Ministerio de Educación,
Deporte y Cultura

REPÚBLICA
DEL ECUADOR

EQUIPO TÉCNICO
Soledad Albán Montalvo
Hamilton Cabrera Brunes
Víctor Pazmiño Puma

DISEÑO, DIAGRAMACIÓN E ILUSTRACIÓN
Adolfo Vasco Cruz

EQUIPO TÉCNICO EXTERNO

Marcelo Javier Sotaminga Cinilin

Primera Edición, 2026

Av. Amazonas N34-451 y Av. Atahualpa
Quito-Ecuador
www.educacion.gob.ec

Ministerio de Educación, Deporte y Cultura

REPÚBLICA DEL ECUADOR

Contenido

1. Introducción

El deepfake, término que combina “deep learning” (aprendizaje profundo) y “fake” (falso), representa uno de los riesgos digitales emergentes más significativos en la actualidad. Estas sofisticadas falsificaciones digitales, creadas mediante inteligencia artificial, pueden generar contenido multimedia manipulado con un realismo sin precedentes, engañando potencialmente a millones de personas.

Su tratamiento en el ámbito escolar es urgente por dos razones fundamentales: primero, la democratización tecnológica ha hecho que estas herramientas sean accesibles para cualquier persona con un dispositivo móvil, incluyendo estudiantes; segundo, plantean serios dilemas éticos como la violación de la privacidad, erosión de la confianza, ciberacoso amplificado y desafíos a la integridad académica.

Los casos documentados en entornos educativos internacionales demuestran que este no es un riesgo teórico, sino una realidad que ya impacta a estudiantes y docentes en diferentes contexto. Un informe de 2024 reveló que un 15% de estudiantes de secundaria en EE.UU. reportaron deepfakes sexuales en sus escuelas, mientras solo el 10% recibió algún tipo de apoyo institucional[1].

Esta situación no es ajena al contexto latinoamericano ni al ecuatoriano. En Ecuador, la penetración de internet en adolescentes supera el 85% (INEC, 2024), con un alto uso de redes sociales visuales como TikTok e Instagram, plataformas donde la difusión de deepfakes es particularmente efectiva. Esta realidad, combinada con la limitada alfabetización mediática en los niveles escolares, sitúa a los estudiantes en una posición de alto riesgo frente a contenidos manipulados.

Adicionalmente, Ecuador ocupa el segundo lugar en Latinoamérica en percepción diaria de información falsa, según una encuesta realizada en 2023, lo que evidencia un terreno fértil para la propagación de deepfakes en el contexto nacional[2].

Por lo tanto, este documento adopta la metodología “Conocer – Identificar – Prevenir”, para dotar a la comunidad educativa de herramientas conceptuales y prácticas que contribuyan a la formación de ciudadanos digitales críticos y responsables frente al riesgo de los deepfakes.

1 https://cdt.org/press/cdt-research-reveals-widespread-tech-powered-sexual-harassment-in-k-12-public-schools/

2 https://www.primicias.ec/noticias/sociedad/america-latina-ecuador-informacion-falsa-fake-news/

2. Ruta de Aprendizaje

2.1 Conocer el riesgo

Definición técnica y pedagógica del deepfake

El término deepfake, fusión de “deep learning” (aprendizaje profundo) y “fake” (falso), se refiere a contenido sintético generado mediante técnicas avanzadas de inteligencia artificial que permite la manipulación o creación de material audiovisual hiperrealista. A diferencia de las simples ediciones fotográficas tradicionales, los deepfakes representan un salto cualitativo en la capacidad de falsificación digital, permitiendo la suplantación de rostros, voces y movimientos con un nivel de realismo que dificulta su detección incluso para observadores experimentados.

Según Ramos-Zaga (2024), la tecnología deepfake utiliza redes neuronales profundas, particularmente las Generative Adversarial Networks (GANs), que son capaces de identificar y replicar patrones complejos en datos visuales y auditivos para generar contenido hiperrealista. Estas redes funcionan mediante un sistema de competencia entre dos algoritmos: uno que genera el contenido falso y otro que intenta detectar si es real o falso, mejorando continuamente la calidad de la falsificación.

Desde una perspectiva pedagógica, los deepfakes representan un desafío educativo multidimensional que requiere el desarrollo de competencias críticas, éticas y técnicas en los estudiantes. Constituyen un fenómeno que trasciende lo meramente tecnológico para convertirse en un tema de alfabetización mediática, ciudadanía digital y pensamiento crítico. Como señala Altieri (2024), los deepfakes obligan a repensar los procesos educativos relacionados con la verificación de información, la construcción de la identidad digital y la ética en entornos virtuales.

Características generales del deepfake

Los deepfakes presentan una serie de características distintivas que es importante conocer para su identificación y prevención:

1. Hiperrealismo: La principal característica de los deepfakes avanzados es su capacidad para generar contenido que resulta prácticamente indistinguible de la realidad para el ojo humano no entrenado.

2. Accesibilidad creciente: Lo que antes requería conocimientos técnicos avanzados y equipos costosos, ahora está al alcance de cualquier persona con un smartphone y acceso a aplicaciones gratuitas o de bajo costo.

