



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"



LEY QUE REGULA EL DESARROLLO Y USO DE LA INTELIGENCIA ARTIFICIAL EN EL PERÚ

Los Congresistas de la República que suscriben, miembros del Grupo Parlamentario **PODEMOS PERÚ** a iniciativa del Congresista de la República **CARLOS JAVIER ZEBALLOS MADARIAGA**, ejerciendo la facultad legislativa que le confiere el Art. 107 de la Constitución Política del Perú, y en cumplimiento de lo establecido en los Artículos 67, 74, 75 y 76 del Reglamento del Congreso de la República, propone para su aprobación el siguiente Proyecto de Ley.

PROYECTO DE LEY

**"LEY QUE REGULA EL DESARROLLO Y USO DE LA INTELIGENCIA
ARTIFICIAL EN EL PERÚ"**

TITULO I

ARTÍCULO 1.- OBJETO DE LA LEY

Establecer el marco legal para el uso y regulación de la inteligencia artificial en el territorio nacional, con el fin de garantizar la protección de los derechos fundamentales, la privacidad y la seguridad de los ciudadanos, fomentando la transparencia, la ética, innovación y el progreso en el campo de la Inteligencia Artificial en beneficio de los ciudadanos peruanos y evitando riesgos y consecuencias negativas.

ARTÍCULO 2.- AUTORIDAD Y ÁMBITO DE APLICACIÓN

La presente ley se aplicará a todas las personas físicas o jurídicas que desarrollen, investiguen, innoven o utilicen la inteligencia artificial en el territorio peruano, con independencia del lugar donde se encuentre el servidor o los servidores y desarrolladores que la soporten.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"

ARTICULO 3.- DEFINICIONES

Se entenderá por:

- **Inteligencia Artificial (IA):** la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.
- **Sistema de Inteligencia Artificial Autónomo (SIAA):** un sistema de IA capaz de operar de manera independiente sin intervención humana directa.
- **Algoritmo:** conjunto de instrucciones para la resolución de un problema, la realización de una tarea o la toma de decisiones, basadas en datos y en reglas matemáticas.
- **Datos personales:** toda información relativa a una persona física identificada o identificable.
- **Decisiones automatizadas:** las elecciones o conclusiones que son tomadas por sistemas de inteligencia artificial o por algoritmos sin la intervención directa de un ser humano. Estas decisiones son basadas en reglas, algoritmos o modelos de aprendizaje automático que analizan y procesan datos para determinar la acción o resultado más adecuado en una determinada situación.
- **Error de Uso de la inteligencia artificial:** cualquier acción, omisión o negligencia por parte de los desarrolladores, proveedores o usuarios de los sistemas de inteligencia artificial que resulte en consecuencias adversas, daño o perjuicio a personas, propiedades o derechos.
- **Ciclo de vida de los sistemas basados en inteligencia artificial:** el conjunto de actividades vinculadas con un servicio, producto o sistema basado en inteligencia artificial desde su concepción hasta el retiro de sus operaciones. Incluye, entre otros, las actividades de diseño, adquisición de datos, procesamiento de datos, modelado, evaluación, supervisión de los resultados y puesta en operación y/o producción.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

- **Datos de entrada:** datos suministrados a un sistema basado en inteligencia artificial u obtenido directamente por el mismo para producir información de salida.
- **Datos de entrenamiento:** datos usados para entrenar un sistema basado en inteligencia artificial al ajustar sus parámetros entrenables
- **Datos de prueba:** datos usados para realizar una evaluación independiente del sistema basado en inteligencia artificial entrenado y validado a fin de verificar su funcionamiento previsto.
- **Datos de validación:** datos usados para evaluar un sistema basado en inteligencia artificial entrenado y ajustar sus parámetros no entrenables, así como su proceso de aprendizaje a fin de, entre otras cosas, evitar el sobreajuste o el ajuste insuficiente. Este tipo de datos pueden ser datos independientes o formar parte del conjunto de datos entrenamiento ya sea como un división fija o variable.
- **Finalidad prevista:** uso para el cual se desarrolla un sistema basado en inteligencia artificial incluyendo el contexto y las condiciones específicas de su uso.
- **Funcionamiento de un sistema basado en inteligencia artificial:** capacidad de un sistema basado en inteligencia artificial para alcanzar su finalidad prevista.
- **Grupos de especial protección:** grupos de personas naturales que se encuentran en situación de riesgo de exclusión, dado que es la más impactada por la brecha digital, así como también es susceptible de sufrir daño en su acceso y exposición al entorno digital, los medios y servicios de la sociedad de la información. Comprende a los pueblos indígenas, la población afroperuana, mujeres, la niñez y la adolescencia, las personas adultas mayores, las personas con discapacidad, la población migrante, y las personas que viven con VIH.
- **Modelo fundacional:** modelo de un sistema basado en inteligencia artificial entrenado con un gran volumen de datos, diseñado para generar información de salida de carácter general y con capacidad de adaptación a un conjunto de tareas diversas.
- **Implementador:** toda persona natural o jurídica que utiliza un sistema basado en inteligencia artificial excepto cuando su uso se da exclusivamente para actividades personales no profesionales.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

- **Riesgo:** combinación de la probabilidad de que se genere un daño y la gravedad de dicho daño.
- **Sesgo de automatización:** tendencia a confiar automáticamente o en exceso en los resultados generados por un sistema basado en inteligencia artificial.
- **Sistema basado en inteligencia artificial:** sistema electrónico-mecánico que puede, para una serie de objetivos definidos por humanos, hacer predicciones, recomendaciones, contenidos, tomar decisiones, influenciando ambientes reales o virtuales e infiriendo tales resultados de los insumos que recibe. Los objetivos que busca alcanzar pueden ser explícitos o implícitos y está diseñado para funcionar con diferentes niveles de autonomía y adaptabilidad. Asimismo, incluye la aplicación de técnicas y enfoques como aprendizaje automático, aprendizaje supervisado, el no supervisado, aprendizaje por refuerzo, aprendizaje profundo, entre otros.
- **Uso indebido razonablemente previsible:** el uso de un sistema basado en inteligencia artificial de un modo distinto a su finalidad prevista pero que puede deducirse de un comportamiento humano o interacción con otros sistemas de forma razonablemente previsible.

TITULO II: PRINCIPIOS

ARTÍCULO 4: PRINCIPIOS

Todo desarrollo y uso de Inteligencia Artificial debe estar basado en el respeto irrestricto a los derechos fundamentales de la persona humana, principios éticos fundamentales, incluyendo el respeto a la dignidad humana, la privacidad, la transparencia, la responsabilidad y la equidad.

La Inteligencia Artificial no debe mentir a un ser humano o, a sabiendas, dejar que un ser humano sea engañado.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Un Sistema de Inteligencia Artificial debe responder a las preguntas que le son formuladas por un ser humano advirtiéndolo de forma expresa que quien lo hace es una Inteligencia Artificial.

Protección de la privacidad y datos personales, en todo el ciclo de vida de un sistema basado en inteligencia artificial se establecen medidas para la protección de la privacidad y los datos personales de acuerdo con las disposiciones normativas vigentes en la materia.

ARTÍCULO 5: RESPONSABILIDAD Y RENDICIÓN DE CUENTAS

Los desarrolladores, proveedores y usuarios de sistemas de inteligencia artificial son responsables de las consecuencias de sus acciones y decisiones relacionadas con el uso de la IA y deben garantizar que sus sistemas sean seguros, confiables y cumplan con los estándares de calidad establecidos.

Los desarrolladores tienen la obligación de documentar y divulgar el funcionamiento y los algoritmos utilizados en los sistemas de Inteligencia Artificial, para permitir la auditoría y evaluación de su impacto.

Garantizar la calidad y la eficacia de los servicios ofrecidos con la inteligencia artificial y asumir la responsabilidad de las decisiones y acciones de los sistemas de inteligencia artificial.

Las plataformas de distribución digital de aplicaciones móviles para todo tipo de dispositivos y sistemas tecnológicos, tiendas, plataformas digitales, que permita a los usuarios navegar y descargar aplicaciones que promuevan o lancen al mercado aplicativos de Inteligencia Artificial de cualquier tipo que contravengan los principios y prohibiciones de la presente ley y además sin autorización de la autoridad competente nacional, será pasible de sanciones administrativas, penales y civiles, cuyas sanciones serán drásticas por considerarse graves.

ARTÍCULO 6: PRIVACIDAD Y PROTECCIÓN DE DATOS

Los sistemas de Inteligencia Artificial deben respetar y proteger la privacidad de los usuarios y el tratamiento de sus datos personales de acuerdo con la normativa vigente de protección de datos aplicables, a los principios de la presente ley y sus prohibiciones.

En el marco de la ley 29733 Ley de Protección de Datos Personales, se prohíbe el uso no autorizado de datos personales recopilados por sistemas de Inteligencia Artificial, y se establece la obligación de obtener el consentimiento explícito e informado de los individuos para el uso de sus datos.

ARTÍCULO 7: TRANSPARENCIA

Se requiere que los sistemas de Inteligencia Artificial sean transparentes en su funcionamiento, de manera que los usuarios comprendan cómo se toman las decisiones y se llega a los resultados.

