Fecha de presentación: mayo, 2024, **Fecha de Aceptación**: junio, 2024, **Fecha de publicación**: julio, 2024

60

ESTRATEGIA EDUCATIVA PARA MITIGAR LA DIVULGACIÓN NO AUTORIZADA DE INFORMACIÓN PERSONAL EN ECUADOR

EDUCATIONAL STRATEGIE TO MITIGATE UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION IN ECUADOR

Pablo Ermely Espinosa Pico[1*]
E-mail: ua.pabloep80@uniandes.edu.ec
ORCID: https://orcid.org/0009-0009-2768-5912
Nathaly Nicole Palate Ayme[1]
E-mail: nathalypa32@uniandes.edu.ec
ORCID: https://orcid.org/0009-0006-5334-9064
Katiusca Brigett Corozo Duarte[1]
E-mail: katiuscacd88@uniandes.edu.ec
ORCID: https://orcid.org/0009-0006-2719-3238
Jimmy Fernando Ramírez Coque[1]
E-mail: jimmyrc18@uniandes.edu.ec
ORCID: https://orcid.org/0009-0001-1759-4613
*Autor para correspondencia:
[1]Universidad Regional Autónoma de Los Andes, Ambato. Ecuador

Cita sugerida (APA, séptima edición)

Espinosa Pico, P. E., Palate Ayme, N. N., Corozo Duarte, K. B., y Ramírez Coque, J. F. (2024). Estrategia educativa para mitigar la divulgación no autorizada de información personal en Ecuador. ***Revista Conrado, 20***(99), 589-598.

RESUMEN

El artículo aborda la problemática de la divulgación no autorizada de información personal en instituciones educativas en Ecuador, destacando sus implicaciones para la privacidad y seguridad. Se propone una estrategia educativa integral que busca concientizar y educar a la población sobre la protección de datos. La metodología combina enfoques cualitativos y cuantitativos, utilizando encuestas y análisis documental. Los resultados muestran un desconocimiento significativo sobre la interacción entre tecnología e información personal. Se destaca la importancia de la educación para mejorar la comprensión pública de las regulaciones de protección de datos. La estrategia propuesta incluye sesiones de capacitación, material educativo multimedia, integración en programas de estudio y campañas en redes sociales. Su implementación se considera crucial para generar conciencia, prevenir divulgaciones no autorizadas y promover una cultura de responsabilidad y ética en el uso de datos personales en Ecuador.

Palabras clave:

Divulgación, estrategia, implementación.

ABSTRACT

The article addresses the issue of unauthorized disclosure of personal information in educational institutions in Ecuador, emphasizing its implications for privacy and security. It proposes a comprehensive educational strategy aimed at raising awareness and educating the population about data protection. The methodology combines qualitative and quantitative approaches, using surveys and documentary analysis. The results reveal a significant lack of knowledge about the interaction between technology and personal information. The importance of education is emphasized to enhance public understanding of data protection regulations. The proposed strategy includes training sessions, multimedia educational material, integration into study programs, and campaigns on social networks. Its implementation is considered crucial to raise awareness, prevent unauthorized disclosures, and promote a culture of responsibility and ethics in the use of personal data in Ecuador.

Keywords:

Disclosure, strategy, implementation.

INTRODUCCIÓN

El avance tecnológico en el siglo XXI se distingue por el rápido progreso en el procesamiento de grandes volúmenes de datos, representando así un hito en la historia científica. No obstante, tanto los sistemas de gestión de información como la tecnología diseñada con estos propósitos están en constante evolución, ejerciendo un fuerte impacto en la sociedad. Numerosas tecnologías han optimizado las distintas modalidades de comunicación, alcanzando una universalidad que abarca a cada individuo. A través de dispositivos como los teléfonos inteligentes y otros medios, cada ciudadano tiene acceso a los beneficios proporcionados por las nuevas tecnologías. En los últimos años, la adopción y utilización de sistemas de compras en línea ha ganado notoriedad, generando diversas problemáticas para los consumidores de dicho sistema (Platero, 2020).

Los datos se han reconocido como el recurso precioso del siglo XXI, valorados por su utilidad en diversas industrias y aplicaciones. En las bases de datos se almacena una amplia gama de información proporcionada por los usuarios. Se ha llegado a la conclusión de que los parámetros que las empresas poseen para gestionar los recursos de información son de suma importancia, destacándose como el "nuevo oro". En la contemporaneidad, se puede afirmar que las diversas entidades, ya sean industrias, empresas u organizaciones, así como otros tipos de sistemas digitales que recopilan información personal del usuario, están obligadas a asegurar y garantizar la protección de dicha información. Es relevante destacar que mantener la información en el sistema facilitará la organización y gestión eficiente de los datos de cada individuo, permitiendo también su adquisición de manera rápida y efectiva. Además, es esencial contar con la accesibilidad necesaria para realizar copias de seguridad, lo que contribuirá a la protección ante posibles pérdidas de información, asegurando así una mayor efectividad en la seguridad proporcionada al usuario. (Shubladze, 2023)

En la época actual, los datos personales están accesibles en las redes de comunicación, gracias a los progresos tecnológicos. La información compartida en Internet y el ámbito del comercio electrónico ha adquirido una significativa importancia y puede ser aprovechada por entidades tanto públicas como privadas. Este fenómeno ha suscitado inquietudes, llevando a las autoridades a promulgar y ajustar leyes relacionadas con la protección de datos personales. La finalidad de estas normativas es prevenir el manejo inadecuado de la información, que podría vulnerar derechos fundamentales como la privacidad, la intimidad y la dignidad humana. Como resultado, se ha establecido de manera continua un marco normativo con el objetivo de salvaguardar el orden y proporcionar garantías legales, evitando así la afectación de derechos fundamentales debido a la evolución tecnológica. Ante esta problemática, varios países han expresado un fuerte interés en implementar nuevas regulaciones para el uso y la protección de los datos personales (Remache, 2019).

