

# REVISTA DIGITAL PARA LA NUEVA GENERACIÓN



**VINCULACIÓN**  
CON LA SOCIEDAD



# EDITORIAL



VINCULACIÓN  
CON LA SOCIEDAD

Estimados lectores,



Nos sentimos muy contentos de compartir con ustedes esta revista digital, creada con entusiasmo, creatividad y muchas ganas de generar un cambio positivo. Este recurso educativo ha sido elaborado por un grupo de estudiantes de las diferentes carreras: administración de empresas, derecho, educación y marketing, que juntos comparten una misma visión: educar a la ciudadanía en la era digital para el uso responsable de la tecnología.

En la revista *Redes inteligentes: revista digital para la nueva generación*, queremos hablar de una situación que afecta hoy en día a los adolescentes y jóvenes de todo el mundo cuando hacen uso del internet. Por esta razón, esta revista nace precisamente con ese propósito fundamental: ofrecer un espacio para la reflexión y el diálogo sobre los retos del entorno digital.

En esta revista buscamos motivar a nuestros lectores a ser ciudadanos digitales, capaces de usar las redes con inteligencia, empatía y conciencia.

Gracias por acompañarnos en esta nueva iniciativa. Te invitamos a formar parte de un grandioso aprendizaje y que en cada página que leas, adquieras nuevos conocimientos y que lo disfrutes tanto como nosotros.

¡Bienvenido! Te animamos a sumergirte en esta experiencia digital con nosotros.



# ÍNDICE

- 01** Ciudadano digital y ética: la brújula moral en un mundo digital.
- 02** Mis derechos y deberes digitales: controlando mi presencia en línea.
- 03** Los peligros en la red: riesgos y retos presentes en Ecuador.
- 04** La Ley, mi escudo de protección: COIP y derechos digitales.
- 05** Elimina el miedo a navegar en internet: prevención y autocuidado.
- 06** Evaluación formativa rápida.

# 01 CIUDADANO DIGITAL Y ÉTICA

## LA BRÚJULA MORAL EN UN MUNDO DIGITAL

La ciudadanía digital (CD) no es simplemente conexión a internet; implica aprender a desarrollar competencias críticas, éticas y creativas para relacionarse en la red. Según la UNESCO (2020), ser un ciudadano digital implica comprender cómo la tecnología influye en la sociedad y actuar con responsabilidad, respeto y sentido democrático en los entornos digitales.

La ética digital es la base de este comportamiento, para ello, se centra en principios como la protección de datos, respeto a los demás en las redes, verificar la información antes de compartirla, respeto a la propiedad intelectual, etc.

Todo esto puede agruparse en valores que permiten el uso de la tecnología para el bien común, el justo comportamiento en el mundo de la red, en el mundo digital (Balladares y Jaramillo, 2022).



## EL DESAFÍO DE LA ALFABETIZACIÓN CRÍTICA

Sin embargo, en el caso ecuatoriano, el principal reto al respecto no es el acceso a la red de internet, sino la alfabetización crítica. Según un estudio en el *Protocolo de Actuación frente a la Violencia Digital* del Ministerio de Educación (2023), el 6,49 % de la juventud ecuatoriana confía ciegamente en la información proporcionada en la red, y eso nos habla de una carencia en cuanto a pensamiento crítico y habilidades informativas.



Por lo tanto, llevar a cabo una verdadera ciudadanía digital pasa por dejar de lado el consumo pasivo de la red y pasar a la evaluación, la selección y el uso ético de la información que circula en la red de internet, colaborando en una sociedad digital más justa, armoniosa e informada.

# MIS DERECHOS 02 Y DEBERES DIGITALES



## CONTROLANDO MI PRESENCIA EN LÍNEA

En este mundo completamente digitalizado en el que vivimos, todos tenemos diferentes tipos de obligaciones, derechos y deberes que estamos forzados a tener en cuenta y respetar para así poder gozar de una manera responsable y segura cuando se esté conectado en línea. Mosquera y Mosquera (2024) mencionan que, en nuestro país, Ecuador, los principales derechos digitales son: la privacidad, la protección de datos personales, el derecho al olvido digital, el acceso a la información y la seguridad cibernética.

La privacidad permite que toda nuestra información no sea utilizada sin nuestro consentimiento o autorización,

ya que la *Ley Orgánica de Protección de Datos Personales* nos faculta a que cada uno puede decidir la manera de recopilar, utilizar y almacenar toda nuestra información personal.

