** A quien empleando cualquier medio y sin el consentimiento de quien legalmente deba otorgarlo se haga pasar por otra persona, utilice su identidad, ejerza sus derechos o se apropie de sus datos personales, o siendo titular de éstos, otorgue su consentimiento para que se efectúen dichas conductas, en beneficio propio o de un tercero, o para producir un daño al titular de la identidad, a su patrimonio, o a persona ajena, se sancionará con pena de prisión de uno a cinco años y de diez a cincuenta días multa.*
>
> *Las sanciones se aumentarán de una mitad del mínimo a una mitad del máximo de las señaladas en el párrafo anterior cuando el sujeto activo:*
>
> *I. Se valga de la homonimia para usurpar la identidad.*
>
> *II. Se aproveche la igualdad física o genética con el sujeto pasivo.*
>
> *III. Tenga conocimiento en las ramas tecnológicas o de ingeniería, o se aproveche de su profesión o empleo.*
> *IV. Sea servidor público o empleado en cualquier institución bancaria, financiera o crediticia."*

Dicho tipo jurídico-penal tiene como bien jurídico tutelado la identidad de las personas, estableciendo una sanción de uno a cinco años de prisión y conteniendo originalmente tres hipótesis agravantes, consistentes en que la pena se incrementará de una mitad del mínimo a una mitad del máximo cuando: **se aproveche homonimia; se aproveche igual física o genética y; cuando el activo sea servidor público o empleado en cualquier institución bancaria, financiera o crediticia.**

De lo anterior se desprende que el tipo penal protege, en su concepción tradicional, el bien jurídico relacionado con la seguridad de la identidad de las personas, conforme al concepto de identidad que jurídicamente prevalecía al momento de su incorporación.

Posteriormente, en noviembre de 2020, atendiendo a los avances tecnológicos y a las nuevas formas de comisión de este delito, se adicionó una fracción III y se recorrió la entonces fracción III a la IV, estableciendo un supuesto de agravación de la sanción cuando el sujeto

activo es experto en cuestiones tecnológicas o se aprovecha de su profesión o empleo para cometer la conducta.

No obstante, esta regulación dejó fuera aquellos casos en los que la persona que tiene acceso, conocimiento o capacidad técnica para obtener, facilitar o utilizar indebidamente información relacionada con la identidad no tiene la calidad de empleado ni actúa necesariamente en ejercicio de una profesión.

Esta circunstancia genera un ámbito de protección insuficiente frente a las formas actuales en que pueden obtenerse y utilizarse ilícitamente los datos de identidad, particularmente los datos biométricos.

Por otro lado, la agravante de la vigente fracción IV sanciona de forma agravada el delito de usurpación de la identidad en el supuesto de que: "*Sea servidor público o empleado en cualquier institución bancaria, financiera o crediticia*", lo que en su tiempo era suficiente. Sin embargo, quedaron fuera de esta hipótesis típica para agravar el comportamiento de los posibles activos de este delito.

Sin duda, en la actualidad el manejo de datos biométricos en el sector público y privado se ha extendido de manera significativa. Particularmente relevantes son los datos biométricos inmutables, es decir, aquellos que no pueden ser modificados o sustituidos por su titular, como las huellas dactilares, el iris, el rostro, la palma de las manos y el ADN.

Este tipo de información ya no se encuentra únicamente bajo resguardo de instituciones bancarias o crediticias. Por diversos trámites y servicios, también es recabada por instituciones educativas públicas y privadas, empresas y otras instituciones particulares, como las compañías de telefonía, así como por organismos públicos descentralizados. Un ejemplo es el Instituto de Seguridad Social del Estado de Guanajuato (ISSEG), que recaba y resguarda información biométrica de sus afiliados y jubilados, entre ella sus huellas dactilares.

En consecuencia, los riesgos de vulneración de estos datos también se han ampliado. La información biométrica puede quedar expuesta por actos realizados por empleados, directivos, apoderados, patrones o cualquier otra persona que, por razón de sus funciones, tenga acceso legítimo a ella dentro de una institución pública o privada. Sin embargo, no todos estos sujetos necesariamente encuadran en los supuestos previstos actualmente en las fracciones III y IV.