3. Diversidad de formatos: Los deepfakes pueden manifestarse como:

– Deepfakes de video: Sustitución de rostros en videos existentes.

– Deepfakes de audio: Clonación de voces para crear declaraciones falsas.

– Imágenes generadas con IA: Creación de fotografías de personas o situaciones inexistentes.

– FaceSwap en tiempo real: Intercambio de rostros en videollamadas o transmisiones en vivo.

4. Potencial de viralización: Por su naturaleza impactante y su capacidad para generar reacciones emocionales, los deepfakes tienden a propagarse rápidamente en redes sociales y plataformas de mensajería.

5. **Dificultad de detección:** A medida que la tecnología avanza, los deepfakes se vuelven más sofisticados y difíciles de detectar, incluso para expertos y software especializado.

6. **Comercialización como servicio:** Ha surgido el concepto “Deepfake as a Service”, donde ciberdelincuentes ofrecen servicios de creación de deepfakes con precios que oscilan entre 10$ para imágenes y 500$ por minutos de vídeo (ISMS Forum, 2025).

Terminología clave asociada

Para comprender adecuadamente el fenómeno de los deepfakes, es fundamental familiarizarse con la siguiente terminología clave:

- **Inteligencia Artificial (IA):** Conjunto de algoritmos y sistemas computacionales diseñados para realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de patrones, el aprendizaje y la toma de decisiones.
- **Aprendizaje Profundo (Deep Learning):** Subcampo de la inteligencia artificial basado en redes neuronales artificiales con múltiples capas, que permite a los sistemas aprender y mejorar a partir de grandes cantidades de datos.
- **Redes Generativas Antagónicas (GANs):** Arquitectura de inteligencia artificial que enfrenta dos redes neuronales, una generadora y otra discriminadora, para producir contenido cada vez más realista.
- **Manipulación audiovisual:** Alteración de contenido audiovisual mediante técnicas digitales para modificar su apariencia, contexto o significado original.
- **Suplantación de identidad digital:** Acto de hacerse pasar por otra persona en entornos digitales, utilizando su imagen, voz o datos personales sin consentimiento.
- **Desinformación:** Difusión deliberada de información falsa o engañosa con la intención de confundir o manipular a la opinión pública.
- **Veracidad digital:** Cualidad de la información digital de ser verdadera, precisa y confiable, cada vez más amenazada por tecnologías como los deepfakes.
- **Ultrafalsificaciones:** Término utilizado en algunos países, como España, para referirse a los deepfakes en contextos legales y educativos.
- **Alfabetización mediática:** Capacidad para acceder, analizar, evaluar y crear contenidos en diversos formatos y plataformas, fundamental para enfrentar los riesgos de los deepfakes.
- **Ciudadanía digital:** Conjunto de normas, habilidades y comportamientos responsables relacionados con el uso de la tecnología, incluyendo la capacidad de discernir contenido auténtico de manipulado.

2.2 Identificar el riesgo

Señales de alerta en contenidos audiovisuales falsos

Identificar un deepfake puede resultar cada vez más difícil debido al constante avance de la tecnología. Sin embargo, existen ciertas señales de alerta que estudiantes y docentes pueden aprender a reconocer:

1. **Anomalías faciales:** Inconsistencias en el movimiento de los ojos, parpadeos poco naturales o inexistentes, asimetrías faciales inusuales, o movimientos descoordinados entre la cara y el resto del cuerpo.
2. **Problemas de sincronización:** Desajustes entre el movimiento de los labios y el audio, o entre las expresiones faciales y el contenido emocional del discurso.
3. **Bordes difusos o irregulares:** Especialmente alrededor del rostro, cuello o cabello, donde la fusión entre la imagen original y la manipulada puede ser imperfecta.
4. **Calidad inconsistente:** Diferencias notables de calidad, iluminación o textura entre distintas partes de la imagen o video.
5. **Distorsiones en accesorios:** Gafas, pendientes, sombreros u otros accesorios que pueden comportarse de manera extraña o desaparecer momentáneamente.
6. **Reflejos anómalos:** Inconsistencias en los reflejos de superficies como gafas, espejos o superficies brillantes.
7. **Metadatos sospechosos:** Información técnica del archivo que no coincide con la supuesta fuente o fecha de creación.
8. **Contexto incongruente:** Declaraciones o comportamientos que contradicen radicalmente lo conocido sobre la persona representada.

Estas señales de alerta son más evidentes en deepfakes de calidad media, mientras que las falsificaciones más sofisticadas pueden requerir herramientas especializadas.

Patrones típicos de uso malicioso en redes sociales, noticias falsas o suplantación de identidad

Los deepfakes suelen seguir patrones reconocibles de uso malicioso que es importante identificar:

1. **Difusión en plataformas de mensajería privada:** Muchos deepfakes, especialmente aquellos de contenido íntimo no consentido, se distribuyen inicialmente a través de aplicaciones como WhatsApp o Telegram, dificultando su rastreo y eliminación.

2. **Viralización rápida sin fuente verificable:** Contenido que se propaga explosivamente sin una fuente original clara o verificable, especialmente en momentos de alta tensión social o política.