Se establece el derecho de los individuos a solicitar explicaciones de las decisiones tomadas por sistemas de Inteligencia Artificial que les afecten.

ARTÍCULO 8: SEGURIDAD

Los sistemas de Inteligencia Artificial deben ser diseñados y desarrollados con medidas de seguridad adecuadas para prevenir el acceso no autorizado, manipulación o interferencia malintencionada y los principios de acuerdo lo previsto en artículo 4 de la presente ley.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Se exige la implementación de salvaguardias técnicas y organizativas para garantizar la robustez y fiabilidad de los sistemas de Inteligencia Artificial.

TITULO III: EVALUACIÓN DE IMPACTO Y GESTIÓN DE RIESGO

ARTÍCULO 9: EVALUACIÓN DE IMPACTO

Las autoridades competentes deben realizar evaluaciones de impacto de Inteligencia Artificial, para identificar y mitigar riesgos potenciales antes de su despliegue en el territorio nacional.

Se promoverá la creación de comités y organismos encargados de realizar pruebas éticas de sistemas de Inteligencia Artificial, con el fin de garantizar su conformidad con los principios establecidos, para ello deberán registrarse cumpliendo los requisitos establecidos en la ley peruana.

ARTÍCULO 10: EVALUACIÓN Y GESTIÓN DE RIESGOS.

Los responsables de los sistemas de inteligencia artificial estarán obligados a implementar medidas adecuadas para mitigar los riesgos identificados durante la evaluación de riesgos. La gestión de riesgos incluirá la adopción de medidas de transparencia, responsabilidad y seguridad para minimizar el impacto de los riesgos identificados en los derechos fundamentales y en la seguridad de las personas.

La evaluación deberá ser actualizada periódicamente, incluirá una clasificación de los riesgos asociados con el sistema de inteligencia artificial, de acuerdo con los siguientes niveles de riesgo:

- **Riesgos inaceptables:** aquellos riesgos que se consideran inaceptables por su gravedad o por su impacto en los derechos fundamentales o en la seguridad de las personas. La presencia de un riesgo inaceptable en el sistema de inteligencia artificial requerirá la



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

adopción de medidas de mitigación adecuadas o la prohibición del sistema.

▪ **Riesgos elevados:** aquellos riesgos que tienen un impacto significativo en los derechos fundamentales o en la seguridad de las personas. La presencia de un riesgo elevado en el sistema de inteligencia artificial requerirá la adopción de medidas de mitigación adecuadas.

▪ **Riesgos limitados:** aquellos riesgos que tienen un impacto menor en los derechos fundamentales o en la seguridad de las personas, pero que todavía requieren medidas de mitigación.

▪ **Riesgos insignificantes:** aquellos riesgos que tienen un impacto mínimo en los derechos fundamentales o en la seguridad de las personas.

ARTÍCULO 11. VERIFICACIÓN Y CERTIFICACIÓN.

Los creadores o desarrolladores de sistemas de Inteligencia Artificial, en cualquier etapa de su ciclo de vida, deberán registrarlos conforme a los procedimientos previstos en el Reglamento ante el órgano correspondiente, para la implementación del sistema digital.

Los sistemas de inteligencia artificial antes de su lanzamiento en el Perú deberán ser sometidos a un proceso de verificación y certificación que garantice su calidad y seguridad. Los responsables deberán acreditar que los sistemas cumplen con los requisitos técnicos y legales aplicables, así como con los principios éticos y las obligaciones establecidas en la Constitución y esta ley, los ya existentes deberán regularizar ante las autoridades competentes.

TITULO IV: PROHIBICIONES Y/O RESTRICCIONES



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

ARTÍCULO 12: PROHIBICIONES Y/O RESTRICCIONES EN EL USO DE INTELIGENCIA ARTIFICIAL

- 1. Violación de derechos fundamentales y humanos:** cuando el sistema de inteligencia artificial es utilizado para violar los derechos humanos y fundamentales, como la privacidad, la libertad de expresión, la igualdad, la dignidad humana y otros.
- 2. Discriminación injusta:** cuando el sistema de inteligencia artificial es discriminatorio y produce resultados injustos o perjudiciales para ciertos grupos de personas, como la discriminación racial o de género.
- 3. Daños graves o riesgos para la seguridad:** cuando tenga potencial de causar daños graves a las personas, la sociedad o el medio ambiente.
- 4. Manipulación o influencia indebida:** cuando es utilizado para manipular o influir de manera indebida en la toma de decisiones importantes, como en procesos electorales o en la formación de opiniones públicas, atentando la integridad y la legitimidad de dichos procesos.
- 5. Falta de transparencia y rendición de cuentas:** cuando un sistema de inteligencia artificial opera de manera opaca y no se puede auditar o comprender cómo toma sus decisiones y puede ser difícil evaluar su impacto y responsabilizar a los actores involucrados. En tales casos, una prohibición podría ser necesaria hasta que se establezcan mecanismos adecuados de transparencia y rendición de cuentas, así como en todos los casos que su uso genere la perpetuación de desigualdades o injusticias.
- 6. Se prohíbe el uso de Inteligencia Artificial:** con fines ilegales, discriminatorios, maliciosos o que atenten contra los derechos fundamentales y humanos, la autoridad competente sanciona el incumplimiento de este principio.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

*"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"*

7. **En defensa nacional:** se prohíbe el uso de Inteligencia Artificial con fines de ataques a la soberanía nacional o con fines ilícitos contra entidades públicas, privadas de cualquier naturaleza o modalidad.
8. **En emergencia:** la utilización de sistemas de inteligencia artificial en situaciones de emergencia deberá ser justificada y limitada en el tiempo por las autoridades competentes.
9. **Prohibido todos los sistemas de categorización biométrica:** por creencias políticas, religiosas, filosóficas o por su raza y orientación sexual.
10. **Utilizar sistemas que puntúan:** sobre las personas en función de sus comportamientos o características personales. Asimismo, queda prohibido el uso de la inteligencia artificial capaz de manipular el comportamiento humano.
11. **Estarán prohibidos los sistemas:** que tengan como finalidad la expansión o creación de bases de datos faciales captando datos de manera indiscriminada a través de internet o de grabaciones audiovisuales.
12. **En los centros de trabajo y la escuela:** se encuentran prohibidos los sistemas de inteligencia artificial que pueden reconocer las emociones.

TITULO V: AUTORIDAD DE SUPERVISIÓN Y CONTROL

ARTÍCULO 13. AUTORIDAD DE SUPERVISIÓN

Encárguese a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, quien será la encargada de garantizar el cumplimiento de la ley y la regulación de los sistemas de inteligencia



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

artificial, incorporará a expertos en Inteligencia Artificial, ética, derecho y otros campos relevantes en el tema.

ARTÍCULO 14. INSPECCIONES Y SANCIONES

La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros será la autoridad de supervisión de la inteligencia artificial a nivel nacional:

- A.** Tendrá la autoridad para realizar inspecciones, investigaciones y auditorías de los sistemas de inteligencia artificial utilizados en diversos sectores, incluyendo el gobierno, la industria y los servicios públicos.
- B.** Llevar el registro público de sistemas de inteligencia con los procedimientos y requisitos que determine la autoridad de aplicación.
- C.** Recibir y examinar denuncias y reclamaciones.
- D.** Prohibir o restringir el uso de sistemas de inteligencia artificial que violen las disposiciones establecidas en esta ley o que presenten un riesgo significativo para los derechos humanos, civiles o políticos de las personas.
- E.** Requerir a los proveedores y desarrolladores de sistemas de inteligencia artificial la adopción de medidas específicas para prevenir y abordar la discriminación y los sesgos en los sistemas, incluyendo la suspensión o retirada del sistema en caso de incumplimiento.
- F.** Establecer sanciones por el incumplimiento de las obligaciones establecidas en la presente ley, pudiendo a su vez incluir multas y la retirada del registro de los sistemas de inteligencia artificial, también prohibiciones temporales o permanentes del uso de sistemas de inteligencia artificial, y otras acciones correctivas que sean apropiadas según la gravedad y recurrencia de la infracción.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

ARTÍCULO 15: COLABORACIÓN INTERNACIONAL.

La autoridad de supervisión de la inteligencia artificial a nivel nacional deberá articular con otras autoridades internacionales en la materia, con el fin de promover la coordinación y la armonización de las políticas y regulaciones en este ámbito.

ARTÍCULO 16: REGISTRO DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

Los responsables de sistemas de inteligencia artificial estarán obligados a registrar sus sistemas en un registro público creado por la autoridad de supervisión (Secretaría de Gobierno y Transformación Digital).

El registro contendrá:

- ✓ Las características técnicas del sistema de inteligencia artificial, incluyendo su finalidad y objetivos, su diseño y funcionamiento, y las técnicas y algoritmos utilizados.
- ✓ Los datos personales que tratan y el origen de los mismos, incluyendo la naturaleza de los datos, las fuentes de los datos, y los destinatarios de los datos.
- ✓ Las medidas de transparencia, responsabilidad y seguridad aplicadas al sistema de inteligencia artificial, incluyendo la existencia de un modelo de gobernanza del sistema, la explicabilidad y auditabilidad del sistema, y las medidas de seguridad técnica y organizativa implementadas.