Por ello, resulta necesario contemplar como agravante aquellos casos en los que el sujeto activo, aprovechando el acceso, custodia o conocimiento que tiene respecto de datos de identidad, los obtenga, disponga de ellos, los facilite o los comercialice indebidamente con terceros. La especial gravedad de estas conductas deriva de la confianza depositada por el titular de la información y de la naturaleza de los datos comprometidos, pues se trata de elementos vinculados directamente con su identidad y, en el caso de los datos biométricos inmutables, de información que el titular no puede sustituir una vez que ha sido vulnerada.
Esta circunstancia representa una afectación particularmente grave al derecho humano a la identidad y al bien jurídico protegido por el tipo penal, por lo que la respuesta punitiva debe

considerar no sólo el resultado de la conducta, sino también la forma en que el sujeto activo obtuvo acceso a la información y abusó de la confianza depositada en él.

Asimismo, deben considerarse como supuestos de mayor gravedad aquellos casos en los que los datos sean obtenidos, generados, facilitados o utilizados ilícitamente mediante herramientas de Inteligencia Artificial u otros mecanismos tecnológicos que permitan su extracción, reproducción, alteración o utilización para suplantar la identidad de una persona.

De igual manera, debe contemplarse la conducta de quienes, sin tener legítimamente bajo su resguardo dichos datos, los obtengan ilícitamente de terceros mediante actos de corrupción, para utilizarlos en la comisión de otros delitos o para comercializarlos en mercados ilícitos de información personal. En estos casos, la afectación trasciende la vulneración inicial de la identidad, pues la información puede convertirse en un instrumento para la comisión de nuevas conductas delictivas.

Por estas razones, la propuesta busca ampliar los supuestos de agravación para abarcar las nuevas formas de obtención, disposición, facilitación y comercialización ilícita de datos de identidad, particularmente cuando se trate de información biométrica, atendiendo a la especial naturaleza de estos datos, a la confianza depositada en quienes tienen acceso a ellos y al riesgo que su utilización indebida representa para sus titulares.

PROPUESTA LEGISLATIVA.

Así, el Grupo Parlamentario del Partido Revolucionario Institucional considera que la legislación penal no puede permanecer ajena a la evolución de las formas en que se vulnera la identidad de las personas. La usurpación de identidad no constituye, en todos los casos, una conducta aislada, sino que puede utilizarse como medio para la comisión de otros delitos que generan afectaciones de mayor alcance, particularmente contra el patrimonio o la seguridad personal de las víctimas.

Ante la evolución de los derechos humanos y de los bienes jurídicos que corresponde proteger al derecho penal, resulta necesario fortalecer la tutela del **derecho humano a la identidad**. Esta necesidad adquiere especial relevancia frente al acelerado desarrollo tecnológico, que ha transformado la forma en que las personas acreditan y proporcionan su identidad.

Tradicionalmente, la identidad se acreditaba mediante documentos como las actas de nacimiento, la credencial para votar, el pasaporte y otros instrumentos de identificación. Actualmente, tanto las instituciones públicas y los organismos descentralizados como las empresas privadas y otros prestadores de servicios recaban, mediante plataformas, dispositivos y sistemas tecnológicos, información biométrica de las personas.

Entre estos datos se encuentran aquellos considerados inmutables, como el rostro, el iris, las huellas dactilares, las huellas de la palma de la mano y el ADN, cuya particularidad radica en que están vinculados a características biológicas o fisiológicas propias de cada individuo y, por ello, no pueden ser sustituidos por su titular de la misma manera que una contraseña, un documento o un número de identificación.

Por esta razón, quienes suscribimos consideramos necesario que el derecho penal sustantivo también evolucione y reconozca las nuevas dimensiones de protección de la identidad personal. En este contexto, la **soberanía digital personal** adquiere especial relevancia como una dimensión de la identidad que debe ser protegida frente al acceso, uso, disposición, facilitación o comercialización ilícita de los datos que permiten identificar a una persona.

En consecuencia, la presente iniciativa propone fortalecer la protección penal de la identidad mediante la incorporación de supuestos agravados para el delito de usurpación de identidad, atendiendo tanto a la gravedad de la conducta como a las circunstancias y calidad del sujeto activo cuando éste aprovecha el acceso legítimo que tiene a los datos personales o biométricos de una persona para disponer de ellos sin su consentimiento.

