Universidad Autónoma de Baja California

Facultad de Economía y Relaciones Internacionales

Posgrado en Estudios del Desarrollo Global

La protección de datos personales en posesión de los particulares: La necesidad del conocimiento de las implicaciones de la privacidad de datos en estudiantes universitarios.

Tesis de grado

Para obtener el título de:

Maestría en Estudios del Desarrollo Global.

Presenta:

Lizeth Guadalupe Valenzuela Álvarez

Director de Tesis:

Arturo Serrano Santoyo

Lectores de Tesis:

Dra. Jocelyne Rabelo

Dr. José Antonio García

Tijuana Baja California, México. Junio del 2023

Para mi pequeña grandiosa familia y
para mi yo del pasado, que no se rindió en los momentos más difíciles
y encontró fuerza para seguir adelante, lo estamos logrando.

Agradecimientos

A mi amada madre, Francisca Alvarez Felix, tus palabras de aliento, tu confianza inquebrantable y tu apoyo incondicional han sido mi mayor fortaleza en este camino. Pero, sobre todo, quiero agradecerte por ese inmenso amor que me has brindado. Es gracias a ti que encuentro la fuerza necesaria para enfrentar los desafíos de la vida.

A mi hermana Alicia Lilian, por ser mi cómplice, ayudarme a encontrar los errores en las fórmulas de excel, por acudir a mi llamado siempre que tenía dudas en algo, por escucharme innumerables horas sobre el mismo tema, y por ser mi lectora informal de tesis.

A mi hermana Dulce María, por siempre creer en mí, su apoyo incondicional me da mucha motivación para hacer las cosas, gracias por leer mis avances, por darme sus opiniones objetivas y sinceras, por demostrar con el ejemplo, el compromiso y dedicación.

A Catalina, Lou, Lars, Lino, Noli y Griselda, la pureza de sus almas siempre me dan paz.

A mi director de tesis, Dr. Arturo Serrano Santoyo, quiero expresar mi más profundo agradecimiento por su confianza, interés y motivación a lo largo de mi trayectoria en la maestría. Cada paso que di en este camino estuvo respaldado por su incondicional apoyo y dedicación. Gracias a su guía y orientación, pude superar obstáculos y alcanzar metas que en algún momento parecían inalcanzables. Estoy eternamente agradecida por su incansable compromiso con mi crecimiento académico. Además de su papel como director de tesis, quiero agradecer por ser un modelo a seguir en términos de integridad, pasión y excelencia intelectual. Su influencia en mi vida académica y profesional ha sido trascendental, y siempre llevaré conmigo el aprendizaje y los valores que he adquirido a su lado.

Deseo expresar mi más sincero agradecimiento a mis lectores, Jocelyne Rabelo Ramirez y Jose Antonio García Macías, por su apoyo constante y guía durante este proceso. La combinación de sus conocimientos y actitudes ha sido fundamental en mi desarrollo académico. Gracias por el tiempo dedicado a la revisión de este trabajo y por sus aportaciones tan valiosas y enriquecedoras.

A la Universidad Autónoma de Baja California, en especial, al posgrado de Estudios del Desarrollo Global y al Consejo Nacional de Ciencia y Tecnología (CONACYT), por la confianza en mí depositada.

Índice.

Introducción General

Los datos son una parte esencial de la economía actual; de hecho, se reporta que nos encontramos en la economía de los datos, sin embargo, al estructurarse y formatearse, estos datos se convierten en información y al procesar la información, generamos conocimiento. Para poder explicar este proceso, la pirámide DIKW[1] (Data Information Knowledge Wisdom) o pirámide del conocimiento es la más apropiada.

Figura 1. Pirámide de datos información conocimiento sabiduría (DIKW)

Fuente: Elaboración propia

Los datos son la materia prima de las tecnologías emergentes, en particular de la Inteligencia Artificial (IA). Mediante el procesamiento conocido como *Big Data* o Macrodatos, algoritmos gestionan grandes cantidades de información. Estos son los factores que hacen posible la aplicación cognitiva de la IA. El uso, y plena concientización de las implicaciones de los datos son un derecho humano[2] para garantizar el bienestar y la legalidad de los creadores de dichos datos y de los usuarios, es decir, el humano. De acuerdo con el entorno actual de la cultura digital de la sociedad, el talento y las habilidades digitales son factores determinantes en el ecosistema de la llamada Cuarta Revolución Industrial (4RI) (Schwab, 2016).

[1] Pirámide DIKW: Conjunto de modelos para representar las relaciones aparentemente estructurales entre Datos, Información, Conocimiento, y en algunos casos sabiduría. González, C. (2017). Big data 2.0.

[2] La Declaración Universal de los Derechos Humanos enuncia que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación”. Artículo 12: derecho a la intimidad
https://www.un.org/es/about-us/universal-declaration-of-human-rights

Las sociedades actuales se encuentran en un proceso de automatización de las actividades claves de los individuos, comunidades e instituciones, no siendo una excepción, la comunidad estudiantil universitaria. Con las experiencias ganadas en el proceso de dotar de acceso a internet a mayores sectores de la población, los aspectos de adopción y alfabetización digital se fueron incorporando gradualmente en las políticas y proyectos de inclusión a nivel global (Jarosz et al., 2020). Este proceso se está llevando a cabo a un ritmo intenso y acelerado, que por un lado limita la reflexión necesaria para entender las implicaciones sociotécnicas del uso y apropiación tecnológica de las miríadas de aplicaciones digitales disponibles; y por otro, crea brechas digitales cada vez más difíciles de mitigar.

En este escenario se ha generado una variante de brecha digital (silenciosa y a veces imperceptible) que afecta profundamente a la sociedad y es complementaria a la brecha digital tradicionalmente caracterizada por indicadores de acceso, habilidades digitales y otros factores socioculturales y económicos. Los procesos de acceso a plataformas y aplicaciones digitales a menudo descuidan, ignoran o minimizan los aspectos de privacidad, seguridad, las dimensiones éticas y morales y las implicaciones psicológicas y culturales sin considerar sus consecuencias intencionadas o no intencionadas. La inteligencia artificial, *Blockchain*, el discurso Metaverso y otras tecnologías emergentes tales como *Chat GPT* (OpenAI, 2022) pueden exacerbar esta condición sin programas educativos apropiados que construyan capacidades para mitigar esta desafiante situación de la sociedad digital (Jasanoff, 2016; Zuboff, 2020).

Los dominios entrelazados de los bits y los átomos forman ya parte de nuestra existencia cotidiana, están en cada procedimiento bancario, de seguridad social y asistencia médica, en los procesos burocráticos, en las solicitudes de empleo, en las compras cotidianas (Eubanks, 2018). Pero, tanto la brecha de innovación como la variante de brecha digital descrita anteriormente contribuyen respectivamente a agravar las condiciones de desigualdad social y a la exclusión de sectores sociales con retos de conectividad a internet (Jasanoff, 2016, Eubanks, 2018,). La naturaleza de la brecha digital en el trayecto final de la inclusión digital está más relacionada con la generación y difusión de conocimiento, el comportamiento humano, la adopción de tecnología y un efecto combinado de los medios sociales y el marketing. Es decir, existen cuatro etapas del trayecto de la sociedad hacia la inclusión digital

que están entrelazadas, son interdependientes y coevolucionan en conjunto, constituyendo un sistema dinámico complejo (Colegio de Tamaulipas, 2022)

Respecto a lo anteriormente expuesto, surge la necesidad de desarrollar capacidades en protección de datos personales, no solo para conocer los respectivos elementos legales que atañen a los usuarios, sino también para garantizar los derechos humanos de los ciudadanos en un entorno sujeto a un cambio tecnológico exponencial. Por otro lado, Houlin Shao, secretario de la Unión Internacional de Telecomunicaciones, habla sobre la urgente necesidad de regular la gestión de los datos en diferentes sectores (ITU, 2020) y menciona que "La regulación colaborativa ha ido ganando impulso de manera constante, lo que refleja un mundo impulsado por los datos donde la demarcación entre el sector de las TIC y otras industrias se ha vuelto cada vez más borrosa."

Ante esta situación, esta contribución plantea la necesidad de señalar y proponer un marco de referencia en el área de protección de datos personales con la propuesta de construir nuevas capacidades a nivel universitario, no solo para conocer los elementos jurídicos respectivos que atañen a los usuarios, sino también para garantizar los derechos humanos de los ciudadanos en un entorno sujeto a un cambio tecnológico exponencial. Dicho marco de referencia se propone para la difusión de los derechos de Acceso, Rectificación, Cancelación y Oposición (De Diputados et al., 2010), y otras herramientas de la protección del uso de datos personales en posesión de los particulares, para que se integre una cultura y educación digital, aunado a los esfuerzos por parte del departamento de protección de datos personales de la Dirección de la Universidad Autónoma de Baja California.

Capítulo 1. Introducción y Planteamiento del Problema

El problema de la presente investigación se plantea en el contexto actual de la 4RI y la economía de los datos. Los aspectos de protección y privacidad son clave para capitalizar los beneficios de las aplicaciones de las tecnologías digitales emergentes (Internet de las Cosas, IA, Automatización, entre otras). Por tal razón, es fundamental el conocer y difundir las implicaciones del uso adecuado de los datos por individuos, comunidades e instituciones. El avance tecnológico exponencial plantea retos especiales que deben ser atendidos para lograr una sociedad empoderada en el actual ecosistema digital. La interrelación entre la abrumadora velocidad de los desarrollos tecnológicos digitales y la falta de mecanismos

regulatorios asociados, han dado lugar al surgimiento de patrones de adopción tecnológica que presentan retos significativos en cuanto al conocimiento y amplia difusión de los aspectos de privacidad y protección de datos personales. Sin embargo, no sólo es importante la falta de conocimiento al respecto, sino también el entendimiento y atención a los efectos del uso de los datos y sus implicaciones éticas y regulatorias asociadas.

Por lo anterior, es fundamental que, en esta "economía de los datos", se pueda alcanzar su uso y protección adecuados para el usuario; esto se convierte en un factor clave y es a la vez una herramienta de desarrollo económico y social. Cuando no existen estrategias para la adecuada protección de los datos, se desaprovecha su potencial, y esta condición es una desventaja en el aprovechamiento de la 4RI. La importancia de la protección de datos ha sido abordada en trabajos recientes donde se señala la aparición de un capitalismo de vigilancia empleado como un modelo por gobiernos y por empresas para perfilar y conocer la población por medio de la captación de sus datos, a menudo sin consentimiento y sin brindar detalles del uso e información de cómo serán dichos datos usados. (Zuboff, 2020).

Dada la trascendencia y desarrollos recientes sobre IA, es importante destacar que en este trabajo se aborda de manera recurrente este tema. La razón de su inclusión en este trabajo es la relevancia de las tecnologías digitales emergentes en la transformación de la economía y la sociedad. Su potencial para mejorar la eficiencia, productividad, innovación y calidad de vida es enorme; Sin embargo, los riesgos asociados a la privacidad y protección de datos constituyen un reto fundamental para la sociedad actual y del futuro. En particular, la IA y la automatización están transformando la forma en que se recopilan, se procesan y se utilizan los datos, lo que hace que la protección y la privacidad de los datos sean especialmente importantes.

Por lo tanto, es importante abordar estos temas en la presente investigación, para tomar en cuenta los cambios que están teniendo lugar y de esta forma, se puedan identificar y abordar los desafíos y oportunidades que plantean estas tecnologías emergentes. Además, es fundamental que se promueva una cultura de ética y responsabilidad en el diseño, en el uso de estas tecnologías, para que se puedan capitalizar los beneficios que ofrecen y mitigar los riesgos asociados.

Véliz, (2021) destaca que el modelo de negocio de la economía de los datos carece de transparencia y que los perjuicios para la privacidad tanto individual como colectiva son mayores que los beneficios que se obtienen (Véliz, 2021). Este y otros estudios recientes exponen las implicaciones de las tecnologías emergentes tanto como modelo de negocio como método de vigilancia estatal. De esta manera, se observa la necesidad de establecer medidas efectivas para proteger la privacidad y los derechos de los ciudadanos frente a la creciente influencia de la tecnología en las vidas humanas.

De la misma forma, la agenda de las Naciones Unidas del 2021, en sus propuestas clave entre los 12 compromisos de la declaración sobre la conmemoración del septuagésimo quinto aniversario de las Naciones Unidas, en el compromiso número siete "*Improve digital cooperation.*" (UN, 2021), así como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) enfatizan la relevancia de los datos considerándolos como condición crítica en las estructuras jurídicas dada su importancia en la calidad de información sensible y sus implicaciones relacionadas.

No sólo organizaciones internacionales han trabajado en la protección de los datos personales, México como integrante de la OCDE[3] desde 1994, atendiendo sus sugerencias, ha elaborado herramientas jurídicas que han dado como resultado la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares desde el 2010[4], ley para la protección y privacidad, los derechos ARCO (De Diputados et al., 2010). Para esto se dedicará un capítulo de la presente tesis.

En este trabajo se argumenta que las dimensiones éticas, así como las implicaciones relacionadas con el acceso a plataformas digitales de gran capacidad, se dan por implicadas, se ignoran o no se consideran relevantes. En muchos casos, estas implicaciones se obvian sin considerar sus consecuencias (Jasanoff, 2016). Las tecnologías digitales emergentes, exhiben

[3] El 18 de mayo de 1994, México se convirtió en el miembro número 25 de la OCDE; el "Decreto de promulgación de la Declaración del Gobierno de los Estados Unidos Mexicanos sobre la aceptación de sus obligaciones como miembro de la Organización de Cooperación y Desarrollo Económicos" fue publicado en el Diario Oficial de la Federación el 5 de julio del mismo año. En un plano de igualdad, México analiza las políticas públicas de los países miembros.https://www.oecd.org/centrodemexico/15aosdemexicoenlaocde.htm#:~:text=El%2018%20de%20mayo%20de,en%20el%20Diario%20Oficial%20de

[4] Ley Federal De Protección De Datos Personales En Posesión De Los Particulares https://www.cide.edu/wp-content/uploads/2021/03/LFPDPPP-Comentada_digital.pdf

un gran potencial para el beneficio de la sociedad, sin embargo, su apropiación inadecuada y la falta de atención a sus consecuencias imprevistas y la proliferación a gran escala de aplicaciones perniciosas, exacerban la brecha digital, por lo que es vital y urgente desarrollar un enfoque centrado en la población y sus necesidades reales, de lo contrario, los derechos humanos se verán comprometidos (Zuboff, 2020). Ante esta situación, Kai Fu Lee (2020), expresa que estamos en una época en la que la cantidad y calidad de datos son esenciales para el éxito de la IA. Para crear algoritmos efectivos, es necesario tener una gran cantidad de datos, capacidad de procesamiento y talentosos ingenieros. En la era actual, los datos son la pieza central para la implementación de la IA, ya que una vez que se alcanza cierto nivel de capacidad de procesamiento y talento de ingeniería, la cantidad y calidad de los datos se vuelven decisivos para determinar la potencia y precisión de los algoritmos (Lee, 2020, p. 29).

Para delimitar el alcance de la presente investigación, se considera que ésta se sitúa en el uso actual percibido sobre la privacidad y protección de los datos personales en posesión de particulares en la comunidad estudiantil de la Facultad de Economía y Relaciones Internacionales (FEyRI) de la Universidad Autónoma de Baja California (UABC).

Por lo anterior, se generan las siguientes preguntas de investigación para esta tesis:

1.- ¿Cuál es el nivel de conocimiento sobre las implicaciones de la protección y privacidad de datos que tienen los estudiantes universitarios de la FEyRI, UABC?

2.- ¿De qué manera se podría dar difusión efectiva a los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), y otras herramientas de protección y privacidad de datos personales en posesión de los particulares, para que se integre una cultura y educación digital en los estudiantes universitarios de FEyRI?

Para justificar esta investigación, se infiere que hay un desconocimiento del tema por parte de los estudiantes, por lo cual se percibe una necesidad de realizar estudios sobre la protección de datos personales en el contexto de gobernanza de internet, los derechos humanos y el cambio tecnológico en la comunidad estudiantil universitaria en la FEyRI, UABC.

Respecto a esto, como ya se ha mencionado anteriormente, el conocimiento de los individuos sobre el tratamiento de sus datos personales es un requisito para lograr su adecuada inserción en la actual economía digital.

El objetivo general es:

Analizar el nivel del conocimiento de la población estudiantil de la FEYRI, UABC sobre las implicaciones de la protección y privacidad en el uso de datos personales en posesión de particulares. Asociados a este objetivo general, se buscan dos objetivos específicos señalados a continuación.

Objetivo Específico

1- Desarrollar un mapa descriptivo para analizar la interrelación de los niveles de conocimiento sobre privacidad, protección de datos y derechos digitales de los estudiantes de la FEyRI, UABC

Objetivo Específico

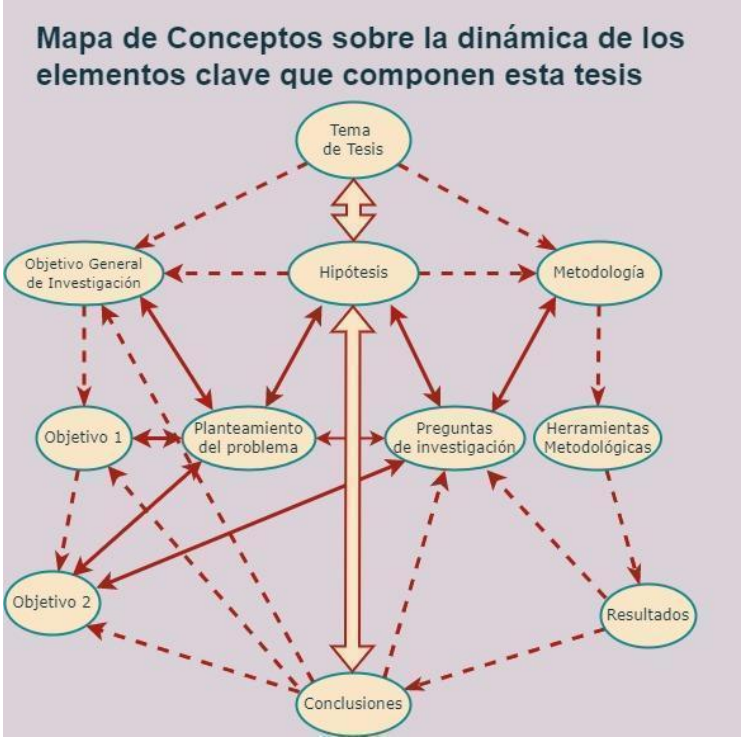
2- Desarrollar un marco de referencia para la construcción de nuevas capacidades en el conocimiento del uso y aplicación adecuada de datos personales en posesión de particulares en función de la legislación vigente mexicana para aprovechar la dinámica de la 4RI en la comunidad universitaria de la FEyRI, UABC.

Estos objetivos buscan encaminar la fundamentación de la hipótesis:

La comunidad estudiantil universitaria requiere fortalecer su conocimiento y habilidades sobre las implicaciones y relevancia de privacidad y protección de datos personales en posesión de particulares en el acceso y uso de dispositivos, sistemas y plataformas digitales en el contexto de la 4RI.

Los elementos que componen la investigación se consideran en el siguiente diagrama:

Figura 2. Mapa de conceptos de los elementos que componen una tesis



Fuente: Elaboración propia.

Capítulo 2. Marco conceptual

La privacidad de los datos no es un tema nuevo, ya que está reconocido como un derecho humano en el artículo 12 de la Declaración Universal de Derechos Humanos. Sin embargo, el surgimiento de la 4RI ha dado lugar a un renovado interés en la ciencia de datos, dada su naturaleza interdisciplinaria y multifactorial. En este contexto, y especialmente en el contexto de la pandemia del COVID-19, la regulación de la privacidad y la protección de los datos personales fue crucial y contribuyo a identificar los desafíos de estructurar, gestionar, diagnosticar, evaluar y aplicar leyes que protejan cada vez más a una sociedad sometida a avances tecnológicos acelerados y exponenciales.

El derecho a la privacidad presenta nuevos desafíos, como el derecho al anonimato y el derecho al olvido (Alvarez, 2015), el impacto de los datos personales en los nuevos modelos económicos (Veliz, 2021), y la competencia entre países por la captura y gestión de grandes cantidades de datos para posicionarse como superpotencias (Lee, 2020). Estos desafíos deben

ser abordados para garantizar que los derechos a la privacidad y la protección de datos personales se respeten y se protejan de manera efectiva en un mundo cada vez más impulsado por la tecnología.

De la misma forma para asegurar un uso ético de las nuevas tecnologías emergentes, es fundamental establecer las bases éticas en el tratamiento de los datos. Klaus Schwab, fundador del Foro Económico Mundial, destaca que la 4RI se diferencia de las anteriores en términos de velocidad, alcance e impacto en los sistemas y la sociedad. Esta revolución avanza a un ritmo exponencial afectando a las industrias, gobierno y sociedad. Los cambios que se están produciendo son amplios y profundos, y presagian la transformación de sistemas completos de producción, gestión y gobernanza. Por lo tanto, es esencial adoptar una perspectiva ética al implementar estas nuevas tecnologías en la sociedad y garantizar que se utilicen de manera responsable y sostenible para el beneficio de todos los individuos y de la sociedad en su conjunto.

Victor Drummond ha señalado que existe una diferencia significativa entre la "Sociedad de la información" y la "Sociedad tecnocomunicacional". En su opinión, la nueva realidad que circula a través de internet y otros medios no se limita a la información, sino que se trata más bien de comunicación. Por lo tanto, el término "sociedad tecnocomunicacional" refleja mejor la relación entre las tecnologías de la información y la comunicación (Drummond, 2004). En este contexto, la difusión de la llamada "comunicación" sin validar la información y sin sustento verídico, no sólo aumenta la cantidad de datos, sino que también puede afectar la calidad de estos, lo que contribuye a un ecosistema complejo que puede poner en riesgo la integridad y la dignidad humana.

Los aspectos de las implicaciones sobre la privacidad y la protección de datos son abordados en estos últimos años por varios autores, quienes señalan los profundos cambios sociales y económicos a los cuales la sociedad ha estado sometida en estas últimas décadas (Zuboff, 2020; Véliz, 2021). En conclusión, la 4RI y la economía de los datos están teniendo un impacto profundo en nuestra sociedad, y es necesario abordar de manera responsable y ética el uso de los datos personales. La velocidad y alcance de estos cambios exigen una toma de conciencia por parte de individuos, comunidades e instituciones sobre las implicaciones del uso de las tecnologías digitales emergentes. La brecha digital en conocimientos sobre el tema, así como la asimetría ética y regulatoria, son retos que deben ser atendidos para lograr una

sociedad empoderada en el actual ecosistema digital. En el siguiente capítulo, “Protección y Privacidad de datos personales”, se profundizará en estos temas y se explorarán medidas para garantizar una gestión adecuada de los datos personales en el contexto de la 4RI y la economía de los datos.

2.1. Protección y privacidad de datos personales

En una sociedad en permanente cambio, en la cual el espacio privado se ve reducido de forma considerable, el problema de la privacidad y de la intimidad, asume un papel crucial. Del panóptico de Foucault hasta el *Big Brother* Orwelliano, el Derecho se encuentra en una trampa en la que los caminos se multiplican, se entrecruzan y convergen (Tenorio, 2019). Ramirez et al. (2017) indican que el derecho a la protección de datos personales, como un derecho fundamental autónomo del derecho a la vida privada, ha tenido un desarrollo asimétrico en los diferentes sistemas de derechos humanos; Estas asimetrías que se han marcado por la evolución y cambio tecnológico, la dinámica social de la digitalización en las relaciones humanas, la globalización y mutación de la economía tradicional a la economía digital, a pesar de las labores de organizaciones y los trabajos realizados por instituciones internacionales y Estado.

El derecho fundamental a la protección de datos personales tiene como finalidad salvaguardar la privacidad y el control que las personas tienen sobre su información personal. Es crucial que tanto individuos como organizaciones comprendan las consecuencias de la protección de datos personales y cumplan con sus responsabilidades al gestionar dicha información, con el fin de prevenir situaciones de riesgo y garantizar los derechos de los propietarios de esos datos (Serrano-Santoyo, 2018).

García (2019) sostiene que la protección de datos personales es un derecho humano fundamental que debe ser respetado por todas las personas y organizaciones. En su trabajo, destaca la importancia de la privacidad y el control de los datos personales por parte de los usuarios para evitar situaciones de vulnerabilidad. Asimismo, resalta que el empoderamiento digital es clave en la protección de los datos personales, ya que los usuarios deben ser conscientes de los riesgos y saber cómo protegerlos. Además, el autor del texto enfatiza la importancia de considerar la privacidad en la creación de políticas de seguridad de la

información, ya que la privacidad es un derecho fundamental de los individuos y es necesario protegerla para garantizar el respeto de la dignidad humana y evitar la discriminación.

Las nuevas tecnologías exponen los desafíos y las amenazas a la privacidad de los datos personales que surgen con el uso de la IA y los macrodatos en la era digital (Martínez Devia, 2019). Este autor argumenta que la recopilación, el procesamiento y el uso de datos personales en las plataformas y aplicaciones digitales genera importantes problemas de privacidad. Sugiere que se actualicen las normas de protección de datos para hacer frente a los desafíos de las nuevas tecnologías y propone que se otorgue a las personas un mayor control sobre sus datos personales. Ya que el proceso de convergencia digital trae consigo importantes retos en términos de protección de datos personales, privacidad, seguridad y confianza en las tecnologías de la información y comunicación (TIC). Es necesario que los usuarios de estas tecnologías se empoderen digitalmente para garantizar una protección adecuada de sus datos personales y una toma de decisiones informada sobre su uso (Serrano-Santoyo, A. (2016).

Carissa Véliz, en su libro "Privacidad es Poder" menciona varios casos donde el alcance de transgresión y el uso de los datos personales, uno de los antecedentes más significativos y mediáticos sobre la vulnerabilidad, a gran escala es sin duda el de la empresa *Cambridge Analytica*, la cual analizó los datos de unos 87 millones de usuarios de la red social con fines políticos. Durante muchos años, *Facebook* permitió que el motor de búsqueda *Bing* de *Microsoft* viera los amigos de los usuarios de la red social sin el consentimiento de estos, y dio a *Netflix* y *Spotify* la capacidad de leer y hasta de borrar mensajes privados de usuarios de *Facebook*. En el 2015, comenzó a registrar todos los mensajes de texto y llamadas de usuarios de Android sin haberles pedido permiso (Véliz, 2021). Otro caso, es el de Malte Spitz el cual se refiere a una demanda legal presentada por el político alemán contra la compañía telefónica, Deutsche Telekom, para obtener los datos de localización de su teléfono móvil. El objetivo de Spitz era demostrar el alcance de la recopilación y el uso de datos personales por parte de las compañías telefónicas y la necesidad de una mayor transparencia y protección de la privacidad de los usuarios.