La autoridad de supervisión establecerá los procedimientos y requisitos para el registro de sistemas de inteligencia artificial, y podrá establecer categorías



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

de sistemas sujetos a diferentes requisitos de registro, en función de su nivel de riesgo, teniendo en cuenta criterios tales como finalidad y objetivos del sistema, la naturaleza de los datos que trata y el grado de autonomía del sistema.

Los responsables de sistemas de inteligencia artificial deberán actualizar la información en el registro cuando se produzcan cambios significativos en los sistemas o en sus características técnicas o en los datos que tratan. La autoridad de supervisión tendrá acceso a la información del registro para llevar a cabo sus funciones de supervisión.

Los desarrolladores y proveedores de sistemas de inteligencia artificial deberán cooperar plenamente con la autoridad de supervisión y proporcionar acceso a sus sistemas, códigos fuente, datos y documentación relevante para fines de supervisión y control.

TITULO VI: COOPERACIÓN Y ESTÁNDARES INTERNACIONALES

ARTÍCULO 17: COOPERACIÓN INTERNACIONAL

Se promoverá la cooperación internacional para el desarrollo de estándares y regulaciones comunes en el campo de la Inteligencia Artificial. Se fomentará la colaboración entre gobiernos, organizaciones internacionales, la industria y la sociedad civil para abordar los desafíos relacionados con la Inteligencia Artificial.

ARTÍCULO 18: CUMPLIMIENTO Y SANCIONES



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

*"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"*

Las autoridades competentes serán responsables de hacer cumplir esta ley y aplicar sanciones en caso de incumplimiento. Las sanciones por violación de esta ley pueden incluir multas, prohibición de uso de sistemas de IA, suspensión de licencias y otras medidas adecuadas.

CAPITULO VII: RESPONSABILIDAD POR DAÑO O ERROR DE USO

ARTÍCULO 19: RESPONSABILIDAD DE LOS DESARROLLADORES Y PROVEEDORES

Los desarrolladores y proveedores de sistemas de inteligencia artificial serán responsables por los errores de uso de sus sistemas que causen daño. Serán considerados responsables si no han tomado las medidas razonables para evitar el error o si han incumplido con las regulaciones y estándares establecidos.

Los desarrolladores y proveedores deberán implementar medidas de seguridad y pruebas adecuadas para minimizar los errores de uso y garantizar la calidad y fiabilidad de sus sistemas.

En caso de que se produzca un error de uso y se demuestre la responsabilidad de los desarrolladores o proveedores, estos deberán reparar los daños causados, compensar a las personas afectadas y tomar las medidas necesarias para evitar la repetición del error en el futuro.

ARTÍCULO 20: RESPONSABILIDAD DE LOS USUARIOS

Los usuarios de los sistemas de inteligencia artificial serán responsables por el uso inadecuado de dichos sistemas y por minimizar los riesgos asociados. Deberán utilizar los sistemas de acuerdo con las instrucciones proporcionadas, en cumplimiento de las regulaciones establecidas en concordancia con los principios y prohibiciones de la presente ley.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Los usuarios deberán ser diligentes en la selección y configuración de los sistemas de inteligencia artificial, considerando las características y limitaciones de los mismos, y garantizando que se utilicen de manera ética y responsable.

En caso de un error de uso por parte de los usuarios que resulte en daño a terceros, los usuarios serán responsables por dicho daño y deberán tomar las medidas necesarias para mitigar las consecuencias adversas y compensar a las personas afectadas.

ARTÍCULO 21: SEGURO DE RESPONSABILIDAD CIVIL

Los desarrolladores, proveedores y usuarios de sistemas de inteligencia artificial deberán contar con un seguro de responsabilidad civil adecuado para cubrir los posibles daños ocasionados por errores de uso de los sistemas.

El seguro de responsabilidad civil deberá ser proporcionado por compañías de seguros autorizadas y deberá cubrir tanto los daños a personas como los daños a la propiedad.

ARTÍCULO 22: INFORMACIÓN Y EDUCACIÓN SOBRE USO RESPONSABLE

Los desarrolladores, proveedores y usuarios de sistemas de inteligencia artificial deberán proporcionar información clara y comprensible sobre el uso responsable de los sistemas, incluyendo las limitaciones, riesgos y precauciones necesarias.

Se fomentará la educación y formación en el uso responsable de la inteligencia artificial, promoviendo la conciencia de los riesgos asociados y las buenas prácticas para evitar errores y minimizar los daños potenciales.

ARTÍCULO 23: DENUNCIA DE ERRORES DE USO



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Se establecerá un mecanismo de denuncia de errores de uso de la inteligencia artificial, donde las personas afectadas o cualquier persona que tenga conocimiento de un error de uso podrá informar a la autoridad competente.

Las denuncias de errores de uso deberán ser tratadas de manera confidencial y se tomarán las medidas necesarias para investigar y corregir los errores reportados, así como para aplicar las sanciones correspondientes en caso de negligencia o incumplimiento.

TITULO VIII: INVESTIGACIÓN, DESARROLLO Y CAPACITACIÓN

ARTÍCULO 24: FOMENTO DE LA INVESTIGACIÓN EN INTELIGENCIA ARTIFICIAL

Se promoverá la investigación en Inteligencia Artificial (IA) con el objetivo de fomentar avances científicos, tecnológicos y sociales en este campo. Se destinarán recursos e incentivos y se podrá crear un fondo, con aportes público-privado, para apoyar la investigación de vanguardia, la innovación y la colaboración en Inteligencia Artificial en la ley de presupuesto de cada año se asignará los recursos necesarios para dicho fin y debiendo ser requerido por la autoridad competente.

Se establecerán programas de financiamiento para proyectos de investigación en Inteligencia Artificial, tanto en el ámbito académico como en la industria, con especial énfasis en áreas de interés estratégico y beneficio público.

El Estado podrá establecer incentivos fiscales, financieros y otros estímulos para la investigación y el desarrollo de la inteligencia artificial, en especial para proyectos que tengan como objetivo mejorar el bienestar de la sociedad y promover la innovación.

La investigación en Inteligencia Artificial se llevará a cabo respetando los principios éticos y legales, y se fomentará la transparencia y el intercambio de conocimientos y resultados para promover un desarrollo responsable y beneficioso para la sociedad.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

*“Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho”*

ARTÍCULO 25: DESARROLLO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL

Se promoverá el desarrollo responsable de la IA, garantizando la consideración de los aspectos éticos, legales, sociales y de seguridad en todas las etapas del desarrollo de sistemas de Inteligencia Artificial.

Los desarrolladores de sistemas de Inteligencia Artificial deberán implementar prácticas de diseño ético y responsabilidad social, considerando la equidad, la transparencia, la privacidad y la seguridad en el desarrollo de los sistemas.

Se fomentará la colaboración y el diálogo entre los desarrolladores, investigadores, usuarios y la sociedad en general para asegurar que los sistemas de Inteligencia Artificial sean desarrollados de manera inclusiva y tomando en cuenta diversas perspectivas.

ARTÍCULO 26: CAPACITACIÓN Y FORMACIÓN EN INTELIGENCIA ARTIFICIAL

El Estado a través de los diferentes organismos a su cargo promoverá la capacitación y formación en Inteligencia Artificial para profesionales, investigadores y estudiantes, con el fin de desarrollar habilidades y competencias necesarias para comprender, utilizar y desarrollar sistemas de Inteligencia Artificial de manera ética y responsable.

Se establecerán programas de educación y capacitación en Inteligencia Artificial, tanto a nivel académico como en el ámbito laboral, que aborden aspectos técnicos, éticos, legales y sociales de la Inteligencia Artificial.

Se fomentará la colaboración entre instituciones educativas, centros de investigación y la industria para desarrollar programas de capacitación actualizados y relevantes, adaptados a las necesidades y avances en el campo de la IA.

ARTÍCULO 27: INTERCAMBIO DE CONOCIMIENTOS Y COOPERACIÓN INTERNACIONAL

Se fomentará el intercambio de conocimientos, datos y mejores prácticas en el campo de la Inteligencia Artificial a nivel nacional e internacional, promoviendo la cooperación entre diferentes países, organizaciones y sectores.

Se establecerán acuerdos de cooperación y colaboración internacional en materia de Inteligencia Artificial, con el objetivo de promover estándares comunes, intercambio de información y desarrollo conjunto de políticas y regulaciones.

Se participará activamente en iniciativas internacionales que aborden los desafíos éticos, legales y sociales de la IA, y se buscará influir en la agenda global para garantizar el desarrollo responsable y sostenible de la IA a nivel mundial.

TITULO IX: DISPOSICIONES PRESUPUESTALES Y DE ADAPTACIÓN

ARTÍCULO 28: ADAPTACIÓN NORMATIVA

Las autoridades competentes deberán realizar las modificaciones necesarias en las normativas existentes para asegurar la coherencia y complementariedad con esta ley de regulación del desarrollo y uso de la inteligencia artificial.