La propuesta también busca actualizar la protección de la soberanía digital personal frente a las nuevas herramientas tecnológicas. Particularmente, cuando los datos biométricos son falsificados, alterados, reproducidos o imitados mediante Inteligencia Artificial u otros mecanismos tecnológicos con la finalidad de cometer un delito, la conducta adquiere una especial gravedad que debe ser considerada por la legislación penal.

De igual forma, se pretende atender aquellos casos en los que esta información sea obtenida o utilizada para su comercialización ilícita, incluso en mercados clandestinos de datos personales, o para facilitar la comisión de otros delitos, como la extorsión. Con ello, se busca que la protección penal de la identidad responda a las condiciones tecnológicas actuales y no únicamente a las formas tradicionales de identificación, garantizando una tutela efectiva frente a los nuevos mecanismos de vulneración de la identidad de las personas.

Es por lo que, mediante la presente iniciativa, proponemos la adición de una fracción V y una fracción VI al artículo 214-a del Código Penal del Estado de Guanajuato, para quedar como sigue:

V. Sea empleado de empresas, instituciones privadas o instituciones descentralizadas de gobierno estatal o municipal que tengan el resguardo de los datos de identidad inmutables de las personas.

VI. Disponga, facilite o comercialice indebidamente los datos digitales biométricos inmutables de las personas o los simule o falsifique mediante inteligencia artificial.

De ser aprobada, la presente iniciativa, tendrá los siguientes impactos, de conformidad con el artículo 176 de la Ley Orgánica del Poder Legislativo del Estado de Guanajuato:

I. Impacto jurídico: Que se materialice en el Código Penal del Estado de Guanajuato, la ampliación a la tutela del bien jurídico a la identidad a través de la protección de los datos biométricos inmutables de las personas, conforme a los avances tecnológicos, manteniendo así la soberanía digital personal como nuevo derecho humano y, por ende, bien jurídico que refuerza la capacidad jurídica de las personas en el estado de Guanajuato.

II. **Impacto socioeconómico:** No se parecía;

III. **Impacto administrativo:** No se aprecia;

IV. **Impacto presupuestario:** No se aprecian costos;

V. **Impacto ambiental:** No se aprecia.

VI. **Impacto de perspectiva de género:** No se aprecia en el presente caso.

Por lo anteriormente expuesto, someto a la consideración de este H. Congreso del Estado de Guanajuato el siguiente:

DECRETO.

ÚNICO: Se adicionan las fracciones V y VI al artículo 214.a del Código Penal del Estado de Guanajuato, para quedar como sigue:

"Artículo 214-a.- A quien empleando cualquier medio…

Las sanciones…:

I.- a la IV. …

V.- Sea empleado de empresas, instituciones privadas o instituciones descentralizadas de gobierno estatal o municipal que tengan el resguardo de los datos de identidad inmutables de las personas.

VI.- Disponga, facilite o comercialice indebidamente los datos digitales biométricos inmutables de las personas o los simule o falsifique mediante inteligencia artificial."

TRANSITORIO.

Artículo Único. El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Estado de Guanajuato.

GUANAJUATO, GTO., A 01 DE OCTUBRE DE 2026.
DIPUTADAS Y DIPUTADO INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL.

DIPUTADA RUTH NOEMÍ TISCAREÑO AGOITIA.

DIPUTADA ROCÍO CERVANTES BARBA.

DIPUTADO ALEJANDRO ARIAS ÁVILA.

PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO

AUTORIDAD CERTIFICADORA

e.congresogto.gob.mx

Información Notificación Electrónica

Folio:	59379
Asunto:	SE PRESENTA INICIATIVA
Descripción:	SE PRESENTA INICIATIVA
Destinatarios:	UNIDAD DE CORRESPONDENCIA DEL CONGRESO DEL ESTADO DE GUANAJUATO - Unidad de Correspondencia, Congreso del Estado de Guanajuato SECRETARIA GENERAL - Buzón Secretaría General, Congreso del Estado de Guanajuato SOFIA RUIZ BACA - Dirección General de Servicios y Apoyo Técnico Parlamentario, Congreso del estado de Guanajuato RUTH NOEMI TISCAREÑO AGOITIA - Diputada de la LXVI Legislatura, H Congreso del Estado de Guanajuato ALEJANDRO ARIAS AVILA - Diputado de la LXVI Legislatura, H Congreso del Estado de Guanajuato ROCIO CERVANTES BARBA - Diputada de la LXVI Legislatura, H. Congreso del Estado de Guanajuato
Archivo Firmado:	File_1828_20260929144854001_0.pdf
Autoridad Certificadora:	AUTORIDAD CERTIFICADORA DEL PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO V2