La demanda de Spitz se basó en la Ley de Protección de Datos alemana, que establece que los usuarios tienen derecho a acceder y solicitar la eliminación de sus datos personales. Deutsche Telekom inicialmente se negó a proporcionar los datos, argumentando que se consideraban

información comercial confidencial. Sin embargo, después de una larga batalla legal, Spitz finalmente obtuvo acceso a los datos de localización de su teléfono móvil.

Este caso ha sido visto como un hito en la lucha por la privacidad de los datos en Alemania y en toda Europa. Como señala el profesor de derecho alemán especializado en privacidad, Alexander Dix[5], este caso ha demostrado que los datos personales son realmente importantes, que tienen un valor y que las empresas no pueden simplemente ignorar los derechos de los usuarios.

Además, este caso ha influido en la legislación de protección de datos de la Unión Europea, incluida la aprobación del Reglamento General de Protección de Datos (RGPD) en 2016. El RGPD establece un marco legal claro y más estricto para la protección de los datos personales de los ciudadanos europeos, incluyendo el derecho de acceso y eliminación de datos. El caso de Malte Spitz ha sido un ejemplo importante de la lucha por la privacidad de los datos personales y ha ayudado a impulsar la legislación de protección de datos en Europa.

Los ejemplos anteriores son sucesos documentados que dejan visible la necesidad de una regulación global y una gobernanza sólida sobre los datos personales.

2.2. Privacidad de los Datos

La privacidad de datos es un tema de gran relevancia en la actualidad debido a los avances tecnológicos y la creciente necesidad de recopilar y utilizar información personal. Los datos personales se refieren a toda aquella información que identifica o hace identificable a una persona y son necesarios para interactuar con otros individuos u organizaciones y cumplir con las leyes. Sin embargo, la creciente cantidad de datos que se recopilan, así como la forma en que se utilizan, ha llevado a preocupaciones sobre la privacidad y la protección de estos datos. Además, como ya se ha reiterado anteriormente la forma en que se recopilan y utilizan los datos personales puede tener implicaciones éticas, económicas y sociales significativas.

[5] Alexander Dix es un experto alemán en derecho y privacidad de datos. Se desempeñó como Comisionado de Protección de Datos y Libertad de Información de Berlín (Berliner Beauftragter für Datenschutz und Informationsfreiheit) desde 2005 hasta 2016. DW.COM. (2009). Lo dijo Alexander Dix. Deutsche Welle. Recuperado el 30 de octubre de 2022, de https://www.dw.com/es/lo-dijo-alexander-dix/a-4810823

En este contexto, es necesario comprender y abordar adecuadamente las cuestiones relacionadas con la privacidad de los datos personales.

Desde la perspectiva de las políticas públicas, la privacidad se ha definido como lo opuesto a lo público, sin embargo esta definición no capta la complejidad del concepto de privacidad. Es cierto que la privacidad se asocia comúnmente con la propiedad privada o la administración de los bienes privados (Tenorio, 2019), pero también puede entenderse como una búsqueda de anonimato y clandestinidad. Los usuarios comunes, aquellos que utilizan dispositivos conectados a internet, se ven en desventaja en este mundo cada vez más público e interconectado. En este sentido, la privacidad se convierte en un derecho fundamental que busca proteger la autonomía, independencia, poder y control de las personas sobre su información personal, tanto en el mundo físico como en el digital.

La privacidad es una dimensión fundamental de la identidad personal y se ha considerado un derecho humano desde hace mucho tiempo. Según la definición del Consejo de Europa, la privacidad se refiere a el derecho a la vida privada, la protección de los datos personales y el derecho a controlar la información sobre uno mismo (Cate, 2019). Es decir, la privacidad no solo se refiere a la propiedad de los bienes privados, sino también a la protección de la información personal que puede ser utilizada para identificar a una persona y afectar su vida diaria.

Lo anterior plantea una serie de desafíos y riesgos para la privacidad de los usuarios, especialmente si estos datos son utilizados sin su consentimiento o son compartidos con terceros y utilizados para fines comerciales, para ofrecer productos o servicios personalizados, pero también pueden ser invasivos y violar la privacidad de los usuarios. De aquí que una regulación adecuada y efectiva que garantice la privacidad y protección de los datos personales de los usuarios en línea es fundamental.

Cabe mencionar adicionalmente que la privacidad es un derecho fundamental que no se limita a la intención de ocultar información, sino que se relaciona con la autonomía, independencia, poder y control de una persona sobre su vida. Es esencial para la dignidad humana, tanto en la vida física como en la digital (Prabhakara, 2021). Habermas (1981) destaca que la confusión entre la esfera privada y la pública es un problema común, y que la privacidad no debe ser sacrificada en aras de la publicidad y la transparencia. Según su

argumento, el ámbito privado, que abarca la necesidad y la transitoriedad, se encuentra en la sombra, mientras que la publicidad se presenta como un reino de la libertad y la continuidad, donde todo es visible para todos (Habermas, 1981, p. 43). En este sentido, la protección de la privacidad es vital para preservar la libertad individual.

De acuerdo a lo anterior, en el entorno de los derechos humanos digitales, se contempla que la vida privada está encaminada por la relevancia suprema de la libertad, que se expresa ante todo a partir de la libertad de la conciencia, en la que el individuo contiene la libertad en su persona de pensar, manifestar, expresar sus sentimientos y opiniones con plena libertad (Tenorio, 2021), que la privacidad es parte fundamental de la ética y de la dignidad humana (Cortina, 2022)

En el año 2010, José Luis Piñar Mañas formuló una pregunta que sigue siendo relevante en la actualidad: ¿existe la privacidad? En los últimos 13 años, los avances tecnológicos y las implicaciones éticas han desafiado el nuevo modelo económico de la gestión de grandes cantidades de datos, lo que hace que la pregunta cobre aún más sentido en la actualidad (Piñar Mañas, 2010). La comodidad que brinda la segmentación de preferencias es evidente, como destaca Tenorio (2021).

Además, Zuboff (2020) argumenta que el capitalismo de la vigilancia reclama unilateralmente la experiencia humana como materia prima gratuita, lo que se traduce en datos de comportamiento. Aunque algunos de estos datos se utilizan para mejorar productos o servicios, el resto es considerado un excedente conductual privativo de las propias empresas capitalistas de la vigilancia. Estos datos se utilizan como insumo de procesos avanzados de producción conocidos como inteligencia de máquinas, con los que se fabrican productos predictivos que prevén lo que las personas harán en un futuro cercano (Zuboff, 2020, pp. 12).

De lo expuesto anteriormente, se puede concluir que mediante los datos personales se conforma la información que se utiliza para identificar o hacer identificable a una persona. La recopilación de datos personales es esencial para establecer la identidad de un individuo, describirlo, identificar su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional, y permitir su interacción con otros individuos y organizaciones, garantizando su cumplimiento con las leyes y regulaciones pertinentes (Mañas et al., 2010).

Además, los datos personales también son fundamentales para el crecimiento económico y la mejora de bienes y servicios, ya que permiten la generación de flujos de información y el análisis de la misma. Sin embargo, es importante tener en cuenta que la utilización de datos personales debe ser realizada de forma ética y transparente, y con el consentimiento explícito del individuo. La recopilación de datos debe ser limitada y la información recopilada solo debe ser utilizada para los fines específicos para los cuales se recopiló. (Mañas et al., 2010).

En conclusión, los datos personales son una parte esencial de la identidad y la interacción social en la era digital, y su uso responsable y ético es fundamental para garantizar la privacidad y la protección de los derechos de los individuos.

2.3. Ley Federal de Protección de Datos Personales en Posesión de Particulares en México

La protección de los derechos humanos es una responsabilidad colectiva en la que todos estamos obligados a respetarlos, protegerlos y garantizar su protección a través de los mecanismos necesarios (Tenorio, 2021). En la sociedad de la información y la transición tecnológica actual, la proximidad de las personas a la información a través de nuevas tecnologías de comunicación ha transformado los modelos industriales, culturales y sociales (Tenorio, 2021). Sin embargo, el cambio de paradigma tecnológico también ha planteado desafíos éticos y de privacidad que requieren una regulación adecuada y la implementación de normas para proteger la dignidad humana (Cortina, 2022).

En la era digital, la cantidad de datos personales que se generan y recopilan en línea es enorme y puede incluir desde la ubicación y los patrones de navegación hasta la actividad en las redes sociales y las compras en línea (Johnson, 2017). Esta información puede ser utilizada para crear perfiles detallados de los usuarios y vender productos o servicios personalizados. En este sentido, es necesario que tanto el Estado como las empresas y organizaciones adopten medidas para proteger los datos personales y asegurar su uso ético y responsable en beneficio de los usuarios y la sociedad en general.

Ramirez et al. (2017) sostienen que el derecho a la protección de datos personales ha tenido su mayor desarrollo en el ámbito europeo, consolidándose por primera vez en el Convenio

108 del Consejo de Europa y posteriormente en la Directiva 95/46/CE de la Unión Europea, como una faceta de la vida privada.[6] Sin embargo, tras la adopción de la Carta de Derechos Fundamentales de la Unión Europea, este derecho adquiere aún más relevancia, reconociendo que el tratamiento de datos personales no cumplir con las condiciones de legitimidad aplicables puede constituir una injerencia en la vida privada o la privacidad. En México, la protección de datos personales se reconoce como un derecho humano diferenciado, aunque relacionado con la vida privada. Es importante destacar que el derecho a la vida privada y la privacidad no son sinónimos, ya que la vida privada se asimila a la vida retirada o anónima, a la vida interior (Carrillo, 2003), mientras que la privacidad se refiere al control que una persona tiene sobre su información personal (Mañas, 2010). Aunque el primer concepto comprende al segundo, en este trabajo se utilizarán como sinónimos para fines prácticos. (Tenorio et al., 2019).

En cuanto al progreso en la materia legal, México ha realizado importantes avances durante las últimas dos décadas. Según Sánchez et al. (2020), se han incorporado leyes, artículos y reformas para regular la protección de datos personales en posesión de particulares. En el año 2002, se publicó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que incluía disposiciones para proteger los datos personales de los sujetos obligados (lftaipg, 2002: art.4), lo que representa el primer antecedente de una ley federal en México que involucra datos personales, según Tenorio et al. (2019). En el 2005, el entonces Instituto Federal de Acceso a la Información (IFAI) publicó los lineamientos de Protección de Datos Personales, con el objetivo de establecer políticas generales y procedimientos que deben cumplir las dependencias federales para garantizar la facultad de decidir sobre el uso y destino de los datos personales.

En 2007, se incorporó por primera vez en la Constitución Federal la referencia al derecho a la protección de datos personales, y se estableció el artículo 6o., el cual contempla los principios y bases que rigen el ejercicio del derecho de acceso a la información. No obstante, la mayor reforma en materia de protección de datos personales en México tuvo lugar el 1 de junio de 2009, cuando se publicó un decreto en el Diario Oficial de la Federación (DOF) que agregó

[6] Cfr. De Hert, P. y Gutwirth, S., “Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action”, en Gutwirth, Serge et al. (eds.), Reinventing Data Protection?, Springer, 2009, Cap. 1, Sección 1.1.2.

un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (Sánchez et al., 2020).

Se debe destacar que previo a la adición del segundo párrafo al artículo 16 constitucional en 2009, se llevó a cabo una reforma a la fracción XXIX-O al artículo 73 constitucional, la cual faculta al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares (Sánchez et al., 2020). Es importante señalar que con estas reformas, se reconoce la protección de datos personales como una garantía individual y se otorga al Congreso de la Unión la facultad de legislar en esta materia (Tenorio et al., 2019).

Es crucial mencionar que el avance tecnológico y la digitalización han permitido la recolección, almacenamiento y procesamiento de grandes cantidades de datos personales. En este sentido, las reformas y leyes en materia de protección de datos personales en México son un paso importante para garantizar la privacidad y seguridad de la información personal de los ciudadanos en la era digital. A medida que se implementan políticas públicas y se fortalecen las leyes en esta materia, es necesario continuar evaluando y actualizando los marcos legales para asegurar que se adapten a las nuevas tecnologías y realidades del mundo digital (Sánchez et al., 2020). En el contexto de las políticas públicas, es fundamental tener en cuenta la privacidad y protección de los datos personales de los ciudadanos. Las políticas públicas deben estar diseñadas para garantizar la seguridad de los datos personales de los ciudadanos y el acceso a ellos por parte de las organizaciones gubernamentales solo debe ser posible bajo ciertas circunstancias. Además, es importante fomentar la educación digital de los ciudadanos para que puedan entender mejor los riesgos y beneficios asociados al uso de sus datos personales, y así poder tomar decisiones informadas sobre su uso (García, 2019).

2.4. Derechos ARCO

El derecho a la protección de datos de carácter personal es un derecho fundamental reconocido internacionalmente. Consiste en un derecho subjetivo, autónomo y de tercera generación que constituye un instrumento jurídico (Tenorio et al., 2019)

Los derechos ARCO surgen en 2009 de la reforma constitucional al artículo 16, donde se reconoce que todas las personas tienen derecho al acceso, rectificación, cancelación u oposición de sus datos personales. (¿Cómo ejercer el derecho al “olvido” en México?, 2015).

Los Derechos Arco es el conjunto de derechos a través de los cuales la Ley Orgánica de Protección de Datos de Carácter Personal, garantiza a las personas el poder de control sobre sus datos personales. Se refiere a aquel derecho que tiene un titular de datos personales, para solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos, ante el Sujeto Obligado que esté en posesión de los mismos[7].

Los derechos ARCO forman el conjunto de facultades reconocidas que favorecen a los titulares para que puedan solicitar y ejercer control respecto a los datos personales en posesión de cualquiera que resultase responsable sujeto a sus disposiciones (Tenorio et al., 2019). En el artículo 22 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante LFPDPPP)[8], en el 87 y 89 de su respectivo reglamento, declaran dos características fundamentales de los derechos ARCO: son personales y son independientes entre sí. El acto de ejercer los derechos ARCO, podrá llevarse a cabo por cualquier titular (o en su defecto, su representante legal), pero únicamente en el contexto de lo relacionado con sus datos personales. Es imperante señalar que nadie a excepción de los mencionados, puede solicitar el acceso, rectificación, cancelación u oposición al tratado de los datos personales de otra persona. En estos casos, los responsables del tratamiento de los datos tienen el derecho y deber de negar una solicitud de este tipo (Tenorio et al., 2019).

Respecto a las personas que califican para ser representadas por otros, son personas menores de edad, personas discapacitadas o en estado de interdicción, estas personas pueden ser representadas en su nombre para la aplicación de los derechos ARCO, esto conforme a las reglas de representación establecidas en el Código Civil Federal (Tenorio et al., 2019).

Con respecto a una persona fallecida, si la persona en vida manifestó fehacientemente su voluntad, o si se cuenta con un mandato judicial al respecto, y desde luego se trate de una solicitud previamente presentada ante una autoridad responsable del sector público, sus datos personales pueden ser representados por una persona que acredite interés jurídico, de acuerdo a las leyes aplicables, esta persona autorizada podrá ejercer los derechos ARCO en nombre de la persona finada.

---

[7] Ejerce tus derechos de Datos Personales ARCO – Sarcoem. (n.d.). Gob.mx., from https://edomex.gob.mx/consulta_sarcoem Art. 43, 44, 45, 46 y 47 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

[8] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Nueva Ley publicada en el Diario Oficial de la Federación el 5 de julio de 2010 https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm

Así mismo, se deben de mantener disponibles a los titulares canales de comunicación tanto locales de comunicación electrónica, como medios remoto u otros que (el responsable) considere pertinentes, y por medio de estos canales pudiendo instaurar sistemas, formularios y otros medios simplificados, para proveer a los titulares medios para el ejercicio de los derechos ARCO. Los Sujetos Obligados, es decir los responsables de la gestión de los datos, deberán informar de todo ello en sus avisos de privacidad (Tenorio et al., 2019).

Por último, se debe mencionar que los derechos fundamentales no son absolutos,[9] es decir, se debe tener presente que los derechos ARCO, pueden restringirse ante razones de disposición de orden público, seguridad nacional, seguridad y salud pública (Como bien lo vimos en la pandemia de COVID-19), o para proteger los derechos de terceros, como bien está estipulado expresamente en el segundo párrafo del artículo 16 constitucional y también por el artículo 88 del reglamento de la LFPDPPP, el cual indica que esta restricción se dará en los casos y con las condiciones previstas en las leyes aplicables en materia, o con una resolución de la debidamente fundada y motivada autoridad competente (Tenorio et al., 2019).

Es fundamental comprender que la efectiva protección de los datos personales no se limita a conocer los derechos ARCO y los medios para ejercerlos, sino que implica un conocimiento profundo de la legislación que los regula y los límites y restricciones que existen para cada uno de ellos. Es decir, se requiere una comprensión plena del funcionamiento de la ley y de los criterios que los responsables pueden utilizar para denegar una solicitud de ejercicio de derechos ARCO, los cuales deben estar debidamente fundamentados. Como señala Tenorio et al. (2019), la falta de comprensión de los límites o restricciones particulares para cada uno de ellos puede conllevar a la omisión de solicitudes fundadas o a la aceptación de respuestas negativas sin un análisis riguroso y exhaustivo. Por lo tanto, es esencial que las personas que deseen ejercer sus derechos ARCO cuenten con una adecuada asesoría legal que les permita hacer valer sus derechos de manera efectiva y evitar posibles vulneraciones a su privacidad y protección de datos personales.

---

[9] No obstante lo anterior, y como hemos dicho, los Derechos Fundamentales no son absolutos ni ilimitados, sino que en verdad se encuentran sometidos a una serie de restricciones o limitaciones que provocan que su titular no pueda ejercer válidamente una determinada prerrogativa en ciertas circunstancias. Tórtora Aravena, Hugo. (2010). LAS LIMITACIONES A LOS DERECHOS FUNDAMENTALES. Estudios constitucionales, 8(2), 167-200. https://dx.doi.org/10.4067/S0718-52002010000200007

De acuerdo al artículo 23 de la LFPDPPP, en el concepto más fundamental, el derecho al acceso constituye la facultad de un titular de datos personales para poder solicitarle a cualquier responsable o sujeto obligado, cierta información sobre el tratamiento y procesamiento de sus datos personales, inclusive en los casos en que el titular no está seguro de la autenticidad o equivalencia exacta de la cantidad, número o tipo de datos que son objeto de tratamiento por parte de los o el responsable (Tenorio et al., 2019).

No es necesario que los titulares tengan conocimiento sobre detalles de los datos o del aviso de privacidad para ejercer su derecho a acceso de sus datos; no existe contradicción si el titular ejerce el derecho de acceso para saber qué datos personales son sometidos a tratamiento por un responsable, y a la vez solicita conocer el aviso de privacidad bajo el cual está regulado su tratamiento. En ciertos casos es probable que un titular pueda conjeturar que sus datos no fueron recabados o recolectados de forma legal y requiere saber, con apoyo de dicho aviso, cuales son los criterios de y las intenciones del tratamiento de sus datos y la información restante que ese documento debería contener y si finalmente se ha seguido su propio aviso de privacidad establecido (Tenorio et al., 2019).

El derecho de acceso a los datos personales es una garantía fundamental en la protección de la privacidad y la autodeterminación informativa del titular. Este derecho permite que el titular pueda conocer y controlar sus datos personales, lo que implica conocer si están siendo tratados, el propósito del tratamiento, la forma en que se están utilizando y la identidad de los destinatarios o personas que tienen acceso a ellos. Es importante destacar que el derecho de acceso no solo se limita a la información en posesión del responsable del tratamiento, sino que también incluye la información que ha sido compartida con terceros o que ha sido transferida a otros países. En definitiva, el derecho de acceso es esencial para que los titulares de datos puedan tomar decisiones informadas sobre el uso de sus datos personales y proteger su privacidad.

Es importante destacar que el derecho de acceso en el marco de la protección de datos personales es un derecho fundamental para los titulares de datos personales. El responsable, como sujeto obligado, tiene la responsabilidad de garantizar este derecho a través de tres vías. En primer lugar, debe informar al titular de la existencia efectiva del tratamiento de sus datos personales. En segundo lugar, el titular tiene derecho a acceder a sus datos personales que están en posesión del responsable. Por último, el responsable debe proporcionar información

completa sobre el tratamiento de los datos personales, incluyendo los tipos de datos personales que se están tratando, los fines del tratamiento, las personas involucradas en el tratamiento, y en caso de transferencias, información sobre los destinatarios y la información transferida. Es importante que los responsables comprendan la importancia de garantizar el derecho de acceso y proporcionar información clara y completa para que los titulares puedan ejercer sus derechos plenamente (Tenorio et al., 2019).

El derecho del titular de los datos que tiene para solicitar el acceso de la información que se encuentra en los sistemas, archivos y bases de datos, así como registros o expedientes del responsable que los tiene, utiliza y/o almacena, también conocer la información referente al uso que se da la información personal. Se dará por cumplido el derecho al acceso a los datos cuando el responsable proporcione a disposición del titular solicitante los datos personales mediante la expedición de copias simples, en sitio, medios electrónicos, magnéticos, sonoros, visuales, holográficos, ópticos, o por medio de otras tecnologías que se hayan estipulado en el aviso de privacidad del responsable (Tenorio et al., 2019).

El derecho a la rectificación se considera como el derecho que tienen los titulares de datos personales a rectificar sus datos personales cuando estos sean incompletos, inexactos o incorrectos. Este un derecho de los Derechos ARCO que puede ejercerse de manera independiente a los demás derechos ARCO, en este derecho basta con que el propio titular sabe que sus datos personales están incompletos, inexactos o incorrectos y manifiesta las intenciones de actualizarlos o completarlos ante un responsable específico o a raíz de un derecho previo de acceso, y el titular conoce que los datos personales en posesión del responsable no están completos o son inexactos (Tenorio et al., 2019).

En cuanto al derecho de cancelación, se debe de comprender su alcance teniendo en cuenta que la descripción del concepto “bloqueo” está intrínsecamente relacionado a este derecho. En el artículo 3, fracción III de la LFPDPPP decreta que por tal se debe entender como: La identificación y mantenimiento de datos personales una vez que se ha cumplido con la finalidad por la cual los datos fueron recabados, con el propósito único de determinar probables responsabilidades referente con su tratamiento, hasta el plazo prescrito legalmente o contractual de éstas. Durante un periodo establecido los datos personales no podrán ser tratados y una vez transcurrido este periodo, se continuará el procedimiento a su cancelación en la base de datos que corresponda (Tenorio et al., 2019).

Como forma de antecedente organizativo y en concordancia con el artículo 3, Fracción III de la LFPDPPP, el responsable sin excepción, y conforme al último párrafo del artículo 108 del Reglamento de la LFPDPPP, el plazo de prescripción legal o contractual correspondiente , será el periodo de bloqueo. Debido a esto la identificación de todos los datos personales objeto de tratamiento es algo indispensable, como su medio de obtención y su fecha, así como el propósito de los cuales es obligatorio o necesario su tratamiento (Tenorio et al., 2019). Complementario a esto, como responsable y como titular de datos personales, se debe tener conocimiento que el artículo 106 del Reglamento de la LFPDPPP determina que los titulares pueden solicitar en cualquier momento la cancelación de sus datos personales y así mismo cuando estimen que el tratamiento de sus datos no están siendo tratados de acuerdo a los principios y obligaciones que indica la normativa.

De igual manera, y tal cual como sucede con cualquier otra respuesta al ejercicio de los derechos ARCO, en caso de que el responsable de una negativa al titular sobre la cancelación de sus datos, hay un organismo al cual pueden asistir, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI), la cual se encuentra facultada para un procedimiento de protección de derechos y se logre una solución a la procedencia o improcedencia de tal negativa (Tenorio et al., 2019).

El derecho de oposición, es un derecho al tratamiento de datos personales, el cual ha sido objeto de varias interpretaciones y con frecuencia suele confundirse con el derecho de cancelación. El INAI ha elaborado una definición concisa de este derecho, y estipula de esta forma: Es el derecho que se tiene de solicitar que los datos personales no sean utilizados para determinados propósitos, o de ser necesario, requerir que finalice el tratamiento de estos, con la finalidad de evitar un daño a la persona titular. Es fundamental mencionar que no siempre será posible que se lleve a cabo el cumplimiento de este derecho de oponerse al uso de los datos personales del titular, por ejemplo cuando sean requeridos para algún fin de cuestión legal, o para el cumplimiento de obligaciones (Tenorio et al., 2019).

En cuanto a toma de decisiones sin intervención humana, es sumamente relevante (para el actual ecosistema digital), para el presente y el futuro de la protección de datos personales entre otros derechos y libertades de la sociedad pero aún el nivel de cumplimiento e importancia brindado a otras disposiciones de la normatividad es alejado, el artículo 112 del

Reglamento de la LFPDPPP establece el primer acercamiento del legislador mexicano para distinguir los derechos de los titulares cuando afectan su esfera jurídica aquellas decisiones automatizadas (sin intervención humana) adoptadas a partir del tratamiento de sus datos personales. La conexión de este tipo de decisiones automatizadas respecto a los derechos ARCO, se sentencia en el segundo párrafo del artículo 112 del Reglamento de la LFPDPPP, y consiste en que estima el reconocimiento de la existencia de tratamientos automatizados de datos personales, el cual su propósito es la toma de decisiones que pudieran afectar a las personas físicas y conjetura el conocimiento de sus disposiciones (Tenorio et al., 2019).