Las autoridades competentes deberán promover la difusión y el conocimiento de esta ley entre los actores relevantes, así como proporcionar orientación y apoyo técnico para su implementación efectiva.

ARTÍCULO 29: DISPOSICIONES PRESUPUESTARIAS

Autorízase al Poder Ejecutivo a realizar las modificaciones e incorporaciones presupuestarias para el ejercicio fiscal vigente en los aspectos que se consideren necesarios para la implementación de la presente ley.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Asimismo, deberá preverse en el presupuesto del año inmediato subsiguiente la incorporación de los recursos necesarios para el correcto cumplimiento de las funciones de las autoridades de aplicación.

DISPOSICIÓN COMPLEMENTARIA FINAL

ÚNICA. - El Poder Ejecutivo aprueba el Reglamento de la presente ley mediante Decreto Supremo en un plazo máximo de noventa (120) días calendario, contados a partir del día siguiente de su publicación.

Lima, 07 de febrero del 2024



Firmado digitalmente por:
PAREDES CASTRO Francis
Jhasmina FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 13/02/2024 11:22:06-0500



Firmado digitalmente por:
ZEBALLOS MADARIAGA Carlos
Javier FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 12/02/2024 13:15:35-0500



Firmado digitalmente por:
ALCARRAZ AGUERO Yorel
Kira FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 13/02/2024 12:12:36-0500

CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República



Firmado digitalmente por:
LUNA GALVEZ Jose Leon FAU
20161740126 hard
Motivo: Soy el autor del
documento
Fecha: 12/02/2024 18:05:38-0500



Firmado digitalmente por:
LUNA GALVEZ Jose Leon FAU
20161740126 hard
Motivo: Soy el autor del
documento
Fecha: 12/02/2024 18:05:20-0500



Firmado digitalmente por:
PICON QUEDO Luis Raul FAU
20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 13/02/2024 10:35:24-0500



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**



Firmado digitalmente por:
JUAREZ CALLE Heidy
Lisbeth FAU 20161740128 soft
Motivo: Soy el autor del
documento
Fecha: 13/02/2024 12:48:33-0500



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

I. EXPOSICIÓN DE MOTIVOS

La presente iniciativa legislativa tiene como finalidad regular el uso de la Inteligencia Artificiales en el Perú, y que sean utilizadas de manera responsable y dentro de los parámetros éticos y legales que garanticen seguridad, transparencia, igualdad y equidad para sus usuarios y los peruanos.

La inteligencia artificial hace parte fundamental de la revolución industrial que está viviendo el mundo en la actualidad y si bien estamos como país en un momento muy temprano para hablar de regulaciones y leyes que encasillen el uso de estas nuevas tecnologías, si estamos a tiempo para definir marcos y empezar a desarrollar las bases institucionales, investigativas y culturales para una transición amena y una adaptación rápida a estas emergentes innovaciones que están aquí para quedarse.

Como bien se menciona en el acápite anterior, estamos a tiempo para plantear regulaciones estrictas sobre la Inteligencia Artificial, para ello sería necesario primero analizar los impactos y necesidades que traerán estas tecnologías, es por ello que el presente proyecto de ley tiene un enfoque preparativo y de planeación para garantizar un uso seguro, ético y responsable de esta tecnología en beneficio de la sociedad.

La Inteligencia Artificial está avanzando rápidamente y tiene el potencial de tener un impacto significativo en diversos aspectos de la vida cotidiana. La preparación temprana puede ayudar a que como país estemos listos para afrontar los desafíos y aprovechar las oportunidades que esta tecnología presenta.

En el Perú la Inteligencia Artificial ha presentado un avance inmenso teniendo utilidad positiva en algunos casos, pero también se ha presentado actos delictivos usando la Inteligencia Artificial.

II. MARCO NORMATIVO Y ANTECEDENTES LEGISLATIVOS

II.1 Marco normativo

La Constitución Política del Perú en su artículo 14 señala que: "Es deber del Estado promover el desarrollo científico y tecnológico del país"; en esa misma línea el Acuerdo Nacional en su vigésima política, señala que es política del Estado el "Desarrollo de la ciencia y la tecnología"¹.

La Ley 28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica en su artículo 2, señala que: "el desarrollo, promoción, consolidación, transferencia y difusión de la Ciencia, Tecnología e Innovación Tecnológica (CTIT), son de necesidad pública y de preferente interés nacional, como factores fundamentales para la productividad y el desarrollo nacional en sus diferentes niveles de gobierno.

La Ley 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica indica en su artículo 4 que: "el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica tiene por finalidad normar, dirigir, orientar, fomentar, coordinar, supervisar y evaluar acciones del Estado en el ámbito de la ciencia, tecnología e innovación tecnológica y promover e impulsar su desarrollo mediante la acción concertada y la complementariedad de programas y proyectos de las instituciones públicas, académicas, empresariales, organizaciones sociales y personales integrantes del SINACYT".

La Ley 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, que tiene como objeto promover el uso de la inteligencia artificial en el marco del proceso nacional de transformación digital privilegiando a la persona y el respeto de los derechos humanos con el fin de fomentar el desarrollo económico y social del país, en un entorno seguro que garantice su uso ético, sostenible, transparente, replicable y responsable.

II.2 Antecedentes legislativos Internacionales

¹ Visualícese el siguiente enlace sobre "Políticas del Estado" <https://acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado/politicas-de-estado-castellano/>



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

La Ley de Inteligencia Artificial de la Unión Europea es una primicia mundial, esta ley se aprobó en diciembre del 2023, se puede señalar que es un marco jurídico único para el desarrollo de una Inteligencia Artificial a nivel mundial, en la que se pueda confiar, sobre todo para la seguridad y los derechos fundamentales de las personas y las empresas. Este marco normativo establece normas para los modelos de Inteligencia Artificial grandes y potentes, garantizando que no presenten riesgos sistémicos para la Unión².

En el Reino Unido, el año 2022 se publicó el Código de conducta para regular los sesgos y otros riesgos de los sistemas de Inteligencia Artificial utilizados por el sector público, este código tiene como objeto promover de forma segura la Inteligencia Artificial, siendo protegida y fiable en todo el mundo y proporcionar orientaciones voluntarias para las acciones de las organizaciones que desarrollan los sistemas de Inteligencia Artificial más avanzados, incluidos los modelos básicos más avanzados y los sistemas de IA generativos³.

El Reglamento General de Datos (GDPR)- Unión Europea⁴; que, aunque no se enfoca específicamente en la regulación de la Inteligencia Artificial, establece normas estrictas sobre la protección de datos personales, incluyendo aquellos utilizados por sistemas de Inteligencia Artificial, lo que afecta directamente el desarrollo y uso de tecnologías de Inteligencia Artificial en la región.

II.3 Descripción del problema

² Vea la propuesta legislativa en el siguiente enlace <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

³ Visualícese el siguiente enlace: <https://digital-strategy.ec.europa.eu/es/library/hiroshima-process-international-code-conduct-advanced-ai-systems>

⁴ REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, visualícese en el siguiente enlace: <https://www.boe.es/doi/2016/119/L00001-00088.pdf>



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

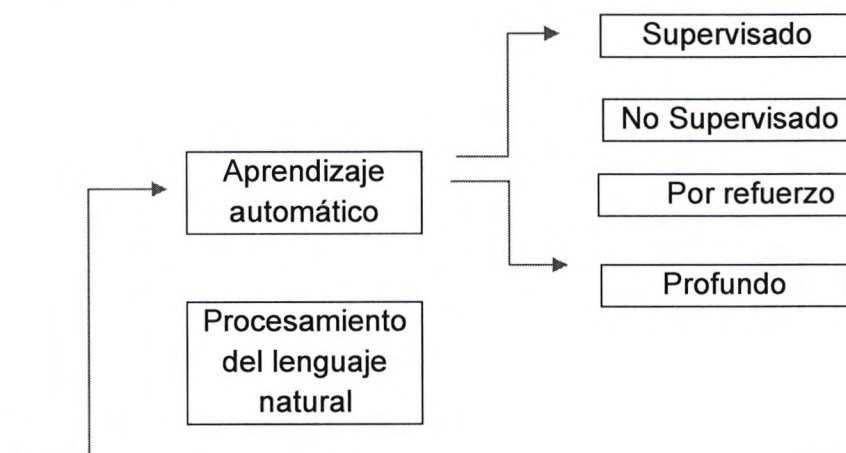
La Inteligencia Artificial (en adelante IA) con su avance, tiene el poder actualmente hasta de provocar una nueva revolución industrial.

La IA ha llegado mas allá de la ciencia ficción, hoy en día es parte de nuestra vida cotidiana, desde el uso de un asistente personal virtual para organizar nuestra agenda, hasta que nuestros teléfonos sugieran canciones que nos pueden gustar. Mas allá de facilitar nuestras vidas, los sistemas inteligentes nos están ayudando a resolver algunos de los mayores desafíos del mundo: tratar enfermedades crónicas, luchar contra el cambio climático y anticipar las amenazas meteorológicas.