Evidencia Criptográfica
Hoja de Firmantes

FIRMA

Nombre Firmante:	RITA GONZALEZ GUTIERREZ	**Validez:**	Vigente
No. Serie:	50.4c.45.47.30.32.00.00.00.00.72	**Revocación:**	No Revocado
Fecha (UTC/CDMX):	29/09/2026 10:47:55 p. m. - 29/09/2026 04:47:55 p. m.	**Estatus:**	Válida
Algoritmo:	RSA - SHA256		
Cadena de Firma:	2c-ed-b0-ad-aa-32-56-9e-63-b5-0a-1a-49-c4-c0-66-6c-23-07-7a-14-21-46-22-6b-84-0d-17-3b-b8-01-b4-26-25-9d-6f-f8-6e-91-be-5e-6e-0b-6e-89-58-6f-56-6f-45-2f-52-4e-7d-04-ec-5d-0c-b7-00-a3-25-77-02-d2-e2-f1-04-dc-88-cd-87-60-4e-4d-06-f2-76-96-c8-00-61-c9-e2-b2-30-82-01-bd-e5-55-4c-73-10-b1-94-84-de-e5-05-3f-5e-91-bf-cc-f8-f0-e4-dc-3b-da-38-5f-c8-20-fd-5f-4f-ab-df-ff-b6-a7-68-d1-34-b2-0f-a5-3b-52-84-20-6a-68-d3-35-11-be-90-24-7b-b7-3a-f8-1c-7e-d7-d4-0f-bf-11-72-f1-50-2d-9a-7d-c7-c5-b0-e4-bc-00-ec-b4-50-53-f7-b5-52-cc-49-35-95-b7-1b-61-21-c9-5e-69-fd-b7-3f-5b-69-27-68-18-2d-33-44-de-ee-7b-8f-13-29-57-69-ff-b5-29-33-a3-d6-82-e2-85-2f-ad-13-e6-8e-3f-44-a4-08-4b-e9-71-99-df-41-7c-f2-dd-3d-17-52-47-84-34-b6-1e-b0-c7-86-b0-6e-9e-b9-fa-05-f9-09-d2-9d-6a-02-72-df-4c-22-d2		

OCSP

Fecha (UTC/CDMX):	29/09/2026 10:48:38 p. m. - 29/09/2026 04:48:38 p. m.
Nombre Respondedor:	Servicio OCSP AC del Poder Legislativo del Estado de Guanajuato
Emisor Respondedor:	AUTORIDAD CERTIFICADORA DEL PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO V2
Número de Serie:	50.4c.45.47.30.32.30.35

TSP

Fecha (UTC/CDMX):	29/09/2026 10:48:38 p. m. - 29/09/2026 04:48:38 p. m.
Nombre Emisor de Respuesta TSP:	Advantage Security PSC Estampado de Tiempo 1
Emisor Certificado TSP:	Autoridad Certificadora Raiz Segunda de Secretaria de Economia
Identificador de Respuesta TSP:	639262973183615903
Datos Estampillados:	3aktaTkj9VXpHtocmzUOfVq4kUc=

CONSTANCIA NOM 151

Índice:	490535371
Fecha (UTC/CDMX):	29/09/2026 10:48:38 p. m. - 29/09/2026 04:48:38 p. m.
Nombre del Emisor:	Advantage Security PSC NOM151
Número de Serie:	2c

• Firma Electrónica Certificada •
Autoridad Certificadora del Poder Legislativo del Estado de Guanajuato