3. **Narrativas sensacionalistas:** Acompañamiento del deepfake con textos que apelan a emociones fuertes o teorías conspirativas para aumentar su impacto y difusión.

4. **Timing estratégico:** Publicación en momentos clave, como períodos electorales, crisis institucionales o escándalos mediáticos, para maximizar su impacto disruptivo.

5. **Suplantación en comunicaciones personales:** Uso de deepfakes de audio o video en llamadas o mensajes para suplantar a personas de confianza y solicitar información sensible o transferencias económicas.

6. **Creación de perfiles falsos:** Utilización de imágenes generadas por IA para crear identidades ficticias en redes sociales, que luego establecen relaciones de confianza con potenciales víctimas.

7. **Manipulación del contexto:** Presentación de contenido real en un contexto falso o manipulado para alterar su significado original.

En el ámbito educativo, los patrones más comunes incluyen la creación de deepfakes para ridiculizar a compañeros o docentes, la manipulación de contenido para crear situaciones comprometedoras, y la suplantación de identidad para acceder a cuentas o información privada.

Factores de riesgo en estudiantes

Ciertos factores aumentan la vulnerabilidad de los estudiantes frente a los deepfakes, tanto como potenciales víctimas como posibles creadores:

1. Factores relacionados con la edad:

- Adolescencia temprana y media (12-16 años): Período de construcción de identidad y alta susceptibilidad a la presión social, con menor capacidad para evaluar riesgos a largo plazo.
- Transición a la adultez (17-19 años): Mayor autonomía digital con supervisión reducida, combinada con experimentación de límites sociales y éticos.

2. Factores relacionados con la alfabetización mediática:

- Limitada capacidad para verificar fuentes de información.
- Escasa experiencia en identificación de contenido manipulado.
- Tendencia a compartir contenido impactante sin verificación previa.
- Desconocimiento de las implicaciones legales y éticas de crear o compartir deepfakes.

3. Factores relacionados con el uso de redes sociales:

- Alta exposición digital mediante publicación frecuente de imágenes y videos personales.
- Configuraciones de privacidad inadecuadas que facilitan el acceso a material utilizable para deepfakes.
- Participación en retos o tendencias que implican compartir contenido personal.
- Amplia red de contactos no verificados o superficiales.

4. Factores psicosociales:

- Experiencias previas de bullying o exclusión social.
- Búsqueda de reconocimiento o popularidad entre pares.
- Dificultades en el manejo de impulsos y evaluación de consecuencias.
- Normalización de comportamientos de riesgo en entornos digitales.

En el marco preventivo, resulta fundamental considerar los lineamientos de la Ley Orgánica de Protección de Datos Personales (LOPDP), vigente en Ecuador desde 2021. Esta normativa garantiza el derecho a la protección de datos personales, incluyendo imágenes, voces y cualquier otro dato biométrico, como un derecho constitucional (Art. 66, numeral 19). En relación con los deepfakes, la utilización no consentida de estos datos para crear contenido manipulado constituye una clara vulneración del consentimiento informado y del tratamiento legítimo de datos (Art. 7 y 8). Por ello, desde las instituciones educativas se debe promover una cultura de respeto, conocimiento y apropiación de la privacidad de cada persona, estableciendo y dando a conocer aspectos como protocolos para la recolección, tratamiento y difusión de datos personales, en conformidad con los principios de legalidad, proporcionalidad y necesidad estipulados en dicha ley.

Casos reales

A continuación, se presentan casos reales que ilustran riesgo relacionado con deepfakes en entornos educativos:

Caso 1: Uso de inteligencia artificial para crear contenido sexual falso en un colegio de Quito

En octubre de 2023, se reportó que dos estudiantes de primero de bachillerato en una institución educativa privada del valle de Los Chillos, en Quito, utilizaron inteligencia artificial para generar imágenes y videos de contenido sexual falso con los rostros de al menos 24 compañeras. Las imágenes originales fueron tomadas sin consentimiento y luego manipuladas digitalmente. Se estima que se crearon alrededor de 700 archivos de este tipo. El caso fue denunciado por la fundación Grupo Rescate Escolar y está siendo investigado por la Fiscalía General del Estado por el presunto delito de pornografía infantil.[3]

Consecuencias (emocionales, sociales, legales, educativas)

Las consecuencias de los deepfakes en entornos educativos son multidimen-

3 https://www.vistazo.com/actualidad/nacional/alumnos-de-un-colegio-de-quito-usaron-inteligencia-artificial-para-crear-videos-sexuales-con-los-rostros-de-sus-companeras-ME6107394

sionales y pueden tener efectos duraderos:

Consecuencias emocionales y psicológicas:

- Ansiedad, depresión y estrés postraumático en víctimas de deepfakes.
- Sentimientos de vergüenza, humillación y violación de la intimidad.
- Pérdida de confianza en uno mismo y en los demás.
- Miedo constante a ser nuevamente victimizado o a la aparición de nuevo contenido falso.
- Desarrollo de conductas de aislamiento y evitación social.

Consecuencias sociales:

Daño reputacional que puede persistir incluso después de demostrar la falsedad del contenido.