> *Artículo 112. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Asimismo, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto, para que, de acuerdo con los mecanismos que el responsable tenga implementados para tal fin, esté en posibilidad de solicitar la reconsideración de la decisión tomada. (Capítulo VII, De los Derechos de los Titulares de Datos Personales y su Ejercicio Sección VI De las decisiones sin intervención humana valorativa)*[10]

El tratamiento de datos personales ocurre cuando el titular consiente en vincular su perfil de redes sociales como parte del proceso de evaluación de su solvencia crediticia. Es importante destacar que los derechos ARCO no proporcionan a los titulares el derecho a conocer en detalle el funcionamiento de los algoritmos ni las consideraciones utilizadas por estos medios automatizados para generar una "decisión" sin la intervención humana valorativa. Los derechos ARCO se limitan a los datos personales del titular evaluado, según Tenorio et al. (2019).

El derecho a la información está estrechamente relacionado con el ejercicio de los derechos ARCO en situaciones particulares como el ejemplo mencionado anteriormente. En este sentido, los titulares tienen la facultad de ejercer su derecho a acceder a sus datos personales utilizados para la toma de decisiones automatizadas y a rectificar cualquier información que pueda estar desactualizada o incorrecta. Estos derechos son de suma importancia cuando se

[10] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (2011, December 21). Www.ordenjuridico.gob.mx. http://www.ordenjuridico.gob.mx/Documentos/Federal/html/wo88475.html

trata de algoritmos, IA y macrodatos que involucran datos personales. Como señala Tenorio et al. (2019), “estos son derechos que las personas tienen facultad de ejercer”

Los responsables deben entablar acciones de consumación al interior de su organización para garantizar el respetar este ejercicio de los titulares, estas acciones van más allá de de la publicación de avisos de privacidad que exhiben la existencia de los medios para ejercerlos, es un requisito que existan departamentos encargados de su gestión o personas encargadas de la gestión para que todas las personas reciba respuesta a una solicitud para ejercer los derechos ARCO, y definitivamente, para prevenir que los responsables caigan en responsabilidad administrativa como consecuencia de una gestión deficiente de las mismas (Tenorio et al., 2019).

Según García (2019), el diseño de políticas públicas relacionadas con el manejo de datos personales debe ser guiado por un enfoque centrado en el usuario y su contexto. Esto implica tener en cuenta las necesidades, expectativas y derechos de los individuos, así como los desafíos que enfrentan al tratar con datos personales. Asimismo, la política pública debe estar basada en un análisis riguroso del contexto de uso de los datos, considerando factores como la sensibilidad de los datos, los riesgos de divulgación y la naturaleza de las relaciones de confianza entre los individuos y las organizaciones que manejan los datos. Esto permitirá desarrollar políticas públicas efectivas y adecuadas para proteger los datos personales de los individuos y garantizar el respeto de sus derechos (García, 2019).

2.5. Relevancia de los aspectos éticos en el desarrollo de las tecnologías digitales emergentes

Este apartado destaca la importancia de que la tecnología sea utilizada en beneficio de la sociedad, y no al revés. En la actualidad, en medio de la revolución industrial, es necesario que los algoritmos sean programados de manera ética, y que se cuide el principio de “No-maleficencia”. Según la filósofa Adela Cortina, la tecnología no debe controlarnos ni sobrepasarse en conocimiento propio. En lugar de ello, debe ser una herramienta que nos ayude a comprender mejor nuestra propia conducta. Es importante recordar que, aunque se

nos llame impersonalmente “usuarios”, somos seres humanos con derechos y necesidades, y la tecnología debe ser utilizada para servirnos a nosotros, y no al contrario (Cortina, 2022).

El término “algoritmo” es algo que la mayoría de la gente ha escuchado, y aunque tengamos una idea general sobre lo que significa, a medida que los algoritmos se vuelven más complejos, nuestra comprensión sobre ellos se hace cada vez más limitada e inaccesible. Estos algoritmos utilizan el vasto conocimiento que tienen de cada usuario para motivar su actividad en diferentes plataformas, redes sociales, programas digitales e incluso en productos llamados inteligentes como relojes, cafeteras y asistentes virtuales en el hogar.

La información contenida en los algoritmos de cada usuario incluye todo lo que hemos sido en cualquier momento del pasado, incluyendo registros de las páginas web que hemos visitado y consultado, y predice lo que podríamos hacer en el futuro, como la paradoja del gato de Schrödinger[11] con sus diferentes posibilidades de una realidad. Para nosotros, los algoritmos son una caja negra, y las consecuencias de su uso parecen inevitables. En resumen, los algoritmos son nuestro “anti-yo” porque saben más sobre nosotros de lo que nosotros mismos sabemos, y seguirán aprendiendo más de nosotros de lo que podremos entender. En última instancia, el algoritmo es nuestra huella digital, nuestra presencia en el mundo digital y en el metaverso.

Turkle sugiere que nuestros personajes en línea pueden convertirse en una especie de máscara, lo que nos permite presentar al mundo una versión cuidadosamente seleccionada de nosotros mismos. Esto puede crear una desconexión entre nuestra identidad digital y la de la vida real (Turkle, 2011).

La privacidad de los datos personales se ha convertido en un verdadero reto ético que enfrenta la sociedad de la información, una sociedad digital, que sin ser consultada, está mutando a ser una sociedad transhumanista (Cortina, 2022). Los procesos y avances deben estar orientados hacia la sostenibilidad social y del planeta, deben ser beneficiosos y estar regidos por el principio de no maleficencia, que implica no producir o ejercer daño y también prevenirlo. En cuanto a la posibilidad de sumisión o control por parte de máquinas, se debe tomar en cuenta el principio de autonomía de las personas y evitar que las máquinas estén en

[11] Cuando el sistema cuántico se rompe, la realidad se define por una de las opciones. Sólo veremos al gato vivo o muerto, nunca ambas. Este proceso de tránsito de la realidad cuántica a nuestra realidad clásica se llama decoherencia, y es la responsable de que veamos el mundo tal y como lo conocemos. Es decir, una única realidad. https://www.astromia.com/astronomia/paradojagato.htm

posición de tomar decisiones éticas inherentes a los seres humanos. Este principio se puede fortalecer mediante el uso de sistemas inteligentes, como el Internet de las cosas y automóviles autónomos, y en cuyas manos deben estar tanto el control como las decisiones significativas donde la privacidad sigue siendo uno de los elementos de la autonomía del ser humano. Además, es necesario considerar los principios de *explicabilidad* y habilidad para asumir responsabilidades como factores que deben ser comprendidos por los usuarios del mundo digital (Cortina, 2022).

La sociedad está subcontratando los recuerdos a la tecnología. Con la capacidad de registrar y almacenar cada momento de las vidas, se depende cada vez más de la tecnología para recordar por los individuos (Turkle, 2011). Turkle argumenta que esto puede conducir a una especie de amnesia digital, en la que olvidamos detalles importantes de nuestras vidas porque dependemos demasiado de la tecnología para recordarlos. Las relaciones humanas con los robots y la IA son cada vez más complejas. A medida que avanza la tecnología, se están desarrollando conexiones emocionales con las máquinas de formas que antes no se creían imposibles. Turkle sugiere que esto puede tener consecuencias tanto positivas como negativas, ya que comenzamos a desdibujar las líneas entre humanos y máquinas (Turkle, 2011).

Según Cortina (2022), hablar de una vida fuera del ecosistema tecnológico en el año 2022 sería similar a sugerir una vida en las cavernas, haciendo referencia al mito de Platón.[12]Las preocupaciones relacionadas con la ética y las implicaciones del uso de la tecnología y la generación de datos no son infundadas, ya que existe el riesgo de que los gobiernos que no defiendan la libertad de pensamiento utilicen la tecnología para criminalizar a aquellos que tengan ciertas creencias y opiniones (Tegmark, 2018).

En este contexto, las tecnologías de la información de última generación presentan un desafío apremiante en cuanto al derecho a la vida privada. Expresiones cada vez más comunes como *big data*, computación en la nube, *e-learning*, ciberacoso, ciberdelitos, etc., están reconfigurando el concepto de vida privada (Tenorio, 2021). Es importante abordar estos nuevos desafíos y garantizar que la tecnología sirva a los humanos y no al revés, que se cuide el principio de No-Maleficencia, que se proteja la privacidad y que se promueva la

[12] La alegoría de la caverna pretende poner de manifiesto el estado en que, con respecto a la educación o falta de ella, se halla nuestra naturaleza, es decir, el estado en que se halla la mayoría de los hombres con relación al conocimiento de la verdad o a la ignorancia. PLATÓN, República, Libro VII, Ed. Gredos, Madrid 1992

explicabilidad y habilidad de asumir responsabilidades como factores esenciales para comprender el mundo digital en el que vivimos (Cortina, 2022).

Al estudiar la IA y la sociedad digital, a menudo se presentan dos posturas: una a favor de la tecnología y otra en contra. Sin embargo, es inevitable la absorción tecnológica tal como se ha implementado por las esferas tomadoras de decisiones. Este es el primer aspecto que se encuentra al investigar sobre la tecnología de la 4RI. Parecería que se debe promover o negar el potencial de la tecnología, pero según Adela Cortina, las ventajas y las implicaciones no son mutuamente excluyentes. Son dos aspectos de un mismo estado. Desde hace 23 años se ha pensado en la complementariedad de la innovación y el diseño seguro de la tecnología para el humano. La idea de que la seguridad y las implicaciones en la tecnología deben considerarse desde la fase de diseño se atribuye comúnmente a Bruce Schneier, un experto en criptografía y seguridad informática que ha escrito extensamente sobre el tema.

Bruce Schneier, (2015)[13] sostiene que la seguridad debe ser una consideración primordial en el diseño de la tecnología, en lugar de ser una ocurrencia tardía. Según Schneier, la seguridad debe ser un aspecto clave que se tenga en cuenta desde el primer momento en el proceso de diseño, y debe ser una preocupación constante a lo largo de todo el ciclo de vida de la tecnología, desde su concepción hasta su implementación final.

La influencia de las ideas de Schneier en el campo de la seguridad informática ha sido significativa, y ha ayudado a dar forma a las mejores prácticas para diseñar e implementar sistemas seguros. Además, su contribución también ha sido relevante en los debates más amplios sobre el papel de la tecnología en la sociedad, y la importancia de considerar las implicaciones éticas de las nuevas tecnologías.

En la actualidad, numerosos especialistas en tecnología han señalado la importancia de considerar las implicaciones éticas en el desarrollo de las tecnologías digitales emergentes desde la fase de diseño, tal como destacó Richard Benjamins[14], durante su intervención en la Conferencia 'IA y Ética', dentro del ciclo 'Ciencia en la Casa de América' (Casa, 2021).
Es necesario tener en cuenta que al igual que se ha logrado un consenso en la fabricación de automóviles para garantizar la seguridad y la funcionalidad, se debe aplicar un enfoque ético similar en el diseño y uso de nuevas tecnologías en la sociedad.

[13] El libro "Secretos y mentiras: seguridad digital en un mundo en red" fue publicado originalmente en el año 2000, y la edición de quince aniversario ha sido considerada para las referencias. Schneier sigue siendo una figura influyente en el campo de la seguridad informática, y sus ideas siguen siendo relevantes en la actualidad, en un mundo cada vez más interconectado e impulsado por la tecnología.
[14] Chief AI & Data Strategist de Telefónica

Además, es importante considerar los aspectos éticos multidimensionales que se plantean, Cortina sugiere que se debe reflexionar sobre la forma en que se desea establecer la relación ética, si la ética debe surgir desde las propias tecnologías hacia los humanos y sus normas, o si por el contrario, debe ser la ética humana la que guíe la manera en que nos relacionamos y manejamos estas tecnologías. En definitiva, la incorporación de la ética en el diseño y uso de tecnologías emergentes es un tema clave en la actualidad, y su consideración temprana es esencial para garantizar un uso responsable y seguro de estas herramientas en la sociedad.

La ética en la era digital es un tema complejo que ha generado brechas entre las diversas aplicaciones que se han desplegado. La agresividad de los algoritmos aplicados en la vida cotidiana ha evolucionado de manera drástica y nuevas tecnologías se siguen aplicando como si las consecuencias fueran inevitables. Según Zuboff (2020), el capitalismo de la vigilancia juega con una lógica que se ha puesto en acción y no es la tecnología en sí. Este tema es profundamente relevante en la era digital actual, donde los tomadores de decisiones, a quienes Zuboff ha llamado "Capitalistas de la Vigilancia", persisten en la modificación y construcción de la opinión social. Se considera que las prácticas, hasta cómo se han manejado hasta este momento, son expresiones inherentes e inevitables de las tecnologías. En su tema "El Titiritero, no el Títere" Zuboff cuestiona a los grandes CEOs sobre este tema.

> En el 2009, la opinión pública se enteró por vez primera de que Google conserva nuestros historiales de búsqueda indefinidamente: y esos datos que están disponibles como si fueran stocks de materias primas de Google también Están a disposición de los servicios de inteligencia y policiales de los Gobiernos. Preguntado por esas prácticas, el antiguo director ejecutivo de la empresa, Eric Schmidt, comentó: «La realidad es que los buscadores, y Google entre ellos, sí conservan esa información durante un tiempo» (pp. 19-20).

Esta autora considera que el capitalismo de la vigilancia ha puesto en marcha una lógica que es necesario repensar y redefinir. Los tomadores de decisiones en el ámbito digital actual deben ser conscientes de su responsabilidad en la creación de opiniones sociales y en la construcción de la ética en la tecnología. Es necesario que se consideren las implicaciones éticas y se implementen prácticas responsables desde el diseño mismo de las tecnologías, tal como lo ha señalado Richard Benjamins.

En última instancia, se trata de un llamado a la reflexión sobre nuestra relación con la tecnología y la importancia de establecer prácticas éticas y responsables en su uso. La ética de la IA no puede ser una ocurrencia tardía o un tema secundario en el diseño y aplicación de tecnologías emergentes. En cambio, debe ser un tema fundamental y prioritario que guíe nuestra toma de decisiones en la era digital actual y en el futuro.

Las implicaciones éticas de la tecnología son numerosas y complejas. En la actualidad, la tecnología permea en todos los aspectos de nuestra vida, desde la forma en que nos comunicamos, trabajamos, nos relacionamos, hasta cómo hacemos transacciones comerciales o incluso como nos divertimos. Por lo tanto, es crucial tener en cuenta las implicaciones éticas relacionadas con la tecnología para garantizar que se utilice de manera responsable y beneficiosa para todos.

A continuación, se presentan algunas consideraciones éticas clave relacionadas con la tecnología.

El ciberdelito. El delito cibernético implica el uso de tecnología para cometer actividades ilegales, como piratería, robo de datos personales o confidenciales, propagación de malware y otras formas de actividades delictivas en línea. Estas acciones pueden causar daños a las personas, las empresas y la sociedad en su conjunto (Schneier, 2015).

Las implicaciones éticas de los delitos cibernéticos surgen del hecho de que estas actividades violan principios morales fundamentales como la honestidad, el respeto a la privacidad y la obligación de proteger la propiedad de otras personas. Los ciberdelincuentes, a sabiendas y deliberadamente, se involucran en actividades que causan daño a otros, lo cual es contrario a los valores éticos y las normas sociales. (Schneier, 2015).

Además, el delito cibernético puede tener un impacto significativo en la sociedad, ya que puede interrumpir la infraestructura crítica, comprometer la seguridad nacional y generar pérdidas financieras para las personas y las empresas. Estas consecuencias pueden tener efectos de gran alcance en la vida de las personas y, por lo tanto, el delito cibernético plantea importantes cuestiones éticas sobre la responsabilidad de las personas y las organizaciones de salvaguardar los sistemas y datos digitales (Schneier, 2018).

Por ejemplo en la obra "Haga clic aquí para matar a todos: seguridad y supervivencia en un mundo hiperconectado" publicado en 2018, analiza las implicaciones de seguridad del internet de las cosas (IoT) y los riesgos asociados con la creciente interconexión de los dispositivos. También examina los desafíos de regular los dispositivos IoT y equilibrar la seguridad y la comodidad (Schneier, 2018).

En conclusión, el ciberdelito no es solo una cuestión legal, sino también ética, ya que implica la violación de principios morales básicos y puede causar un daño significativo a las personas y la sociedad.

Por otro lado, el ciberacoso es el uso de tecnologías digitales, como redes sociales, las aplicaciones de mensajería o foros en línea, para acosar, intimidar o dañar a personas o grupos. Esta forma de intimidación puede tener graves efectos psicológicos y emocionales en las víctimas, como ansiedad, depresión e incluso suicidio (Shariff, 2009).

Las implicaciones éticas del ciberacoso surgen del hecho de que viola principios morales fundamentales como el respeto, la compasión y la dignidad. El ciberacoso es un acto intencionado que causa daño a los demás y va en contra de los valores éticos que promueven el bienestar y la dignidad de todas las personas.

El ciberacoso puede tener consecuencias de gran alcance tanto para la víctima como para el perpetrador. Puede conducir a la pérdida de reputación, exclusión social y consecuencias legales. Además, puede crear un entorno en línea tóxico que daña no solo a la víctima sino también a la comunidad en general (Kowalski, Limber, & Agatston, 2012).

Por lo tanto, el ciberacoso plantea importantes cuestiones éticas sobre la responsabilidad de las personas y las organizaciones de crear un entorno en línea seguro y respetuoso. Es fundamental reconocer las implicaciones éticas del ciberacoso y actuar para prevenirlo y brindar apoyo a las víctimas.

Sesgo y discriminación: la tecnología se puede programar con sesgos, lo que puede conducir a resultados discriminatorios, como algoritmos sesgados o tecnología de reconocimiento facial que es menos precisa para ciertos grupos. Es crucial abordar estos sesgos para

garantizar que la tecnología sea justa y equitativa para todos (Lee, 2020). Los algoritmos utilizados en la IA y el aprendizaje automático a menudo se basan en datos históricos que reflejan las desigualdades existentes en la sociedad. Como resultado, pueden perpetuar la discriminación y la desigualdad, lo que es inaceptable desde una perspectiva ética. Es fundamental que los desarrolladores y los reguladores trabajen juntos para garantizar que los algoritmos sean justos e imparciales.

Automatización y pérdida de empleos: a medida que la tecnología se vuelve más avanzada, es cada vez más capaz de realizar tareas que antes realizaban los humanos. Esto puede conducir a la pérdida de empleos y la desigualdad económica, ya que algunas personas pueden no tener las habilidades necesarias para competir en una fuerza laboral automatizada. Es importante considerar el impacto de la tecnología en el empleo y desarrollar estrategias para apoyar a los trabajadores en la transición a una economía automatizada (Ford, 2015).

Sistemas Autónomos y Responsabilidad: Con el desarrollo de sistemas autónomos, como los autos sin conductor, surgen dudas sobre quién es responsable cuando estos sistemas cometen errores o que causen daños. Es esencial garantizar que el desarrollo y la implementación de estos sistemas se realicen de manera ética y comprendiendo los riesgos potenciales (Yudkowsky, 2007).

Impacto ambiental: la producción y eliminación de tecnología puede tener un impacto ambiental significativo, como el uso de metales raros y la generación de desechos electrónicos. Es importante considerar el impacto ambiental de la tecnología y desarrollar estrategias para minimizar sus efectos negativos (Jackson, 2016; Raworth, 2017; Zuboff, 2020)

Dependencia de la tecnología: apego excesivo, desmedido e incontrolable a la tecnología digital, esta dependencia extrema a la tecnología puede tener impactos negativos en la salud mental y el bienestar de las personas, así como en la capacidad de las personas para funcionar sin la tecnología. El uso excesivo de la tecnología, incluyendo las redes sociales, puede llevar a la aparición de trastornos psicológicos y emocionales. Un estudio de Rosen y colaboradores (2013) encontró una relación entre el uso de Facebook y síntomas de trastornos psiquiátricos, incluyendo ansiedad, depresión y trastornos de atención, lo que sugiere que la dependencia de la tecnología puede tener impactos negativos en la salud mental y el bienestar de las personas.

Privacidad y protección de datos (este aspecto no se podía dejar fuera, y así mismo se mencionara brevemente como parte fundamental de este listado de implicaciones éticas clave): con la creciente cantidad de datos personales recopilados y almacenados por empresas y gobiernos, existen preocupaciones sobre la privacidad y la seguridad de esos datos. Es esencial garantizar que los datos se recopilen y utilicen de manera ética, y que las personas tengan control sobre su información personal.(Solove, 2008; Schneier, 2018; Zuboff, 2020). En este trabajo intenta conectar esta parte en el entorno de los derechos digitales en los estudiantes universitarios.

En general, las implicaciones éticas de la tecnología son complejas y multifacéticas. Es esencial considerar las implicaciones éticas en el desarrollo y uso de la tecnología para garantizar que las tecnologías se desarrollen y utilicen de manera benéfica y equitativa para todos. Las implicaciones éticas de la tecnología son amplias y abarcan desde la privacidad y la discriminación hasta la salud mental y el bienestar. Es crucial que las empresas, los reguladores y los consumidores trabajen juntos para garantizar que la tecnología se utilice de manera responsable y para el beneficio de la sociedad en general.

Capítulo 3. Contexto: La 4RI y la economía de los datos en un entorno universitario

En un entorno universitario, la 4RI y la economía de los datos presentan tanto oportunidades como desafíos. Por un lado, las universidades pueden aprovechar las tecnologías de la Industria 4.0 y los datos para mejorar la enseñanza, la investigación y la gestión. Por otro lado, las universidades también deben enfrentar los desafíos que plantea la protección de datos, la privacidad y la ética.

En cuanto a las oportunidades que presenta la llamada Industria 4.0 para la educación superior, un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) señala: Las tecnologías digitales pueden ayudar a mejorar la calidad y la relevancia de la educación superior, hacerla más accesible y asequible, y crear nuevas oportunidades para la innovación y la colaboración (OCDE, 2019, p. 11).

Sin embargo, también es importante considerar los desafíos que la Industria 4.0, como parte de la 4RI plantea para las universidades. Un estudio de la Asociación Nacional de Universidades e Instituciones de Educación Superior de Estados Unidos (NASPA, por sus siglas en inglés) destaca que la protección de datos y la privacidad son desafíos importantes que las universidades deben abordar, ya que las tecnologías de la Industria 4.0 y la economía de los datos requieren una gestión cuidadosa de la información personal y sensible (NASPA, 2021, p. 4). La 4RI y la economía de los datos están transformando el mundo en el que vivimos, y las universidades no son una excepción.

Por otro lado, es importante destacar que la 4RI y la economía de los datos también pueden impactar positivamente en la investigación universitaria. Según un informe de la Comisión Europea, el acceso a grandes cantidades de datos de diversas fuentes, combinado con nuevas técnicas de análisis y visualización, puede permitir avances significativos en la investigación y el descubrimiento (Comisión Europea, 2016, p. 4).

Además, la Industria 4.0 también está impulsando la innovación en la gestión universitaria. Según un estudio de Deloitte, la digitalización y la automatización pueden mejorar la eficiencia y la calidad de los procesos universitarios, desde la admisión y la matrícula hasta la gestión de la investigación y la colaboración con la industria (Deloitte, 2019, p. 4).

Sin embargo, también es importante considerar los desafíos que la Industria 4.0 y la economía de los datos plantean para la educación superior. Uno de los principales desafíos es el de la formación de los estudiantes en las habilidades necesarias para la nueva era digital. Según el Foro Económico Mundial, las habilidades más importantes para el futuro son la resolución de problemas complejos, el pensamiento crítico, la creatividad, la colaboración, la inteligencia emocional y la capacidad de aprender continuamente (Foro Económico Mundial, 2020, p. 2).

Otro desafío importante es el de la protección de datos y la privacidad. Según un estudio de la firma de consultoría PwC, la gestión de datos es un tema cada vez más complejo y delicado, y las universidades deben tomar medidas para garantizar la privacidad y la seguridad de la información de los estudiantes, el personal y los colaboradores (PwC, 2018, p. 2).

Según el informe de la European University Association (EUA) de 2018, la 4RI y la economía de los datos están transformando el panorama de la educación superior en Europa. El informe destaca la importancia de la tecnología digital y la gestión de datos en la educación superior, y señala que la digitalización se ha convertido en una parte integral de la enseñanza y el aprendizaje en todas las disciplinas (EUA, 2018, p. 10). Además, el informe de la EUA destaca que la digitalización también está cambiando la forma en que se realizan las investigaciones universitarias. Según el informe, los datos masivos y la IA tienen el potencial de transformar la investigación en todas las disciplinas (EUA, 2018, p. 14).

Jara, Fernandez-Llatas y Ibanez-Sanchez (2018), destaca la importancia de la Industria 4.0 en la educación universitaria. Según los autores, la Industria 4.0 representa una oportunidad única para transformar la educación, permitiendo a las universidades formar a los estudiantes para los empleos del futuro (Jara et al., 2018, p. 240).

Kalaitzidis y Lian (2017), abordan el impacto de la 4RI y la economía de los datos en la educación superior. Los autores destacan que la digitalización y la automatización pueden mejorar la eficiencia y la calidad de los procesos universitarios, y señalan que la adopción de tecnologías digitales es necesaria para garantizar la competitividad de las universidades y preparar a los estudiantes para el mundo del trabajo (Kalaitzidis y Lian, p. 3).

Para aprovechar al máximo las oportunidades que ofrece la Industria 4.0, es importante que las universidades adopten un enfoque proactivo y estratégico para la gestión de los datos, al mismo tiempo que mantienen un compromiso sólido con la ética, la privacidad y la protección de datos. La 4RI y la economía de los datos también están transformando el panorama de la educación superior en México.

La educación superior enfrenta el desafío de incorporar tecnologías que permitan una mejor gestión de la información y los datos, la personalización de la enseñanza, y la adopción de métodos pedagógicos más eficaces (SEP, 2020, p. 9). El informe destaca que la digitalización y la economía de los datos también pueden mejorar la investigación universitaria en México, ya que los datos masivos y la IA pueden ayudar a los investigadores a descubrir patrones y relaciones que de otra manera serían difíciles de detectar (SEP, 2020, p. 17).

En un estudio reciente se destaca la importancia de que las universidades mexicanas adopten un enfoque estratégico para aprovechar las oportunidades que ofrece la Industria 4.0. Según los autores, la 4RI ofrece una oportunidad única para que las universidades mexicanas mejoren la calidad de la educación, fomenten la innovación y mejoren la competitividad de los estudiantes y del país en general (Sánchez-García y Rojas-López, 2018, p. 4).