En tal sentido la Constitución de la República del Ecuador en el artículo 66, número 19 se detalla que: El derecho a la salvaguarda de los datos personales, englobando la facultad de acceder y determinar la información y datos de esta índole, conjuntamente con su resguardo correspondiente, implica que la obtención, almacenamiento, procesamiento, distribución o divulgación de dichos datos o información necesitará contar con la aprobación expresa del titular o ajustarse a lo dispuesto por la legislación vigente. (Ecuador. Asamblea Nacional Constituyente, 2008)

La información de carácter personal de cada usuario se considera de índole privada, dado que cualquier intento de utilización por parte de un tercero requiere previamente la obtención del consentimiento del propietario de dicha información. El consentimiento, en este contexto, se define como la autorización otorgada por el titular de la información para su uso específico. Además de obtener el consentimiento, es imperativo garantizar la seguridad de la información personal durante todo el proceso, desde la recopilación hasta cualquier forma de utilización, con el objetivo de preservar la confidencialidad y la integridad de los datos. Este enfoque no solo salvaguarda los derechos individuales, sino que también aborda la necesidad crítica de proteger la privacidad en el contexto de la gestión de datos personales.

Las plataformas de redes sociales, como Facebook, WhatsApp, Twitter e Instagram, han adquirido un papel muy importante, consolidándose como herramientas de influencia en la sociedad actual. Estas plataformas no solo han redefinido la comunicación interpersonal, sino que también emergen como agentes de poder en la configuración de dinámicas sociales y culturales. La interconexión global facilitada por estas redes sociales da lugar a una amplia difusión de información y una rápida transmisión de ideas, influyendo de manera significativa en la percepción, opinión y comportamiento de los usuarios. Este fenómeno subraya la creciente relevancia de las redes sociales como medios de comunicación poderosos, desempeñando un papel central en la construcción y transformación de la realidad social contemporánea (Steijvers, 2024).

La sociedad se ve cada vez más inmersa en el uso de medios tecnológicos, considerándolos esenciales dado que han evolucionado como herramientas fundamentales

de comunicación que facilitan la interacción entre individuos. La génesis de Facebook, ideada por su fundador Mark Zuckerberg durante sus estudios en Harvard, inicialmente como "Facemash", responde a la necesidad de mantener a los estudiantes conectados, ofreciendo un espacio para el intercambio de opiniones y experiencias. A lo largo del tiempo, Facebook ha evolucionado hasta convertirse en una plataforma de alcance global, permitiendo la comunicación entre individuos ubicados en diversas partes del mundo. Sin embargo, este fenómeno no está exento de riesgos, evidenciados por filtraciones de información de usuarios que han afectado la seguridad y privacidad de los mismos (Downing, 2022)we analyzed health-advertising tactics of digital medicine companies (n = 5.

Un caso paradigmático se registró en el año 2018, durante la campaña presidencial de Donald Trump, donde se produjo una filtración masiva de datos personales. En este episodio, se recopilaron datos sin el debido consentimiento de los usuarios, utilizándolos con fines políticos. Este incidente se convierte en una de las filtraciones más notables en la historia, donde la información obtenida fue empleada para construir perfiles psicográficos y determinar las características de personalidad de los usuarios de Facebook. Esto permitió al equipo de Trump enviar mensajes personalizados a cada uno de los votantes en la plataforma digital. Aunque no se ha demostrado de manera concluyente que la campaña haya utilizado ilegalmente esta información, la filtración generó repercusiones significativas (Zuboff, 2019).

Es relevante subrayar que en la actualidad existen diversas plataformas, tanto de índole social como profesional, y cada usuario ejerce su libertad al decidir qué información compartir. Asimismo, es crucial reflexionar sobre las implicaciones de estas decisiones, dado que, en el pasado, los datos eran considerados íntimos y privados. Sin embargo, la proliferación de sistemas de obtención de datos a gran escala en tiempos recientes ha contribuido a la disolución del concepto de privacidad asociado a la información. Una de las problemáticas que se ha generado al momento de acceder a la creación de una cuenta, es que pocos usuarios son lo que verifican, leen términos y condiciones de privacidad llegando así a un proceso en donde la información queda expuesta a cualquier persona, y cualquier persona podrá obtener la información que se proporciona, de manera autorizada por el propietario (Pöhn, 2023)therefore, access to related user accounts. The security of user accounts, again, is tied to the security of the corresponding primary and fallback authentication methods. Accounts can be linked to each other – by fallback authentication, through SSO, or by using the same authentication devices – creating an account network. These account networks enhance login comfort and are needed in case of account recovery, but they also increase each account's attack surface. In addition, misconfigurations might result in account inaccessibility. However, these problems can only be detected by analyzing single accounts first and then the resulting account networks. Despite the importance to understand account security and accessibility, almost no analysis methods exist. To address this need, this article presents the Authentication Analysis Framework (AAF.