- Ruptura de relaciones personales, familiares y de amistad.
- Estigmatización y exclusión de grupos sociales.
- Normalización de la desconfianza en las interacciones digitales.
- Polarización y conflictos en la comunidad educativa.

Consecuencias legales:

- Responsabilidad penal por delitos como suplantación de identidad, difamación, acoso o distribución de contenido íntimo sin consentimiento.
- En Ecuador, aunque no existe legislación específica sobre deepfakes, estos pueden ser procesados bajo figuras como la suplantación de identidad (Art. 212 del COIP) o la difusión de información de circulación restringida (Art. 229).
- Responsabilidad civil por daños y perjuicios causados a la víctima.
- Sanciones disciplinarias dentro de las instituciones educativas, que pueden incluir suspensión o expulsión.

Consecuencias educativas:

- Deterioro del rendimiento académico de las víctimas debido al impacto emocional.
- Absentismo escolar por miedo a enfrentar situaciones de acoso o humillación.
- Erosión de la confianza en el entorno educativo como espacio seguro.
- Distracción del proceso de aprendizaje por la gestión de crisis relacionadas con deepfakes.
- Cuestionamiento de la autenticidad de materiales educativos y evaluaciones.

Las consecuencias de los deepfakes trascienden el momento de su difusión inicial y pueden afectar la trayectoria educativa y el desarrollo psicosocial de los estudiantes a largo plazo, especialmente cuando las instituciones desconocen o aplican incorrectamente los protocolos para abordar estos incidentes.

2.3 Prevenir el riesgo

Estrategias de prevención desde el rol del estudiante

La prevención efectiva de los riesgos asociados a los deepfakes requiere un enfoque proactivo por parte de los estudiantes, quienes pueden implementar las siguientes estrategias:

Desarrollo del pensamiento crítico

El pensamiento crítico constituye la primera línea de defensa contra la desinformación y el contenido manipulado. Los estudiantes deben:

- Cuestionar sistemáticamente la veracidad de contenidos audiovisuales impactantes o sorprendentes.
- Analizar el contexto completo de la información, no solo fragmentos aislados.
- Identificar posibles motivaciones detrás de la creación y difusión de ciertos contenidos.
- Reconocer sus propios sesgos cognitivos que pueden hacerlos vulnerables a la manipulación.

El pensamiento crítico no es una habilidad innata sino una competencia que debe desarrollarse mediante la práctica constante y la reflexión guiada.

Verificación de fuentes

Los estudiantes deben adoptar hábitos rigurosos de verificación:

- Contrastar la información con múltiples fuentes confiables antes de aceptarla como verdadera.
- Verificar la autenticidad de las fuentes originales de vídeos o audios.
- Utilizar herramientas de búsqueda inversa de imágenes para comprobar la procedencia de fotografías.
- Consultar sitios especializados en verificación de hechos (fact-checking).
- Examinar la trayectoria y credibilidad de quienes difunden el contenido.

Gestión responsable de la identidad digital

Para reducir la vulnerabilidad ante posibles deepfakes, los estudiantes deben:

- Limitar la cantidad de material audiovisual personal que comparten en redes sociales.
- Configurar adecuadamente las opciones de privacidad en todas sus cuentas digitales.
- Revisar periódicamente su huella digital para detectar posibles suplantaciones.
- Utilizar autenticación de dos factores en todas sus cuentas importantes.
- Ser selectivos con las aplicaciones a las que otorgan permisos de acceso a su cámara o micrófono.

Alfabetización mediática específica

Los estudiantes deben desarrollar competencias específicas para la era de los deepfakes:

- Familiarizarse con las características técnicas básicas de los contenidos manipulados.
- Aprender a identificar inconsistencias en videos e imágenes sospechosas.
- Comprender cómo funcionan los algoritmos de recomendación que pueden amplificar la desinformación.
- Reconocer las estrategias emocionales utilizadas para hacer más virales los contenidos falsos.

Comportamiento ético digital

Es fundamental que los estudiantes:

Rechacen participar en la creación o difusión de deepfakes, incluso aquellos aparentemente inofensivos.

Denuncien contenido sospechoso a las autoridades escolares y plataformas correspondientes.

Apoyen a compañeros que puedan ser víctimas de deepfakes.

Promuevan una cultura de respeto a la privacidad y la imagen personal en entornos digitales.

Recomendaciones para docentes y familias

Para docentes:

Formación continua

- Mantenerse actualizados sobre las nuevas tecnologías y riesgos digitales.
- Participar en programas de capacitación sobre alfabetización mediática y detección de deepfakes.
- Colaborar con otros educadores para compartir recursos y estrategias efectivas.

Integración curricular

- Incorporar el análisis crítico de medios digitales en diversas asignaturas.
- Diseñar actividades que promuevan la verificación de fuentes y el contraste de información.
- Utilizar ejemplos de deepfakes educativos para desarrollar habilidades de detección.
- Vincular los contenidos curriculares con situaciones reales relacionadas con la desinformación digital.