Por otro lado, Gutiérrez-Maldonado y Reyes-López (2021), abordan el impacto de la economía de los datos en la educación superior mexicana. Los autores destacan que la economía de los datos puede mejorar la eficiencia y la calidad de la educación superior en México, pero es necesario que se establezcan políticas claras y se proteja la privacidad y la seguridad de los datos (Gutiérrez-Maldonado y Reyes-López, 2021, p. 7). Respecto al empleo y de acuerdo con el informe "El futuro del trabajo y la educación en México" del Banco Interamericano de Desarrollo (BID), la digitalización y la automatización pueden redefinir los trabajos y adquirir nuevas habilidades en áreas como la programación, la ciencia de datos y la IA (BID, 2019, p. 24).

En este sentido, es importante que las universidades mexicanas se adapten a las demandas del mercado laboral y ofrezcan programas de estudio que incorporen habilidades tecnológicas y digitales, como lo señala el informe "La 4RI y el futuro del trabajo en México" de la Organización para la Cooperación y el Desarrollo Económicos (OCDE): las universidades mexicanas deben adaptar sus planes de estudio para incluir habilidades y conocimientos relacionados con la automatización, la digitalización y la economía de los datos (OCDE, 2018, p. 50).

En el mismo informe, se destaca la necesidad de que las universidades fomenten la innovación y la investigación en el ámbito tecnológico, ya que esto puede contribuir al desarrollo económico y social del país: "las universidades mexicanas deben ser actores clave en la creación de nuevas tecnologías y en la promoción de la innovación empresarial y social" (OCDE, 2018, p. 50).

Por otro lado, también es importante abordar los retos éticos y de privacidad que surgen en el contexto de la economía de los datos. Hernández-Fuentes y Ortiz-López (2020), destaca la necesidad de que las universidades mexicanas aborden estos temas en sus planes de estudio, las universidades mexicanas deben formar profesionales que sean sensibles a los desafíos

éticos y de responsabilidad social que surgen en el contexto de la 4RI y la economía de los datos (Hernández-Fuentes y Ortiz-López, 2020, p. 81).

Es importante que las universidades se adapten a las demandas del mercado laboral y fomenten la innovación y la investigación en el ámbito tecnológico, al mismo tiempo que abordan los retos éticos y de privacidad que surgen en este contexto.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en coordinación con el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California (ITAIPBC), han llevado a cabo diversas acciones en materia de transparencia y protección de datos personales en la entidad. En un informe conjunto de ambas instituciones, se destacan algunas de las acciones realizadas en Baja California, entre las que se encuentran la capacitación y asesoría a los sujetos obligados en materia de transparencia y protección de datos personales, la implementación de programas de capacitación y actualización para el personal del ITAIPBC, y la realización de campañas de difusión y sensibilización para fomentar la cultura de la transparencia y protección de datos personales en la sociedad.

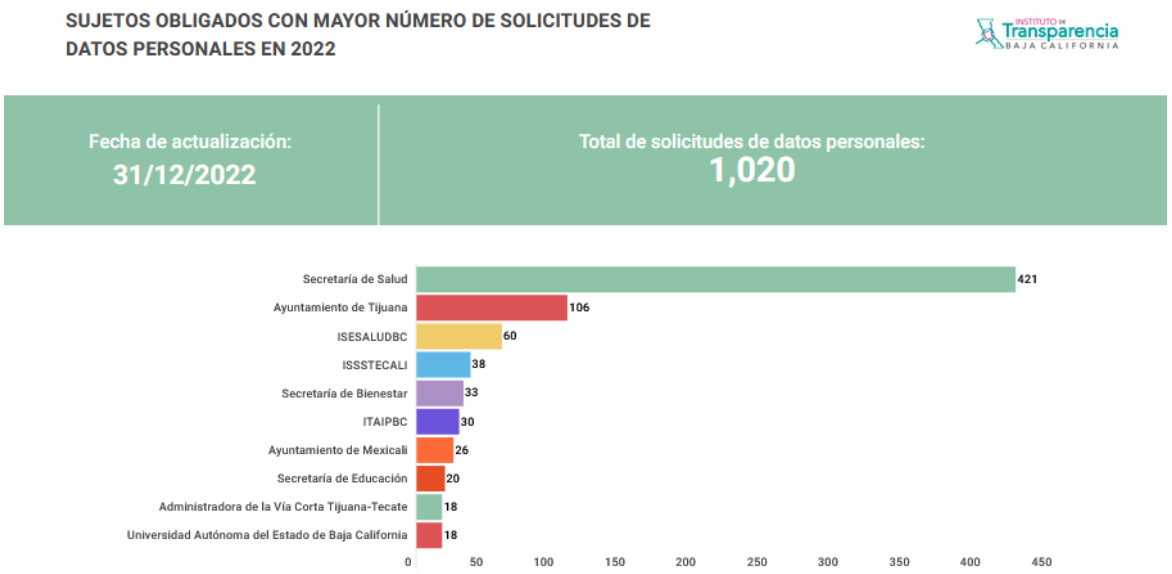
Además, se destaca que el ITAIPBC ha fortalecido su plataforma tecnológica para mejorar los procesos de atención a los ciudadanos y la gestión de solicitudes de información y protección de datos personales. Según el informe del INAI y el ITAIPBC, estas acciones han permitido mejorar la transparencia y la protección de datos personales en la entidad, así como promover una mayor cultura de la transparencia y la protección de datos en la sociedad.

El Estado de Baja California ha llevado a cabo iniciativas para promover la transparencia y el acceso a la información a través de la creación de la Red Estatal de Datos Abiertos (REDA), en colaboración con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California (ITAIPBC). De hecho, REDA se ha implementado en Baja California, convirtiéndose en el segundo estado del país en hacerlo. Según De Prensa UV (2022), el Estado de Veracruz fue el primero en unirse a la Iniciativa de Contrataciones Abiertas en México

El Estado de Baja California ha implementado la Red Estatal de Datos Abiertos (REDA), una iniciativa de transparencia y datos abiertos promovida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California (ITAIPBC) (ItaipBC, 2022). La REDA tiene como objetivo fomentar la adopción del Estándar de Datos de Contrataciones Abiertas (EDCA) y del Estándar de Datos de Contrataciones Abiertas para Infraestructura (EDCAPI), para generar, administrar y divulgar datos y documentos sobre los proyectos de infraestructura y contrataciones con recursos públicos.

Además, el Gobierno del Estado, el Ayuntamiento de Tijuana y Ayuntamiento de Tecate han participado en el "Reto de Infraestructura Abierta 2022" convocado por el INAI, como parte de los esfuerzos para garantizar los derechos de acceso, rectificación, cancelación y oposición (ARCO) (de Prensa UV, 2022). Aunque las estadísticas sobre solicitudes de acceso a datos personales en posesión de particulares por parte de sujetos obligados están en proceso, la población puede solicitar información a las instituciones gubernamentales que se consideran sujetos obligados (ItaipBC, 2022).

Imagen 1. Solicitudes de datos personales en el 2022 en ITAIPBC.



Fuente: Instituto de Transparencia de Baja California, https://www.itaipbc.org.mx/itaipBC-2019/informacion-estadistica/

Estos organismos en el Estado están respondiendo a la creciente necesidad de la protección a los datos personales en el ecosistema de la 4RI y la economía de los datos. El Estado de Baja California es uno de los más avanzados en materia de transparencia, Aunque las estadísticas sobre solicitudes de acceso a los datos personales en posesión de particulares a los sujetos obligados aún se encuentran en progreso, se espera que con la difusión efectiva de los derechos ARCO, la ciudadanía pueda facultarse y empoderarse en la toma de decisiones respecto al manejo de sus datos (ItaipBC, 2022).

En el Estado de Baja California, las universidades están tomando medidas para adaptarse a la 4RI y la economía de los datos y preparar a sus estudiantes para el futuro. Por lo tanto, surge la pregunta sobre cómo estas universidades están abordando estos temas en su oferta educativa.

En Baja California, algunas universidades están implementando programas educativos que incorporan la 4RI y la economía de los datos. Por ejemplo, la Universidad Autónoma de Baja California (UABC) ofrece la licenciatura en Ciencia de Datos, que busca formar profesionales capaces de analizar grandes conjuntos de datos para la toma de decisiones. Según la UABC, los graduados estarán en capacidad de contribuir a la transformación digital de diferentes sectores productivos y de servicios, públicos y privados, al utilizar técnicas avanzadas de minería de datos, aprendizaje automático, IA y visualización de datos (UABC, 2022).

Otra universidad en Baja California que está abordando la 4RI y la economía de los datos es el Instituto Tecnológico de Tijuana (ITT). El ITT ofrece la maestría en Ingeniería en Sistemas de Manufactura, que incluye cursos sobre Industria 4.0, internet de las Cosas, big data y analítica de datos, entre otros temas relacionados. Según el ITT, la maestría tiene como objetivo formar especialistas capaces de diseñar, desarrollar e implementar sistemas de manufactura avanzados y sistemas de gestión empresarial basados en tecnologías de la información (ITT, 2022).

3.1. Entorno de la economía digital

La economía digital y la tecnología están transformando la forma en que las empresas, los gobiernos y los individuos interactúan entre sí. Esto ha llevado a un aumento en la cantidad

de datos personales que se generan, almacenados y compartidos, lo que ha aumentado las preocupaciones en torno a la privacidad y la seguridad de estos datos. La protección de los datos personales y la privacidad se han convertido en temas fundamentales en la era digital y han llevado a la necesidad de establecer políticas públicas claras para abordar estos desafíos (Rabelo, 2018).

El entorno de la economía digital se caracteriza por el uso generalizado de tecnologías digitales e internet para facilitar las transacciones e interacciones económicas. Según la Unión Europea, la economía digital se define como la economía basada en la conectividad digital, que abarca todas las actividades económicas que utilizan tecnologías digitales como internet, la IA, el big data y la nube (Comisión Europea, 2021).

En la economía digital, se utilizan una variedad de herramientas y tecnologías digitales para facilitar las transacciones y las interacciones económicas. Esto incluye el uso de dispositivos móviles, plataformas de redes sociales, computación en la nube, análisis de big data e IA (IA), entre otros (UNCTAD, 2019).

Clive Humby hizo la declaración "Los datos son el nuevo petróleo" en una entrevista de 2006 con el periódico The Guardian[15]. En la entrevista, Humby, cofundador de la firma de análisis de datos dunnhumby, habló sobre la creciente importancia de los datos en la sociedad moderna y cómo se están convirtiendo en un recurso valioso para las empresas y los gobiernos. Sin embargo, la cita "Los datos y la información son el oro del siglo XXI" también es un sentimiento similar y se ha atribuido a varias fuentes, incluida Ginni Rometty, ex directora ejecutiva de IBM y el fundador del fondo de capital riesgo *Sinovation Ventures*, Kai Fu Lee[16]. Es posible que esta cita haya sido utilizada por varias personas y es difícil atribuirle a una sola persona. Lo que sí es evidente y claro es que el augurio, ahora una predicción que se está cumpliendo con los medios de producción tecnológicos de la 4RI, impulsando el desarrollo de estos modelos económicos y nichos de mercado tan vastos como el metaverso.

---

[15] Arthur, C. (2013, August 23). Tech giants may be huge, but nothing matches big data. The Guardian; The Guardian. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

[16] Kai-Fu Lee, fundador del fondo de capital riesgo Sinovation Ventures, es tan popular en China como lo es Elon Musk en Occidente. Con 50 millones de seguidores en la red social Weibo (el Twitter chino), Wired no duda en definirlo como un auténtica estrella de rock de la escena tecnológica china. BBVA. (2018, April 17). Kai- Fu Lee, el "rockstar" chino de la IA. BBVA NOTICIAS. https://www.bbva.com/es/kai-fu-lee-rockstar-chino-inteligencia-artificial/

La comparación de los datos con el petróleo ha sido muy popular en la era digital, pero críticos como John Naughton, escritor y académico británico sobre tecnología, argumentan que esta metáfora es defectuosa y engañosa. En su artículo "Los datos no son el nuevo petróleo, es el nuevo plutonio" (Naughton, 2021), publicado en The Guardian[17] sugiere que los datos se parecen más al plutonio debido al daño potencial que pueden causar si caen en las manos equivocadas. Esta idea es compartida por otros críticos de la metáfora "los datos son el nuevo petróleo", quienes argumentan que simplifica demasiado la naturaleza compleja de los datos y sus implicaciones para la sociedad. En palabras de Naughton, la metáfora que enmarca los datos como petróleo tiene un poder de manipulación similar al que señala Matt Locke. La metáfora ha llevado a la despersonalización de los datos personales, lo que representa un riesgo para la privacidad y la seguridad de las personas. En este sentido, es importante encontrar una mejor metáfora para los datos que permita comprender su complejidad y su importancia en las vidas humanas (Locke, 2021).

Estas metáforas exponen a los datos públicos como majestuosos recursos, sin explotar y pasivos, como lagos de objetos que únicamente tienen valor al extraerse y procesarse. Pero esto elimina completamente la entidad individual que creó esos objetos en primera instancia. (Locke, 2021). Si analizamos un poco la analogía del petróleo, sigue Locke, (2021), está formado por millones de años de transformación química de algas y pequeños animales marinos, años de compresión en las capas de la corteza terrestre. Entonces los datos no tienen que ver en ese sentido, los datos se crean en tiempo real, en la medida que se está activo haciendo clic y navegando en internet. Definitivamente la metáfora podría funcionar en un sentido económico, pero no describe qué son los datos como material. No es el petróleo, es la gente (Locke, 2021).

Otros críticos han sugerido metáforas alternativas, como los datos como un recurso natural que debe administrarse de manera sostenible, o los datos como una forma de moneda que requiere una regulación y supervisión cuidadosas. Como ilación al colectivo imaginario de explotar los datos personales tal si fuera el oro negro que es el petróleo, la ciberdelincuencia

[17] Naughton, J. (2021, May 29). *Data isn't oil, whatever tech commentators tell you: it's people's lives | John Naughton*. The Guardian. https://www.theguardian.com/commentisfree/2021/may/29/data-oil-metaphor-tech-companies-surveillance-capitalism

se manifiesta y agrega un factor más al ya complejo fenomeno multifactorial que es el ecosistema digital.

Las grandes cantidades de datos que se generan cada segundo y las plantas de energía resilientes utilizadas por los bancos, las corporaciones multinacionales e incluso las plataformas de redes sociales son los principales objetivos de los ataques en los últimos años. Con la creciente demanda de datos personales para completar diversas transacciones en la nueva normalidad, constantemente surgen métodos de ataque nuevos y cada vez más sofisticados (Fuentes, 2023)

En este contexto, es pertinente explorar una variedad de perspectivas en torno a la economía digital, incluyendo metáforas alternativas como los datos como un recurso natural que debe administrarse de manera sostenible, o los datos como una forma de moneda que requiere una regulación y supervisión cuidadosas. Al hacerlo, se espera proporcionar una visión más completa de la complejidad de los datos en la economía digital y sus implicaciones para la sociedad.

La economía digital se refiere a la actividad económica que surge de miles de millones de conexiones en línea entre personas, empresas, dispositivos y datos. Abarca una amplia gama de industrias, como el comercio electrónico, los medios digitales, el desarrollo de software y la publicidad en línea, entre otras (Tapscott & Osorio, 1997).

Según Don Tapscott las tecnologías digitales están transformando la forma en que hacemos negocios, el auge de las tecnologías digitales, como internet, los dispositivos móviles y las redes sociales, está cambiando fundamentalmente la forma en que operan las empresas. El autor argumenta que las empresas que no logran adaptarse a esta nueva realidad corren el riesgo de quedarse atrás. De la misma forma, sostiene que la economía digital está creando nuevas oportunidades, está creando nuevos modelos de negocio, nuevas industrias y nuevas formas de crear valor. Argumenta que las empresas que aprovechen estas oportunidades podrán prosperar en el nuevo panorama digital.

La tecnología Blockchain, por otra parte, cambia las reglas del juego, el autor cree que tiene el potencial de transformar la forma en que hacemos negocios. Argumenta que blockchain

puede permitir transacciones seguras y descentralizadas sin la necesidad de intermediarios, lo que podría conducir a sistemas más eficientes, rentables y confiables.

La confianza digital es esencial, la confianza es el fundamento en la economía digital y que la tecnología blockchain puede ayudar a establecer la confianza en un sistema descentralizado.

La economía digital a menudo se asocia con las siguientes características:

Alcance global: internet permite a las empresas conectarse con clientes y socios en todo el mundo, lo que permite el comercio y la competencia globales. Según la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la globalización digital ha aumentado el comercio internacional de bienes y servicios, lo que ha llevado a un aumento en la productividad y el crecimiento económico (OCDE, 2019).

Rápida innovación: las tecnologías digitales están en constante evolución, lo que lleva a la rápida creación de nuevos productos y servicios. Según el Informe Mundial sobre el Comercio 2020 de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), la economía digital ha acelerado la innovación y la creación de nuevos modelos de negocios (UNCTAD, 2020).

Toma de decisiones basada en datos: la abundancia de datos generados por las interacciones digitales permite a las empresas tomar decisiones más informadas y adaptar sus productos y servicios a las necesidades de los clientes. Según un informe de McKinsey Global Institute, las empresas que utilizan análisis de big data para tomar decisiones tienen un 5-6% de ventaja en productividad y rentabilidad en comparación con sus competidores (McKinsey, 2019).

Efectos de red: el valor de las plataformas digitales a menudo aumenta a medida que más usuarios se unen y contribuyen a la plataforma, creando poderosos efectos de red. Según un informe del Foro Económico Mundial, los efectos de red pueden llevar a la creación de monopolios naturales, lo que puede dificultar la entrada de nuevos competidores en el mercado (Foro Económico Mundial, 2019).

Potencial disruptivo: la economía digital tiene el potencial de alterar las industrias y los modelos comerciales tradicionales, creando nuevas oportunidades y desafíos tanto para las

empresas como para los gobiernos. Según la OCDE, la economía digital ha cambiado la forma en que operan las empresas y ha creado nuevos desafíos en términos de competencia, privacidad y seguridad (OCDE, 2019).

Hoy en día, la economía digital no se limita a un sector de modelo económico, hoy en día las actividades convencionales como el pago de impuestos, recibos de servicios públicos, citas para trámites gubernamentales, e infinidad de actividades se hace de manera digital, nuestra parte digital ya no se limita únicamente a la huella digital del individuo

3.2. Entorno UABC, Facultad FEyRI

Cada vez más se observa mayor conciencia y educación en el ámbito de los derechos digitales en los estudiantes, muchas escuelas están tomando medidas para educar a los estudiantes sobre sus derechos y responsabilidades digitales, incluidos temas como la privacidad en línea, el ciberacoso y la propiedad intelectual (ISTE, 2017).

Las escuelas están implementando medidas de protección de datos más estrictas para garantizar que la información personal de los estudiantes se mantenga segura y privada (NCES, 2018), El Centro Nacional de Estadísticas Educativas (National Center for Education Statistics [en adelante NCES], 2018) describe la responsabilidad de las escuelas en la protección de los datos de los estudiantes y aborda aspectos a considerar como la necesidad de que las escuelas cumplan con las leyes federales y estatales: el NCES sugiere que las escuelas deben cumplir con las leyes federales y estatales relacionadas con la privacidad de los datos de los estudiantes, como la Ley de Privacidad y Derechos Educativos de la Familia (FERPA)[18].

Algunas recomendaciones del National Center for Education Statistics (NCES) en relación a la protección de los datos de los estudiantes en las escuelas, se mencionan a continuación.

La importancia de obtener el consentimiento de los padres: Ya que el NCES recomienda que las escuelas obtengan el consentimiento de los padres antes de recopilar, usar o compartir

[18] La Ley de Privacidad y Derechos Educativos de la Familia (FERPA) es una ley federal en los Estados Unidos. Fue aprobada por el Congreso en 1974 y rige la privacidad de los registros educativos de los estudiantes.

datos de los estudiantes. La necesidad de que las escuelas tengan políticas y procedimientos claros, es este sentido el NCES sugiere que las escuelas deben tener políticas y procedimientos claros para recopilar, usar y compartir datos de los estudiantes y comunicar estas políticas a los padres, estudiantes y personal.

La importancia de las medidas de seguridad de datos: El NCES recomienda que las escuelas implementen medidas de seguridad de datos, como el cifrado y la protección con contraseña, para proteger los datos de los estudiantes del acceso no autorizado. Es trascendental que se sugiera el rol y las responsabilidades, por ejemplo el NCES sugiere que las escuelas deben brindar capacitación al personal y a los educadores sobre privacidad y seguridad de datos para garantizar que comprendan sus responsabilidades y sigan las mejores prácticas.

La necesidad de que las escuelas brinden capacitación al personal y a los educadores es un importante requerimiento. El informe de NCES enfatiza la importancia de proteger los datos de los estudiantes y describe las responsabilidades clave de las escuelas al hacerlo. Sugiere que las escuelas deben cumplir con las leyes, obtener el consentimiento de los padres, tener políticas y procedimientos claros, implementar medidas de seguridad de datos y brindar capacitación al personal y a los educadores para proteger la privacidad de los datos de los estudiantes.

Políticas de uso aceptable: Muchas escuelas han implementado políticas de uso aceptable que describen las reglas y pautas para usar la tecnología y los recursos escolares, lo que ayuda a proteger tanto a los estudiantes como a la escuela, según el Departamento de Educación de los Estados Unidos (US Department of Education, 2019), proteger la privacidad de los estudiantes es una prioridad máxima. El departamento de educación de los estados unidos recomienda que las escuelas solo recopilen y utilicen los datos de los estudiantes con fines educativos legítimos y no los compartan con terceros sin el consentimiento de los padres o de los estudiantes en el caso de las universidades. También que las escuelas protejan los datos de los estudiantes a través de prácticas seguras de administración de datos: el departamento sugiere que las escuelas deben salvaguardar los datos de los estudiantes mediante el uso de prácticas seguras de administración de datos, como el cifrado, la protección con contraseña y la limitación del acceso al personal autorizado (US Department of Education, 2019).

El Departamento de Educación de los Estados Unidos (US Department of Education, 2019) adicionalmente propone proporcionar a los padres acceso a los registros educativos de sus hijos: el departamento recomienda que las escuelas proporcionen a los padres acceso a los registros educativos de sus hijos y les permitan corregir cualquier inexactitud en los datos. Así como desarrollar e implementar planes de respuesta a la filtración de datos: el departamento sugiere que las escuelas deben desarrollar e implementar planes de respuesta a la filtración de datos para mitigar el impacto de cualquier posible filtración de datos. El educar a los estudiantes, los padres y el personal sobre la privacidad de los datos es crucial, el departamento recomienda que las escuelas eduquen a los estudiantes, los padres y el personal sobre la privacidad y la seguridad de los datos para aumentar la conciencia y la comprensión de estos problemas.

Algo que sugiere el Departamento de Educación es que proteger la privacidad de los estudiantes es crucial para garantizar que la información personal de los estudiantes se mantenga segura y protegida, y que las escuelas deben tomar medidas proactivas para proteger los datos de los estudiantes y educar a las partes interesadas sobre la privacidad y la seguridad de los datos (US Department of Education, 2019).

Esfuerzos de colaboración: Las escuelas están trabajando con padres, estudiantes y otras partes interesadas para garantizar que todos entiendan la importancia de los derechos digitales y cómo protegerlos. La UNESCO (2015) sugiere que se debe repensar la educación para crear un bien común global.

El informe de la UNESCO (2015) "Repensar la educación: ¿hacia un bien común mundial?" sugiere varios puntos clave sobre la necesidad de repensar la educación para crear un bien común global. como la necesidad de que la educación sea un derecho humano fundamental: El informe sostiene que la educación es un derecho humano fundamental y que toda persona debe tener acceso a una educación de calidad.

La importancia de la educación para el desarrollo sostenible: El informe destaca el papel de la educación en el logro de los objetivos de desarrollo sostenible y la promoción de la sostenibilidad ambiental. La necesidad de que la educación promueva la ciudadanía global: El informe sugiere que la educación debe promover la ciudadanía global animando a los

estudiantes a involucrarse en temas globales y desarrollar un sentido de responsabilidad hacia el mundo.

La importancia de la educación en la promoción de la paz y la no violencia: El informe sostiene que la educación juega un papel crucial en la promoción de la paz y la no violencia al fomentar la comprensión, la tolerancia y el respeto por la diversidad.

Finalmente, el papel de la tecnología en la transformación de la educación: El informe destaca el potencial de la tecnología para transformar la educación aumentando el acceso, mejorando la calidad y promoviendo la innovación. El informe de la UNESCO sugiere que la educación debe re-pensarse y transformarse para abordar los desafíos globales del siglo XXI y promover un mundo más justo, equitativo y sostenible.

Por lo que respecta a México, la implementación de la Estrategia Digital para la Educación en México (Estrategia Digital Nacional para la Educación), busca promover el uso de la tecnología en la educación al tiempo que protege la privacidad y seguridad de los datos de los estudiantes. (Secretaría de Educación Pública [en adelante SEP], 2020).

La creación del Programa de Cultura Ciudadana Digital (Programa de Cultura Ciudadana Digital) por parte de la Estrategia Digital Nacional (Estrategia Digital Nacional) para promover el comportamiento digital responsable entre estudiantes y docentes. (Presidencia de la República, 2020).

El gobierno mexicano ha llevado a cabo varias acciones para fortalecer la protección de datos personales en el entorno digital y promover el uso de la tecnología en la educación. En 2020, se modificó la Ley Federal de Protección de Datos Personales en Posesión de Particulares para incluir una mayor protección de los datos personales, incluidos los datos de los estudiantes (Cámara de Diputados del H. Congreso de la Unión, 2020). Además, en 2019 se estableció el Consejo Nacional de Estrategia Digital con el objetivo de promover el uso de la tecnología en diversos sectores, incluida la educación, y garantizar la protección de los derechos digitales (Diario Oficial de la Federación, 2019). Estas acciones son un paso importante para garantizar la seguridad y privacidad de los datos de los estudiantes en el entorno digital y fomentar la implementación de tecnologías digitales en la educación.

Estos avances reflejan un reconocimiento creciente de la importancia de los derechos digitales y la necesidad de protegerlos en el ámbito escolar en México.