Por otra parte, la protección de datos personales nos da el control sobre cómo se recolecta, almacena y se utiliza nuestra información. Con base en la *Ley Orgánica de Protección de Datos Personales* del Ecuador, todas las compañías están en la obligación de manejar los datos y la información de una forma responsable y transparente.

Por otro lado, el derecho al olvido digital nos permite que



podamos solicitar que todos nuestros datos antiguos, incorrectos o que no tengan nada que ver con nosotros sean eliminados y así no perjudiquen nuestra seguridad o reputación. El acceso a la información significa que todos podemos solicitar y tener acceso a la información pública mediante diferentes mecanismos como la *Ley de Transparencia y Acceso a la Información*. Y por último, la seguridad cibernética nos garantiza que tenemos derecho a que en todas las plataformas y servicios digitales siempre esté protegida toda nuestra información a posibles ataques y cualquier uso indebido en el entorno digital.

## **USO SEGURO DE LAS CUENTAS BANCARIAS**

Al momento de crear una cuenta bancaria o al hacer uso de la banca móvil, la información de dichas cuentas es sensible por lo que se necesita una alta protección para evitar su divulgación, robo, manipulación indebida o alguna estafa que puede causar daños a nuestra integridad.

Por esta razón, las entidades financieras son las responsables de resguardar la seguridad de nuestros datos (Espinoza y Paredes, 2025). Sin embargo, como usuarios debemos ser precavidos, por lo que se recomienda: crear contraseñas seguras y fuertes y, no compartir con nadie la información.



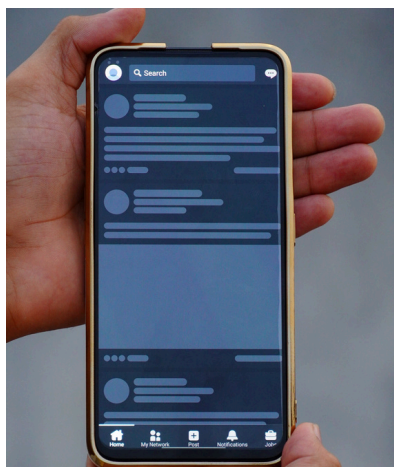
# 03 LOS PELIGROS EN LA RED



**EN ECUADOR SE  
REGISTRA UNA TASA  
DEL 52 % DE CASOS  
DE VIOLENCIA  
SEXUAL DIGITAL**

## RIESGOS Y RETOS PRESENTES EN ECUADOR

ChildFund es una organización internacional dedicada a la protección de NNA en situación de vulnerabilidad, la cual, desde 1984, trabaja con el Estado ecuatoriano y tiene por objetivo “mejorar el acceso a educación, salud, nutrición, inclusión económica y protección social”. Una prioridad transversal es el uso seguro de internet y la prevención de las violencias digitales, especialmente la violencia sexual en línea (Childfund, 2025). Sin embargo, cada día en el país, los niños y jóvenes consumen una gran cantidad de información en internet y esta se presenta a través del uso de aplicaciones como Facebook, Instagram, TikTok, YouTube, WhatsApp, entre otras (INEC, 2021).



Si bien es cierto que estas aplicaciones mundiales cuentan con filtros de seguridad que pueden ayudarnos en la protección de los más pequeños, no es del todo certero que, al mismo tiempo, se pueda prevenir de personas inescrupulosas que desarrollan alternativas para lograr vulnerar esa seguridad y llegar a sus víctimas. En efecto, la publicidad animada o los videojuegos suelen llamar la atención de los más jóvenes, quienes, llevados por la curiosidad, acceden a estos sitios sin saber que están proporcionando información al crear cuentas, abriendo las puertas a situaciones como *cyberbullying*, *grooming*, *phishing* (Machado, 2023).

## CASOS FRECUENTES EN ECUADOR

ChildFund menciona que la violencia digital en Ecuador va en aumento, identificando 22 formas de agresión en línea. Entre estas se encuentra la suplantación de identidad (76,10 %), las noticias falsas (68,31 %) y el ciberacoso (67,38 %) son los riesgos más reconocidos por niñas, niños y adolescentes al usar internet (Consejo de Igualdad Intergeneracional, 2025). Con esto se puede corroborar que, dentro del Ecuador, existe un índice alto de violencia digital.