Creación de espacios seguros

- Establecer canales de comunicación confidenciales para que los estudiantes reporten incidentes.
- Implementar protocolos claros de actuación ante casos de deepfakes en la comunidad educativa.
- Fomentar un ambiente de confianza donde los estudiantes se sientan cómodos discutiendo sus experiencias digitales.

Evaluación adaptada

- Diseñar métodos de evaluación que consideren la nueva realidad de los deepfakes.
- Implementar estrategias de verificación de autenticidad en trabajos audiovisuales.
- Valorar el proceso de creación y no solo el producto final para reducir incentivos de fraude.

Para familias:

Comunicación abierta

- Mantener conversaciones regulares sobre experiencias digitales sin juicios previos.
- Crear un ambiente donde los hijos se sientan cómodos compartiendo situaciones problemáticas.
- Establecer acuerdos familiares sobre el uso responsable de tecnología.
- Supervisión equilibrada
- Implementar controles parentales apropiados según la edad, sin invadir la privacidad.
- Conocer las aplicaciones y plataformas que utilizan los hijos.
- Monitorear cambios de comportamiento que puedan indicar problemas en entornos digitales.

Modelado de comportamiento

- Demostrar hábitos saludables de verificación de información.
- Practicar y promover el respeto a la privacidad y la imagen de otros.
- Utilizar la tecnología de manera equilibrada y consciente.

Colaboración con la escuela

- Participar en talleres y actividades formativas sobre ciudadanía digital.
- Mantener comunicación regular con docentes sobre el comportamiento digital de los hijos.
- Apoyar las iniciativas escolares de prevención de riesgos digitales.

Buenas prácticas en entornos digitales y herramientas de verificación

Buenas prácticas generales

1. Principio de precaución digital: Ante la duda sobre la autenticidad de un contenido, abstenerse de compartirlo hasta verificar su legitimidad.
2. Actualización constante: Mantener dispositivos y aplicaciones con las últimas actualizaciones de seguridad.
3. Diversificación de fuentes: Consultar múltiples medios y perspectivas antes de formarse una opinión sobre temas controvertidos.
4. Gestión del tiempo digital: Establecer períodos de desconexión para reducir la exposición constante a posible desinformación.
5. Comunicación responsable: Practicar la empatía digital y considerar el impacto potencial antes de crear o compartir contenido.

Herramientas específicas de verificación

Para verificación de imágenes:

- TinEye: Buscador de imágenes que puede encontrar versiones modificadas de fotografías originales. https://tineye.com/
- FotoForensics: Analiza metadatos y patrones de compresión para detectar manipulaciones. https://www.fotoforensics.com/
- Forensically: Herramienta gratuita que ofrece análisis de nivel de error, detección de clonación y otros métodos forenses. https://29a.ch/photo-forensics/#clone-detection

Para verificación de videos:

- InVID: Herramienta desarrollada por la Unión Europea para verificar la autenticidad de videos. https://www.invid-project.eu/tools-and-services/invid-verification-plugin/
- Amnesty International's YouTube DataViewer: Extrae metadatos y fotogramas clave para análisis. https://citizenevidence.amnestyusa.org/

Para verificación de audio:

- Resemble Detect: Plataforma gratuita que permite identificar si una voz ha sido clonada mediante inteligencia artificial. https://www.resemble.ai/detect

Plataformas educativas:

- MediaWise: Plataforma educativa impulsada por Poynter Institute, ofrece herramientas de alfabetización mediática para jóvenes, docentes y familias.

  https://www.poynter.org/mediawise/

Cabe mencionar que ninguna herramienta es infalible, por lo que se recomienda utilizar una combinación de ellas junto con el juicio crítico y la consulta a expertos cuando sea necesario.

Derechos digitales involucrados

La prevención de riesgos asociados a los deepfakes está intrínsecamente vinculada a la protección y ejercicio de diversos derechos digitales:

Derecho a la privacidad

- Control sobre la propia imagen y voz, incluyendo su uso en entornos digitales.
- Protección contra la vigilancia y el seguimiento no consentido.
- Derecho al olvido y a la eliminación de contenido personal no autorizado.

La Constitución de la República del Ecuador, en su artículo 66 numeral 20, reconoce y garantiza "el derecho a la intimidad personal y familiar" y en el artículo 92 "...solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación", fundamentos legales para la protección contra deepfakes no consentidos.

Derecho a la identidad

- Reconocimiento de la identidad digital como extensión de la identidad personal.
- Protección contra la suplantación y el uso indebido de la identidad.
- Derecho a la rectificación de información falsa que afecte la reputación.

El Código Orgánico Integral Penal (COIP) de Ecuador tipifica en su artículo 212 la suplantación de identidad como delito, aplicable a casos de deepfakes utilizados para este fin. (COIP 2014).

Derecho a la información veraz

- Acceso a información precisa y verificable.
- Protección contra la manipulación deliberada de hechos.
- Derecho a conocer el origen y proceso de creación de contenidos digitales.

La Ley Orgánica de Comunicación de Ecuador establece en su artículo 22 el derecho a recibir información verificada, oportuna, contextualizada y plural, principio extensible a los entornos digitales educativos.

Derecho a la educación digital

- Formación en competencias digitales necesarias para la era actual.
- Acceso a recursos educativos sobre seguridad y ciudadanía digital.
- Entornos de aprendizaje libres de acoso y manipulación digital.