Si bien las universidades han creado instancias especializadas enfocadas en la atención y difusión de la privacidad y protección de datos personales para el ámbito académico, como resultado de la revisión de literatura en esta investigación, se observa que es recomendable realizar ajustes a aspectos estructurales, administrativos y sobre todo, de construcción de capacidades y difusión. En la primera parte de nuestro análisis, se identifican los agentes más relevantes del Ecosistema de Protección de Datos de la Universidad Autónoma de Baja California (UABC). La Figura 3 muestra una versión simplificada del Ecosistema de Protección de Datos de la UABC. Los principales protagonistas son las personas (estudiantes, profesores y administradores) y organismos implicados en la Protección y gestión de datos en el ámbito universitario.

Con esto en mente, se presenta un marco exploratorio que considerara dos pilares principales: desarrollo de capacidades y acción social. La idea es recomendar el despliegue de programas integrales de desarrollo de capacidades en materia de protección de datos en relación con el uso de herramientas, recursos y acceso a la información educativos digitales en los esfuerzos de aprendizaje y adquisición de conocimientos para los actores universitarios y, muy significativamente, para extender estos esfuerzos gradualmente al público.

Considerando la importancia de la protección de datos y privacidad en la sociedad actual, nuestro marco incorpora acciones para abordar cuestiones de gobernanza de internet, derechos humanos, ética y cambio tecnológico. En este sentido, los conocimientos adquiridos en torno al desarrollo de una cultura de privacidad y protección de datos serán un logro significativo en la transformación digital de la Universidad Autónoma de Baja California (UABC).

La Universidad Autónoma de Baja California (UABC) ha desarrollado iniciativas y programas importantes para fomentar el conocimiento y la aplicación de la protección de datos, la privacidad y temas relacionados, dirigidos tanto a estudiantes de pregrado como posgrado. Entre ellas se encuentra la Agencia de Transparencia y Acceso a la Información Pública (UTAIP), cuyo objetivo es fomentar la cultura de la información y el tratamiento de datos. En este sentido, la UTAIP ha emitido su aviso de privacidad general en distintas

categorías y secciones, incluyendo avisos de privacidad para partes interesadas internas y externas, y ha establecido procedimientos para el acceso o rectificación de datos personales en relación con la aplicación de los derechos ARCO (Transparencia UABC, 2022). La implementación de estas acciones en la UABC promueve la cultura de la privacidad y protección de datos en la institución, y representa un avance significativo en la transformación digital de la universidad.

Figura 3. Ecosistema de Protección de Datos para la UABC.

Fuente : Elaboración propia.

La tarea de enseñar a leer y escribir en la sociedad digital actual implica enseñar el uso de los medios digitales de información y comunicación, así como el desarrollo personal y colectivo en una cultura donde las interacciones personales y virtuales se entremezclan. Según Capurro (2000), para propiciar una cultura digital sólida en Latinoamérica es necesario que los latinoamericanos la creen y difundan por sí mismos, teniendo en cuenta los derechos digitales que ya se han legislado sobre el uso de datos personales, su privacidad y protección. En este sentido, la difusión efectiva del conocimiento sobre estos temas es indispensable.

La propuesta de Capurro (2000) para el desarrollo de una cultura digital sólida se enfoca en el fomento de iniciativas de base que surjan paralelamente a una política estatal que desarrolle servicios digitales en sus propias instituciones. Él sugiere que las bibliotecas públicas son un recurso existente adecuado para llevar a cabo este enfoque. Aunque la propuesta de Capurro

fue sugerida en un marco cultural específico, en Latinoamérica, incluyendo Colombia hace 23 años, sigue siendo una propuesta acertada. En México, aún no ha sido abordada como una iniciativa de educación pública o en la agenda política.

Una política de información liberal no implica fomentar una economía que perjudique aún más a los marginados, sino todo lo contrario: debe respaldar los proyectos destinados a fomentar la iniciativa y la creatividad de aquellos que, por razones de aislamiento geográfico, económico, técnico o de infraestructura, se han quedado rezagados en el proceso educativo (Capurro, 2000).

La propuesta de utilizar las bibliotecas públicas como recurso para la educación digital es sin duda interesante. Sin embargo, no se puede pasar por alto el potencial de los docentes como capital humano capacitado para propagar el conocimiento digital. Además de enseñar tecnología, los docentes pueden utilizarla como una herramienta pedagógica para fomentar el aprendizaje de los estudiantes.

Según Competencias digitales México (2022), el proceso de enseñanza y aprendizaje requiere que se empodere a los estudiantes, mientras que los docentes deben estar capacitados para hacer frente a las exigencias de la era digital. El instrumento de autoevaluación de competencias digitales consta de seis áreas de evaluación, y una de ellas se centra en el empoderamiento de los estudiantes. Esta área se divide en tres subtemas: accesibilidad e inclusión, diferenciación y personalización, y participación activa de los estudiantes (Competencias digitales México, 2022).

El primer subtema señala la necesidad de garantizar el acceso a actividades y recursos de aprendizaje para todos los estudiantes, incluyendo aquellos con necesidades especiales. Además, se sugiere considerar y responder a las expectativas, habilidades y limitaciones de los estudiantes en el uso de herramientas digitales.

El segundo subtema destaca el uso de herramientas digitales para cubrir las necesidades de aprendizaje diversas de los estudiantes y ofrecer opciones para progresar al ritmo individual hacia el aprendizaje.

El tercer subtema promueve la participación activa y creativa de los estudiantes en el contenido y el uso de las tecnologías digitales para fomentar sus habilidades y expresión creativa. El objetivo de la encuesta es identificar las competencias digitales que los docentes necesitan para enfrentar los desafíos actuales.

La evaluación de competencias digitales en el proceso de enseñanza y aprendizaje se divide en seis áreas, según Competencias Digitales México (2022). La última área es "Facilitar la competencia digital de los estudiantes" y se compone de cinco puntos de evaluación que buscan evaluar la capacidad del docente para fomentar y desarrollar las habilidades digitales de los estudiantes.

En la primera área, "Información y alfabetización mediática", se espera que el docente pueda enseñar a los estudiantes a encontrar, organizar, procesar, analizar e interpretar información en entornos digitales, así como a evaluar críticamente la credibilidad y confiabilidad de la información y sus fuentes.

La segunda área, "Comunicación y colaboración digital", busca que el docente enseñe a los estudiantes a usar herramientas digitales de manera efectiva y responsable para la comunicación, la colaboración y el compromiso cívico.

En la tercera área, "Creación de contenidos digitales", se espera que el docente pueda enseñar a los estudiantes a expresarse a través de medios digitales y crear contenidos digitales en diferentes formatos, aplicando los derechos de autor y las licencias al contenido digital. En la cuarta área, "Bienestar", se busca que el docente tome medidas para garantizar el bienestar físico, psicológico y social de los estudiantes al utilizar las tecnologías digitales y empoderar a los estudiantes para gestionar el riesgo y utilizar las tecnologías digitales para apoyar su propio bienestar social, psicológico y físico.

Finalmente, en la quinta área, "Solución digital de problemas", se espera que el docente enseñe a los estudiantes a identificar y resolver problemas técnicos o transferir creativamente conocimientos tecnológicos a nuevas situaciones. La evaluación docente en competencias digitales es importante para garantizar una educación integral y actualizada acorde a las exigencias del mundo digital.

La creación de capacidades y como indica Tenorio (2021) la apropiación tecnológica es, por lo tanto, un elemento esencial para la privacidad y la protección de datos en el escenario de convergencia digital global.

La 4RI representa una oportunidad para transformar la educación superior y mejorar la formación de profesionales en áreas relacionadas con la tecnología y los datos (Linares et al., 2018). Las instituciones educativas deben adaptar sus planes de estudio para incluir competencias digitales y habilidades relacionadas con la Ciencia de Datos, la IA, el internet de las Cosas, entre otros, que son fundamentales en la era digital (Orozco, 2019).

En Baja California, se han realizado estudios sobre las competencias en la educación superior ante la 4RI, donde se destaca la importancia de la formación en habilidades digitales y la necesidad de integrar nuevas tecnologías en el proceso de enseñanza-aprendizaje (Silva-Ayala et al., 2019).

En un estudio realizado en la Universidad Autónoma de Baja California, se identificaron las habilidades digitales que deben desarrollarse en los estudiantes universitarios para enfrentar los desafíos de la 4RI, incluyendo la capacidad para procesar y analizar grandes volúmenes de datos, programación, seguridad de la información y trabajo colaborativo en línea (Vega-Rivera & Martínez-Rodríguez, 2020).

En conclusión, la 4RI y la economía de los datos están impactando la educación superior en Baja California, y las universidades están buscando adaptarse a estos cambios. La oferta educativa en esta región incluye programas de formación en Ciencia de Datos, Ingeniería en Sistemas de Manufactura y otros campos relacionados. Estos programas buscan formar profesionales capaces de enfrentar los desafíos de la 4RI y la economía de los datos en un entorno cada vez más digital y globalizado.

Capítulo 4. Marco Metodológico

4.1 Criterios de encuesta y evaluación

Se llevó a cabo un análisis documental, apoyado por una herramienta de exploración tipo encuesta aplicada a la comunidad estudiantil universitaria de la facultad de Economía y Relaciones Internacionales en UABC. El objetivo fue determinar el nivel de conocimiento que tiene esta población sobre la protección, uso, aplicación e implicaciones de los datos.

Se utilizó un método cualitativo y se calculó el tamaño de la muestra total de la población estudiantil mediante la fórmula descrita en el artículo de Aguilar-Barojas (2005) titulado "Fórmulas para el cálculo de la muestra en investigaciones de salud" (p. 335).

$$n = \frac{NZ\text{^}2\ pq}{d\text{^}2\ (N-1) + Z\text{^}2\ pq}$$

La fórmula descrita en el artículo de Aguilar-Barojas (2005) es aplicable en diferentes ámbitos, incluido el campo de la salud. Esta fórmula se utiliza para calcular el tamaño de la muestra necesario en una investigación, considerando aspectos como el tamaño de la población, el nivel de confianza deseado, el margen de error permitido y la distribución esperada de los datos.

En el caso específico de determinar el nivel de conocimiento de una población sobre la protección, uso, aplicación e implicaciones de los datos personales, la fórmula puede ser aplicada. Utilizando los parámetros mencionados a continuación:

N= tamaño de población (estudiantes FEyRI) 1395[19]
z= 1.96 (para un 95% de confianza)
p=q= 0.5
d=0.05 (margen de error)

[19] De acuerdo a Coordinación General de Servicios Estudiantiles y Gestión Escolar la población estudiantil en FEyRI al último periodo observado 2022-02, la cantidad de matriculados es de 1395, http://cgsege.uabc.mx/web/cgsege/estadisticas

Al aplicar la fórmula con estos valores, se obtendrá el tamaño de muestra necesario para obtener resultados representativos y confiables en la investigación sobre el nivel de conocimiento de la población en cuanto a la protección, uso, aplicación e implicaciones de los datos.

Es importante destacar que esta fórmula es ampliamente utilizada en el campo de la investigación y ofrece una aproximación estadística para determinar el tamaño de muestra necesario.

Con una población de 1395 y un margen de error del 5%, se ha calculado que el tamaño teórico de muestra necesario para esta investigación será de 301 estudiantes. Este número se confirmó mediante la aplicación de la fórmula correspondiente y la verificación a través de calculadoras en línea[20]

Para llevar a cabo esta investigación, se utilizó un cuestionario diseñado en *Google Forms*, que consta de 28 preguntas en formato de ítems. El objetivo del cuestionario es evaluar el nivel de conocimiento de los estudiantes de la facultad de FEyRI sobre la protección, uso, aplicación e implicaciones de los datos, y determinar su grado de conciencia en relación a la privacidad y la protección de datos personales.

El cuestionario se organizó por bloques temáticos relacionados con la privacidad y la protección de datos personales, cada uno de ellos compuesto por cuatro preguntas de opción múltiple con las opciones "sí", "no" y "tal vez", y una pregunta de control de respuesta múltiple con las opciones "a", "b" y "c".

Las respuestas de los encuestados se clasifican de la siguiente manera: la opción "sí" será considerada como "informado", la opción "no" como "no informado" y la opción "tal vez" como "poco informado". Para la pregunta de control, sólo se considerará la opción correcta, que se clasificará como "informado".

Con este cuestionario, se obtiene información relevante sobre el nivel de conocimiento de los estudiantes de FEyRI en relación a la privacidad y la protección de datos personales, y así

[20] Calculadora de muestras de Calculadora Datum https://www.datum.com.pe/calculadora

poder establecer una mejor comprensión del ecosistema de protección de datos en la comunidad estudiantil universitaria.

Tabla 1. Rangos de medida de escala.

Rangos de medida de escala.	
Informado	2
Poco informado	1
Nada informado	0

Fuente: Elaboración propia.

Ya que el cuestionario consta de 28 preguntas agrupadas en siete bloques temáticos. Cada bloque estará compuesto por cuatro preguntas de opción múltiple y una pregunta de control de respuesta múltiple.

Las categorías de preguntas se dividen en siete bloques temáticos, que se presentan en la tabla de la siguiente manera:

Tabla 2. Temas que aborda la encuesta.

Categorías de preguntas	Bloque	Preguntas
Ética	B1	1-4
Derechos Humanos Digitales	B2	5-8
Regulación	B3	9-12
Seguridad de Datos	B4	13-16
Protección y Privacidad	B5	17-20
Generación de capacidades	B6	21-24
Adaptación Tecnológica	B7	25-28

Fuente: Elaboración propia.

La tabla proporciona una descripción detallada de las diferentes categorías de preguntas que se incluirán en el cuestionario para evaluar el nivel de conocimiento de los estudiantes de la facultad de Economía y Relaciones Internacionales (FEyRI) sobre la protección, uso, aplicación e implicaciones de los datos.

Cada categoría de preguntas está diseñada para evaluar un aspecto específico del conocimiento de los estudiantes sobre la protección de datos personales y la privacidad. Al agrupar las preguntas en bloques temáticos, se busca obtener una visión global y completa del nivel de conocimiento de los estudiantes sobre el tema.

Los bloques temáticos se organizaron de la siguiente manera:

Ética: Este bloque temático incluye preguntas que buscan medir el nivel de conocimiento de los estudiantes sobre los valores éticos y las normas de conducta en el manejo de datos personales. Las preguntas específicas van del 1 al 4.

Derechos Humanos Digitales: En este bloque temático se incluyen preguntas diseñadas para medir el nivel de conocimiento de los estudiantes sobre los derechos humanos digitales y su relación con la protección de datos personales. Las preguntas específicas van del 5 al 8.

Regulación: Este bloque temático se enfoca en medir el conocimiento de los estudiantes sobre las leyes y regulaciones relacionadas con la protección de datos personales. Las preguntas específicas van del 9 al 12.

Seguridad de Datos: En este bloque temático se incluyen preguntas que buscan medir el nivel de conocimiento de los estudiantes sobre los aspectos técnicos de la seguridad de datos y las herramientas de protección disponibles. Las preguntas específicas van del 13 al 16.

Protección y Privacidad: Este bloque temático incluye preguntas diseñadas para medir el nivel de conocimiento de los estudiantes sobre los conceptos de protección y privacidad de datos personales. Las preguntas específicas van del 17 al 20.

Generación de capacidades: En este bloque temático se incluyen preguntas que buscan medir el nivel de conocimiento de los estudiantes sobre las habilidades y competencias necesarias para proteger y gestionar datos personales. Las preguntas específicas van del 21 al 24.

Adaptación Tecnológica: Este bloque temático se enfoca en medir el nivel de conocimiento de los estudiantes sobre la adaptación tecnológica y su impacto en la protección de datos personales. Las preguntas específicas van del 25 al 28.

Con la información recopilada a través de esta tabla, se realiza un análisis más detallado y preciso de los datos obtenidos en la encuesta, lo que permite obtener resultados más confiables y útiles para la investigación.

En general, el cuestionario tiene el objetivo de evaluar la capacidad de los estudiantes de FEyRI para comprender y aplicar conceptos relacionados con la protección de datos personales, la privacidad y la seguridad en el entorno digital. De esta manera, se busca identificar áreas de mejora en el conocimiento de los estudiantes sobre estos temas y, en consecuencia, proponer estrategias de capacitación y formación que contribuyan a mejorar la conciencia y el conocimiento sobre la importancia de la protección de datos personales.

A continuación se presenta la tabla de operacionalización de variables, la cual tiene como objetivo establecer las variables a medir y definir las categorías para su análisis. En esta parte se ve en “Definición operacional” la explicación de la variable elegida, pero también indica que número de pregunta de acuerdo a su numeración extraída de las 28 preguntas de la encuesta, se seleccionaron 12 preguntas, después de esta tabla la numeración de las 12 preguntas extraídas, será del 1 al 12, se consideró pertinente hacer esta mención para mayor claridad en la presentación de los datos.

Tabla 3. Operacionalización de las variables

	Operalización de variables				
	Nombre de la variable	Definición operacional	Pregunta	Escala de medición	Categoría o valores
Bloque 1. Ética	Conocimiento sobre ética en aplicaciones digitales	La comprensión del usuario sobre si las aplicaciones digitales informan de manera ética a los usuarios sobre la forma en que recuperan su inversión o generan beneficios a partir de su uso. específicamente en relación con las opciones de respuesta proporcionadas en la pregunta #1	Puede ser que las aplicaciones digitales son un beneficio para tu vida diaria, ¿conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?	Sí = 2 Tal vez = 1 No = 0	"Si" (sería informado): El encuestado indica que conoce la forma en que las aplicaciones digitales recuperan su inversión o generan beneficios. "Tal vez" (poco informado): El encuestado indica que tiene un conocimiento limitado o incierto sobre cómo las aplicaciones digitales obtienen beneficios económicos. "No" (no informado): El encuestado indica que no tiene conocimiento sobre cómo las aplicaciones digitales obtienen beneficios económicos.

Bloque 2. Derechos Humanos Digitales	Derechos humanos digitales	Se refiere a la percepción del estudiante acerca de si los derechos digitales sobre los datos personales son parte de los derechos humanos, en relación con las opciones de respuesta proporcionadas en la pregunta #5	¿Los derechos digitales sobre tus datos personales son parte de los derechos humanos?	Sí = 2 Tal vez = 1 No = 0	Si: La respuesta "si" indica que el estudiante considera que los derechos digitales sobre los datos personales son parte de los derechos humanos. Tal vez: La respuesta "tal vez" indica que el estudiante no está seguro o tiene dudas acerca de si los derechos digitales sobre los datos personales son parte de los derechos humanos. No: La respuesta "no" indica que el estudiante no considera que los derechos digitales sobre los datos personales son parte de los derechos humanos.
Bloque 2. Derechos Humanos Digitales	Nomenclatura de los derechos ARCO	Se refiere a la capacidad del estudiante para identificar la nomenclatura correcta de los derechos ARCO, en relación con las opciones de respuesta proporcionadas en la pregunta #8	¿Cuál de estas opciones es la correcta nomenclatura de los derechos ARCO? a) Acción, Rectificación, Corrección, y Objeción. b) Acceso, Rectificación, Cancelación y Oposición. c) Acceso, Registro, Contraposición, y Obstaculización.	a) Acción, Rectificación, Corrección, y Objeción = 0 b) Acceso, Rectificación, Cancelación y Oposición = 2 c) Acceso, Registro, Contraposición, y Obstaculización =0	A: La respuesta "a" indica que el estudiante identifica una nomenclatura incorrecta de los derechos ARCO. B: La respuesta "b" indica que el estudiante identifica la nomenclatura correcta de los derechos ARCO. C: La respuesta "c" indica que el estudiante no identifica la nomenclatura correcta de los derechos ARCO.
Bloque 3. Regulación	Conocimiento sobre datos menores de edad	Se refiere a la capacidad del estudiante para responder correctamente si los menores de edad son titulares de sus datos personales, en relación con las opciones de respuesta proporcionadas en la pregunta #11	Según tu conocimiento respecto a los datos personales ¿Los menores de edad, son titulares de sus datos personales?	Sí = 2 Tal vez = 1 No = 0	Si: La respuesta "si" indica que el estudiante sabe que los menores de edad son titulares de sus datos personales. Tal vez: La respuesta "tal vez" indica que el estudiante no está seguro o tiene un conocimiento limitado sobre si los menores de edad son titulares de sus datos personales. No: La respuesta "no" indica que el estudiante cree que los menores de edad no son titulares de sus datos personales.
Bloque 3. Regulación	Conocimiento sobre la ley	Se refiere a la capacidad del estudiante para identificar correctamente la ley que protege la privacidad de los datos personales, en relación con las opciones de respuesta proporcionadas en la pregunta #12	¿Cual de estas es la ley que protege tu privacidad de tus datos personales? a) Ley Federal de Transparencia y Acceso a la Información Pública. b) Ley Federal de Protección de Datos Personales en Posesión de los Particulares. c) Ley General de Protección de Datos Personales en posesión de sujetos obligados.	a) Ley Federal de Transparencia y Acceso a la Información Pública = 0 b) Ley Federal de Protección de Datos Personales en Posesión de los Particulares = 2 c) Ley General de Protección de Datos Personales en posesión de sujetos obligados = 0	A: La respuesta "a" indica que el estudiante no conoce la ley que protege la privacidad de los datos personales. B: La respuesta "b" indica que el estudiante sabe que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es la ley que protege la privacidad de los datos personales. C: La respuesta "c" indica que el estudiante cree que la Ley General de Protección de Datos Personales en posesión de sujetos obligados es la ley que protege la privacidad de los datos personales.

Bloque 4. Seguridad de Datos	Conocimiento del departamento derechos digitales.	Conocimiento que tiene el estudiante acerca de la existencia del departamento de la universidad que brinda asesoría en caso de necesitar ayuda en temas relacionados con sus derechos digitales, con las opciones proporcionadas en la pregunta #14	¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda?	Sí = 2 Tal vez = 1 No = 0	Si: Valor de 2 puntos, indicando que el estudiante conoce el departamento de asesoría en derechos digitales en su la institución académica. Tal vez: Valor de 1 punto, indicando que el estudiante tiene un conocimiento limitado o incierto sobre el departamento de asesoría en derechos digitales. No: Valor de 0 puntos, indicando que el estudiante no tiene conocimiento del departamento de asesoría en derechos digitales.
Bloque 5. Protección y Privacidad	Conocimiento de responsabilidades de instituciones académicas	La capacidad de los estudiantes para conocer y comprender las responsabilidades que tienen las instituciones académicas en cuanto al manejo de los datos personales de los estudiantes, con las opciones proporcionadas en la pregunta #19	¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?	Sí = 2 Tal vez = 1 No = 0	"Si": Indica que el estudiante tiene conocimiento sobre las responsabilidades de las instituciones académicas en cuanto al manejo de los datos personales. "Tal vez": Indica que el estudiante tiene un conocimiento parcial o limitado sobre las responsabilidades de las instituciones académicas en cuanto al manejo de los datos personales. "No": Indica que el estudiante no tiene conocimiento sobre las responsabilidades de las instituciones académicas en cuanto al manejo de los datos personales.
Bloque 5. Protección y Privacidad	Conocimiento sobre privacidad	Capacidad del encuestado para identificar y seleccionar la definición correcta de privacidad entre las opciones dadas, en la pregunta #20	¿Qué es privacidad? a) Referente a los datos personales, trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no. b) Referente a los datos personales, significa la capacidad de una persona para determinar por sí misma cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal. c) Se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información.	a) Referente a los datos personales, trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no = 0 b) Referente a los datos personales, significa la capacidad de una persona para determinar por sí misma cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal = 2 c) Se entiende el conjunto de medidas preventivas y reactivas que permiten	A: La respuesta "a" indica que el estudiante no conoce la definición de privacidad en el contexto de datos personales. B: La respuesta "b" indica que el estudiante indica correctamente que la privacidad en el contexto de datos personales se refiere a la capacidad de una persona para determinar cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal. C: La respuesta "c" indica que el estudiante no conoce la definición de privacidad en el contexto de datos personales.

				resguardar y proteger la información = 0	
Bloque 6. Generación de capacidades	Capacitación sobre derechos digitales	Se refiere a si la persona ha recibido alguna capacitación, curso o información formal sobre sus derechos digitales en su facultad o universidad. Esto entre las opciones dadas en la pregunta #21	¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?	Sí = 2 Tal vez = 1 No = 0	"Si": La persona ha recibido una capacitación o curso informativo sobre sus derechos digitales en su facultad, lo cual indica un mayor conocimiento y conciencia sobre la protección de sus derechos digitales. "Tal vez": La persona puede haber recibido o no una capacitación o curso informativo sobre sus derechos digitales en su facultad, lo cual indica una incertidumbre en cuanto al conocimiento de sus derechos digitales. "No": La persona no ha recibido una capacitación o curso informativo sobre sus derechos digitales en su facultad, lo cual indica una falta de conocimiento y conciencia sobre la protección de sus derechos digitales.
Bloque 6. Generación de capacidades	Capacitación en tecnología	Se refiere a si la persona ha tomado algún curso o capacitación sobre tecnología y/o sus implicaciones. Esto entre las opciones dada en la pregunta #23	¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?	Sí = 2 Tal vez = 1 No = 0	"Sí" (sería informado): La persona ha tomado un curso o capacitación sobre tecnología y/o sus implicaciones. "Tal vez" (poco informado): La persona no está segura o ha tomado cursos o capacitaciones limitadas sobre tecnología y/o sus implicaciones. "No" (no informado): La persona no ha tomado ningún curso o capacitación sobre tecnología y/o sus implicaciones. Esta variable indica el nivel de conocimiento y preparación que la persona tiene en cuanto a la tecnología y sus implicaciones. Las respuestas "Sí" y "Tal vez" indican que la persona ha recibido algún tipo de formación, mientras que la respuesta "No" indica falta de conocimiento formal en esta área.
Bloque 7. Adaptación Tecnológica	Conocimiento de implicaciones del uso no autorizado de datos	Esta variable se refiere al nivel de conocimiento de una persona acerca de las consecuencias que puede tener el uso de sus datos personales sin su consentimiento. Esto dado en las opciones de la pregunta #25	¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?	Sí = 2 Tal vez = 1 No = 0	Si (informado): se refiere a la persona que ha identificado al menos una implicación del uso de sus datos personales sin su consentimiento. Tal vez (poco informado): se refiere a la persona que no está segura o no conoce completamente las implicaciones del uso de sus datos personales sin su consentimiento. No (no informado): se refiere a la persona que no tiene conocimiento o no ha identificado ninguna implicación del uso de sus datos personales sin su consentimiento.