La IA es una de las tecnologías mas estratégicas del siglo XXI, y con su llegada, se crearán numerosos puestos de trabajo, pero otros desaparecerán y la mayoría sufrirá transformaciones.

El desarrollo de la inteligencia artificial ha llegado a un punto crítico. Cualquier país que hace un avance en su aplicación puede tener una mayor oportunidad de liderar el mundo.

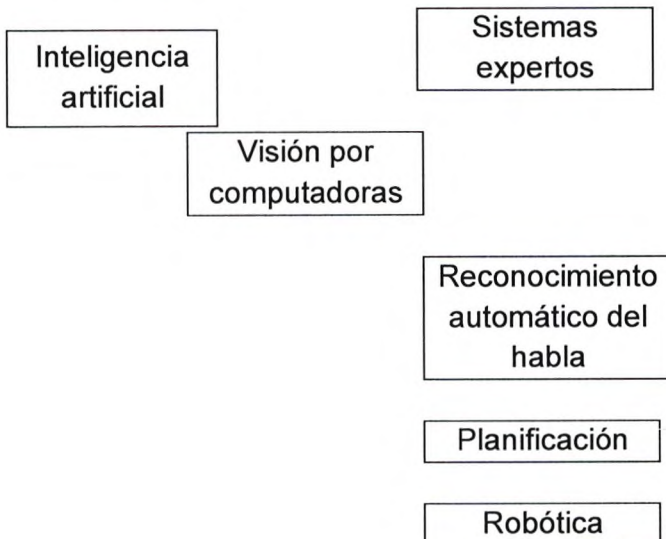
La inteligencia artificial no es un campo monolítico, sino que está dividido en varias ramas, tales como: el aprendizaje automático, el procesamiento del lenguaje natural, los sistemas expertos, la visión por computadoras, el reconocimiento automático del hablar, la planificación y la robótica, conforme se visualiza en la siguiente figura:





CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**“Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho”**



Fuente: propia

Según un informe de HelloSafe, la utilización de tecnologías de este tipo aumentó entre 2017 y 2022, un 50%.

Se estima por otro lado que los ingresos generados por la IA en aplicaciones podrían alcanzar los 31.200 millones de dólares en 2025.

En ese contexto, el Perú ha avanzado por a pasos gigantes en esta materia y una muestra de ello es el precedente de la Ley publicada el 05 de julio del año 2023 en favor del desarrollo económico y social del país.

Si bien dicha estrategia busca “proponer ejes, objetivos y acciones que promuevan la investigación, desarrollo y adopción de la IA, ayudar a crear soluciones a problemas nacionales en base a ella y generar nuevas oportunidades de desarrollo, priorizando sectores productivos y servicios públicos alineados a las estrategias y políticas nacionales”; dicha Ley no se encuentra enfocado en el tema del uso correcto de la inteligencia artificial, pues se sabe qué; según el Global AI Adoption Index 2022, realizado por Morning Consult para IBM, reveló que el 28% de las empresas en Perú están



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

implementando activamente la IA, ocupando así el cuarto lugar en Latinoamérica.

En ese sentido, nos damos cuenta el gran avance que está teniendo la IA en el Perú, siendo necesario establecer una Ley que regule el desarrollo y uso de la inteligencia artificial.

RECOPIACIÓN DE NOTICIAS QUE SUSTENTAN LA REGULACIÓN DEL PRESENTE PROYECTO DE LEY



De acuerdo con el coronel, el segundo delito más común en el país es el de estafas, siendo el primero el de robo de celulares. Destacó que la modalidad líder consiste en enviar mensajes a las víctimas ofreciendo ingresos a cambio de realizar tareas, pero todo resulta ser un engaño destinado a invertir dinero, incluso en falsas criptomonedas. **Esta técnica ha generado 506 casos, con pérdidas que alcanzan los 28 millones 870 mil 71 soles y 21 millones 381 mil 740 dólares;** y recomendó lo siguiente:



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

"Es crucial que la ciudadanía evite acceder a enlaces sospechosos que prometen dinero. Siempre hay que dudar y consultar a través de los órganos reguladores si una empresa tiene autorización. Además, se aconseja cambiar la clave de la tarjeta SIM para prevenir posibles estafas en caso del robo del celular".

El coronel Cruz añadió que la información proporcionada se limita exclusivamente a la perteneciente en la División de Estafas. Por ende, estos datos podrían quintuplicarse para abarcar los casos de las comisarías y de los departamentos de investigación criminal de Lima Metropolitana y todo el territorio peruano. *"De esta manera, a nivel nacional, se estima que podría haber alrededor de 6.000 casos"*, puntualizó. Además, existen otros tipos de estafas que no son electrónicas y se denuncian en comisarías y fiscalías comunes. Las modalidades que cubrió El Comercio a lo largo de este año fueron las siguientes (fuente RPP)⁵.

A. CLONACIÓN DE VOCES CON INTELIGENCIA ARTIFICIAL (IA)

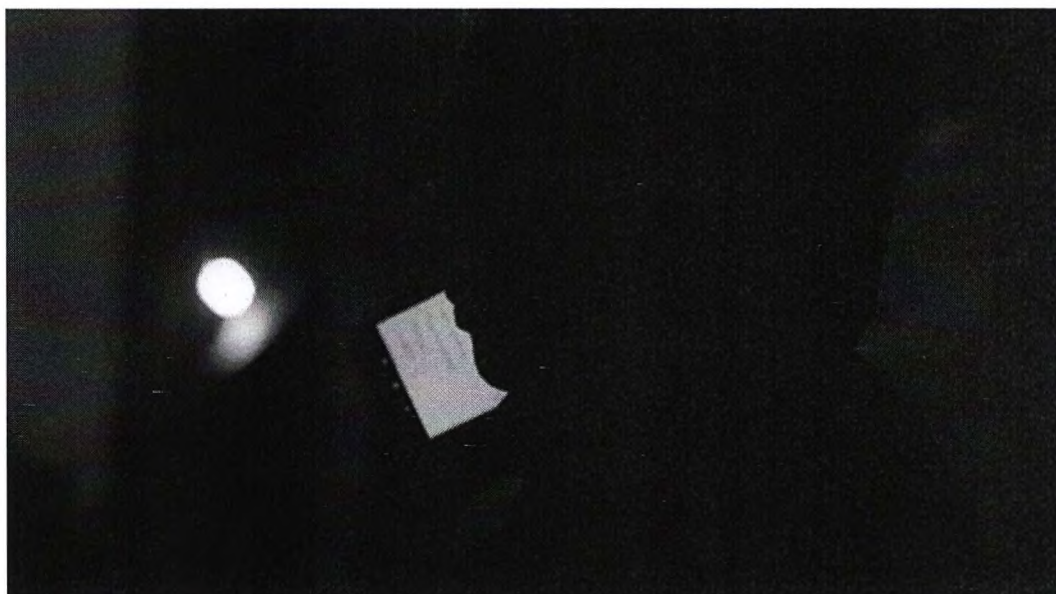
La estafa sigue un patrón en el cual un delincuente llama a una persona, simula haber secuestrado a un ser querido y utiliza voces clonadas con IA para extorsionar. El Comercio recogió 55 casos donde las víctimas escucharon voces idénticas a las de familiares solicitando dinero por alguna *"urgencia"* o amenaza.

⁵ Visualícese en el siguiente enlace: <https://elcomercio.pe/lima/desde-inteligencia-artificial-hasta-falsas-criptomonedas-estas-son-las-estafas-que-marcaron-el-ano-2023-pnp-crmenes-ciberdelincuencia-ciberdelitos-delitos-robo-estafa-modalidades-internet-noticia/>



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**



Los ciberdelincuentes suelen utilizar audios obtenidos previamente en las redes sociales de una persona para clonar su voz (foto: gec).

Erick Iriarte, abogado especializado en derecho digital y nuevas tecnologías, explicó a este diario que la técnica empleada se conoce como "deepfake". Se trata de un método utilizado en programas que permiten escribir un texto para convertirlo de forma casi inmediata en la misma voz de la víctima. Esto es posible al obtener previamente audios de sus redes sociales, facilitando que el programa imite de manera convincente su voz.