La LOEI (Ley Orgánica de Educación Intercultural) de Ecuador reconoce implícitamente este derecho al establecer como uno de sus fines “la alfabetización digital y el uso de las tecnologías de la información y comunicación en el proceso educativo”.

3. Enfoque educativo

Relación del riesgo con el currículo nacional

El abordaje del deepfake como riesgo digital se integra de manera transversal en el currículo nacional ecuatoriano, estableciendo vínculos significativos con diversas áreas de conocimiento y ejes formativos:

Tecnologías de la Información y Comunicación (TIC)

El currículo nacional ecuatoriano contempla el área de TIC como fundamental para el desarrollo de competencias digitales en el Bachillerato General Unificado. La comprensión del fenómeno de los deepfakes se alinea directamente con los objetivos de aprendizaje propuestos en esta área. Por ejemplo:

"Utiliza las tecnologías de la información y la comunicación de manera responsable, ética y segura, para acceder, buscar, seleccionar, analizar y comunicar información y sus representaciones."

"Desarrolla habilidades de pensamiento crítico y creativo para analizar problemas, elaborar contenidos y aplicaciones informáticas que reflejen sus ideas y su contexto cultural." (Ministerio de Educación del Ecuador, 2022)

El estudio de los deepfakes permite concretar estos objetivos mediante actividades que promuevan el análisis crítico de contenidos digitales, la identificación de manipulaciones audiovisuales y la creación responsable de información en entornos digitales.

Educación para la Ciudadanía

Esta asignatura, presente en el Bachillerato General Unificado, aborda temas fundamentales para comprender las implicaciones sociales y éticas de los deepfakes:

- **CE.CS.EC.5.3:** "Examina el funcionamiento de la democracia representativa, mediante el análisis de las formas de participación ciudadana, la legitimidad de los procesos democráticos y el respeto a las opiniones diversas".

La proliferación de deepfakes representa un desafío para la democracia y la participación ciudadana informada, por lo que su estudio contribuye directamente a este criterio de evaluación, fomentando la reflexión sobre la importancia de la información veraz en los procesos democráticos.

Lengua y Literatura

El área de Lengua y Literatura también ofrece espacios para abordar la problemática de los deepfakes:

- **CE.LL.5.5:** "Consulta bases de datos digitales y otros recursos de la web con capacidad para seleccionar fuentes según el propósito de lectura, y valorar la confiabilidad e interés o punto de vista de las fuentes escogidas".

Este criterio se relaciona directamente con la necesidad de verificar la autenticidad de contenidos audiovisuales y textuales, habilidad esencial para enfrentar los riesgos de los deepfakes.

Tutoría

El espacio de Tutoría, establecido en la normativa educativa ecuatoriana como un momento para el acompañamiento y orientación de los estudiantes, constituye un escenario ideal para:

- Abordar situaciones específicas relacionadas con riesgos digitales que afecten a la comunidad educativa.
- Desarrollar habilidades socioemocionales necesarias para enfrentar situaciones de acoso o manipulación mediante deepfakes.
- Crear espacios de diálogo sobre experiencias digitales y estrategias de protección.
- Implementar programas de prevención adaptados a las necesidades específicas de cada grupo de estudiantes.

La tutoría debe promover "el desarrollo de habilidades para la vida y la prevención de problemáticas psicosociales", categoría donde se incluyen los riesgos digitales emergentes como los deepfakes.

Principios pedagógicos

El abordaje educativo de los deepfakes debe fundamentarse en principios pedagógicos que garanticen un aprendizaje significativo, contextualizado y transformador:

Principio de inclusión

La educación sobre riesgos digitales debe considerar la diversidad de realidades y necesidades de los estudiantes:

- Adaptar los contenidos y estrategias según los diferentes niveles de acceso tecnológico.
- Considerar las particularidades culturales y lingüísticas de las diversas comunidades ecuatorianas.
- Atender las necesidades específicas de estudiantes con discapacidad.
- Incorporar perspectivas de género que visibilicen los impactos diferenciados de los deepfakes.

Este principio se alinea con el Art. 2, literal v, de la LOEI, que establece la "equidad e inclusión" como principio fundamental de la educación ecuatoriana.

Principio de participación

El aprendizaje sobre deepfakes debe ser activo y participativo:

- Promover metodologías que posicionen al estudiante como protagonista de su proceso de aprendizaje.
- Fomentar el diálogo y el intercambio de experiencias entre pares.
- Involucrar a la comunidad educativa ampliada (familias, organizaciones locales) en las estrategias de prevención.
- Crear espacios para que los estudiantes desarrollen sus propias campañas de concientización.

La participación activa en la creación de soluciones aumenta significativamente la efectividad de los programas de prevención de riesgos digitales.

Principio de gamificación

La incorporación de elementos lúdicos y de juego en el abordaje de temas complejos como los deepfakes:

- Utilizar simulaciones y juegos de rol para practicar la identificación de contenido manipulado.
- Implementar sistemas de insignias o reconocimientos por el desarrollo de habilidades de verificación.
- Crear desafíos colaborativos que motiven la investigación sobre seguridad digital.
- Diseñar experiencias inmersivas que permitan comprender las consecuencias de los deepfakes.