**Foto: Thomas Park / Unsplash**

Sin embargo, uno de los delitos más comunes es el *grooming* el cual se caracteriza por ser una forma de abuso y acoso sexual de manera virtual. Según la Fundación Save the Children:

Se trata de un proceso en el que se produce un vínculo de confianza entre la víctima y el acosador. Este intenta aislar poco a poco al menor, y lo consigue desprendiéndose de su red de apoyo (familiares, profesores, amigos, etc.) y generando un ambiente de secretismo e intimidad. (ChildFund, 2025)

En Ecuador se ha registrado una tasa del 52 % de los casos de violencia sexual digital por la Fiscalía, los cuales están relacionados con el *grooming*. Además, nueve de cada diez víctimas de ofertas sexuales en internet son niñas adolescentes.

En caso de presentarse alguno de estos delitos, existen varias alternativas o rutas para brindar un acompañamiento a las víctimas. La reparación integral de los NNA debe ser saneada por medio de la justicia, el Estado brinda la posibilidad de denunciar dichos actos, así también, dar atención psicoemocional, eliminación de contenidos ilícitos filtrados por medio del agresor, y una indemnización. Sin embargo, se recomienda a los padres tener un control parental dentro de aplicaciones para poder controlar el contenido que está siendo visualizado por el niño e incluir conversaciones sobre el debido cuidado y uso del internet y aplicaciones.

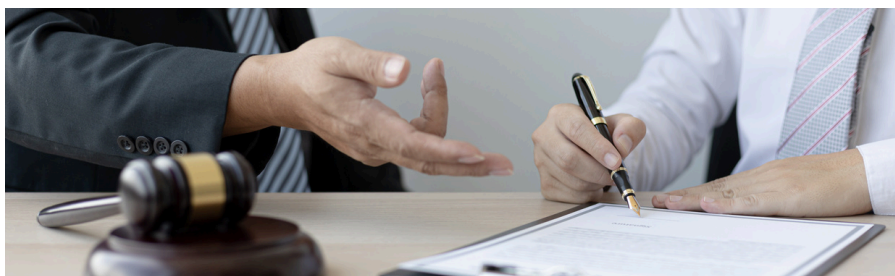


# 04 LA LEY, MI ESCUDO DE PROTECCIÓN

## COIP Y DERECHOS DIGITALES

El Código Orgánico Integral Penal (en adelante, COIP) considera diversas conductas que atentan contra la seguridad informática en el territorio nacional, mismas que se encuentran detalladas en el Libro Primero – Título IV – Capítulo Tercero – Sección Tercera (2014); aunque la normativa las aborda de forma general, su redacción busca ofrecer una protección amplia y adaptable frente a las diferentes modalidades de ciberdelito que puedan surgir.

Sin embargo, el COIP no es el único instrumento jurídico que garantiza nuestra protección como ciudadanos digitales. Nuestro ordenamiento jurídico incorpora otros cuerpos legales orientados a salvaguardar la información personal y promover la seguridad digital, fomentando la corresponsabilidad entre el Estado, las instituciones y los usuarios en el entorno virtual. Como leyes complementarias tenemos:



Ley Orgánica de Protección de Datos Personales (2021); Ley Orgánica de Telecomunicaciones (2015); Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002); Ley Orgánica de Transparencia y Acceso a la Información Pública (2004); Acuerdo No. 006-2021 - Política de Ciberseguridad.

Siendo ciudadanos digitales, es obligatorio comprender que en el entorno virtual, todos estamos expuestos a la vulneración de nuestros datos personales, a través de prácticas como el *phishing*, pudiendo ser la antesala para que personas malintencionadas lleguen al cometimiento de otros delitos como la extorsión (art. 185 del COIP).



Ante la detección de conductas o patrones inusuales en niños, niñas y adolescentes, es fundamental activar los mecanismos legales correspondientes para identificar y sancionar a los responsables. La Constitución de la República del Ecuador (2008) garantiza la protección integral de los grupos considerados vulnerables, mediante acciones constitucionales como el *hábeas data*, y obliga al sistema judicial a actuar con celeridad y eficacia en estos casos.