La difusión de información personal a través de estas plataformas ha resultado en violaciones directas a la privacidad, lo que destaca la importancia de implementar una autorregulación en estos espacios en línea. Dado que son entornos de libre acceso, se requiere la colaboración de la sociedad, los proveedores de servicios y el Estado para abordar esta situación. Dado el crecimiento actual del número de usuarios en las redes sociales, que ahora cuenta con una población de millones de personas que comparten todo tipo de información personal, los derechos de intimidad, privacidad y protección de datos se han visto comprometidos. Los usuarios son responsables de la información que transmiten, pero hasta ahora las propuestas de solución ante los desafíos diarios en estos espacios en línea y los riesgos asociados han sido insuficientes (Tejada, 2019).

La filtración de datos personales en instituciones educativas es un fenómeno preocupante que implica la divulgación no autorizada de información sensible de estudiantes, personal académico y administrativo. Esta problemática compromete la privacidad y seguridad de los individuos afectados, además de tener consecuencias significativas en el ámbito educativo. La divulgación no autorizada de datos en instituciones educativas abarca diversos escenarios, como la exposición de calificaciones, información financiera, datos de contacto y otros detalles personales.

Por tanto, en el presente artículo se plantea como objetivo, proponer estrategias educativas efectivas destinadas a mitigar la divulgación no autorizada de información personal en Ecuador. Se pretende fortalecer la conciencia, conocimiento y prácticas relacionadas con la protección de datos entre la población ecuatoriana, contribuyendo así a la preservación de la privacidad y seguridad de la información personal en un entorno digital en constante evolución.

MATERIALES Y MÉTODOS

La metodología empleada en la investigación adopta un enfoque aplicado en el ámbito educativo, caracterizado

por su orientación cualitativa (Orozco, 2018). La propuesta resultante se sustenta en procesos teóricos y metodológicos, así como en categorías apriorísticas y emergentes, abordando aspectos vinculados a la construcción de la propuesta mediante la modelación. Además, se lleva a cabo la recopilación de información documental, obtenida de diversas fuentes, que incluyen proyectos de leyes y artículos a nivel mundial. Estos documentos buscan regular la protección de datos personales y la privacidad del usuario, involucrando procesos de codificación, triangulación y otros elementos inherentes a la propuesta en estudio (Hernández, 2018).

En el curso de este estudio, se utiliza el enfoque analítico-sintético. Este método implica la descomposición de la información recopilada de la bibliografía para luego sintetizar de manera organizada el tema propuesto, manteniendo la coherencia en la estructura sintáctica (Finol, 2020).

También se llevaron a cabo encuestas, las cuales fueron empleadas para obtener resultados de naturaleza cuantitativa. Estas encuestas se implementaron a través de la plataforma Google Forms, una herramienta que posibilita la creación de formularios en línea con el propósito de recopilar información de manera sistemática y eficaz. Su uso es frecuente en la realización de encuestas, cuestionarios, formularios de inscripción, evaluaciones y cualquier otra actividad que implique la recolección de datos con respuestas estructuradas (da Silva, 2019). Dichas encuestas fueron destinadas a individuos de la sociedad en general, y contaron con la participación de 50 personas que respondieron a la encuesta respectiva. Las preguntas planteadas en las encuestas abarcaron los siguientes aspectos:

1. ¿Usted ha sentido que por medios digitales su información personal ha sido robada?
2. ¿Sus cuentas personales han sido hackeadas?
3. ¿Usted ha aceptado términos y condiciones sin leer al respecto de lo que se trata?
4. ¿Alguna vez usted ha sido suplantado por otra persona con su información?
5. ¿Usted ha utilizado inteligencia artificial (Ej. Chat GPT)
6. ¿Diariamente qué tiempo usted utiliza redes sociales?
7. ¿Sabe los beneficios que brinda la ley orgánica de protección de datos personales?
8. ¿Sabía usted que, al aceptar términos y condiciones sin leer, puede otorgar el acceso a su información personal?
9. ¿Considera usted que la tecnología es peligrosa?

RESULTADOS Y DISCUSIÓN

Las encuestas representan una herramienta crucial en la recopilación de datos, ofreciendo una visión panorámica de las percepciones, actitudes y experiencias de la población en relación con nuestro objeto de estudio. Diseñadas meticulosamente, estas encuestas han capturado valiosas respuestas que nos permiten desentrañar patrones, identificar tendencias y arrojar luz sobre las complejidades inherentes a la divulgación no autorizada de información personal. El nivel de participación y las respuestas proporcionadas no solo constituyen un reflejo de la diversidad de perspectivas en la muestra, sino que también actúan como pilares fundamentales para la formulación de análisis y conclusiones robustas. Con esta premisa en mente, procederemos a presentar de manera detallada los resultados obtenidos, desglosando cada elemento para ofrecer una comprensión completa de la dinámica subyacente en la investigación.