FIRMA

Nombre Firmante:	ROCÍO CERVANTES BARBA	**Validez:**	Vigente
No. Serie:	50.4c.45.47.30.32.00.00.00.00.c7	**Revocación:**	No Revocado
Fecha (UTC/CDMX):	29/09/2026 09:04:29 p. m. - 29/09/2026 03:04:29 p. m.	**Estatus:**	Válida
Algoritmo:	RSA - SHA256		
Cadena de Firma:	21-3c-0a-e2-20-b5-8b-85-73-34-c8-07-c2-d0-41-c6-e6-3b-8d-59-af-e3-9d-40-c0-c0-dc-11-f9-1d-ba-05-6e-97-87-bf-f6-44-37-b1-af-4a-0f-e3-2d-b7-40-56-a5-23-af-a3-35-62-5e-54-a2-7c-dc-0d-2a-2b-30-31-e7-8c-5b-d9-f8-0f-b6-24-67-fc-f4-30-55-6a-17-62-aa-b0-e8-4f-1b-ab-16-99-ca-ac-0b-0a-9a-8a-53-2d-4d-89-c1-f9-88-68-d2-cf-a9-83-57-61-bf-5e-ac-f9-b8-f5-7b-be-eb-64-8f-6c-da-d8-c8-58-56-90-fe-b0-39-c7-45-13-eb-2d-1d-6f-d4-bf-61-1a-12-17-55-da-41-8d-cb-07-2a-f4-39-67-12-9b-65-fa-6b-2a-e6-8a-d4-03-35-28-15-05-1e-4e-2a-e0-79-ba-af-8c-84-44-20-b4-b7-89-f8-7c-97-a5-8d-11-05-c9-2a-c4-da-6b-9c-7b-a9-59-8b-8c-41-e0-34-1e-c0-c9-d8-4c-27-2d-18-fa-2c-be-7c-e7-8c-21-35-c5-93-dd-cc-35-d1-07-f9-74-68-74-26-73-84-6a-f5-e9-86-2c-26-6c-05-9f-85-04-dc-50-ce-0f-8d-b6-a4-9f-64-3d-57-fd-d6-f7		

OCSP

TSP

CONSTANCIA NOM 151

Fecha (UTC/CDMX):	29/09/2026 09:05:11 p. m. - 29/09/2026 03:05:11 p. m.	**Fecha (UTC/CDMX):**	29/09/2026 09:05:11 p. m. - 29/09/2026 03:05:11 p. m.	**Índice:**	490501367
Nombre Respondedor:	Servicio OCSP AC del Poder Legislativo del Estado de Guanajuato	**Nombre Emisor de Respuesta TSP:**	Advantage Security PSC Estampado de Tiempo 1	**Fecha (UTC/CDMX):**	29/09/2026 09:05:12 p. m. - 29/09/2026 03:05:12 p. m.
Emisor Respondedor:	AUTORIDAD CERTIFICADORA DEL PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO V2	**Emisor Certificado TSP:**	Autoridad Certificadora Raiz Segunda de Secretaria de Economia	**Nombre del Emisor:**	Advantage Security PSC NOM151
Número de Serie:	50.4c.45.47.30.32.30.35	**Identificador de Respuesta TSP:**	639262911117437207	**Número de Serie:**	2c
		Datos Estampillados:	3vickdH6W4ycDk1fO8lK2xPQCTI=		

• Firma Electrónica Certificada •
Autoridad Certificadora del Poder Legislativo del Estado de Guanajuato

FIRMA

Nombre Firmante:	ALEJANDRO ARIAS AVILA	**Validez:**	Vigente
No. Serie:	50.4c.45.47.30.31.00.00.00.0b.57	**Revocación:**	No Revocado
Fecha (UTC/CDMX):	29/09/2026 09:51:46 p. m. - 29/09/2026 03:51:46 p. m.	**Estatus:**	Válida
Algoritmo:	RSA - SHA256		
Cadena de Firma:	02-d1-84-d2-d8-c1-44-a3-07-c2-2c-37-fb-7e-30-a1-aa-20-7e-b4-cb-bc-c7-17-9a-1e-db-ee-e4-d8-73-20-e8-24-d8-ca-76-0f-ee-f9-a8-9c-ea-e5-12-78-10-c8-1e-35-5f-6f-41-77-0a-57-8f-55-de-64-fc-b2-e4-55-45-e7-70-49-b2-ee-f0-db-40-f6-5c-5b-70-bd-41-00-e8-2d-bd-94-58-05-54-26-3f-82-7e-18-37-c2-17-a0-c8-6a-30-75-3a-29-25-2e-ce-2d-8f-22-74-42-90-64-1d-39-83-57-cc-d1-3a-6f-09-5d-8f-7e-47-f8-97-ce-91-2a-15-98-ec-e1-54-d3-68-a6-9a-ed-92-0e-c1-52-4f-4c-f4-3d-69-c7-b1-00-22-10-de-78-76-26-16-93-98-a3-10-09-84-95-c2-22-23-b1-51-92-31-41-46-1b-9d-93-43-5c-31-89-1a-64-f0-26-ab-c0-8f-86-e4-af-5c-3a-f8-6e-f2-5c-3e-25-60-47-85-81-20-36-f8-60-c7-39-1d-81-16-fa-8d-03-02-56-af-1d-0e-bc-0f-75-0b-13-67-8b-7d-f5-5b-b1-39-b6-41-c4-fb-32-30-27-14-44-e9-77-f6-8c-93-3f-86-e0-ab-36-9b-0b-c3-39		