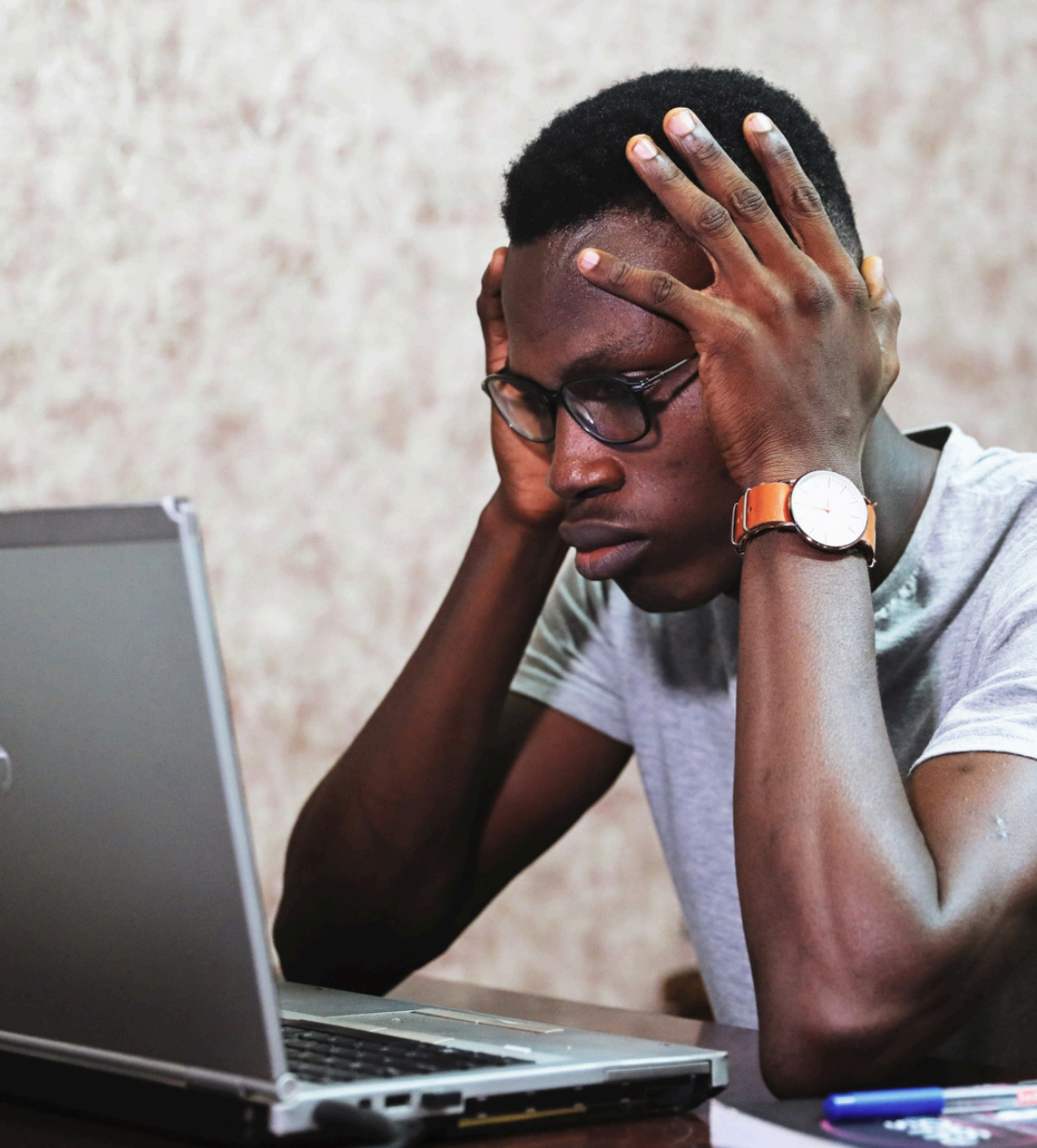


## PENALIZACIÓN DE LA VIOLACIÓN A LA INTIMIDAD

El *phishing* es una de las prácticas más comunes en nuestro entorno, aprovechando la “ignorancia digital”, existen personas que se dedican a enviar, principalmente, por correo electrónico, mensajes con características muy similares a las que usan los bancos, donde solicitan que el cliente ingrese sus datos de acceso, con una “advertencia” de que, al no hacerlo, se le van a bloquear los servicios. Este hecho configura el delito de acceso no consentido a sistemas informáticos previsto en el artículo 234 del COIP, y la posterior apropiación del dinero constituye transferencia electrónica de activo patrimonial, sancionada en el artículo 231 del mismo cuerpo legal. La pena privativa de libertad por este delito oscila entre los tres y cinco años.