Según los resultados obtenidos de la primera pregunta del cuestionario se identifica que, el hecho de que 27 personas afirmaran haber experimentado esta preocupación sugiere una alta sensibilidad y conciencia acerca de los posibles riesgos asociados con la seguridad de la información en línea. Estas respuestas afirmativas indican una creciente inquietud en la población sobre la vulnerabilidad de sus datos personales en el entorno digital. Por otro lado, los 5 participantes que respondieron “No” reflejan un nivel de confianza en las medidas de seguridad existentes o, posiblemente, una falta de percepción de riesgo en este aspecto. La respuesta “Quizás” por parte de 18 participantes es digna de atención, ya que indica una incertidumbre o una percepción ambivalente respecto a la seguridad de la información personal en línea. Estas respuestas mixtas destacan la complejidad de las actitudes y experiencias individuales en relación con la seguridad de los datos digitales.

Referente a la pregunta 2 del cuestionario sobre si las cuentas personales de los participantes han sido hackeadas, las respuestas proporcionan una visión detallada de las experiencias individuales en materia de seguridad digital. Un total de 26 participantes afirman haber experimentado el hackeo de sus cuentas personales, indicando una incidencia significativa en la vulnerabilidad de la seguridad en línea. Este alto número de respuestas afirmativas señala la relevancia y la prevalencia de este problema en la muestra encuestada. Por otro lado, 17 participantes declaran que no han experimentado el hackeo de sus cuentas, lo cual sugiere prácticas de seguridad más efectivas o una menor exposición a riesgos cibernéticos. La respuesta “Quizás” de 7 participantes introduce una dimensión de incertidumbre, relacionada con situaciones

no confirmadas o dudas sobre posibles eventos de hackeo. Este análisis diferenciado de las respuestas contribuye a comprender la diversidad de experiencias y actitudes en cuanto a la seguridad de las cuentas personales en entornos digitales.

La información obtenida de la tercera pregunta del cuestionario, revela patrones discernibles en las respuestas. Un total de 35 encuestados admitieron haber aceptado términos y condiciones sin revisar su contenido, indicando una práctica común de aceptación rápida y una falta de atención a los detalles legales. Por otro lado, 10 participantes afirmaron no haber aceptado términos y condiciones sin previamente informarse sobre su contenido, lo cual refleja una actitud más cautelosa y consciente al respecto. La respuesta "Quizás" de 5 encuestados sugiere una posición indecisa o ambivalente, revelando la complejidad de las decisiones relacionadas con la aceptación de condiciones legales en el ámbito digital. Estos resultados confirman el bajo conocimiento de las posibles implicaciones de esta práctica generalizada en la seguridad y privacidad de la información personal.

El análisis de las respuestas a la pregunta sobre si los participantes han experimentado la suplantación de su identidad revela patrones distintivos en la percepción y experiencia de la muestra encuestada. Un total de 12 encuestados afirman haber sido víctimas de suplantación de identidad, lo que subraya la relevancia y la actualidad de esta problemática en el entorno digital. Esta cifra sugiere que un segmento significativo de la población ha enfrentado situaciones donde su información personal fue utilizada por terceros de manera indebida. Por otro lado, la mayoría de 30 participantes respondieron negativamente, indicando que no han experimentado suplantación de identidad. Estas respuestas sugieren un nivel general de confianza en las medidas de seguridad actuales, una menor prevalencia de casos de suplantación. Los 8 participantes que respondieron "Quizás" introducen un matiz de incertidumbre, señalando la posibilidad de experiencias ambiguas o dudas en relación con la suplantación de identidad.

El análisis de las respuestas a la pregunta sobre el uso de inteligencia artificial, específicamente mencionando Chat GPT u otras formas similares, proporciona una visión interesante del grado de adopción de esta tecnología entre los encuestados. Un total de 30 participantes afirman haber utilizado inteligencia artificial, evidenciando una aceptación y familiaridad significativas con esta herramienta. Esta respuesta mayoritaria sugiere una integración exitosa de la inteligencia artificial en las interacciones cotidianas de los encuestados. Por otro lado, los 15 participantes que respondieron "No" indican una falta de experiencia o interacción con este tipo de tecnología, o quizás una preferencia por métodos más convencionales. Los 5 participantes que respondieron "Quizás" ofrecen una perspectiva ambivalente, sugiriendo una cierta indecisión o falta de claridad en cuanto a la utilización de la inteligencia artificial.

El análisis de las respuestas a la pregunta sobre el tiempo diario dedicado al uso de redes sociales revela patrones significativos en los hábitos de los participantes. La mitad de las personas encuestadas indicó utilizar las redes sociales durante todo el día, señalando un alto nivel de involucramiento y presencia constante en estas plataformas digitales. En contraste, 12 participantes mencionan utilizar las redes solo cuando es necesario, lo que indica un enfoque más selectivo y deliberado en el uso de plataformas digitales. Además, 13 participantes indicaron dedicar de 2 a 3 horas diarias al uso de redes sociales. Estas respuestas proporcionan una comprensión detallada de los diversos patrones de comportamiento en el uso de redes sociales, desde la inmersión constante hasta un enfoque más moderado y selectivo.

La investigación sobre el conocimiento de los beneficios proporcionados por la Ley Orgánica de Protección de Datos Personales genera resultados divergentes entre los participantes. Un total de 15 encuestados afirman tener conocimiento de dichos beneficios, lo cual sugiere cierto grado de conciencia y comprensión de las disposiciones contenidas en la legislación de protección de datos. Por otro lado, 32 participantes responden negativamente, indicando una falta de familiaridad con los beneficios establecidos por la ley. Este hallazgo subraya una brecha significativa en la comprensión general de las disposiciones legales destinadas a salvaguardar la privacidad y seguridad de los datos personales. La respuesta "Quizás" por parte de 3 encuestados refleja una posición intermedia, sugiriendo una posible ambigüedad o falta de claridad en cuanto al alcance y las ventajas específicas de la ley.