La gamificación aumenta la retención de conocimientos sobre seguridad digital en un 40% comparado con métodos tradicionales de enseñanza.

Principio de contextualización

El aprendizaje debe vincularse con la realidad concreta de los estudiantes:

- Utilizar ejemplos relevantes para el contexto ecuatoriano.
- Analizar casos que reflejen las dinámicas sociales y culturales locales.
- Adaptar las estrategias de prevención a los recursos tecnológicos disponibles en cada comunidad.
- Considerar las particularidades del uso de redes sociales y plataformas digitales en Ecuador.

Este principio se fundamenta en la visión del Buen Vivir que orienta el sistema educativo ecuatoriano, promoviendo aprendizajes situados y culturalmente pertinentes.

Rol activo del estudiante como ciudadano digital crítico y responsable

El enfoque educativo para abordar los deepfakes debe posicionar al estudiante como un agente activo en la construcción de entornos digitales seguros y éticos:

Estudiante como verificador crítico

Más allá de ser consumidor pasivo de información, el estudiante debe desarrollar capacidades para:

- Analizar críticamente los contenidos que recibe y comparte.
- Aplicar protocolos de verificación antes de aceptar la veracidad de un contenido audiovisual.
- Cuestionar las fuentes y motivaciones detrás de información impactante o controversial.
- Desarrollar escepticismo saludable frente a contenidos virales sin fuentes verificables.

Estudiante como creador responsable

La ciudadanía digital implica también la producción ética de contenidos:

- Comprender las implicaciones éticas y legales de la creación y manipulación de contenidos digitales.
- Respetar los derechos de imagen y privacidad de otras per-

sonas.

- Utilizar tecnologías creativas de manera constructiva y respetuosa.
- Aplicar principios éticos en la edición y compartición de material audiovisual.

Estudiante como agente de cambio

El rol activo trasciende lo individual para proyectarse en la transformación social:

- Participar en campañas de concientización sobre riesgos digitales.
- Convertirse en mentor digital para compañeros y familiares.
- Proponer iniciativas para mejorar la seguridad digital en su comunidad educativa.
- Colaborar en la creación de protocolos de respuesta ante incidentes relacionados con deepfakes.

Estudiante como defensor de derechos digitales

La ciudadanía digital crítica implica el conocimiento y defensa de derechos:

- Reconocer situaciones de vulneración de derechos en entornos digitales.
- Conocer los mecanismos de denuncia y protección ante abusos digitales.
- Promover una cultura de respeto a la privacidad y la dignidad en espacios virtuales.
- Participar en diálogos sobre políticas y normativas relacionadas con la seguridad digital.

El empoderamiento de los estudiantes como ciudadanos digitales activos no solo los protege individualmente, sino que contribuye a la creación de comunidades virtuales más seguras y éticas para todos.

Este enfoque de ciudadanía digital crítica y responsable se alinea con la visión del perfil de salida del Bachillerato ecuatoriano, que busca formar ciudadanos “justos, innovadores y solidarios”, capaces de contribuir positivamente a la sociedad en todos los ámbitos, incluyendo el digital.

4. Anexos

4.1 Glosario de términos clave relacionados con el deepfake

Aprendizaje automático (Machine Learning): Rama de la inteligencia artificial que permite a los sistemas aprender y mejorar automáticamente a partir de la experiencia sin ser programados explícitamente.

Aprendizaje profundo (Deep Learning): Subcampo del aprendizaje automático que utiliza redes neuronales con múltiples capas para analizar diversos factores de datos con una estructura similar a la del cerebro humano.

Autenticación biométrica: Sistema de seguridad que utiliza características físicas o conductuales únicas de una persona para verificar su identidad.

Ciberacoso: Forma de intimidación que utiliza tecnologías digitales para hostigar, amenazar o humillar a una persona.

Ciudadanía digital: Conjunto de normas, habilidades y comportamientos responsables relacionados con el uso de la tecnología, incluyendo la capacidad de discernir contenido auténtico manipulado.

Clonación de voz: Tecnología que permite replicar la voz de una persona con suficiente precisión como para engañar a sistemas de reconocimiento o a otros humanos.

Deepfake: Técnica de inteligencia artificial que utiliza el aprendizaje profundo para crear, alterar o sintetizar imágenes o vídeos realistas de personas diciendo o haciendo cosas que nunca ocurrieron en realidad.

Desinformación: Difusión deliberada de información falsa o engañosa con la intención de confundir o manipular a la opinión pública.

Face swapping (intercambio de rostros): Técnica que permite sustituir el rostro de una persona por el de otra en imágenes o videos.

FaceSwap en tiempo real: Aplicación de la tecnología de intercambio de rostros durante transmisiones en vivo o videollamadas.

Fact-checking: Proceso de verificación de hechos para determinar la veracidad y precisión de afirmaciones o contenidos publicados.

Fake news: Noticias falsas diseñadas para desinformar o engañar a los lectores, a menudo con fines políticos o económicos.