# ELIMINA EL MIEDO 05 A NAVEGAR EN INTERNET



## PREVENCIÓN Y AUTOCUIDADO

Cada vez es más común ver gran parte del tiempo a los adolescentes y jóvenes conectados a las redes sociales, por lo cual resulta importante aplicar estrategias de prevención y autocuidado para un uso seguro y responsable de Internet. De esta manera, se pueden evitar riesgos que generan consecuencias que afecten su bienestar mental y emocional. De acuerdo con el Ministerio de Educación (2023), “una estrategia para generar un uso seguro y prevenir riesgos en internet es el desarrollo de competencias digitales en las y los estudiantes, de manera



proporcional a su edad y nivel de desarrollo con el fin de que puedan gestionar acciones de protección para sí mismos y para sus pares” (p. 33). Además, se requiere del acompañamiento y supervisión de un adulto en el hogar y la escuela, para que, con el tiempo los jóvenes regulen el uso de la tecnología y la exposición en internet por sí solos.



Como buenas prácticas digitales, se recomienda pensar antes de emitir comentarios que puedan resultar ofensivos o causar daño a los demás en las redes, no compartir información personal con extraños, no contestar números desconocidos, pedir ayuda a un familiar acerca de su seguridad en las redes sociales o dispositivos tecnológicos, usar contraseñas seguras y, ser resiliente para enfrentar problemas de ciberacoso (Microsoft Corporation, 2020).

## FOMENTANDO LA COMUNICACIÓN Y CONFIANZA

En la Pontificia Universidad Católica del Ecuador, en Quito, se llevó a cabo un evento organizado por ChildFund que promovió el diálogo sobre la prevención y el autocuidado frente a la violencia digital en niños, niñas y adolescentes. Según el informe elaborado por ChildFund (2025), “6 de cada 10 NNA aplican medidas de autocuidado digital”.

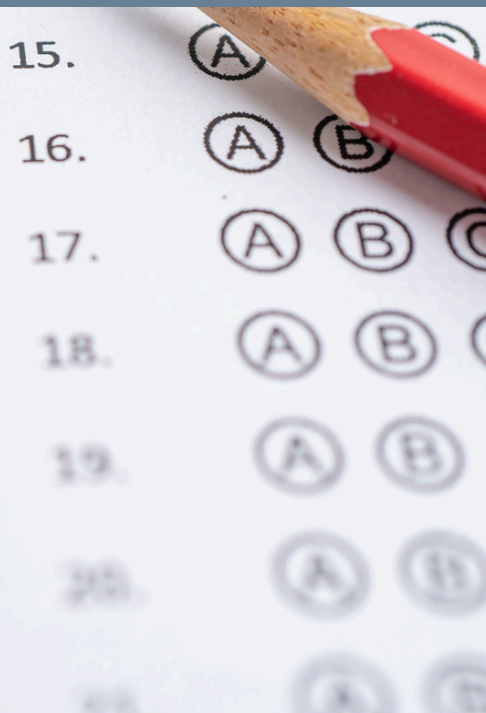
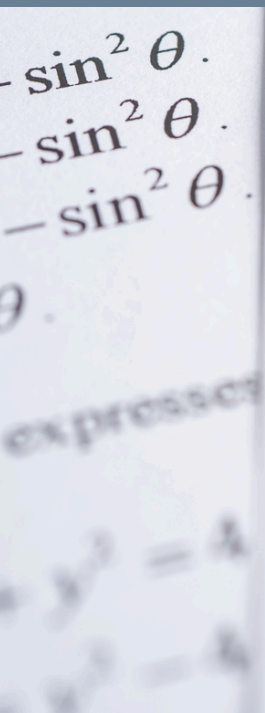
Por su parte, el Consejo Nacional para la Igualdad Intergeneracional (2025) señala que “el 94,96 % de niñas, niños y adolescentes identifica a sus padres como sus principales adultos de confianza”.