La pregunta sobre la conciencia de los participantes respecto a la posibilidad de otorgar acceso a su información personal al aceptar términos y condiciones sin leer genera respuestas equitativas y sugiere una división de conocimientos en la muestra. Un total de 25 participantes indican que sí estaban al tanto de esta implicación, mientras que otros 25 admiten no tener conocimiento al respecto. Estos resultados reflejan una dicotomía interesante en la comprensión de los usuarios sobre las consecuencias de aceptar términos y condiciones de servicios en línea. Estos resultados proporcionan una base valiosa para diseñar estrategias educativas y de divulgación que aborden las lagunas de conocimiento identificadas en la muestra.

Las respuestas a la pregunta sobre si los participantes consideran que la tecnología es peligrosa reflejan una diversidad de opiniones dentro de la muestra encuestada. Un número de 28 participantes, expresan que sí perciben la tecnología como peligrosa, lo cual sugiere una preocupación generalizada sobre los riesgos asociados con el uso de la tecnología en diversos aspectos de la vida cotidiana. Por otro lado, la minoría de 3 participantes que respondieron "No" indican una percepción más optimista o confiada en la seguridad de la tecnología. La respuesta "Quizás" por parte de 19 participantes resalta una posición intermedia y revela una ambigüedad en la evaluación de los riesgos tecnológicos.

En relación con los descubrimientos realizados, se destaca un notable desconocimiento en cuanto a la interacción entre los medios tecnológicos y la información personal. Los resultados obtenidos revelan la existencia de desafíos significativos que demandan atención inmediata para abordar las deficiencias en la divulgación de las regulaciones que rigen los datos personales. Es crucial resaltar que la existencia de normativas sobre la protección de datos y sus consecuencias resulta infructuosa si la sociedad carece de una comprensión adecuada y no se encuentra facultada para ejercer plenamente sus derechos en este ámbito.

Este déficit de conocimiento y empoderamiento se convierte en una faceta crítica que requiere intervenciones educativas y divulgativas más profundas. Mejorar la comprensión pública sobre la importancia y aplicación de las normativas de protección de datos se vuelve esencial. Este proceso no solo implica informar sobre las regulaciones existentes, sino también fortalecer la conciencia de los ciudadanos sobre cómo resguardar su propia información y ejercer activamente sus derechos en la era digital. La implementación de programas educativos y campañas de concientización se presenta como una estrategia clave para abordar este vacío de conocimiento y empoderar a la sociedad en la gestión responsable de sus datos personales.

En el ámbito de la normativa global de protección de datos personales, se destaca el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece estándares fundamentales para la gestión y salvaguarda de la información personal. A nivel nacional, en Ecuador, se encuentra la Ley Orgánica de Protección de Datos Personales, la cual establece lineamientos específicos para la protección de la privacidad de los individuos.

Conforme a estas normativas, se asegura la privacidad y confidencialidad de los datos personales mediante la implementación de medidas técnicas y organizativas necesarias. Es crucial tener una comprensión clara de la finalidad con la que se recopilan los datos. Por ejemplo, el Ministerio de Ciencia e Innovación recolecta datos con la finalidad específica de generar o proporcionar servicios a personas directamente interesadas en obtener dicha información (España, 2023).

El proceso de obtención de datos personales debe llevarse a cabo con transparencia y claridad, indicando el propósito específico para el cual se recopilan los datos. Además, se establece la obligación de preservar estos datos por un tiempo determinado para garantizar la prestación continua y mejorada de servicios.

El ejercicio de derechos por parte del usuario implica la posibilidad de acceder y utilizar repetidamente la información personal proporcionada. En caso de que los datos no se manejen de acuerdo con las normativas establecidas, el usuario tiene la facilidad de presentar una reclamación ante una autoridad de control. Este proceso asegura la rendición de cuentas y la protección de los derechos individuales en el contexto de la gestión de datos personales.

Es imprescindible que la sociedad tenga conocimiento de su derecho a acceder a información pública, un principio respaldado por modificaciones en la Constitución de 2008. Estas enmiendas garantizan que las personas tengan la posibilidad de acceder a dicha información, incluso cuando se les haya denegado el acceso o si la información proporcionada es incompleta o poco fiable. Asimismo, se establece el derecho de solicitar acceso a información considerada secreta o confidencial. Sin embargo, en el caso de información clasificada como reservada, es imperativo que esta sea declarada como tal por una autoridad competente previamente (Asamblea Nacional Constituyente, 2008).

En esta perspectiva, el artículo 178 del Código Orgánico Integral Penal aborda los delitos vinculados a las vulnerabilidades o sustracción de información. Se establecen las disposiciones legales que regulan la violación y divulgación indebida de datos personales, especialmente en el contexto de delitos que afectan la identidad de los usuarios. El código penal prohíbe expresamente la publicación o compartición de los datos personales de un individuo sin su consentimiento o el consentimiento de sus familiares (Ecuador. Asamblea Nacional, 2021).