Generative Adversarial Networks (GANs): Tipo de arquitectura de inteligencia artificial que enfrenta dos redes neuronales entre sí (una generadora y otra discriminadora) para producir nuevos datos sintéticos que parecen auténticos.

Huella digital: Rastro de datos que una persona deja en internet a través de sus actividades en línea.

Inteligencia Artificial (IA): Simulación de procesos de inteligencia humana por sistemas informáticos, especialmente sistemas de aprendizaje y resolución de problemas.

Manipulación audiovisual: Alteración de contenido de audio o video mediante técnicas digitales para modificar su apariencia, contexto o significado original.

Metadatos: Datos que proporcionan información sobre otros datos, como la fecha de creación de un archivo, su autor o la cámara utilizada para tomar una fotografía.

Pornografía no consentida: Distribución de imágenes o videos de contenido sexual sin el consentimiento de las personas que aparecen en ellos.

Redes neuronales: Sistemas computacionales inspirados en las redes neuronales biológicas que constituyen el cerebro humano, utilizados para reconocer patrones y aprender de los datos.

Síntesis de medios: Creación de contenido multimedia (imágenes, audio, video) mediante algoritmos computacionales en lugar de captura directa del mundo real.

Suplantación de identidad digital: Acto de hacerse pasar por otra persona en entornos digitales, utilizando su imagen, voz o datos personales sin consentimiento.

Ultrafalsificaciones: Término utilizado en algunos países, como España, para referirse a los deepfakes en contextos legales y educativos.

Verificación de fuentes: Proceso de evaluación de la credibilidad y fiabilidad de las fuentes de información.

Veracidad digital: Cualidad de la información digital de ser verdadera, precisa y confiable, cada vez más amenazada por tecnologías como los deepfakes.

5. Referencias Bibliográficas

Altieri, M. (2024). Deepfakes in education: Legal and ethical challenges. Journal of Educational Technology, 15(2), 45–62. Citado en MiAulaTec (2025). https://miaulatec.com/featured/deepfake-cuando-el-lado-oscuro-de-la-inteligencia-artificial-amenaza-las-aulas/

Asamblea Nacional del Ecuador. (2019). Ley Orgánica de Comunicación. Ministerio de Telecomunicaciones y de la Sociedad de la Información. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/01/Ley-Organica-de-Comunicaci%C3%B3n.pdf

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales (Registro Oficial Suplemento 459, 26 de mayo de 2021). https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

BBC News. (2023, septiembre 23). AI-generated naked child images shock Spanish town of Almendralejo. https://www.bbc.com/news/world-europe-66877718

El País México. (2023, octubre 14). Acusado un universitario de alterar con inteligencia artificial miles de imágenes de alumnas para venderlas como pornografía. https://elpais.com/mexico/2023-10-14/acusado-un-universitario-de-alterar-con-inteligencia-artificial-miles-de-imagenes-de-alumnas-para-venderlas-como-pornografia.html

INEC. (2024). Tecnologías de la información y comunicación-TIC. Instituto Nacional de Estadística y Censos. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2024/202407_Tecnologia_de_la_Informacion_y_Comunicacion-TICs.pdf

ISMS Forum. (2025). Deepfakes: Riesgos, casos reales y desafíos en la era de la IA. Observatorio de Deepfake de ISMS Forum. https://www.ismsforum.es/ficheros/descargas/deepfake-final1742458135.pdf

Karnouskos, S. (2020). Artificial intelligence in digital media: The era of deepfakes. IEEE Transactions on Technology and Society, 1(3), 138–147. https://doi.org/10.1109/TTS.2020.3001312

Ministerio de Defensa del Ecuador. (2021). Código Orgánico Integral Penal (COIP). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Ministerio de Educación del Ecuador. (2022). Currículo priorizado con énfasis en competencias comunicacionales, matemáticas, digitales y socioemocionales: Bachillerato General Unificado. https://educacion.gob.ec/wp-content/uploads/downloads/2022/03/Curriculo-con-enfasis-en-CC-CM-CD-CS_-Bachillerato.pdf

Ministerio de Educación del Ecuador. (2023). Programa de participación estudiantil. Ministerio de Educación. https://educacion.gob.ec/programa-de-participacion-estudiantil/

UNESCO. (2024a). Informe de seguimiento de la educación en el mundo 2024, informe sobre género: La tecnología en los términos de ellas. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. https://doi.org/10.54676/PVKW6667

UNESCO. (2024b). La UNESCO advierte sobre el impacto de las redes sociales en las jóvenes. https://www.unesco.org/gem-report/es/articles/un-nuevo-informe-de-la-unesco-advierte-que-las-redes-sociales-afectan-al-bienestar-el-aprendizaje-y

Asamblea Nacional del Ecuador. (2017). Ley Orgánica de Educación Intercultural (LOEI) codificada. Ministerio de Educación del Ecuador. https://educacion.gob.ec/wp-content/uploads/downloads/2017/02/Ley_Organica_de_Educacion_Intercultural_LOEI_codificado.pdf

Ministerio de Educación,
Deporte y Cultura

@MinisterioEducacionEcuador

@Educacion_Ec

www.educacion.gob.ec