Bloque 7. Adaptación Tecnológica	Identificación de implicaciones del uso no consentido de datos personales	Esta variable se refiere a la capacidad del encuestado para identificar las posibles implicaciones del uso de sus datos personales por parte de terceros sin su consentimiento en situaciones específicas. En este caso, se presentan tres opciones y se pregunta si el encuestado puede identificar alguna implicación para cada una de ellas. Esto dado en las opciones de la pregunta #28	¿Podrías identificar de las siguientes opciones alguna implicación del uso de tus datos personales tomados sin tu consentimiento? a) Teclear tu nombre en el buscador de internet, y que aparezca en una lista de asistencia de alguna clase. b) La publicación de tu matrícula en una carta de aceptación. c) Una foto tuya en la publicación de alguien más.	a) Teclear tu nombre en el buscador de internet, y que aparezca en una lista de asistencia de alguna clase = 2 b) La publicación de tu matrícula en una carta de aceptación = 0 c) Una foto tuya en la publicación de alguien más = 0	Si el encuestado seleccionó la opción a), significa que el estudiante tiene conocimiento y capacidad para identificar al menos una implicación del uso de sus datos personales sin su consentimiento en la situación específica presentada. Si seleccionó la opción b) o c), indica que el estudiante no tiene conocimiento o no puede identificar una implicación en la situación presentada.

Fuente: Elaboración propia.

La tabla presenta una lista de variables relacionadas con la ética, los derechos humanos digitales y la regulación en el contexto de las aplicaciones digitales. Cada variable se define operacionalmente para clarificar lo que se está midiendo y cómo se medirá. Además, se proporciona una pregunta específica y una escala de medición para cada variable, junto con los valores o categorías que se asignan a cada respuesta.

Por ejemplo, en el bloque 1 sobre ética, la variable "Conocimiento sobre ética en aplicaciones digitales" se define como la comprensión del usuario sobre si las aplicaciones digitales informan de manera ética a los usuarios sobre la forma en que recuperan su inversión o generan beneficios a partir de su uso. La pregunta específica es "¿Conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?" y se utiliza una escala de medición de 0 a 2 para asignar valores a las respuestas "Sí", "Tal vez" y "No". Esta pregunta se extrajo de la encuesta con la idea de que los usuarios deben tener una comprensión clara y consciente de cómo las aplicaciones digitales manejan su información y generan ingresos.

Por ejemplo, en un estudio sobre la privacidad en línea de los usuarios de redes sociales, los autores concluyen que "la falta de comprensión de los usuarios de cómo se utilizan sus datos personales puede llevar a la toma de decisiones inapropiadas y potencialmente dañinas" (Madden y Rainie, 2015, p. 10). Además, un estudio sobre la privacidad de los datos en las

aplicaciones móviles encontró que "la falta de transparencia sobre cómo se recopilan, utilizan y comparten los datos personales puede afectar negativamente la confianza de los usuarios en las aplicaciones móviles" (Li et al., 2016, p. 299). Por lo tanto, es importante que los usuarios comprendan cómo se utilizan sus datos personales y cómo las aplicaciones digitales generan ingresos para que puedan tomar decisiones informadas sobre su privacidad y seguridad en línea.

En el bloque 2 sobre derechos humanos digitales, se incluyen variables como "Derechos humanos digitales" y "Nomenclatura de los derechos ARCO". La primera se refiere a la percepción del estudiante sobre si los derechos digitales sobre los datos personales son parte de los derechos humanos, mientras que la segunda se refiere a la capacidad del estudiante para identificar la nomenclatura correcta de los derechos ARCO. La protección de los derechos humanos digitales es un tema cada vez más relevante debido al aumento del uso de tecnologías de la información y la comunicación. La privacidad y la protección de datos personales son elementos clave en el marco de los derechos humanos en el entorno digital (Nations, 2016). Además, el derecho a la privacidad se ha considerado una parte integral de los derechos humanos en la era digital, y se ha reconocido como tal por varias organizaciones internacionales, incluida la Organización de las Naciones Unidas (ONU) (Office of the High Commissioner for Human Rights, 2014).

En este sentido, algunos estudios han explorado la percepción de los estudiantes sobre los derechos humanos digitales. Por ejemplo, en un estudio realizado por Boroumand et al. (2018) se encontró que los estudiantes universitarios consideraban que la privacidad en línea era un derecho humano fundamental. Además, otro estudio realizado por Kang y Stein (2019) concluyó que los estudiantes universitarios tienen una comprensión limitada de los derechos digitales como parte de los derechos humanos, lo que sugiere la necesidad de mejorar la educación en este tema. La percepción del estudiante sobre si los derechos digitales son parte de los derechos humanos es una variable importante en el contexto de la educación en la protección de datos personales y la privacidad en línea. La protección de estos derechos es fundamental para garantizar el respeto y la dignidad de las personas en el entorno digital.

En cuanto a los derechos ARCO, el derecho a la protección de datos personales es un derecho fundamental reconocido por la mayoría de las constituciones y tratados internacionales de derechos humanos. En México, este derecho está regulado por la Ley Federal de Protección

de Datos Personales en Posesión de Particulares (LFPDPPP), que establece los derechos de acceso, rectificación, cancelación y oposición (ARCO) de los titulares de los datos personales. Es importante que los estudiantes comprendan la nomenclatura correcta de estos derechos para poder ejercerlos correctamente y proteger su información personal. Por ejemplo, en un estudio realizado por Ramírez-Alvarez, Rodríguez-Gómez y Vázquez-Cano (2020) se encontró que la mayoría de los usuarios de redes sociales en México no conocen sus derechos ARCO y no saben cómo ejercerlos. Esto demuestra la importancia de educar a los estudiantes sobre estos derechos para que puedan proteger su información personal.

Respecto a el bloque 3 sobre Regulación, la variable "Conocimiento sobre datos menores de edad" , la variable se respalda en la Ley de Protección de Datos Personales de México, la cual establece en su artículo 3, fracción XVIII, que los menores de edad son titulares de sus datos personales y que, por lo tanto, deben ser tratados con la debida protección. Asimismo, la Norma Oficial Mexicana NOM-024-SSA3-2013 establece que los menores de edad tienen derecho a la protección de sus datos personales en el ámbito de la salud. Otra referencia relevante es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece en su artículo 8 que los menores de 16 años deben contar con el consentimiento de sus padres o tutores legales para el tratamiento de sus datos personales en relación a servicios de la sociedad de la información. El RGPD también establece que los estados miembros pueden rebajar la edad mínima requerida para prestar su propio consentimiento, siempre que no sea inferior a los 13 años.

En cuanto a la variable "Conocimiento sobre la ley" perteneciente al bloque 3, el conocimiento sobre la ley es un factor crítico en la protección de la privacidad de los datos personales. La comprensión de las leyes y reglamentos relacionados con la privacidad de los datos personales es esencial para garantizar que los datos personales se manejen de manera responsable y se protejan adecuadamente contra el acceso no autorizado, el uso indebido o la divulgación.

Por ejemplo, en México, la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) es una ley que establece las obligaciones y responsabilidades que deben seguir las organizaciones que recopilan, procesan o almacenan datos personales. Además, esta ley establece los derechos de los titulares de los datos, como el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO).

En la variable "Conocimiento del departamento derechos digitales" se cita a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México, la cual establece en su artículo 37 que los responsables del tratamiento de datos personales deberán contar con mecanismos para que los titulares puedan ejercer sus derechos ARCO y recibir asesoría en relación con la protección de sus datos personales. Además, algunas universidades cuentan con un departamento o área encargada de brindar asesoría en temas relacionados con la privacidad y protección de datos personales, como la UABC, y como lo señala la Universidad de Guadalajara en su Reglamento de Protección de Datos Personales en el Artículo 26, donde se establece que la institución contará con un área responsable de la protección de datos personales y de la atención a solicitudes de acceso, rectificación, cancelación u oposición (ARCO).

La variable de Bloque 5. Protección y Privacidad, "Conocimiento de responsabilidades de instituciones académicas" se consideró ya que en las instituciones académicas es un tema importante que debe ser abordado adecuadamente. Las instituciones académicas tienen la responsabilidad de proteger los datos personales de los estudiantes, asegurando que se manejen de manera responsable y ética. De esta manera, se puede garantizar que los estudiantes no sufran ningún tipo de daño o perjuicio como resultado del mal uso de sus datos personales. Por ejemplo, según la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México, las instituciones académicas están obligadas a cumplir con ciertos requisitos en cuanto a la protección de datos personales de los estudiantes. Estas obligaciones incluyen el obtener el consentimiento de los estudiantes antes de recolectar, utilizar o compartir sus datos personales, y tomar medidas adecuadas para proteger dichos datos.

Asimismo, la Comisión Nacional de los Derechos Humanos (CNDH) de México establece que las instituciones académicas deben garantizar la privacidad y seguridad de los datos personales de los estudiantes, así como asegurarse de que los estudiantes tengan acceso a su información personal y la posibilidad de corregirla o actualizarla en caso de ser necesario. Es fundamental que los estudiantes comprendan la responsabilidad que tienen las instituciones académicas en cuanto al manejo de sus datos personales. Conocer las obligaciones de las instituciones académicas en este ámbito puede ayudar a los estudiantes a tomar decisiones

informadas acerca del manejo de su información personal y a exigir el cumplimiento de sus derechos en caso de que sean violados.

Otra variable del bloque 5, "Conocimiento sobre privacidad" se abordará ya que la privacidad es un concepto fundamental en la protección de los datos personales, y es esencial que los estudiantes comprendan su significado y su importancia en el entorno digital.

Un estudio realizado por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en 2015 encontró que la mayoría de los jóvenes no comprenden completamente el concepto de privacidad en línea y las implicaciones que tienen sus decisiones en línea en cuanto a la protección de sus datos personales (OCDE, 2015). Otro estudio realizado en España en 2020 encontró que el 60% de los jóvenes entre 16 y 24 años cree que sus datos personales no están lo suficientemente protegidos en línea (Centro de Investigaciones Sociológicas, 2020).

Una variable del bloque 6 Generación de capacidades la “Capacitación sobre derechos digitales” se fundamenta en la importancia de la educación y capacitación en materia de derechos digitales para los individuos. Según la UNESCO (2020), "la educación en derechos digitales es fundamental para garantizar que los ciudadanos tengan las habilidades necesarias para ejercer sus derechos humanos en línea" (p. 1). Asimismo, la capacitación en derechos digitales es considerada una herramienta clave para empoderar a los individuos en su capacidad de proteger su privacidad y seguridad en línea (Kernaghan, 2019). En cuanto a la importancia de la capacitación en el ámbito académico, se ha destacado la necesidad de que las instituciones educativas incorporen la educación en derechos digitales en sus planes de estudio (UNESCO, 2020). Esto se debe a que los estudiantes, al igual que los ciudadanos en general, necesitan contar con conocimientos y habilidades para poder hacer frente a los desafíos que plantea el entorno digital actual.

En otra variable más del bloque 6, “Capacitación en tecnología” se consideró relevante ya que la apropiación tecnológica encamina a el empoderamiento de esta, existen estudios que muestran la importancia de la capacitación en tecnología para el desarrollo de habilidades digitales y el manejo adecuado de los datos personales en el entorno digital. Por ejemplo, un estudio de la Unión Internacional de Telecomunicaciones (UIT) señala que la capacitación en tecnología es fundamental para la inclusión digital y el desarrollo de habilidades digitales en

la población en general (UIT, 2017). Otro estudio realizado por la Universidad de California en Los Ángeles (UCLA) encontró que la capacitación en tecnología puede mejorar la seguridad y privacidad de los datos personales en línea (Buckner et al., 2018).

Respecto al bloque 7, y último, "Adaptación Tecnológica", se extrajeron dos variables, la primera "Conocimiento de implicaciones del uso no autorizado de datos" debido a su gran importancia para la sociedad digital Según un estudio realizado por la firma de seguridad informática Kaspersky en 2019, el 64% de los usuarios de internet en todo el mundo están preocupados por la seguridad de sus datos personales. Además, el 46% de los encuestados no confía en que las empresas hagan un uso adecuado de sus datos. Esta falta de confianza puede deberse en gran medida a los casos de uso no autorizado de datos que han sido ampliamente publicitados en los medios de comunicación en los últimos años, lo que ha llevado a un mayor interés y conciencia sobre la privacidad y la seguridad de los datos personales (Kaspersky, 2019).

Finalmente la última variable es "Identificación de implicaciones del uso no consentido de datos personales" representa la capacidad de una persona para identificar las posibles implicaciones del uso de sus datos personales por parte de terceros sin su consentimiento es un aspecto importante en la protección de la privacidad y la seguridad de los datos personales. Un estudio realizado por Vakulenko et al. (2021) encontró que la mayoría de los usuarios de internet no son conscientes de los riesgos asociados con la recolección y el uso no autorizado de datos personales, lo que destaca la importancia de la educación y la conciencia sobre este tema. Pérez-Montoro y Minguillón (2016) señalaron que el conocimiento de los usuarios sobre la protección de datos personales puede influir en su comportamiento en línea y en su disposición a compartir información personal. Esto sugiere que aquellos que son capaces de identificar las implicaciones del uso no consentido de sus datos personales pueden ser más cautelosos y conscientes al compartir su información en línea.

La identificación de las implicaciones del uso no consentido de datos personales es importante por varias razones:

Protección de la privacidad: Al conocer las posibles implicaciones del uso no consentido de los datos personales, las personas pueden tomar medidas para proteger su privacidad y evitar que sus datos sean utilizados indebidamente.

Prevención de fraudes: El uso no consentido de datos personales es comúnmente utilizado por delincuentes para realizar fraudes financieros y otras actividades delictivas. Al identificar las implicaciones de este uso, las personas pueden tomar medidas para protegerse y prevenir ser víctimas de fraudes.

Conciencia de los riesgos: Al tener conocimiento de las posibles implicaciones del uso no consentido de los datos personales, las personas pueden tener una mejor comprensión de los riesgos asociados con el uso de tecnologías y servicios en línea, lo que les permite tomar decisiones informadas y responsables.

Cumplimiento de la ley: En muchos países, el uso no consentido de datos personales es ilegal y puede ser sancionado. Al identificar las implicaciones del uso no consentido de los datos personales, las personas pueden tomar medidas para cumplir con la ley y evitar sanciones.

En resumen, la identificación de las implicaciones del uso no consentido de los datos personales es importante para proteger la privacidad, prevenir fraudes, aumentar la conciencia de los riesgos y cumplir con la ley.

En conclusión, estas doce variables están relacionadas con diferentes aspectos del conocimiento y la comprensión de los derechos digitales, la privacidad y la protección de datos personales en un contexto universitario. Su importancia radica en que permiten evaluar la capacidad de los estudiantes para entender y aplicar estos conceptos en su vida diaria y profesional.

La identificación y comprensión de estos temas son fundamentales para garantizar una sociedad más informada y consciente de sus derechos digitales, así como para fomentar la adopción de prácticas éticas y responsables en el uso de la tecnología. Estas variables son útiles para diseñar y evaluar programas de educación y capacitación en derechos digitales y para medir la eficacia de las políticas y regulaciones en materia de privacidad y protección de datos.

4.2 Características de la muestra

Para llevar a cabo un estudio sobre el conocimiento en la Facultad de Economía y Relaciones Internacionales (FEyRI) sobre la privacidad y protección de datos personales en la comunidad estudiantil incluyendo aspectos éticos y de derechos humanos digitales, se implementó una encuesta a una muestra representativa de la población estudiantil, que abarcó tanto a los estudiantes de licenciatura como a los de posgrado. La encuesta constó de varias preguntas que se centraron en aspectos relevantes relacionados con los derechos digitales, como la nomenclatura de los derechos ARCO, el conocimiento sobre el manejo de datos de menores de edad, la ley, los departamentos de derechos digitales, las responsabilidades de las instituciones académicas, la privacidad, la capacitación sobre derechos digitales, la capacitación en tecnología, y las implicaciones del uso no autorizado de datos personales.

La muestra inicial constó de 301 encuestados, seleccionados con precisión y representatividad para garantizar la validez y la confiabilidad de los resultados. Sin embargo, con el fin de aumentar la precisión de los resultados, se decidió ampliar la muestra en un 11.63% del valor original, lo que se tradujo en la encuesta de un total de 336 estudiantes de la FEyRI. Con esta estrategia, se buscó obtener una visión más amplia y precisa sobre el conocimiento y la percepción de los estudiantes sobre los derechos digitales y su aplicación en el ámbito académico.

A continuación, se detallan los pasos y medios utilizados para seleccionar la muestra y realizar la encuesta:

Selección de la muestra: Se utilizaron varios canales de comunicación para llegar a los estudiantes de la FEyRI. Como primer paso, se proporcionó el cuestionario a la dirección de la facultad para obtener su consentimiento y autorización. Fue un trabajo conjunto con el apoyo de la dirección para la aplicación de la encuesta, autoridades administrativas y docentes tanto de Posgrado como de Licenciatura hicieron posible la aplicación efectiva de la encuesta. Después de una reunión con el subdirector de la facultad para revisar detalles para la aplicación de la encuesta, se difundió la encuesta durante una reunión con los jefes de grupo de la licenciatura y se les envió un correo a estos con los enlaces correspondientes para el ingreso a la encuesta. Asimismo, se envió un correo electrónico por parte de la

subdirección autorizando y permitiendo el ingreso a las aulas para solicitar a los alumnos el llenado de la encuesta en dos ocasiones.

Comunicación inicial: Se utilizaron diferentes medios de comunicación para informar a los estudiantes sobre la encuesta. Se colocó una hoja con el código QR de la encuesta en cada salón de clases y laboratorios de cómputo, con la debida identificación de contacto y propósito de esta. Además, se difundió la encuesta en la página oficial de Facebook de la Facultad de Economía y Relaciones Internacionales (FEyRI). La Coordinación de Posgrado también dio su consentimiento para colocar la hoja con el código QR en las aulas y envió un correo a todos los estudiantes activos de posgrado, tanto de maestría como de doctorado, para solicitar el llenado e informarles del propósito de la encuesta.

Aplicación de la encuesta: Se realizaron dos rondas de aplicación de la encuesta presencial en las aulas. La primera fue una visita breve para la invitación general para que los estudiantes llenaran la encuesta. Posteriormente, se programó una segunda ronda de aplicación a los quince días, con el objetivo de guiar a los estudiantes durante el ingreso y llenado de la encuesta en tiempo real, con el apoyo y consentimiento de los docentes que se encontraron en ese momento.

La implementación de esta estrategia de muestreo y aplicación de la encuesta permitió obtener una muestra representativa de la población estudiantil de la Facultad FEyRI, brindando la oportunidad de recopilar datos relevantes y significativos sobre el conocimiento y la conciencia de los estudiantes en relación con los derechos digitales y la protección de datos personales.

En el marco de esta investigación, es importante destacar que se informó a los estudiantes encuestados sobre el propósito de la encuesta y la relevancia de sus respuestas en el estudio. Se les brindó una explicación concisa y clara sobre el tema en una charla de diez minutos, con el objetivo de contextualizarlos y asegurar su comprensión de la importancia de su participación en el estudio.

Sin embargo, desde el inicio del proyecto se acordó en las asesorías que los estudiantes no serían informados de los resultados de manera individual. Esta decisión fue tomada con el propósito de medir el nivel de conocimiento de los participantes en su estado natural, sin

influencias externas que puedan inhibir o sesgar sus respuestas. Se consideró que proporcionar una calificación individual podría generar desmotivación en los estudiantes y, en algunos casos, desistimiento en el llenado de la encuesta. Además, existía la preocupación de que la divulgación de las respuestas correctas pudiera influir en la propagación de las mismas o incentivar a los participantes a buscar las respuestas en internet, lo cual afectaría la validez de los datos obtenidos.

Cabe mencionar que se tiene previsto publicar esta tesis como repositorio en la sección correspondiente de la página de posgrado. Aunque los alumnos encuestados no serán notificados de manera individual sobre los resultados, se les proporcionó el correo de contacto de la persona a cargo de la encuesta para que puedan hacer consultas o plantear dudas relacionadas con el estudio.

Con esta estrategia, se garantizó la confidencialidad de las respuestas de los estudiantes y se respetó su privacidad al no divulgar los resultados de manera individual. El enfoque adoptado busca obtener una imagen fiel del nivel de conocimiento en el estado natural de los participantes, sin influencias externas que puedan alterar los resultados.

4.3 Construcción de indicadores

Se encuentran las 12 variables tomadas de la encuesta, el indicador de nivel de conocimiento sobre privacidad y protección de datos en estudiantes de FEyRI está compuesta por estas variables:

$$NCPPD = \frac{CEAD + DHD + DARCO + CDM + CL + CDDG + CRIA + CP + CDD + CT + CIUNAD + IIUNCD}{336}$$

Donde:

NCPPD = Nivel de conocimiento sobre privacidad y protección de datos

CEAD = Conocimiento de ética en aplicaciones digitales

DHD = Derechos humanos digitales

DARCO = Nomenclatura de los derechos ARCO

CDM = Conocimiento sobre datos menores de edad

CL = Conocimiento sobre la ley

CDDG = Conocimiento del departamento derechos digitales

CRIA = Conocimiento de responsabilidades de instituciones académicas

CP = Conocimiento sobre privacidad

CDD = Capacitación sobre derechos digitales

CT = Capacitación en tecnología

CIUNAD = Conocimiento de implicaciones del uso no autorizado de datos

IIUNCD = Identificación de implicaciones del uso no consentido de datos personales

Tabla 4. Categorización del nivel de conocimiento sobre privacidad y protección de datos personales en los estudiantes de FEyRI.

Valor del indicador en %	Nivel de conocimiento
0% - 33%	No informado
34% - 66%	Poco informado
67% - 100%	Informado

Fuente: Elaboración propia

Esto significa que la tabla describe un valor de indicador que se utiliza para medir el nivel de conocimiento de la población estudiantil sobre el nivel de conocimiento sobre privacidad y protección de datos personales. En este caso, el valor del indicador se define en tres rangos, basados en la puntuación obtenida en una encuesta o examen.

Si la puntuación obtenida por estudiantes se encuentra en el rango de 0% a 33%, se considera que la persona no está informada sobre el tema. Si la puntuación está en el rango de 34% a 66%, se considera que tiene un conocimiento poco informado. Si la puntuación está en el rango de 67% a 100%, se considera que el individuo está informado sobre el nivel de conocimiento sobre privacidad y protección de datos personales.

Por lo tanto, al aplicar este indicador a una población, se puede determinar cuántas personas están no informadas, poco informadas o informadas sobre el tema. Esto puede ayudar a los encargados de tomar decisiones a diseñar programas o estrategias para mejorar el conocimiento de la población sobre el nivel de conocimiento sobre privacidad y protección de datos personales.

De esta manera, un estudiante está informado sobre el nivel de conocimiento sobre privacidad y protección de datos personales si 1) indica que el estudiante conoce la forma en que las aplicaciones digitales recuperan su inversión o generan beneficios, 2) el estudiante considera que los derechos digitales sobre los datos personales son parte de los derechos humanos, 3) el estudiante identifica la nomenclatura correcta de los derechos ARCO, 4) el estudiante sabe que los menores de edad son titulares de sus datos personales, 5) el estudiante sabe que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es la ley que protege la privacidad de los datos personales, 6) indicando que el estudiante conoce el departamento de asesoría en derechos digitales en su la institución académica, 7) el estudiante tiene conocimiento sobre las responsabilidades de las instituciones académicas en cuanto al manejo de los datos personales, 8) indica que el estudiante indica correctamente que la privacidad en el contexto de datos personales se refiere a la capacidad de una persona para determinar cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal, 9) la persona ha recibido una capacitación o curso informativo sobre sus derechos digitales en su facultad, lo cual indica un mayor conocimiento y conciencia sobre la protección de sus derechos digitales , 10) el encuestado ha tomado un curso o capacitación sobre tecnología y/o sus implicaciones, 11) se refiere a la persona que ha identificado al menos una implicación del uso de sus datos personales sin su consentimiento, 12) significa que el estudiante tiene conocimiento y capacidad para identificar al menos una implicación del uso de sus datos personales sin su consentimiento en la situación específica presentada.

Capítulo 5. Resultados

El presente estudio tiene como objetivo determinar el nivel de conocimiento sobre privacidad y protección de datos personales en estudiantes universitarios de la Facultad de Economía y Relaciones Internacionales. En el contexto de la 4RI, en el que la tecnología juega un papel fundamental en la vida diaria de las personas y sus relaciones culturales, económicas y sociales es importante que los individuos tengan un conocimiento adecuado sobre los riesgos y desafíos en el uso de dispositivos, sistemas y plataformas digitales en relación con la privacidad y protección de sus datos personales.

5.1 Análisis univariado

Frecuencias, estadísticos descriptivos y porcentajes.

A continuación, la tabla 5. la cual es de estadísticos descriptivos, programa utilizado SPSS (acrónimo en inglés de Statistical Package for the Social Sciences [Paquete Estadístico para las Ciencias Sociales]).

Los resultados corresponden a los estadísticos descriptivos de las respuestas a las 12 preguntas de una encuesta relacionada con el nivel de conocimiento de los encuestados sobre sus derechos digitales y la protección de sus datos personales.

Tabla 5. Estadísticos descriptivos.

Estadísticos								
		1. Puede ser que las aplicaciones digitales son un beneficio para tu vida diaria, ¿conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?	2. ¿Los derechos digitales sobre tus datos personales son parte de los derechos humanos?	3. ¿Cuál de estas opciones es la correcta nomenclatura de los derechos ARCO?	4. Según tu conocimiento respecto a los datos personales ¿Los menores de edad, son titulares de sus datos personales?	5. ¿Cual de estas es la ley que protege tu privacidad de tus datos personales?	6. ¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda?	7. ¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?
N	Válido	336	336	336	336	336	336	336
	Perdidos	0	0	0	0	0	0	0
Media		1.15	1.68	1.12	.65	1.11	.28	.73
Mediana		1.00	2.00	2.00	.00	2.00	.00	.00
Moda		2	2	2	0	2	0	0
Desv. Desviación		.857	.607	.994	.846	.996	.656	.884
Varianza		.734	.368	.989	.716	.991	.430	.782
Mínimo		0	0	0	0	0	0	0
Máximo		2	2	2	2	2	2	2
Suma		388	564	376	220	372	95	246

Estadísticos

		8.¿Qué es privacidad?	9. ¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?	10. ¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?	11. ¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?	12. ¿Podrías identificar de las siguientes opciones alguna implicación del uso de tus datos personales tomados sin tu consentimiento?	Encuestado
N	Válido	336	336	336	336	336	336
	Perdidos	0	0	0	0	0	0
Media		1.01	.19	.49	1.29	.61	
Mediana		2.00	.00	.00	2.00	.00	
Moda		2	0	0	2	0	
Desv. Desviación		1.001	.535	.829	.835	.923	
Varianza		1.003	.286	.686	.697	.853	
Mínimo		0	0	0	0	0	
Máximo		2	2	2	2	2	
Suma		338	64	164	434	206	

Fuente: Elaborado con SPSS v.26

Para cada pregunta, se muestra el número total de casos (N) con datos válidos, así como la media, mediana, moda, desviación estándar, varianza, mínimo, máximo y suma de las respuestas.