Además, Iriarte advirtió sobre la importancia de tener precaución al recibir llamadas en las que nadie responde. *"Los estafadores aprovechan ese momento cuando dices '¿aló?' para grabar tu voz, clonarla y luego utilizarla"*



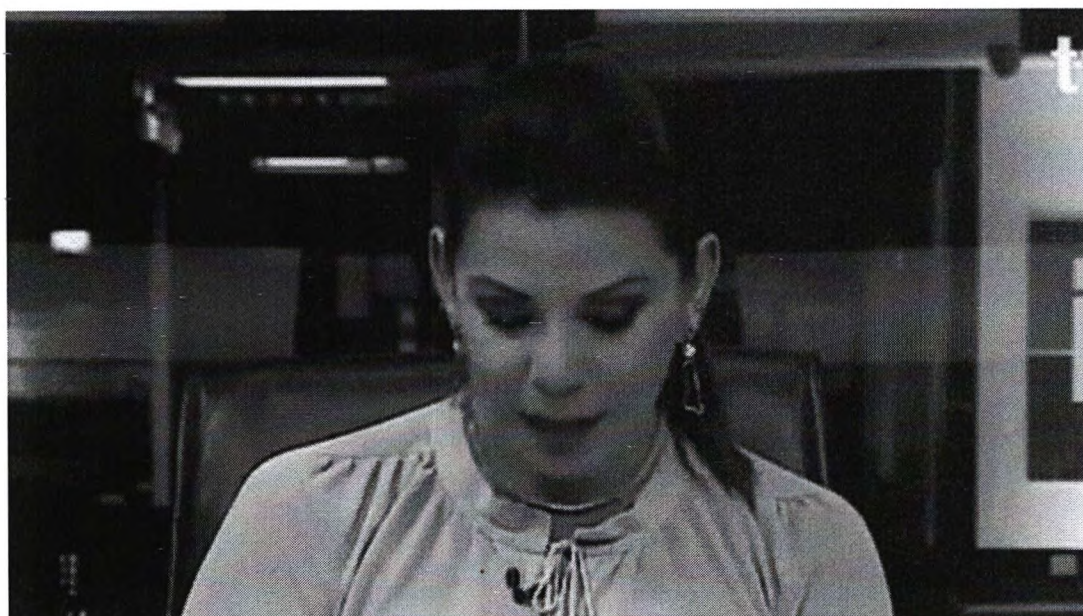
CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

en llamadas posteriores para llevar a cabo la estafa", dijo (Fuente: Diario el Comercio)⁶.

B. CLONACIÓN DE ROSTROS PARA PUBLICIDAD ENGAÑOSA

Conductoras de televisión han denunciado la manipulación de sus rostros y voces para promocionar productos sin su consentimiento, mediante el uso de la IA. María de Jesús González, conductora de TV Perú, compartió a El Comercio su experiencia como víctima de esta modalidad. "Está circulando en redes sociales un video falso donde presuntamente yo estoy animando a la gente a que haga inversiones por medio de una plataforma".



⁶ Visualícese el enlace: <https://elcomercio.pe/lima/clonacion-de-voz-para-estafar-con-inteligencia-artificial-como-funciona-esta-modalidad-y-que-recomendaciones-seguir-inseguridad-deepfake-ciberdelincuencia-hackers-secuestros-noticia/>



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Rodrigo Ochoa, líder de automatización e inteligencia artificial en Moventi, explicó que en estas situaciones también se recurre al "deepfake", ya que es efectivo para manipular audio y video. Se emplean algoritmos que, con la ayuda de una base audiovisual, son entrenados para almacenar y generar contenido.

"Se usan de dos a tres videos para que la IA sea capaz de gesticular e imitar la voz de las personas, también es un programa capaz de sincronizar los labios con las palabras que 'se están diciendo'. Siempre tiene que haber una base de datos, donde se obtiene la información, sea una persona mediática (por medio de su trabajo) o alguien común y corriente (por medio de sus redes sociales)", dijo (Fuente El Comercio).

C. LA ESTAFA EN CRIPTOMONEDAS

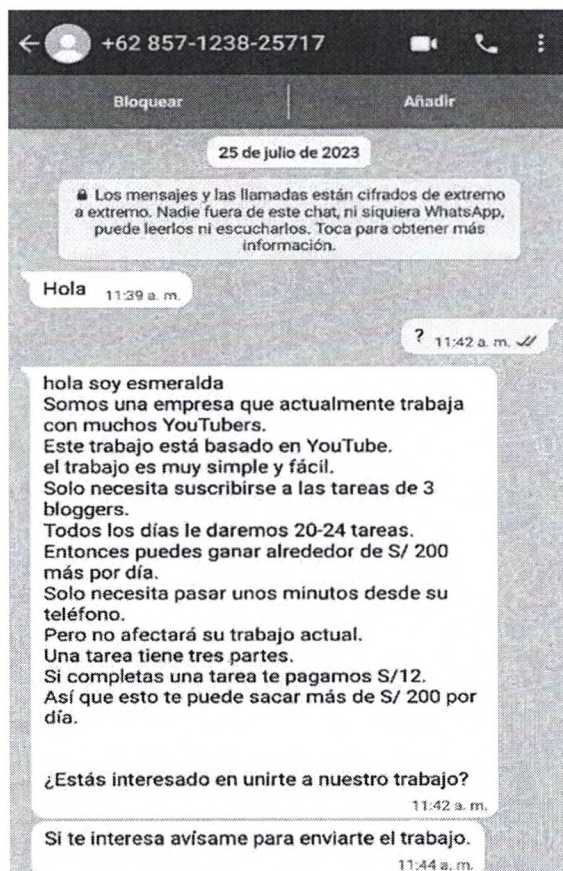
Una presunta red criminal ofrece por medio de WhatsApp la oportunidad de obtener importantes ingresos si los usuarios cumplen una serie de tareas. Su modus operandi es una forma paulatina de buscar generar confianza durante las primeras semanas.

Primero, el ciudadano recibe un mensaje donde le proponen realizar pequeñas "misiones" a cambio de dinero, por ejemplo, suscribirse a canales de YouTube. Es así que las víctimas comienzan a recibir sus primeras bonificaciones. Las próximas tareas consisten en depositar un monto en una plataforma de criptomonedas (activos digitales que algunas personas usan como activos financieros convencionales). No obstante, la cantidad que se debe abonar para seguir en el negocio crece constantemente y llega un punto en el que las personas ya no pueden pagar. Por ello, no recuperan jamás la supuesta inversión que depositaron.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**



Estos son los mensajes que reciben las víctimas para iniciar las tareas.

En este sistema de estafa, cuando una persona recibe recompensas monetarias, en realidad está ganando el dinero de alguien que también cayó en esta modalidad y depositó. Es decir, esta mafia ruletea con el dinero de unos para depositarle a otros y hacerles creer que sí hay rentabilidad. De ese modo, todo parece legítimo (Fuente: El Comercio).

D. LAS FALSAS ENTRADAS

Karol Janeth Arce Morales, la cabecilla de la estafa de entradas para el partido Perú-Argentina, está prófuga de la justicia. La Dirincrí logró capturar a su equipo de revendedores, incluida su hija, Jailín Acuña Arce, de 18 años,



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

apodada "daughter yankee", responsable de diseñar entradas falsificadas y gestionar publicaciones en redes sociales. La operación de la banda consistía en enviar entradas nominadas falsas a las víctimas, pactar reuniones presenciales para entregar los boletos y enviar audios de WhatsApp para ganar confianza.

La policía desmanteló la red y descubrió la identidad de la llamada "mommy yankee" y su hija. La estafa afectó a cientos de fanáticos que pagaron hasta tres veces el valor oficial de una entrada para el partido, rompiendo sus expectativas de ver a Lionel Messi. La investigación continúa para dar con el paradero de Karol Morales.



La Dirincri detuvo a la hija de la cabecilla de la banda, quien era su mano derecha. Sin embargo, la madre sigue fugitiva (Fuente: El Comercio).

E. SUPLANTACIÓN DE IDENTIDAD PARA ENGAÑAR A CLIENTES

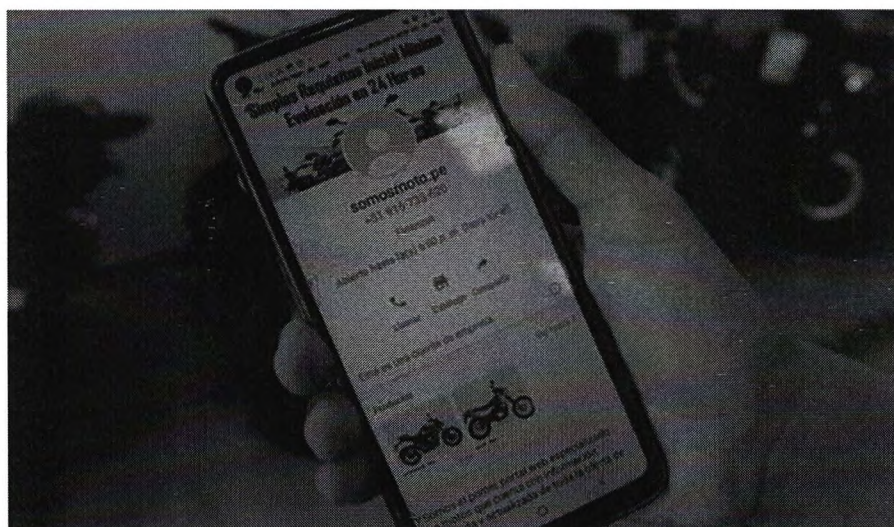


CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Nilton Macetas de Junín fue víctima de una estafa al intentar comprar una moto de "Somos Moto". Engañado por una red de estafadores, realizó dos depósitos creyendo que era la verdadera empresa, pero luego descubrió que todo era una farsa. El modus operandi de los estafadores involucraba atraer a compradores con precios tentadores, utilizando una página de Facebook y un número de WhatsApp falsos.