La trascendencia de salvaguardar la integridad de los datos personales y la necesidad imperante de establecer regulaciones robustas han propiciado que diversos países, Ecuador incluido, implementen estrategias con el objetivo de minimizar los riesgos inherentes a la gestión

de información y resguardar la privacidad de los individuos. La creciente interconexión digital y el vertiginoso avance tecnológico han planteado desafíos significativos, requiriendo respuestas normativas y medidas específicas para garantizar una gestión ética, segura y conforme a los derechos fundamentales de la sociedad en el contexto de la recopilación, procesamiento y almacenamiento de datos personales. En este contexto, la promulgación y aplicación de regulaciones efectivas se convierte en un pilar esencial para abordar los riesgos asociados con la protección de datos y asegurar la confianza de los individuos en la gestión de su información personal en la era digital (Platero, 2019).

Es de suma importancia destacar que el principio de responsabilidad proactiva en el manejo de datos personales conlleva una mejora eficaz en la protección de la información personal, tal como se contempla en el RGPD de la Unión Europea. Este enfoque, comparado con otras normativas, podría ser transferido con facilidad al contexto latinoamericano. El objetivo primordial a considerar es asegurar la protección de los datos personales, lo cual ha inducido un cambio de perspectiva en la sociedad, generando impactos en los ámbitos económico, social y en el escenario nacional e internacional (Santamaría, 2020).

De manera pormenorizada se especifican las disposiciones respecto a las medidas de índole proactiva que propiciaron que el RGPD se sustente en el principio de responsabilidad proactiva, en lugar de una responsabilidad general. La responsabilidad proactiva, lejos de contravenir las normativas de protección, representa un beneficio para cada individuo en lo concerniente a sus datos personales. Por otro lado, esta responsabilidad proactiva debe complementarse con otros mecanismos, como el anunciado por el RGPD, como es el caso de la evaluación de impacto, donde un responsable designado en el área de protección de datos será el encargado de detallar y supervisar los procedimientos (Santamaría, 2020).

En la época actual, Ecuador ha implementado una legislación de protección de datos personales, la cual establece las correspondientes obligaciones y responsabilidades para las empresas y organizaciones que gestionan información personal. La salvaguarda de datos resulta crucial para prevenir el uso inapropiado de información personal, la suplantación de identidad, el hostigamiento cibernético, la discriminación y la infracción de la privacidad. Además, la protección de datos desempeña un papel esencial en el desarrollo de la economía digital, facilitando la generación de confianza entre los usuarios y promoviendo el intercambio seguro de información en entornos en línea (Idrovo, 2011).

La Ley Orgánica de protección de datos (LOPD) establece en el Artículo 37 que la persona encargada del tratamiento de los datos personales debe seguir el principio de seguridad de datos personales. Además, es responsabilidad del responsable o encargado del tratamiento de datos implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficacia y efectividad para garantizar y mejorar la seguridad de tratamiento de datos personales.

Asimismo, en el Artículo 65 se especifica que en caso de que se produzca un incumplimiento de la ley de protección de datos personales, la autoridad de protección de datos está facultada para implementar medidas correctivas con el propósito de prevenir la repetición de las infracciones. Estas medidas comprenden el tratamiento de datos bajo condiciones específicas, la supresión de datos y la imposición de medidas técnicas o administrativas diseñadas para asegurar un tratamiento adecuado de los datos personales. La autoridad procederá a tomar dichas medidas tras recibir un informe de la unidad técnica competente, con el fin de corregir o eliminar comportamientos contrarios a lo estipulado por la ley (Aguilar, 2022).

Los resultados del estudio revelan que, a pesar de los principios sólidos y claros establecidos por la LOPD para el manejo de datos personales, subsisten desafíos significativos en la prevención de filtraciones de datos. Actualmente, se encuentra en curso un debate en torno a la actualización y mejora de las regulaciones existentes, lo cual es crucial para proteger el derecho a la intimidad y garantizar un tratamiento adecuado de los datos personales. La discusión sobre la importancia de equilibrar el derecho a la libertad de expresión con la protección de la privacidad ha generado un impacto significativo en la circulación de información en Internet. La necesidad de abordar estas cuestiones se vuelve evidente al considerar las posibles consecuencias negativas que pueden surgir si no se toman medidas preventivas.

En este contexto, se propone una estrategia educativa integral que no solo promueve la comprensión de los principios y regulaciones establecidos por la LOPD, sino que también aborda de manera específica las implicaciones de la libertad de expresión en el entorno digital. La estrategia se enfoca en la concientización sobre la importancia de salvaguardar la privacidad en línea y proporciona herramientas prácticas para prevenir la divulgación no autorizada de información personal. Además, se busca fomentar una cultura de responsabilidad y ética en el uso de datos personales, contribuyendo así a la creación de un entorno digital más seguro y respetuoso de los derechos individuales.

Para implementar esta estrategia, se proponen varias iniciativas. En primer lugar, llevar a cabo sesiones de capacitación y talleres interactivos que aborden los principios fundamentales de la LOPD y destaquen los desafíos específicos relacionados con la libertad de expresión en línea. Estas actividades se diseñarán de manera participativa, alentando la discusión y el intercambio de ideas entre los participantes.

Además, se desarrollará material educativo multimedia, como videos informativos y material gráfico, que ilustre de manera efectiva los conceptos clave y brinde ejemplos prácticos de situaciones en las que la divulgación no autorizada de datos personales ocurre. Este material se distribuirá ampliamente a través de plataformas en línea y se adaptará para llegar a diferentes audiencias, incluyendo estudiantes, profesionales y la sociedad en general. Se propondrá la integración de módulos educativos sobre protección de datos y ética digital en los programas de estudio. Estos módulos se diseñarán de manera que sean atractivos y accesibles para los estudiantes, fomentando la comprensión desde edades tempranas.