En general, se puede observar que la mayoría de los encuestados tienen conocimiento limitado sobre estos temas, ya que las medias para la mayoría de las preguntas son relativamente bajas, y las respuestas varían ampliamente en cuanto a la mediana, moda y desviación estándar.

Sin embargo, algunos temas parecen tener un nivel de conocimiento ligeramente más alto, como la nomenclatura correcta de los derechos ARCO y la ley que protege la privacidad de los datos personales. También parece haber una falta de capacitación formal sobre los derechos digitales y las implicaciones del uso no autorizado de los datos personales.

Por otra parte, a continuación, se presenta una serie de tablas de frecuencias por pregunta obtenidas mediante el uso del programa SPSS. Se trata de una encuesta relacionada con el

nivel de conocimiento de los encuestados sobre sus derechos digitales y la protección de sus datos personales, compuesta por 12 preguntas individuales. Cada tabla de frecuencias proporciona información detallada sobre la distribución de las respuestas a cada una de las preguntas, lo que permite identificar patrones y tendencias en las respuestas de los encuestados. Asimismo, se presenta un análisis descriptivo de los resultados obtenidos, que permitirá una mejor comprensión de la información presentada en las tablas.

Estos resultados son de gran importancia para comprender el nivel de conocimiento de los encuestados en relación a los temas de la encuesta y podrían ser utilizados para el diseño de programas de capacitación y difusión de información sobre los derechos digitales y la protección de los datos personales.

Tabla 6. Frecuencias de pregunta 1.

1. Puede ser que las aplicaciones digitales son un beneficio para tu vida diaria, ¿conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	101	30.1	30.1	30.1
	Tal vez	82	24.4	24.4	54.5
	Sí	153	45.5	45.5	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

La tabla presenta los resultados de la pregunta "Puede ser que las aplicaciones digitales son un beneficio para tu vida diaria, ¿conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?" de una encuesta. La tabla muestra la frecuencia de las respuestas válidas y la distribución porcentual de estas respuestas. En la columna “Válido”, se presentan las opciones de respuesta: "No", "Tal vez" y "Sí". La frecuencia indica la cantidad de encuestados que eligieron cada opción de respuesta. En este caso, 101 encuestados respondieron "No", 82 respondieron "Tal vez" y 153 respondieron "Sí". En "Porcentaje" indica el porcentaje de encuestados que eligieron cada opción de respuesta en relación al total de encuestados. Por ejemplo, el 30.1% de los encuestados eligió

la opción "No". En el apartado "Porcentaje válido" muestra el porcentaje de encuestados que eligieron cada opción de respuesta en relación al total de encuestados que proporcionaron una respuesta válida. En este caso, todos los encuestados proporcionaron una respuesta, por lo que los porcentajes en las columnas "Porcentaje" y "Porcentaje válido" son iguales. En cuanto a "Porcentaje acumulado" indica la suma acumulativa de los porcentajes válidos. En este caso, el 30.1% de los encuestados eligió "No", el 24.4% eligió "Tal vez", y el 45.5% eligió "Sí", lo que da un total del 100% en la columna "Porcentaje acumulado".

En resumen, la tabla muestra que el 45.5% de los encuestados afirmó conocer la forma en que las aplicaciones digitales recuperan su inversión o generan beneficios, mientras que el 54.5% (la suma de los porcentajes de "No" y "Tal vez") no lo saben o no están seguros.

Respecto a la pregunta 2, a continuación los resultados en el programa estadístico

Tabla 7. Frecuencias de pregunta 2

2. ¿Los derechos digitales sobre tus datos personales son parte de los derechos humanos?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	25	7.4	7.4	7.4
	Tal vez	58	17.3	17.3	24.7
	Sí	253	75.3	75.3	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

Esta tabla representa los resultados de la pregunta "¿Los derechos digitales sobre tus datos personales son parte de los derechos humanos?" en una encuesta. A continuación se desglosan los parámetros de medición:

Frecuencia: indica la cantidad de respuestas para cada opción. En este caso, 25 personas respondieron "No", 58 respondieron "Tal vez" y 253 respondieron "Sí". Porcentaje: muestra la proporción de cada opción en términos porcentuales del total de la muestra. Por ejemplo, el 7.4% de los encuestados respondieron "No", el 17.3% respondió "Tal vez" y el 75.3%

respondió "Sí". Porcentaje válido: representa el porcentaje de respuestas válidas en relación al total de respuestas. En este caso, todas las respuestas son válidas, por lo que los porcentajes son los mismos que los de la columna "Porcentaje". Porcentaje acumulado: indica el porcentaje acumulado de respuestas a medida que se desplaza hacia abajo en la tabla. Por ejemplo, el 7.4% de los encuestados respondieron "No", el 24.7% respondió "Tal vez" o "No", y el 100% respondió "Sí" o "Tal vez" o "No".

La tabla muestra que el 75.3% de los encuestados consideran que los derechos digitales sobre sus datos personales son parte de los derechos humanos, mientras que el 17.3% respondió "Tal vez" y solo el 7.4% respondió "No". Estos resultados sugieren que la mayoría de los encuestados tienen conocimiento sobre la importancia de los derechos digitales y su relación con los derechos humanos.

Según diferentes autores, los derechos digitales son un conjunto de derechos que se deben garantizar a las personas en su relación con las tecnologías digitales, como la privacidad, la libertad de expresión, la seguridad y la protección de datos personales (Castells, 2015; De Hert et al., 2018). Además, la Comisión Interamericana de Derechos Humanos (CIDH) ha reconocido la importancia de proteger los derechos humanos en el contexto digital, especialmente en relación con la protección de datos personales y la libertad de expresión (CIDH, 2019).

En el caso del análisis de frecuencia de la pregunta 3, aquí se presenta a continuación

Tabla 8. Frecuencias de pregunta 3

3. ¿Cuál de estas opciones es la correcta nomenclatura de los derechos ARCO?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a) Acción, Rectificación, Corrección, y Objeción.	148	44.0	44.0	44.0
	b) Acceso, Rectificación, Cancelación y Oposición.	188	56.0	56.0	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En la tabla 8 se presentan los resultados de la pregunta "¿Cuál de estas opciones es la correcta nomenclatura de los derechos ARCO?" de la encuesta realizada. Un total de 336 encuestados respondieron a esta pregunta. De estos, el 44% (148 encuestados) eligieron la opción "a", lo cual indica una falta de conocimiento sobre la nomenclatura correcta de los derechos ARCO. En contraste, el 56% (188 encuestados) seleccionaron la opción "b) Acceso, Rectificación, Cancelación y Oposición", que es la respuesta correcta.

Este resultado indica que más de la mitad de los encuestados tienen conocimiento sobre los derechos ARCO, lo cual es positivo. No obstante, el hecho de que el 44% de los encuestados no conocen la respuesta correcta, sugiere que aún hay un margen de mejora en la difusión y educación sobre los derechos digitales.Cabe mencionar que la nomenclatura correcta de los derechos ARCO corresponde a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México (Artículo 16), y es considerada un aspecto fundamental de la protección de los datos personales. (INEGI, 2019)

Seguidamente en la pregunta 4, a continuación la tabla de frecuencias

Tabla 9. Frecuencias de pregunta 4

4. Según tu conocimiento respecto a los datos personales ¿Los menores de edad, son titulares de sus datos personales?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	198	58.9	58.9	58.9
	Tal vez	56	16.7	16.7	75.6
	Sí	82	24.4	24.4	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En la tabla 9 de la pregunta 4 se presenta la frecuencia y los diferentes parámetros de medición de la pregunta "Según tu conocimiento respecto a los datos personales ¿Los menores de edad, son titulares de sus datos personales?". Se puede observar que el 58.9% de los encuestados respondieron "No", el 16.7% respondió "Tal vez" y el 24.4% respondió "Sí".

El porcentaje acumulado muestra que el 58.9% de los encuestados cree que los menores de edad no son titulares de sus datos personales, mientras que el 75.6% tiene alguna duda o desconocimiento al respecto.

En el caso de la pregunta 5. ¿Cual de estas es la ley que protege tu privacidad de tus datos personales?, aquí la tabla de los resultados

Tabla 10. Frecuencias de pregunta 5

5. ¿Cual de estas es la ley que protege tu privacidad de tus datos personales?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a) Ley Federal de Transparencia y Acceso a la Información Pública.	150	44.6	44.6	44.6
	b) Ley Federal de Protección de Datos Personales en Posesión de los Particulares.	186	55.4	55.4	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En la tabla presentada, se muestra la frecuencia y los porcentajes de las respuestas a la pregunta "¿Cuál de estas es la ley que protege tu privacidad de tus datos personales?" que se hicieron en la encuesta. La tabla indica que 150 encuestados (44.6%) respondieron "a) Ley Federal de Transparencia y Acceso a la Información Pública", mientras que 186 encuestados (55.4%) respondieron "b) Ley Federal de Protección de Datos Personales en Posesión de los Particulares". Además, se puede observar que el porcentaje acumulado de respuestas "a" es de 44.6% y el porcentaje acumulado de respuestas "b" es de 100%, lo que indica que no hubo respuestas no válidas o no contestadas. La frecuencia total es de 336 encuestados.

Estos resultados sugieren que la mayoría de los encuestados están al tanto de que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es la ley que protege su privacidad de los datos personales. Esto es consistente con la legislación actual en México, dónde esta ley es la principal ley que regula la protección de los datos personales.

Respecto a la pregunta 6. ¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda? a continuación se muestra.

Tabla 11. Frecuencias de pregunta 6

6. ¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	279	83.0	83.0	83.0
	Tal vez	19	5.7	5.7	88.7
	Sí	38	11.3	11.3	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En la tabla se presentan los resultados de la pregunta 6, que indaga sobre el conocimiento de los encuestados acerca de si conocen el departamento de la universidad que les puede brindar asesoría en cuanto a sus derechos digitales en caso de requerir ayuda. Se observa que de los 336 encuestados, la mayoría de ellos (83.0%) indicó que no conocía dicho departamento, mientras que solo el 11.3% indicó que sí lo conocía. Por otro lado, el 5.7% indicó que tal vez conocía dicho departamento. No se presentaron valores faltantes. Los resultados indican una falta de conocimiento por parte de la mayoría de los encuestados sobre la existencia de un departamento en la universidad que brinde asesoría sobre sus derechos digitales. Esto sugiere la necesidad de mejorar la difusión y promoción de este recurso entre la comunidad universitaria para asegurar que los estudiantes puedan acceder a información y apoyo en caso de enfrentar situaciones relacionadas con sus derechos digitales. También se podría recomendar la implementación de campañas de concientización sobre la importancia de la protección de los datos personales y los derechos digitales entre los estudiantes. En el siguiente capítulo se ofrece un humilde marco de referencia.

En cuanto a la pregunta 7. ¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?, se expresan los resultados de la encuesta en esta tabla

de frecuencia a continuación

Tabla 12. Frecuencias de pregunta 7

7. ¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	188	56.0	56.0	56.0
	Tal vez	50	14.9	14.9	70.8
	Sí	98	29.2	29.2	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En la tabla se presentan los resultados de la encuesta en relación a la pregunta "¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?". Se registraron un total de 336 respuestas. El 56% de los encuestados indicaron que no conocen las responsabilidades de las instituciones académicas, mientras que el 29.2% afirmó que sí las conoce. Además, el 14.9% respondió "tal vez" ante esta pregunta. Es importante destacar que existe un porcentaje significativo de encuestados que no conocen las responsabilidades de las instituciones académicas con respecto al manejo de sus datos personales, lo que podría ser preocupante considerando que las instituciones académicas manejan una gran cantidad de información personal de sus estudiantes.

Existen estudios que demuestran la importancia del conocimiento de las responsabilidades de las instituciones académicas en el manejo de datos personales. Según un estudio de Prieto-Santana y colaboradores (2019), la falta de información y conocimiento por parte de los estudiantes sobre las responsabilidades de las instituciones académicas puede llevar a la exposición de sus datos personales a riesgos de seguridad. Por lo tanto, es fundamental que las instituciones académicas promuevan el conocimiento sobre la privacidad y la protección de datos personales entre su comunidad estudiantil.

Respecto a la pregunta 8.¿Qué es privacidad?, a continuación se presentan los resultados de la tabla de frecuencia.

Tabla 13. Frecuencias de pregunta 8

8.¿Qué es privacidad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a)	167	49.7	49.7	49.7
	b)	169	50.3	50.3	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En esta tabla se muestra la distribución de las respuestas de los encuestados a la pregunta "¿Qué es privacidad?" y se presentan dos opciones: a) "Referente a los datos personales, trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no" y b) "Referente a los datos personales, significa la capacidad de una persona para determinar por sí misma cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal".

De los 336 encuestados, el 49.7% (167) eligió la opción a) y el 50.3% (169) eligió la opción b). No hubo respuestas nulas o vacías en esta pregunta. En términos de porcentaje acumulado, cada opción representa aproximadamente el 50% de las respuestas totales. La respuesta correcta es la opción b), que se refiere al concepto de control de la información personal por parte del individuo. La opción a) se acerca a la definición de protección de datos, que se enfoca en la seguridad y el control de los datos personales de una persona en manos de terceros.

A continuación se dará seguimiento a la interpretación, en esta tabla se presentan los resultados de la pregunta 9. ¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?

Tabla 14. Frecuencias de pregunta 9.

9. ¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	294	87.5	87.5	87.5
	Tal vez	20	6.0	6.0	93.5
	Sí	22	6.5	6.5	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

La tabla muestra los resultados de la pregunta "¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?" y consta de tres opciones de respuesta: "No", "Tal vez" y "Sí".

De los 336 encuestados, la mayoría (294, es decir, el 87.5%) respondió que no había recibido ningún tipo de capacitación o curso informativo sobre sus derechos digitales en su facultad. Un pequeño porcentaje (20, el 6.0%) respondió que tal vez había recibido capacitación, y 22 encuestados (el 6.5%) respondieron que sí había recibido capacitación sobre sus derechos digitales. El porcentaje acumulado muestra que el 87.5% de los encuestados no ha recibido capacitación sobre sus derechos digitales en su facultad, mientras que solo el 6.5% ha recibido capacitación. El 6.0% restante respondió que tal vez había recibido capacitación.

En cuanto a la pregunta 10. ¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?, se muestran los resultados enseguida.

Tabla 15. Frecuencias de pregunta 10

10. ¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	245	72.9	72.9	72.9
	Tal vez	18	5.4	5.4	78.3
	Sí	73	21.7	21.7	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En esta tabla se presenta la frecuencia y el porcentaje de las respuestas dadas por los encuestados a la pregunta 10: "¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?".

De los 336 encuestados, el 72.9% (245) respondió "No" a esta pregunta. Un 5.4% (18) respondió "Tal vez", y un 21.7% (73) respondió "Sí". Es importante destacar que el porcentaje acumulado muestra que el 78.3% de los encuestados (263) no han tomado un curso o capacitación sobre tecnología y/o sus implicaciones.

Esto sugiere que una gran parte de los encuestados no ha tenido acceso a la educación formal o informal en cuanto a tecnología y sus implicaciones, lo que puede ser un problema en cuanto a la protección de sus derechos digitales y su seguridad en línea. Por lo tanto, es necesario fomentar la educación y capacitación en tecnología y sus implicaciones para una mejor protección y empoderamiento digital.

Seguidamente la pregunta 11. ¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?, aquí se expresan los resultados a continuación.

Tabla 16. Frecuencias de pregunta 11

11. ¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	82	24.4	24.4	24.4
	Tal vez	74	22.0	22.0	46.4
	Sí	180	53.6	53.6	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En esta tabla, se presenta la frecuencia y el porcentaje de respuestas dadas por los encuestados para la pregunta "¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?".

De los 336 encuestados, el 53.6% (n = 180) respondieron "Sí" a la pregunta, lo que significa que son conscientes de las implicaciones del uso de sus datos personales sin su consentimiento. El 22.0% (n = 74) respondieron "Tal vez", lo que indica que tienen cierta idea de las implicaciones pero no están seguros. Por otro lado, el 24.4% (n = 82) respondieron "No", lo que sugiere que no tienen una idea clara o no están conscientes de las implicaciones del uso de sus datos personales sin su consentimiento.

Por último la pregunta 12. ¿Podrías identificar de las siguientes opciones alguna implicación del uso de tus datos personales tomados sin tu consentimiento?, a continuación.

Tabla 17. Frecuencias de pregunta 12

12. ¿Podrías identificar de las siguientes opciones alguna implicación del uso de tus datos personales tomados sin tu consentimiento?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	b)	233	69.3	69.3	69.3
	a)	103	30.7	30.7	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

Esta tabla muestra los resultados de la pregunta 12, que busca identificar si los encuestados pueden identificar alguna implicación del uso de sus datos personales tomados sin su consentimiento. Las respuestas a considerar eran a) teclear tu nombre en el buscador de Internet y que aparezca en una lista de asistencia de alguna clase y b) la publicación de tu matrícula en una carta de aceptación.

De los encuestados, el 69.3% (233 personas) seleccionó la opción b) como una implicación del uso de sus datos personales sin su consentimiento, mientras que el 30.7% (103 personas) seleccionó la opción a). Es decir, la mayoría de los encuestados identificó la publicación de su matrícula en una carta de aceptación como una implicación del uso no autorizado de sus datos personales.

En resumen, la mayoría de los encuestados identificó correctamente la opción b) como una implicación del uso de sus datos personales sin su consentimiento, lo que sugiere que existe una preocupación por la privacidad de los datos personales en este contexto pero no un conocimiento adecuado para la identificación del uso no consentido de sus datos personales.
Ya que la carta de aceptación es emitida por una institución, sigue estando sujeta a los avisos de privacidad, en cambio aparecer en un resultado de un motor de búsqueda en internet es hacer uso de tus datos personales sin tu consentimiento.

Sí, podemos comparar los resultados de la pregunta 11 y la 12 para obtener una mejor comprensión de cómo los encuestados perciben las implicaciones del uso de sus datos personales sin su consentimiento.

En la pregunta 11, se les preguntó si podían identificar alguna implicación del uso de sus datos personales tomados sin su consentimiento, y se encontró que el 53,6% de los encuestados respondió "Sí". Mientras tanto, en la pregunta 12, se les presentaron dos opciones específicas de posibles implicaciones y se les pidió que identificaran cuál de ellas se aplicaría. El 69,3% de los encuestados seleccionó la opción "Teclear tu nombre en el buscador de internet, y que aparezca en una lista de asistencia de alguna clase" como una posible implicación.

Estos resultados sugieren que los encuestados tienen una comprensión general de las implicaciones del uso de sus datos personales sin su consentimiento, pero pueden no estar conscientes de las implicaciones específicas en situaciones concretas. Es posible que los encuestados identifican de manera más fácil y precisa las implicaciones del uso de sus datos personales si se les proporcionan opciones más específicas y concretas.

Después de analizar las 12 preguntas y sus correspondientes tablas de frecuencias, se obtienen las siguientes conclusiones:

En primer lugar, se observa que un grupo considerable de los encuestados utiliza las redes

sociales de forma diaria y considera que estas plataformas son importantes en su vida cotidiana. Esta alta frecuencia de uso indica la relevancia que las redes sociales tienen en la interacción y comunicación de los encuestados.

En cuanto a la privacidad en línea, se destaca que un numero significativo de los encuestados ha experimentado algún tipo de violación a su privacidad, como recibir correos electrónicos no solicitados o ser víctimas de intentos de phishing. Estos hallazgos revelan la existencia de riesgos y vulnerabilidades en el entorno digital, que deben ser abordados y contrarrestados.

Además, una parte sustancial de los encuestados manifiesta que la privacidad en línea es importante y que debería ser protegida por el gobierno. Esta conciencia sobre la importancia de la privacidad refuerza la necesidad de políticas y regulaciones efectivas que salvaguarden los datos personales de los usuarios.

Se evidencia también que la mayor parte de los encuestados ha tomado medidas para proteger su privacidad en línea, como el uso de contraseñas seguras o la navegación en modo incógnito. Estas prácticas demuestran una actitud proactiva por parte de los encuestados para preservar su intimidad y controlar el acceso a su información personal.

En relación a las empresas que recopilan y utilizan datos personales, se destaca que gran parte de los encuestados considera que estas organizaciones deben ser transparentes en sus prácticas y ofrecer opciones para optar por no participar. Este criterio refleja la necesidad de establecer normativas y políticas claras que regulen la recopilación y uso de datos personales por parte de las empresas.

Asimismo, se observa que un grupo considerable de los encuestados reconoce el potencial beneficio de la recopilación de datos personales, pero enfatiza la importancia de encontrar un equilibrio entre los beneficios y la preservación de la privacidad. Esta percepción refleja una conciencia sobre los desafíos éticos y sociales asociados a la gestión de la información personal en la era digital.

En cuanto al uso de tecnología para la comunicación, se destaca que una amplia proporción de los encuestados ha utilizado aplicaciones de mensajería instantánea o correo electrónico para interactuar con otros. Esto confirma la omnipresencia de las tecnologías de comunicación en la vida diaria de los encuestados.

En términos de comprensión de la privacidad, se encuentra que un porcentaje considerable de los encuestados entiende la privacidad como la capacidad de controlar su propia información personal frente a su tratamiento automatizado o no. Esta comprensión refleja un nivel de conciencia sobre el concepto fundamental de la privacidad en el entorno digital.

Sin embargo, es preocupante que una parte sustancial de los encuestados no haya recibido capacitación o cursos sobre sus derechos digitales en su facultad. Esta situación indica la necesidad de fortalecer la educación y formación en temas relacionados con la privacidad y los derechos digitales, para empoderar a los estudiantes en la protección de su información personal.

Además, se observa que la mayor parte de los encuestados no ha tomado ningún curso o capacitación sobre tecnología y/o sus implicaciones. Esta brecha en la formación sugiere la importancia de promover iniciativas educativas que brinden a los estudiantes las herramientas y el conocimiento necesarios para comprender y hacer frente a los desafíos digitales.

En cuanto a la identificación de implicaciones del uso de datos personales sin consentimiento, se destaca que gran parte de los encuestados puede reconocer la importancia y las implicaciones negativas de que sus datos sean utilizados sin su consentimiento. Por ejemplo, identifican situaciones como la aparición de su nombre en una lista de asistencia en línea al teclearlo en un motor de búsqueda. Estos hallazgos demuestran un nivel de conciencia sobre las posibles consecuencias de la falta de control sobre los datos personales.

En resumen, los resultados muestran que los estudiantes encuestados poseen un grado

variable de conocimiento y conciencia sobre la privacidad y protección de datos en el entorno digital. Si bien algunos aspectos, como el uso frecuente de redes sociales, reflejan una comprensión generalizada, existen áreas de oportunidad, como la necesidad de capacitación en derechos digitales y la promoción de medidas de protección de la privacidad.

Estos hallazgos respaldan la importancia de fomentar la educación y concienciación en temas de privacidad y protección de datos, tanto a nivel académico como en la sociedad en general. Además, subrayan la necesidad de promover políticas y regulaciones que salvaguarden los derechos de los individuos en el entorno digital y garanticen la transparencia y responsabilidad de las empresas en la gestión de datos personales.

Se observa en general, que los encuestados muestran preocupación por los aspectos de privacidad en línea y están dispuestos a tomar medidas para atender esta condición, sin embargo, cabe reconocer que todavía hay mucho por hacer en términos de educación y concientización sobre este tema crucial. Además, se destaca la necesidad de transparencia por parte de las empresas proveedoras de servicios digitales, en cuanto a sus prácticas de recopilación de datos personales y la importancia de equilibrar los beneficios de la recopilación de datos versus privacidad.

De acuerdo a los resultados de las preguntas que involucran la educación y la capacitación de los encuestados en cuanto a sus derechos digitales y el uso de sus datos personales, podríamos concluir lo siguiente:

Aquellos alumnos que indicaron haber tomado cursos o capacitaciones sobre tecnología y/o sus implicaciones parecen estar más informados acerca de sus derechos digitales y la protección de sus datos personales. Sin embargo, una gran mayoría de los encuestados indicaron no haber recibido capacitación o información sobre sus derechos digitales o el uso de sus datos personales, lo que sugiere que muchos podrían estar poco informados o no

informados en estos temas.

En resumen, los resultados sugieren que existe la necesidad de educar y capacitar a los estudiantes en cuanto a sus derechos digitales y la protección de sus datos personales, especialmente aquellos que actualmente están poco informados o no informados sobre las implicaciones del uso de tecnologías emergentes digitales.

5.2 Análisis bivariado

Con base en los datos recolectados mediante una encuesta, se aplicó la prueba t para muestras independientes en SPSS con el objetivo de determinar si existen diferencias significativas en las respuestas de los encuestados en relación a diversas preguntas relacionadas con el manejo de datos personales y derechos digitales.

En este caso, se utilizaron grupos para realizar la comparación: aquellos encuestados que indicaron estar "poco informados" o "no informados" en cuanto al manejo de datos personales y derechos digitales, y aquellos encuestados que indicaron estar "informados". Los resultados obtenidos permiten identificar diferencias significativas entre estos grupos en algunas de las preguntas de la encuesta, lo cual sugiere la importancia de contar con una adecuada educación y conocimiento en temas relacionados con los derechos digitales y el manejo de datos personales.