OCSP

Fecha (UTC/CDMX):	29/09/2026 09:52:29 p. m. - 29/09/2026 03:52:29 p. m.
Nombre Respondedor:	Servicio OCSP de la AC del Poder Legislativo del Estado de Guanajuato
Emisor Respondedor:	AUTORIDAD CERTIFICADORA DEL PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO
Número de Serie:	50.4c.45.47.30.31.30.35

TSP

Fecha (UTC/CDMX):	29/09/2026 09:52:30 p. m. - 29/09/2026 03:52:30 p. m.
Nombre Emisor de Respuesta TSP:	Advantage Security PSC Estampado de Tiempo 1
Emisor Certificado TSP:	Autoridad Certificadora Raiz Segunda de Secretaria de Economia
Identificador de Respuesta TSP:	639262939502679737
Datos Estampillados:	vlpQMkfZGAcZtjgB7CPODpXecck=

CONSTANCIA NOM 151

Índice:	490512666
Fecha (UTC/CDMX):	29/09/2026 09:52:30 p. m. - 29/09/2026 03:52:30 p. m.
Nombre del Emisor:	Advantage Security PSC NOM151
Número de Serie:	2c

• Firma Electrónica Certificada •
Autoridad Certificadora del Poder Legislativo del Estado de Guanajuato

FIRMA

Nombre Firmante:	JHOANNA ESCARLETT LEON LOPEZ	**Validez:**	Vigente
No. Serie:	50.4c.45.47.30.31.00.00.00.0a.75	**Revocación:**	No Revocado
Fecha (UTC/CDMX):	29/09/2026 10:33:00 p. m. - 29/09/2026 04:33:00 p. m.	**Estatus:**	Válida
Algoritmo:	RSA - SHA256		
Cadena de Firma:	9c-55-08-05-1b-65-ba-b0-e5-e1-6b-7a-84-5f-f1-69-a5-ea-fa-d5-cf-28-39-8c-9f-3d-b8-39-f1-43-c8-62-f6-de-b8-d2-df-9f-a5-35-16-7e-07-e7-7b-a4-e1-63-d9-c5-2e-ee-75-37-4a-58-f2-3e-f8-36-00-8f-fe-83-6f-d1-31-df-35-e9-1c-0e-dd-2e-c6-88-c3-d8-bf-07-27-e9-1e-e2-9e-4c-92-ee-9f-23-73-82-08-6b-d5-61-75-48-26-7d-ca-f6-71-30-9c-90-72-fd-4f-b9-54-3d-0b-64-89-37-57-21-12-ff-48-52-8d-4b-71-9f-d3-e6-ab-38-fd-08-1c-ff-cf-a8-5f-1f-e5-13-88-37-9f-23-89-55-ae-34-69-13-59-3b-a6-02-31-66-c6-d4-18-6d-fa-96-2b-47-71-7b-44-ba-99-77-d0-57-6d-c7-da-4e-ad-a0-72-b0-4c-c9-e9-8f-92-9f-32-8f-35-57-ad-03-5f-26-b5-9f-8b-42-0b-b5-ea-d1-00-d1-15-82-a3-f5-80-10-ee-0e-bb-4e-75-75-87-4b-42-ce-90-3a-02-cf-da-73-38-2d-d1-ee-12-0a-08-36-70-fd-2d-5b-06-88-9f-39-4e-f2-5a-80-91-ec-55-04-28-86-5a-69-43-26		

OCSP

Fecha (UTC/CDMX):	29/09/2026 10:33:43 p. m. - 29/09/2026 04:33:43 p. m.
Nombre Respondedor:	Servicio OCSP de la AC del Poder Legislativo del Estado de Guanajuato
Emisor Respondedor:	AUTORIDAD CERTIFICADORA DEL PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO
Número de Serie:	50.4c.45.47.30.31.30.35