Asimismo, se establecerá una campaña de sensibilización en redes sociales y otros medios digitales, con el objetivo de difundir mensajes clave sobre la importancia de la responsabilidad y ética en el uso de datos personales. Esta campaña busca involucrar a la comunidad en general, promoviendo la participación activa en la protección de la privacidad en línea. A continuación, se detalla la estrategia propuesta. Tabla 1

Tabla 1. Detalles de la estrategia propuesta

"Protección digital en Ecuador: Educación para la salvaguarda de la privacidad"	
Objetivo:	Promover la concientización y el conocimiento público sobre la importancia de salvaguardar la privacidad en línea y prevenir la divulgación no autorizada de información personal en Ecuador.
Acciones y actividades propuestas.	
Sesiones de capacitación y talleres.	Diseñar y ejecutar sesiones de capacitación presenciales y virtuales en comunidades, instituciones educativas y empresas. Temas clave incluirán la legislación de protección de datos en Ecuador, los riesgos asociados con la divulgación no autorizada y las mejores prácticas para la gestión segura de la información personal.
Material educativo multimedia.	Crear videos informativos, infografías y recursos gráficos que expliquen de manera clara y accesible los conceptos relacionados con la protección de datos. Distribuir el material a través de plataformas en línea, redes sociales y colaboraciones con medios de comunicación locales.
Incorporación en programas de estudio.	Proponer la inclusión de módulos educativos sobre protección de datos y ética digital en los programas de estudio de escuelas y universidades. Estos módulos se adaptarán a diferentes niveles educativos y se enfocarán en aspectos prácticos y relevantes para la vida cotidiana.
Campaña de sensibilización en redes sociales.	Lanzar una campaña activa en redes sociales para aumentar la conciencia sobre la importancia de proteger la información personal. Fomentar la participación activa de la comunidad a través de desafíos, encuestas y contenido interactivo.
Eventos comunitarios.	Organizar eventos comunitarios, charlas y ferias educativas en áreas urbanas y rurales para llegar a diversos grupos demográficos. Invitar a expertos en protección de datos, líderes comunitarios y representantes gubernamentales para compartir información y responder preguntas.
Creación de recursos interactivos.	Desarrollar aplicaciones móviles y plataformas interactivas que brinden información y consejos personalizados sobre seguridad de datos. Facilitar el acceso a recursos de ayuda y líneas directas en caso de divulgación no autorizada.
Evaluación continua y retroalimentación.	Implementar encuestas y evaluaciones periódicas para medir el impacto de la estrategia educativa. Recopilar retroalimentación para ajustar y mejorar las actividades según las necesidades identificadas.

Fuente: Elaboración propia.

Esta estrategia educativa aborda de manera integral la problemática de la divulgación no autorizada de información personal, involucrando a la comunidad, instituciones educativas, empresas y medios de comunicación para crear un entorno digital más seguro y consciente en Ecuador.

La implementación de la estrategia educativa, "Protección digital en Ecuador: Educación para la salvaguarda de la privacidad", es de vital importancia por varias razones:

1. Genera un aumento en la conciencia pública sobre la importancia de proteger la privacidad en línea, destacando los riesgos asociados con la divulgación no autorizada de información personal.

2. Contribuye al cumplimiento de las normativas de protección de datos existentes en Ecuador al educar a la población sobre sus derechos y responsabilidades.
3. Ayuda a prevenir la divulgación no autorizada de información personal al proporcionar a las personas y organizaciones las herramientas y conocimientos necesarios para gestionar sus datos de manera segura.
4. Promueve una cultura de responsabilidad y ética en el uso de datos personales, influyendo en el comportamiento digital individual y colectivo.
5. Disminuye la vulnerabilidad de la población ante amenazas cibernéticas al mejorar la comprensión de las prácticas seguras en línea y alentar la adopción de medidas preventivas.
6. Empodera a la comunidad al proporcionar conocimientos prácticos y accesibles, permitiéndoles tomar decisiones informadas sobre la gestión de su información personal.
7. Facilita la adaptación continua a los cambios tecnológicos al educar sobre los riesgos emergentes y las mejores prácticas en el manejo de datos en un entorno digital en constante evolución.
8. Contribuye a la generación de confianza en el uso de servicios en línea y plataformas digitales al demostrar un compromiso activo con la seguridad de los datos personales.
9. Establece las bases para un impacto sostenible a largo plazo al incorporar la educación sobre la protección de datos en la cultura y prácticas cotidianas de la sociedad ecuatoriana.

CONCLUSIONES

La filtración de datos personales es un asunto muy preocupante que puede tener graves consecuencias para la privacidad y seguridad de las personas afectadas, lo cual subraya la necesidad de implementar autorregulación en estos espacios, exigiendo colaboración entre la sociedad, proveedores de servicios y el Estado. El crecimiento exponencial de usuarios en redes sociales expone a millones de personas a riesgos de violación de privacidad. Es evidente que los derechos de intimidad, privacidad y protección de datos se ven comprometidos en este entorno. La filtración de datos en instituciones educativas representa un problema grave, afectando la privacidad y seguridad de estudiantes y personal. La divulgación no autorizada abarca desde calificaciones hasta información financiera, requiriendo medidas preventivas efectivas.