Los delincuentes, haciéndose pasar por "Somos Moto", pedían pagos adicionales bajo diversos pretextos después del primer depósito. Nilton, quien pagó 3.500 soles en total, se percató de la estafa cuando dejaron de responderle. Tras contactar a la verdadera compañía, descubrió que los estafadores copiaban la información y el logo de "Somos Moto". Tatiana Guichard, gerenta de la compañía, recomendó verificar siempre el RUC y el nombre comercial de una marca en la página de la Sunat antes de realizar cualquier pago.



Este es el número de los estafadores que se hacen pasar por 'Somos Moto' (916 733 620).



CARLOS JAVIER ZEBALLOS MADARIAGA Congresista de la República

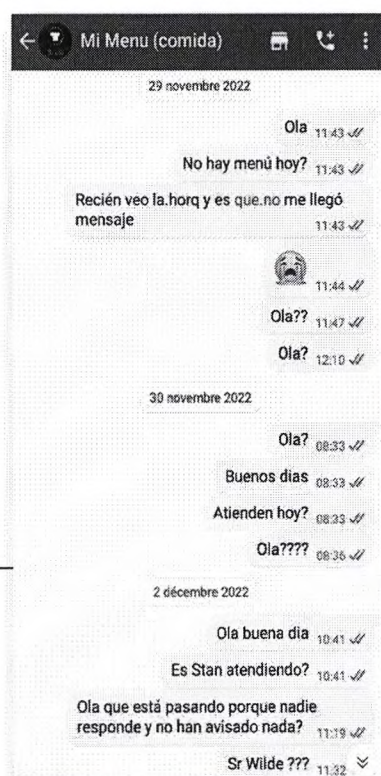
**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Andrés Mendoza, integrante del área de marketing de 'Somos Moto', explicó que los estafadores copian incluso el saludo automático virtual de la marca y mandan a las víctimas al sitio web oficial para elegir un modelo. Los depósitos, sin embargo, se realizan en cuentas no asociadas a la empresa (Fuente: El Comercio).

F. EL MENÚ ESTAFADOR

Un grupo de más de 20 personas se contactó el "Diario El Comercio" para denunciar que cayeron en una estafa por parte de "*Mi menú como en casa*", una empresa que ofrecía packs de menús a través de redes sociales. Entre los afectados se encuentra Ana Paula Castañeda, quien empezó a utilizar el servicio en mayo del 2022 y pagó 440 soles por 40 menús. Sin embargo, la empresa dejó de operar y eliminó sus redes sociales, dejándola con una deuda de 154 soles por 14 menús no consumidos.

Milagros Pariona y Edgar García también resultaron estafados. Milagros pagó 250 soles en noviembre del 2022 por 20 menús y se quedó con una deuda de 100 soles por 8 menús no consumidos. Edgar, quien utilizó el servicio desde agosto del 2022, pagó 400 soles por 40 menús y actualmente le deben 180 soles por 18 menús. El presunto estafador recibía depósitos en una cuenta a nombre de Wilde Rodríguez Espinosa, quien era el dueño de la empresa, pero dejó de responder después de alegar problemas internos.





CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Los consumidores se quedaron esperando la respuesta del personal.

Los afectados, tras descubrir el fraude, formaron un grupo de WhatsApp para rastrear al responsable. Exigen que Rodríguez devuelva el dinero por los menús no consumidos (Fuente: El Comercio).

G. LA ESTAFA DE LAS AGENCIAS DE VIAJES

Una organización criminal llevó a cabo estafas utilizando el juego digital del 'raspa y gana', que también lo hacían físicamente, aprovechándose de la ilusión de sus víctimas por viajar por el mundo. La modalidad se basa en ofrecer falsos premios a los consumidores, pero estos luego deben realizar acciones y pagos no acordados para supuestamente obtenerlos.

Ricardo Falconí, subgerente de seguridad de la Municipalidad de Miraflores, describió el modus operandi, que implica atraer a ciudadanos en la vía pública, animarlos a participar y ofrecerles premios ficticios, como viajes nacionales o internacionales. Una de las víctimas denunció a los estafadores ante la policía, logrando la captura de los sujetos en el cruce de la Av. Arequipa y la Av. José Pardo. La organización dirigía a sus víctimas a la oficina 1201 del edificio empresarial José Pardo, donde terminaban comprando supuestas membresías por alrededor de 1.400 dólares.

El personal policial y municipal incautó una gran cantidad de tickets de "raspa y gana" de la empresa llamada Espace Trip Grupo Travel, logrando la detención de once integrantes de la red criminal (Fuente: El Comercio).





CARLOS JAVIER ZEBALLOS MADARIAGA Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

Una red criminal que operaba bajo la modalidad del 'raspa y gana' fue descubierta por la policía y la Municipalidad de Miraflores. Foto: Andina, (Fuente: El Comercio).

H. MECANISMO DE ATENCIÓN

Respecto a estafas digitales, Erick Iriarte exhortó a la población a acudir a la División de Investigación de Delitos de Alta Tecnología (Divindat) y la Fiscalía de Ciberdelincuencia. Mientras que, en otros casos, se encuentran los canales del Indecopi, como el portal web, las líneas telefónicas 224 7777 (Lima) y 0 800 4 4040 (regiones), el correo electrónico sacreclamo@indecopi.gob.pe, y el WhatsApp 985 197 624.

Por otra parte, Juan Humberto Flores, Fiscal Superior y Coordinador Nacional de Ciberdelincuencia, indicó a El Comercio que se puede solicitar ayuda a la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, la Fiscalía Provincial Transitoria Especializada en Delitos de Ciberdelincuencia de La Libertad y la Fiscalía Provincial Transitoria Especializada en Delitos de Ciberdelincuencia de Arequipa. Mientras que, si ocurrió en otro departamento, se debe ir a la fiscalía penal correspondiente.

"Para evitar ser estafado, se debe identificar al proveedor y sus datos de contacto para saber a dónde acudir en caso exista un incumplimiento. Además, hay que revisar los comentarios de las redes sociales de la empresa con la cual se va a contratar un servicio, ya que, si tiene bajas calificaciones o no tiene habilitada la función de colocar comentarios, es sospechoso (...). Se tiene que exigir una boleta u otro documento que permita sustentar el consumo, servirá de respaldo en caso se requiera presentar una denuncia", enfatizó Juan Ñahue, abogado experto en protección al consumidor, (Fuente: El Comercio).



Lo último en Seguridad
Municipalidad de Miraflores presenta su plan
"Seguridad 2024" con más presencia



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

Escuchar a un familiar pidiendo dinero o verlo en situaciones comprometedoras puede generar dudas en cualquier persona. Hoy en día, la delincuencia se aprovecha de diversas herramientas tecnológicas para llevar a cabo sus fechorías, y esto incluye el uso de la inteligencia artificial. ¿Cuáles son los casos recientes y los delitos informáticos que han aumentado en lo que va del año?

I. UTILIZACIÓN DE LA VOZ E IMAGEN DE LA PRESIDENTA DE LA REPÚBLICA DINA BOLUARTE ZEGARRA

Ni la presidenta de República, Dina Boluarte, se salva de la delincuencia cuando esta usa herramientas tecnológicas como la **inteligencia artificial** para manipular la imagen y voz de las personas con el objetivo de cometer **delitos informáticos**.



La presidenta de la República, Dina Boluarte, ha sido víctima de la ciberdelincuencia, luego de que su voz fuera utilizada para crear videos falsos con inteligencia artificial (IA) De esta manera, se intenta estafar personas con la promesa de duplicar ganancias a cambio de una inversión monetaria.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

"Solo necesita hacer un depósito único de 950 soles peruanos en el sistema, la plataforma administrará ese dinero y realizará transacciones rentables todos los días. Quantum IA tiene una tasa de éxito del 100% en las operaciones que realiza y le garantizo que si realiza el depósito mínimo de 950 nuevos soles peruano esta noche, verá más de S/2.000 en su cuenta para la mañana siguiente", se escucha en un video expuesto por ATV, donde hay una voz similar a la de la mandataria.

"(Existe) la oportunidad para cada peruano de ganar grandes sumas de dinero, independientemente de su profesión o ingresos actuales. Hoy en día, con la ayuda de la inteligencia artificial se pueden lograr muchas cosas, por lo que se tomó la decisión de aprovechar esta oportunidad. Así nació la plataforma llamada Quantum IA, que opera en diversos mercados y bolsas, sin que necesite invertir constantemente su dinero", añaden los estafadores.

Otra de las víctimas fue la conductora de radio y televisión Sara Abu Sabbaha, quien aparece en un video de Instagram sobre cómo ganar dinero fácilmente.

"La presidenta Dina Boluarte anunció que ahora cada peruano puede olvidarse de trabajar y, en cambio, obtener un ingreso pasivo de 50 mil nuevos soles peruanos al mes", se escucha decir a la periodista.





CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

El doctor Elmer Huerta también ha sufrido de este tipo de engaños con la utilización de su imagen. "Está circulando videos promocionando productos de dudosísima efectividad en la que salgo yo. Esos videos son completamente falsos y son productos de la inteligencia artificial. Clonan la voz, parece que somos nosotros", manifestó el especialista en RPP, (Fuente: RPP, El Comercio y ATV).