TSP

Fecha (UTC/CDMX):	29/09/2026 10:33:43 p. m. - 29/09/2026 04:33:43 p. m.
Nombre Emisor de Respuesta TSP:	Advantage Security PSC Estampado de Tiempo 1
Emisor Certificado TSP:	Autoridad Certificadora Raiz Segunda de Secretaria de Economia
Identificador de Respuesta TSP:	639262964238823079
Datos Estampillados:	vZnb/a+V90PcIn7jM4oTcjkvC3c=

CONSTANCIA NOM 151

Índice:	490528852
Fecha (UTC/CDMX):	29/09/2026 10:33:44 p. m. - 29/09/2026 04:33:44 p. m.
Nombre del Emisor:	Advantage Security PSC NOM151
Número de Serie:	2c

FIRMA

Nombre Firmante:	RUTH NOEMI TISCAREÑO AGOITIA	**Validez:**	Vigente
No. Serie:	50.4c.45.47.30.31.00.00.00.0b.58	**Revocación:**	No Revocado
Fecha (UTC/CDMX):	29/09/2026 08:49:27 p. m. - 29/09/2026 02:49:27 p. m.	**Estatus:**	Válida
Algoritmo:	RSA - SHA256		

Cadena de Firma:

38-ed-81-1c-08-71-48-08-41-42-20-66-ae-b5-9c-a1-53-c9-22-d0-2a-cd-dc-68-1c-b8-e6-9a-41-3d-7d-ed-1f-87-60-e8-0c-7f-48-20-2d-58-a2-69-60-77-29-06-45-08-7d-5a-c2-87-7e-dc-db-e9-7f-05-10-4e-aa-f0-db-6d-f8-8f-34-20-b4-01-cd-f7-4c-e6-db-6d-e8-68-03-a2-a6-20-1d-4d-8e-8c-d8-00-a0-b1-72-98-5c-7c-24-14-15-7e-67-a9-66-d8-30-d9-c8-3f-7f-b5-58-69-6f-24-0b-0f-d3-c5-4b-fd-57-70-2b-7f-0a-a4-57-f6-d0-04-ce-c6-6f-77-44-23-b4-97-28-d5-85-9c-6f-de-49-9a-c2-5a-cb-9d-37-00-d9-c1-cc-cb-78-61-fc-3d-fd-94-ee-fb-c1-56-db-e3-19-18-53-8b-70-ee-2b-9e-81-df-b6-15-1f-41-13-d5-ff-92-77-14-ec-74-c2-81-d2-f2-e5-a4-a6-50-03-17-33-03-fa-b3-4b-15-3a-ae-9b-85-ad-19-45-d5-06-f7-dc-02-60-89-64-86-ec-05-63-37-8e-c3-a6-07-30-b9-4d-7e-32-0b-ab-a7-ae-28-b8-bc-bf-b3-c7-29-65-d7-a0-82-45-ad-ca-62-f8-c3

OCSP

Fecha (UTC/CDMX):	29/09/2026 08:50:09 p. m. - 29/09/2026 02:50:09 p. m.
Nombre Respondedor:	Servicio OCSP de la AC del Poder Legislativo del Estado de Guanajuato
Emisor Respondedor:	AUTORIDAD CERTIFICADORA DEL PODER LEGISLATIVO DEL ESTADO DE GUANAJUATO
Número de Serie:	50.4c.45.47.30.31.30.35

TSP

Fecha (UTC/CDMX):	29/09/2026 08:50:09 p. m. - 29/09/2026 02:50:09 p. m.
Nombre Emisor de Respuesta TSP:	Advantage Security PSC Estampado de Tiempo 1
Emisor Certificado TSP:	Autoridad Certificadora Raiz Segunda de Secretaria de Economia
Identificador de Respuesta TSP:	639262902098979101
Datos Estampillados:	S8vhNN0VPGJQZXFXz9zunSd7mP4=

CONSTANCIA NOM 151

Índice:	490497228
Fecha (UTC/CDMX):	29/09/2026 08:50:10 p. m. - 29/09/2026 02:50:10 p. m.
Nombre del Emisor:	Advantage Security PSC NOM151
Número de Serie:	2c