La metodología empleada combina enfoques cualitativos y cuantitativos, utilizando herramientas como encuestas para obtener datos específicos. La investigación se basa en procesos teóricos, metodológicos y la recopilación de información documental. Los hallazgos revelan un marcado desconocimiento sobre la interacción entre tecnología e información personal. Esto destaca la necesidad urgente de abordar las deficiencias en la divulgación de regulaciones de protección de datos. La estrategia propuesta fortalece la conciencia, conocimiento y prácticas relacionadas con la protección de datos en Ecuador. Su objetivo es preservar la privacidad y seguridad de la información personal en un entorno digital en constante evolución.

La estrategia educativa integral propuesta aborda diversos aspectos, desde sesiones de capacitación hasta campañas en redes sociales. Su implementación se considera crucial para aumentar la conciencia y el conocimiento público sobre la protección de datos. La misma, no solo buscar abordar la problemática inmediata, sino establecer las bases para un cambio cultural y comportamental.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, M. (2022). La protección de datos personales en Ecuador. ***Estudios Del Desarrollo Social: Cuba y América Latina, 10***(especial 1), 1–14. https://revistas.uh.cu/revflacso/article/view/3594/3138

da Silva, J. (2019). Utilização do Google Forms na pesquisa acadêmica. ***Humanidades & Inovação, 6***(12), 371–373. https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/1106

Downing, A. (2022). Health advertising on Facebook: Privacy and policy considerations. ***Patterns, 3***(9), 100561. https://www.sciencedirect.com/science/article/pii/S2666389922001726

Ecuador. Asamblea Nacional. (2021). ***Código orgánico integral penal, COIP***. Registro Oficial Suplemento 180 https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Ecuador. Asamblea Nacional Constituyente. (2008). ***Constitución del Ecuador. Decreto Legislativo 0***. Registro Oficial 449. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

España, Gobierno. (2023). ***Política de privacidad y protección de datos.*** Ministerio de Ciencia, Innovación y Universidades. https://www.ciencia.gob.es/InfoGeneralPortal/Politica-de-privacidad-y-proteccion-de-datos.html

Finol, M. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. ***Mundo Recursivo, 3***(1), 1–24. https://atlantic.edu.ec/ojs/index.php/mundor/article/view/38

Hernández, R. (2018). ***Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta***. Mc Graw Hill Education. http://repositorio.uasb.edu.bo:8080/handle/54000/1292

Idrovo, S. (2011). ***La protección de datos de carácter personal en el Ecuador***. [Trabajo de Conclusión de Carrera presentado como requisito parcial para la obtención del título de Abogado de los Tribunales de Justicia de la República del Ecuador, con especialidad mayor en Derecho Empresarial y con especialidad menor en Derecho Internacional Comercial.] Cuenca: Universidad Del Pacifico. https://upreposito-rio.upacifico.edu.ec/handle/123456789/134

Orozco, J. (2018). ***El Marco Metodológico en la investigación cualitativa. Experiencia de un trabajo de tesis doctoral***. ***Revista Científica de FAREM-Estelì, 7***(27), 25–37. https://rcientificaesteli.unan.edu.ni/index.php/rcientifica/article/view/1440

Platero, A. (2019). La seguridad como elemento clave en el tratamiento de datos personales en Europa: especial referencia al régimen de responsabilidad civil derivado de las brechas de seguridad. ***Lex (Lima), 17***(23), 55–74. https://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/1670/1763

Platero, A. (2020). Lexnet como máximo exponente del sistema de justicia electrónica en España: especial referencia a su tratamiento de datos personales. ***Revista de Ciencias Jurídicas, 152***, 13–42. https://www.kerwa.ucr.ac.cr/handle/10669/85204

Pöhn, D. (2023). A framework for analyzing authentication risks in account networks. ***Computers & Security, 135***(Especial), 103515. https://www.sciencedirect.com/science/article/abs/pii/S016740482300425X

Remache, J. (2019). ***Análisis de los aspectos técnicos del marco regulatorio para la protección de datos personales en Ecuador*** [Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones] Quito: Universidad de las Américas. https://dspace.udla.edu.ec/bitstream/33000/11581/1/UDLA-EC-TIRT-2019-19.pdf

Santamaría, F. (2020). El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. ***Derecho PUCP, 85***, 139–174. http://www.scielo.org.pe/pdf/derecho/n85/2305-2546-derecho-85-00139.pdf

Shubladze, S. (2023). ***Las claves para utilizar correctamente "el nuevo oro": los datos***. Forbes Argentina. https://www.forbesargentina.com/innovacion/las-claves-utilizar-correctamente-el-nuevo-oro-datos-n31324

Steijvers, L. (2024). The role of social network structure and function in moderate and severe social and emotional loneliness: The Dutch SaNAE study in older adults. ***Heliyon, 10***(1), e23734. https://www.sciencedirect.com/science/article/pii/S240584402310942X

Tejada, E. (2019). Los hábitos de uso en las redes sociales de los preadolescentes. ***Revista Iberoamericana de Educación a Distancia. 22***(2), 119–133. https://addi.ehu.es/handle/10810/41993

Zuboff, S. (2019). ***The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power***. PublicAffairs. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791