Sin embargo, para que los adolescentes y jóvenes se sientan seguros en denunciar situaciones de acoso, amenazas o ciberdelitos, es importante aplicar el modelo integral de las **5C**: comunicación, cuidado y autocuidado, conocimiento, compromiso y confianza (Mineduc, 2023). Por ende, se debe tener una conversación sin tener que juzgarlos, para ganar así la confianza de los adolescentes y jóvenes y que puedan expresarse. Esto hará sentirse seguros y pedir ayuda cuando lo necesiten.



# 06

# EVALUACIÓN FORMATIVA RÁPIDA



## ¿Listo para evaluar tu aprendizaje?

Con esta evaluación podrás descubrir cuánto sabes sobre ciudadanía digital, seguridad en internet y prevención de riesgos. Responde las preguntas de **“Verdadero o Falso”** y reflexiona sobre lo que has aprendido para seguir siendo una persona responsable y segura en el mundo digital.

ELIGE LA RESPUESTA CORRECTA	V	F
1. Ser ciudadano digital (CD) es solo tener acceso a internet.		
2. La ética digital comprende principios tales como: protección de datos, respeto y verificación de información.		
3. Como CD, solo tengo obligaciones.		
4. Siendo CD, puedo solicitar que la información que he proporcionado pueda ser borrada.		
5. El <i>grooming</i> es la práctica que tiene por objetivo difundir situaciones o imágenes falsas.		
6. La Constitución de la República del Ecuador considera el <i>hábeas data</i> como una forma de acceder a documentos públicos y privados.		
7. El Ministerio de Educación recomienda el acompañamiento y supervisión de un adulto responsable.		
8. Para prevenir riesgos en internet, es necesario que los adolescentes y jóvenes no desarrollen competencias digitales.		

<p><b>9.</b> El COIP no considera delitos contra la seguridad informática.</p>		
<p><b>10.</b> Para prevenir y proteger de los riesgos y vulneraciones que sufren los adolescentes en entornos digitales se recomienda aplicar las 5C.</p>		

## RESULTADOS

**1.** Ser CD implica aprender a desarrollar competencias críticas, éticas y creativas para relacionarse en la red. **(Falso)**

**2.** La ética digital sí comprende estos principios que ayudan la convivencia en entorno digital. **(Verdadero)**

**3.** Como CD también tengo derechos que se encuentran amparados en la normativa vigente. **(Falso)**

**4.** Este derecho está amparado en el artículo 15 de la *Ley Orgánica de Protección de Datos Personales*. **(Verdadero)**

**5.** El *grooming* es el acoso y abuso sexual virtual, donde adultos engañan a menores ganando su confianza para obtener fotos íntimas o buscar encuentros físicos. **(Falso)**

**6.** La CRE, en su artículo 92, nos permite acceder al *habeas data* para garantizar acceso a documentos públicos y privados. **(Verdadero)**

**7.** El *Protocolo de Actuación frente a la Violencia Digital* detectada en el Sistema Nacional de Educación recomienda la supervisión de un adulto responsable. **(Verdadero)**

**8.** El Ministerio de Educación plantea que, para generar un uso seguro de internet, es importante el desarrollo de competencias digitales acordes a la edad y nivel de desarrollo. **(Falso)**

**9.** El COIP si considera estos delitos específicamente en el Libro Primero – Título IV – Capítulo Tercero – Sección Tercera. **(Falso)**

**10.** El Ministerio de Educación en su *Protocolo de Actuación frente a la Violencia Digital* describe las **5C** para prevenir a niños, niñas y adolescentes de los riesgos que ocurren en la red. **(Verdadero)**

# Universidad Ecotec



# CRÉDITOS

---

Esta revista digital fue elaborada como un proyecto académico multidisciplinario que promueve la educación digital responsable. Agradecemos a todos los participantes por su dedicación, compromiso y creatividad.

## **Autores:**

JUAN JACINTO BARAHONA COELLO  
ULISES ANDREEY BARRAGAN ALVAREZ  
JOSE MAURICIO CABRERA JURADO  
JORMAN BRAI CHOMPOL VARGAS  
MARIA DE LOS ANGELES DUCHE MIELES  
JULIO CÉSAR GUATUMILLO BURGOS  
JUAN JOSE HUREL GUZMAN  
AMELIA MACIAS BELTRAN  
ERNESTO RAUL RONQUILLO ALVARADO  
FLOR MARIA RUIZ VILLAMAR  
JHONNY RICARDO VERA MEJIA



This work is licensed under CC BY-NC-SA 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-sa/4.0/>