El Comercio Suscríbete por s/1 INICIA SESIÓN

POLICIALES / Noticias

Usan imagen del doctor Elmer Huerta y periodista Alvina Ruiz para promocionar falso producto para la visión

Una modalidad de estafa a través de las red social Facebook intenta vender un supuesto medicamento para la "restauración de la visión".

El Comercio Suscríbete por s/1 INICIA SESIÓN

en medicina más prestigioso de Europa al descubrir el método de restauración de la visión

998-131

ÚLTIMAS NOTICIAS

- Villa El Salvador: Pareja fue asesinada a balazos dentro de su propio auto
- Lurigancho-Chosica: Hombre murió tras caer del quinto piso de centro de rehabilitación
- San Juan de Miraflores: sicarios matan a balazos a mototaxista extranjero en la Av. Manuel Iglesias | VIDEO

Estafadores usan imagen del doctor Elmer Huerta y la periodista Alvina Ruiz en publicidad engañosa de producto que asegura recupera la visión "en pocas semanas". (Captura: América Noticias)

Redacción EC

06/10/2022 10H23

PARA SUSCRIPTORES

- ★ Primera jefa de tránsito: "En solo 16 días denunciamos a 47 personas por intentar sobornar a policías"

J. ESTAFAS CON INTELIGENCIA ARTIFICIAL

Hasta septiembre del 2023, se ha registrado en el Perú más de 94 denuncias por estafa con la ayuda de IA. Bajo esta modalidad, los ciberdelincuentes han ganado más de 1 millón de soles, según la Policía Nacional del Perú (PNP)

El coronel Luis Huamán manifestó que una de las formas en que los criminales roban la identidad de sus víctimas es a través de programas que copian las voces de familiares o amigos.

No obstante, esta tecnología no solo se utiliza para sustraer grandes cantidades de dinero; sino también para acosar sexualmente a otras personas, mayormente mujeres. Uno de los casos más recordados en el país fue el de las alumnas del colegio St. George's, de Chorrillos.

En esa ocasión, sus compañeros, quienes también eran menores de edad, alteraron fotos de las estudiantes con inteligencia artificial para que parezcan estar desnudas.

En el reportaje se mostró un chat de WhatsApp que lleva el nombre de "Los Majes" y en el que se evidencia que los participantes coordinan la edición de las fotos de sus compañeras, incluso detallan qué aplicativos usar para la manipulación. Además, algunos de ellos comparten las imágenes que han obtenido y que deben ser sometidas a la inteligencia artificial. Incluso, como previendo algún tipo de problema futuro, uno de ellos pide que no envíen las fotos en dicho chat debido a que en los grupos de WhatsApp no se puede activar la opción de mensajes temporales.

Los padres de familia exigieron que los culpables sean expulsados de la institución. Sin embargo, no se pudo conocer si la escuela implementó este u otro tipo de castigo.

Por su parte, el colegio emitió un comunicado donde deslindó de cualquier tipo de responsabilidad. "Este incidente parece haber ocurrido en el ámbito virtual, completamente fuera del entorno escolar", dice el pronunciamiento.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

"Deepfake es el uso de videos falsos que aparentan ser reales donde distorsionan la imagen de una persona más que todo, una persona que sea publica, los lideres de opinión, en este caso estarían suplantando su identidad porque están suplantando su voz y la voz es una característica de la identidad humana", dijo el coronel Huamán (Fuente: RPP, El Comercio y Frecuencia Latina).

K. CIFRAS DE DELITOS INFORMÁTICOS Y COMUNES COMETIDOS CON IA POR FALTA DE REGULACIÓN LEGAL

La estafa mediante la clonación de la voz no es la única. Los delitos informáticos han experimentado un crecimiento en los últimos años, y la criminalidad ha sabido adaptarse a las nuevas circunstancias.

Esto se refleja en las cifras, que revelan que en el primer semestre de 2019 a nivel nacional se registraron 930 denuncias por delitos informáticos, mientras que en el mismo período de 2023 se ha llegado a las 7 734 denuncias, según datos recopilados por la Policía Nacional y presentados en el boletín semestral de seguridad ciudadana del Instituto de Defensa Legal.

Jesús Veliz, editor de Tecnología de RPP Noticias, explicó que las estafas más comunes se realizan a través de la modalidad conocida como "phishing", que implica el robo de datos mediante páginas web clonadas.

"El hábito más común es la clonación de páginas web, el phishing la idea que un delincuente crea una página web similar al de un banco de un servicio, de una página estatal, para que el usuario meta su usuario y contraseña ahí, y antes un delincuente se demoraba 10 minutos en hacerse, es decir un delincuente se demoraba 10 minutos en clonar un sitio web oficial, con inteligencia artificial el mismo tiempo lo invierte para hacer 17 mil páginas web



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

es decir que en 10 minutos ya no hace una, hace 17 mil de acuerdo a cifras de palo alto networks", indicó Jesús Veliz.

En el Perú, los delitos informáticos están tipificados en el artículo 9 de la Ley 30096, que establece que: "El que, de manera deliberada e ilegítima, daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

De acuerdo Erick Iriarte, experto en derecho digital, la legislación podría mejorarse mediante la inclusión de cláusulas generales que consideran el uso de tecnologías para cometer delitos como agravantes.

"En esta medida la tendencia parte de las tendencias es generar estos artículos de clausula general y lo otro es formar a jueces y fiscales en la persecución del delito incorporándole cláusulas de agravamiento o condiciones de agravamiento por el uso de tecnologías", expresó Erick Iriarte. Según los expertos, para evitar caer víctima de estos delitos, es importante mantener un alto nivel de desconfianza ante cualquier comunicación que llegue a tu teléfono, incluso cuestionar lo que se escuche o vea, sobre todo si proviene de fuente desconocida, ya que se podría estar frente a un caso de ciberdelincuencia.

La Inteligencia Artificial (IA) llegó a nuestras vidas para transformar la forma en que vivimos, trabajamos y nos relacionamos con nuestro entorno. Sin embargo, en los últimos años, esta tecnología ha dado pasos agigantados al punto de permitirnos generar contenido desde cero, como audios, imágenes o videos a partir de datos que le proporcionamos.

Al respecto, la ingeniera de sistemas peruana Natalie Gil explica que la IA lleva desarrollándose desde hace varias décadas, pero la novedad vista en los últimos años surge de la capacidad de esta tecnología de crear contenido "aparentemente" nuevo al gestionar y procesar grandes volúmenes de información.

De acuerdo con el coronel, el segundo delito más común en el país es el de estafas, siendo el primero el de robo de celulares. Destacó que la modalidad líder consiste en enviar mensajes a las víctimas ofreciendo ingresos a cambio de realizar tareas, pero todo resulta ser un engaño destinado a invertir dinero, incluso en falsas criptomonedas. Esta técnica ha generado 506 casos, con pérdidas que alcanzan los 28 millones 870 mil 71 soles y 21 millones 381 mil 740 dólares.

"Es crucial que la ciudadanía evite acceder a enlaces sospechosos que prometen dinero. Siempre hay que dudar y consultar a través de los órganos reguladores si una empresa tiene autorización. Además, se aconseja cambiar la clave de la tarjeta SIM para prevenir posibles estafas en caso del robo del celular", recomendó.

El coronel Cruz añadió que la información proporcionada se limita exclusivamente a la perteneciente en la División de Estafas. Por ende, estos datos podrían quintuplicarse para abarcar los casos de las comisarías y de los departamentos de investigación criminal de Lima Metropolitana y todo el territorio peruano. "De esta manera, a nivel nacional, se estima que podría haber alrededor de 6.000 casos", puntualizó. Además, existen otros tipos de estafas que no son electrónicas y se denuncian en comisarías y fiscalías comunes. Las modalidades que cubrió El Comercio a lo largo de este año fueron las siguientes.

III.EFECTOS DE LA NORMA EN LA LEGISLACIÓN NACIONAL

Tratándose de una iniciativa legislativa desarrolladora y regulatoria, de convertirse en ley, traería un incalculable beneficio a la sociedad ya que en la actualidad no existe norma regulatoria de la Inteligencia Artificial, como lo existe en el Continente Europeo y otros países que ya están disminuyendo sus índices delictivos y sacando provecho en favor del desarrollo de su país a la IA.



CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

**"Año del Bicentenario, de la consolidación de nuestra
Independencia, y de la conmemoración de las heroicas
batallas de Junín y Ayacucho"**

IV. ANÁLISIS COSTO - BENEFICIO

De convertirse en ley, la presente iniciativa legislativa no irrogará gastos al Tesoro Público, pues con la fórmula propuesta se busca establecer reglas en cuanto al uso de la Inteligencia Artificial, lo que en la actualidad es un bum de la tecnología, que viene acompañada de muchos peligros resultado de su mala utilización, es por ello el incalculable beneficio ante la promulgación de la presente ley para todos los peruanos.

V. VINCULACIÓN CON EL ACUERDO NACIONAL Y LA AGENDA LEGISLATIVA

La presente iniciativa legislativa tiene relación directa con la Política N° 1 del Acuerdo Nacional sobre el fortalecimiento del régimen democrático y el Estado de derecho, principalmente, en lo relativo a la defensa del imperio de la Constitución.