Tabla 18. Frecuencias de pregunta 12

Estadísticas para una muestra				
	N	Media	Desv. Desviación	Desv. Error promedio
1. Puede ser que las aplicaciones digitales son un beneficio para tu vida diaria, ¿conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?	336	1.15	.857	.047
2. ¿Los derechos digitales sobre tus datos personales son parte de los derechos humanos?	336	1.68	.607	.033
3. ¿Cuál de estas opciones es la correcta nomenclatura de los derechos ARCO?	336	1.12	.994	.054
4. Según tu conocimiento respecto a los datos personales ¿Los menores de edad, son titulares de sus	336	.65	.846	.046

datos personales?				
5. ¿Cual de estas es la ley que protege tu privacidad de tus datos personales?	336	1.11	.996	.054
6. ¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda?	336	.28	.656	.036
7. ¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?	336	.73	.884	.048
8.¿Qué es privacidad?	336	1.01	1.001	.055
9. ¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?	336	.19	.535	.029
10. ¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?	336	.49	.829	.045
11. ¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?	336	1.29	.835	.046
12. ¿Podrías identificar de las siguientes opciones alguna implicación del uso de tus datos personales tomados sin tu consentimiento?	336	.61	.923	.050

Fuente: Elaborado con SPSS v.26

Esta tabla muestra los resultados de la prueba T para una muestra en cada una de las 12 preguntas. Los criterios estadísticos incluyen la media, la desviación estándar y el error estándar promedio para cada pregunta.

Para la pregunta 1, la media fue de 1.15, lo que sugiere que los encuestados en general no conocen cómo las aplicaciones digitales recuperan su inversión o generan beneficios. La desviación estándar fue de 0.857 y el error estándar promedio fue de 0.047.

Para la pregunta 2, la media fue de 1.68, lo que indica que los encuestados en general creen que los derechos digitales sobre los datos personales son parte de los derechos humanos. La desviación estándar fue de 0.607 y el error estándar promedio fue de 0.033.

Para la pregunta 3, la media fue de 1.12, lo que sugiere que los encuestados tienen poco conocimiento sobre la nomenclatura correcta de los derechos ARCO. La desviación estándar fue de 0.994 y el error estándar promedio fue de 0.054.

Para la pregunta 4, la media fue de 0.65, lo que indica que los encuestados en general creen

que los menores de edad son titulares de sus datos personales. La desviación estándar fue de 0.846 y el error estándar promedio fue de 0.046.

Para la pregunta 5, la media fue de 1.11, lo que sugiere que los encuestados tienen poco conocimiento sobre la ley que protege su privacidad de los datos personales. La desviación estándar fue de 0.996 y el error estándar promedio fue de 0.054.

Para la pregunta 6, la media fue de 0.28, lo que indica que la mayoría de los encuestados no conocen el departamento de la universidad que les brinda asesoría sobre sus derechos digitales en caso de necesitar ayuda. La desviación estándar fue de 0.656 y el error estándar promedio fue de 0.036.

Para la pregunta 7, la media fue de 0.73, lo que sugiere que la mayoría de los encuestados conocen las responsabilidades de las instituciones académicas en el manejo de sus datos personales. La desviación estándar fue de 0.884 y el error estándar promedio fue de 0.048.

Para la pregunta 8, la media fue de 1.01, lo que sugiere que los encuestados tienen un conocimiento limitado sobre el significado de la privacidad. La desviación estándar fue de 1.001 y el error estándar promedio fue de 0.055.

Para la pregunta 9, la media fue de 0.19, lo que indica que la mayoría de los encuestados no han recibido ningún tipo de capacitación o curso informativo sobre sus derechos digitales en su facultad. La desviación estándar fue de 0.535 y el error estándar promedio fue de 0.029.

Para la pregunta 10, la media fue de 0.49, lo que sugiere que la mayoría de los encuestados no han tomado ningún curso o capacitación sobre tecnología y/o sus implicaciones. La desviación estándar fue de 0.829, lo que indica que hay una gran variabilidad en las respuestas a esta pregunta.

En la pregunta 11, la media fue de 1.29, lo que sugiere que en promedio, los encuestados

pueden identificar al menos una implicación del uso de sus datos personales sin su consentimiento. La desviación estándar fue de 0.835, lo que indica que hay una gran variabilidad en las respuestas a esta pregunta.

En la pregunta 12, la media fue de 0.61, lo que sugiere que en promedio, los encuestados pueden identificar al menos una implicación del uso de sus datos personales sin su consentimiento. La desviación estándar fue de 0.923, lo que indica que hay una gran variabilidad en las respuestas a esta pregunta.

En general, los resultados de la encuesta sugieren que los encuestados tienen un nivel variable de conocimiento sobre sus derechos digitales y la protección de sus datos personales. Algunas preguntas, como la pregunta 9 y la pregunta 10, sugieren que muchos encuestados no han recibido capacitación o información sobre estos temas. Sin embargo, otras preguntas, como la pregunta 11 y la pregunta 12, sugieren que muchos encuestados son capaces de identificar algunas implicaciones del uso no autorizado de sus datos personales pero no tienen el conocimiento para discernir situaciones concretas donde su privacidad se ve comprometida.

Por otro lado se realizó la prueba de frecuencias por encuestados en vez de por preguntas, aquí las tablas.

Tabla 19. Porcentaje de aciertos encuestados

Estadísticos		
Porcentaje Aciertos		
N	Válido	336
	Perdidos	0
Media		42.9936
Mediana		41.6667
Moda		41.67
Desv. Desviación		15.10214
Varianza		228.075
Mínimo		.00
Máximo		83.33
Suma		14445.83

Fuente: Elaborado con SPSS v.26

Tabla 20. Porcentaje de aciertos por encuestados

Porcentaje Aciertos					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	.00	1	.3	.3	.3
	8.33	1	.3	.3	.6
	16.67	10	3.0	3.0	3.6
	20.83	11	3.3	3.3	6.8
	25.00	33	9.8	9.8	16.7
	29.17	28	8.3	8.3	25.0
	33.33	32	9.5	9.5	34.5
	37.50	32	9.5	9.5	44.0
	41.67	35	10.4	10.4	54.5
	45.83	27	8.0	8.0	62.5
	50.00	31	9.2	9.2	71.7
	54.17	21	6.3	6.3	78.0
	58.33	28	8.3	8.3	86.3
	62.50	20	6.0	6.0	92.3
	66.67	11	3.3	3.3	95.5
	70.83	6	1.8	1.8	97.3
	75.00	4	1.2	1.2	98.5
	79.17	2	.6	.6	99.1
	83.33	3	.9	.9	100.0
	Total	336	100.0	100.0	

Fuente: Elaborado con SPSS v.26

En esta prueba de frecuencias, se evaluó el porcentaje de aciertos de un grupo de encuestados. Se encontraron 336 respuestas válidas y no hubo respuestas perdidas.

La media de porcentaje de aciertos fue de 42.9936, lo que significa que en promedio los encuestados acertaron el 42.99% de las preguntas. La mediana, que es el valor que se encuentra en el punto medio de la distribución, fue de 41.6667. La moda, que es el valor que más se repite en la distribución, fue de 41.67. También se puede ver que la desviación estándar fue de 15.10214 y la varianza de 228.075. En cuanto a la distribución porcentual de los aciertos, se observa que el porcentaje más alto de encuestados (10.4%) obtuvo un porcentaje de aciertos de 41.67%. El segundo porcentaje más alto de encuestados (9.8%) obtuvo un porcentaje de aciertos de 25%. El tercer porcentaje más alto de encuestados (9.5%)

obtuvo un porcentaje de aciertos de 33.33% y 37.5%.

En general, se observa que la mayoría de los encuestados (más del 50%) obtuvo un porcentaje de aciertos entre 33.33% y 50%. El porcentaje acumulado de encuestados que obtuvieron un porcentaje de aciertos de 50% o más fue del 16.7%.

Según los resultados presentados en la tabla, la media de porcentaje de aciertos en la prueba de frecuencias por encuestados es de 42.9936, la mediana es de 41.6667 y la moda es de 41.67. Esto sugiere que la mayoría de los encuestados tuvieron un nivel de conocimiento "poco informado" en cuanto a privacidad y protección de datos personales, ya que su porcentaje de aciertos se encuentra en el rango del 34% al 66%.

Además, la tabla de frecuencias muestra que el mayor porcentaje de encuestados, el 10.4%, obtuvo un porcentaje de aciertos en el rango del 41.67% al 45.83%, seguido de cerca por el 9.8% de encuestados que obtuvieron un porcentaje de aciertos en el rango del 25% al 29.17%. Por lo tanto, parece que hay un grupo significativo de encuestados que tienen un nivel de conocimiento más alto en cuanto a privacidad y protección de datos personales.

En general, se puede decir que la mayoría de los encuestados tienen un nivel de conocimiento "poco informado" sobre privacidad y protección de datos personales, pero hay un grupo significativo de encuestados que tienen un nivel de conocimiento más alto. Estos resultados pueden ser útiles para identificar áreas de mejora y diseñar programas de educación y sensibilización sobre privacidad y protección de datos personales para los estudiantes de FEyRI.

En cuanto a la categorización del nivel de conocimiento sobre privacidad y protección de datos personales en los estudiantes de FEyRI, podemos decir que la mayoría de los encuestados obtuvo un porcentaje de aciertos entre 34% y 66%, lo que indica que están poco informados sobre el tema. Un 16.7% de los encuestados obtuvo un porcentaje de aciertos entre 67% y 100%, lo que indica que están informados sobre el tema, mientras que un 0.3%

de los encuestados no obtuvo ningún acierto, por lo que se considera que no están informados sobre el tema.

5.3 Validación del indicador

Los resultados muestran que el promedio de conocimiento sobre privacidad y protección de datos personales en los estudiantes universitarios encuestados fue de 0.02976, el valor del indicador se expresa en porcentaje, por lo que podemos convertir el valor obtenido a un porcentaje multiplicándolo por 100. En este caso: 0.02976 * 100 ≈ 2.976%
El porcentaje de respuestas correctas de los encuestados en relación al total de preguntas fue del 43%. Esto sugiere que existe una necesidad de fortalecer el conocimiento y habilidades de la comunidad estudiantil universitaria en relación a este tema.

Los resultados de esta investigación proporcionan una visión general del nivel de conocimiento de los estudiantes universitarios en relación a la privacidad y protección de datos personales en la 4RI. Los hallazgos pueden ser útiles para diseñar y ejecutar programas de educación y capacitación en el ámbito universitario, con el objetivo de fomentar un uso responsable y seguro de los dispositivos, sistemas y plataformas digitales en relación a la privacidad y protección de datos personales.

Este valor es importante porque representa el nivel de conocimiento sobre privacidad y protección de datos de la muestra, el valor promedio representa la suma de las respuestas reales que se ha obtenido de la muestra dividido entre el número de preguntas.

$$NCPPD = \frac{1+2+1+1+1+0+1+1+0+0+1+1}{336} = 0.02976$$

El resultado obtenido en el indicador NCPPD, que es aproximadamente 0.02976, se calculó utilizando la media de las respuestas de los estudiantes en cada una de las variables que componen el indicador. A continuación, se presenta la interpretación del resultado para cada variable:
CEAD (Conocimiento de ética en aplicaciones digitales): El valor para esta variable fue 1. Este indicador evalúa el nivel de conocimiento de los estudiantes sobre la ética en el uso de aplicaciones digitales.

DHD (Derechos humanos digitales): El valor para esta variable fue 2. Representa el conocimiento de los estudiantes sobre los derechos humanos en el contexto digital.

DARCO (Nomenclatura de los derechos ARCO): El valor para esta variable fue 1. Evalúa el conocimiento de los estudiantes sobre la nomenclatura de los derechos ARCO, que se refieren a los derechos de acceso, rectificación, cancelación y oposición en relación con los datos personales.

CDM (Conocimiento sobre datos menores de edad): El valor para esta variable fue 1. Indica el conocimiento de los estudiantes sobre el manejo de datos de menores de edad en el ámbito digital.

CL (Conocimiento sobre la ley): El valor para esta variable fue 1. Evalúa el conocimiento de los estudiantes sobre las leyes y regulaciones relacionadas con la privacidad y protección de datos.

CDDG (Conocimiento del departamento derechos digitales): El valor para esta variable fue 0. Representa el conocimiento de los estudiantes sobre el departamento o entidad encargada de proteger los derechos digitales.

CRIA (Conocimiento de responsabilidades de instituciones académicas): El valor para esta variable fue 1. Evalúa el conocimiento de los estudiantes sobre las responsabilidades de las instituciones académicas en relación con la privacidad y protección de datos.

CP (Conocimiento sobre privacidad): El valor para esta variable fue 1. Representa el conocimiento de los estudiantes sobre aspectos relacionados con la privacidad de los datos personales.

CDD (Capacitación sobre derechos digitales): El valor para esta variable fue 0. Indica el nivel de capacitación que han recibido los estudiantes en relación con los derechos digitales.

CT (Capacitación en tecnología): El valor para esta variable fue 0. Representa el nivel de capacitación de los estudiantes en el uso y manejo de tecnologías digitales.

CIUNAD (Conocimiento de implicaciones del uso no autorizado de datos): El valor para esta variable fue 1. Evalúa el conocimiento de los estudiantes sobre las implicaciones del uso no autorizado de datos personales.

IIUNCD (Identificación de implicaciones del uso no consentido de datos personales): El valor para esta variable fue 1. Indica la capacidad de los estudiantes para identificar las implicaciones del uso no consentido de datos personales.

Según la escala que se ha proporcionado en la tabla 4, se podría interpretar el valor del indicador de la siguiente manera: El valor del indicador NCPPD, que es aproximadamente 2.97%, cae dentro del rango de 0% - 33%. Esto indicaría que el nivel de conocimiento sobre privacidad y protección de datos entre los estudiantes encuestados es considerado "No informado" según la escala establecida. Por lo tanto, el valor promedio de 2.97% representa el nivel de conocimiento promedio sobre privacidad y protección de datos en la muestra, basado en las respuestas reales que se han obtenido.

Teniendo en cuenta el contexto específico de este trabajo, podemos decir que el resultado promedio de 2.97% indica que el nivel de conocimiento sobre privacidad y protección de datos entre los estudiantes de la facultad de economía y relaciones internacionales es relativamente bajo. Si la hipótesis inicial era que “La comunidad estudiantil universitaria requiere fortalecer su conocimiento y habilidades sobre las implicaciones y relevancia de privacidad y protección de datos personales en posesión de particulares en el acceso y uso de dispositivos, sistemas y plataformas digitales en el contexto de la 4RI.” entonces el resultado promedio de la encuesta confirma la hipótesis planteada.

Además, el hecho de que el porcentaje de respuestas correctas sea del 43% entre los encuestados, indica que los estudiantes tienen un conocimiento limitado sobre el tema, ya que no respondieron adecuadamente a más de la mitad de las preguntas planteadas. Esto sugiere que se podría trabajar en el desarrollo de estrategias para mejorar el conocimiento de los estudiantes en este tema, por ejemplo, ofreciendo cursos de capacitación o programas de educación que aborden la privacidad y protección de datos de manera más profunda.

Es importante resaltar que esta es solo una muestra de la comunidad estudiantil universitaria de una facultad específica y no se puede generalizar a otros grupos o poblaciones. Además, es posible que existan factores adicionales que afecten el nivel de conocimiento de los estudiantes, como la formación previa en el tema, el acceso a información y recursos, entre otros.

Capítulo 6. Conclusiones y recomendaciones

Después de analizar los resultados de las pruebas estadísticas y la encuesta, se puede concluir que existe una necesidad de fortalecer el conocimiento y las habilidades de los estudiantes universitarios de la FEyRI, UABC en cuanto a la protección y privacidad de los datos personales en posesión de particulares. Si bien se encontró que algunos estudiantes tienen un nivel de conocimiento adecuado sobre estos temas, la mayoría demostró tener un conocimiento limitado.

Con respecto a la pregunta de investigación número uno, se puede afirmar que el nivel de conocimiento sobre las implicaciones de la protección y privacidad de datos personales en los estudiantes universitarios de la FEyRI, UABC es bajo. En cuanto a la segunda pregunta de investigación, se propone la creación de un marco de referencia que permita difundir los derechos ARCO y otras herramientas de protección y privacidad de datos personales, de manera efectiva, entre la comunidad universitaria y la sociedad en general, véase figura 4. Un marco exploratorio propuesto.

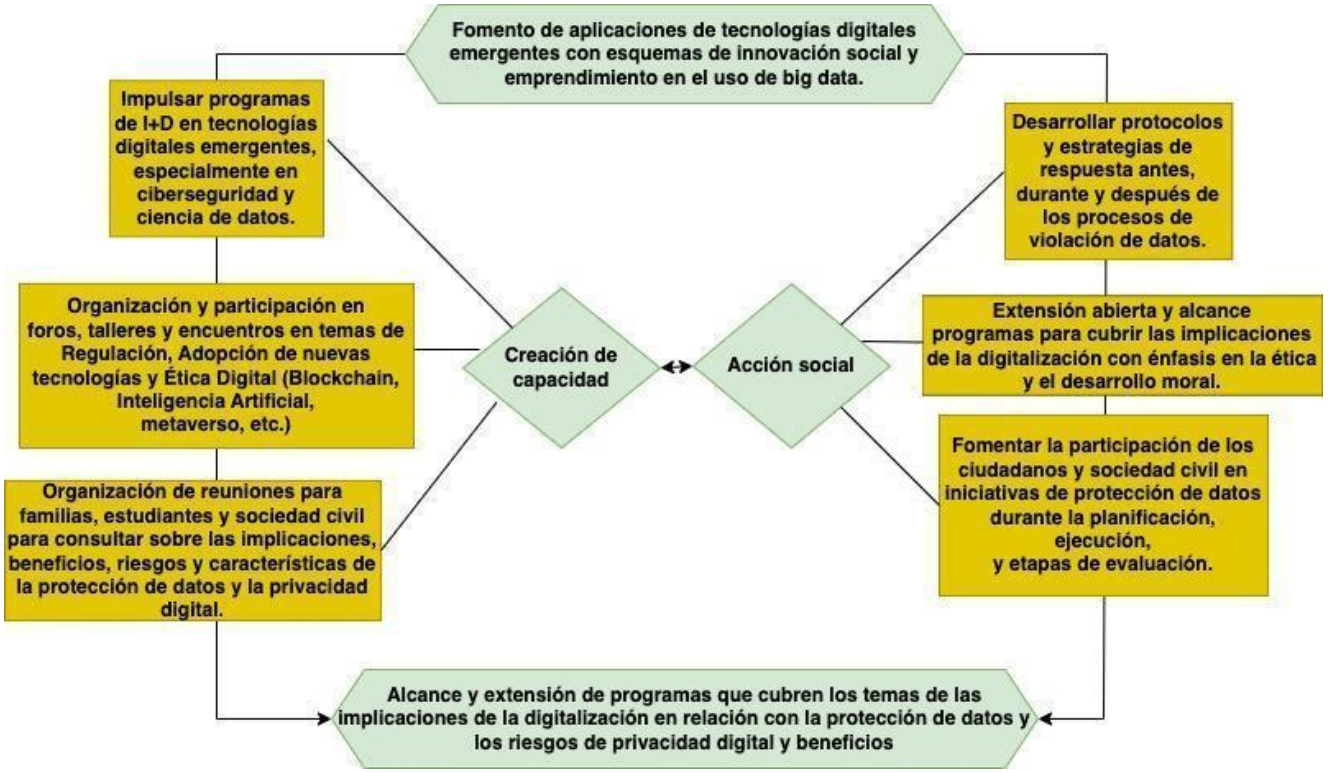
Este trabajo ofrece una modesta propuesta como una contribución que puede dar pie a complementar los resultados obtenidos en diferentes contextos. Es una contribución enfocada en un marco exploratorio para la Universidad Autónoma de Baja California. Desde esta perspectiva, la educación superior debe ser el semillero de creación de capacidades actualizadas a la par de las exigencias del ecosistema digital.

Debe ser, así mismo, el motor de estrategias y acciones que posibiliten que las tecnologías digitales emergentes sean de beneficio y desarrollo integral como vínculos de prosperidad y bienestar social y no solo motivo de entretenimiento, consumo, sujeción económica y herramientas de mercadeo.

La figura 4, muestra la propuesta de un marco exploratorio planteado para contribuir a la reducción de la brecha digital, y a la vez buscar propiciar una cultura de privacidad y protección de datos personales en el entorno educativo.

El marco propuesto, intenta coadyuvar a la construcción de capacidades entre administrativos, académicos y estudiantes, para lograr una adopción tecnológica balanceada que contribuya al mejoramiento del modus operandi universitario y haga frente a los retos de la 4RI (Kergroach, 2017).

Figura 4. Marco exploratorio propuesto



Fuente: Elaboración propia del autor.

La hipótesis planteada al inicio de la investigación, la cual afirma que la comunidad estudiantil universitaria requiere fortalecer su conocimiento y habilidades sobre las implicaciones y relevancia de la privacidad y protección de datos personales, ha sido respaldada por los resultados obtenidos. Se recomienda que la FEyRI, UABC implemente programas y actividades que fomenten una cultura y educación digital en los estudiantes, y

que se difundan los derechos ARCO y otras herramientas de protección y privacidad de datos personales de manera clara y accesible.

Trabajos futuros en este campo podrían incluir la realización de investigaciones adicionales para evaluar la efectividad de los programas y actividades implementados, así como la exploración de nuevas herramientas y estrategias para mejorar la educación y concienciación sobre la protección y privacidad de datos personales en posesión de particulares. También podría ser útil comparar los resultados obtenidos en esta investigación con los de otras instituciones educativas, para determinar si existen diferencias significativas en el nivel de conocimiento de los estudiantes sobre estos temas en diferentes contextos.

La aplicación de la encuesta en otras escuelas y facultades de la Universidad Autónoma de Baja California (UABC) puede adaptarse considerando las particularidades de cada contexto, pero es posible conservar las preguntas relacionadas con el conocimiento sobre privacidad y protección de datos personales, derechos digitales y otros aspectos relevantes. A continuación, se sugieren algunas consideraciones para la aplicación de la encuesta en dichas instituciones:

Adaptación de la encuesta: Se recomienda revisar y adaptar la encuesta original para asegurar que las preguntas sean pertinentes y adecuadas al contexto de la escuela o facultad específica. Es posible mantener las preguntas relacionadas con los derechos digitales, la privacidad y la protección de datos personales, pero se pueden agregar o modificar preguntas según las necesidades y particularidades de cada institución.

Revisión y validación: Antes de aplicar la encuesta en otras escuelas o facultades, es importante realizar una revisión exhaustiva y validar su contenido. Esto implica asegurarse de que las preguntas sean claras, comprensibles y relevantes para los estudiantes de cada institución en particular.

Selección de la muestra: Al igual que en el caso anterior, se debe realizar un proceso de selección de muestra representativa para garantizar la validez de los resultados. Esto implica definir los criterios de selección de los participantes, como el nivel educativo (secundaria, preparatoria, licenciatura, posgrado), la facultad o escuela específica, entre otros.

Comunicación y difusión: Es fundamental establecer canales de comunicación adecuados para informar a los estudiantes sobre la encuesta y fomentar su participación. Esto puede incluir el uso de medios electrónicos como correo electrónico, redes sociales institucionales, sitios web, anuncios en aulas, entre otros. Se debe proporcionar información clara sobre el propósito de la encuesta, su importancia y la confidencialidad de las respuestas.

Aplicación de la encuesta: La metodología de aplicación puede seguir un enfoque similar al descrito anteriormente. Se puede optar por realizar una charla introductoria para contextualizar a los estudiantes sobre el tema y explicar el propósito de la encuesta. Se puede utilizar un enfoque anónimo para garantizar la confidencialidad de las respuestas y evitar influencias externas.

Es importante tener en cuenta que cada escuela o facultad de la UABC puede tener sus propias consideraciones y requisitos específicos. Por lo tanto, es recomendable coordinar con las autoridades y responsables de cada institución para adaptar la metodología de aplicación de la encuesta de acuerdo con las políticas y procedimientos establecidos.

En resumen, la aplicación de la encuesta en otras escuelas y facultades de la UABC implica adaptar el contenido de las preguntas, establecer una comunicación efectiva, garantizar la confidencialidad de las respuestas y seguir una metodología que se ajuste a las particularidades de cada institución.

Es fundamental tener la capacidad de comprender las implicaciones de la privacidad y la importancia de proteger los datos personales para hacer frente a los desafíos de la sociedad digital en constante evolución. Es necesario implementar acciones e iniciativas que conciencien a la población sobre los beneficios, la naturaleza y el impacto de la digitalización en la vida cotidiana de las personas. Al mismo tiempo, se deben desarrollar, implementar y evaluar de manera continua programas educativos y generación de capacidades para mitigar los posibles daños y perjuicios causados por los efectos perniciosos de las tecnologías exponenciales, tal como lo han señalado expertos y académicos en ética de la IA como Cortina (2021), Zuboff (2020), Lee (2019) y Jasanoff (2016).

Finalmente, en el proceso de aclarar e intentar vislumbrar y fijar una postura sobre los límites de la digitalización y el futuro de la sociedad digital, se considera que los aspectos de brecha digital, la protección de datos, privacidad, confidencialidad y certidumbre, son cruciales. De la misma manera, en los aspectos de desarrollo ético y moral, los procedimientos de ciberseguridad, la regulación de Estado y de órganos internacionales, son bastiones fundamentales. En la ausencia de atención adecuada a estos factores, el porvenir de la sociedad digital está en juego. El sector educativo juega un papel clave en el tránsito de la sociedad hacia la 4RI de acuerdo a valores sociales y objetivos en común que buscan vida digna y bienestar en el actual ecosistema digital. (Tegmark, 2018).

Como lo dice Schwab (2016)...

> "Cuanto más pensemos en cómo aprovechar la revolución tecnológica, más nos examinaremos a nosotros mismos y analizaremos los modelos sociales subyacentes que estas tecnologías encarnan y habilitan y tendremos más oportunidades de dar forma a la revolución de una manera que mejore el estado del mundo" (p.13).

Referencias

-Estadísticas - CGSEGE. (n.d.). Cgsege.uabc.mx. http://cgsege.uabc.mx/web/cgsege/estadisticas

-Estadísticas - CGSEGE. (n.d.). Uabc.mx. Retrieved February 02, 2023, from http://cgsege.uabc.mx/web/cgsege/estadisticas

¿Cómo ejercer el derecho al "olvido" en México? (2015, April 28). https://recht.com.mx/ejercer/

Aguilar-Barojas, S., (2005). Fórmulas para el cálculo de la muestra en investigaciones de salud. Salud en Tabasco, 11(1-2), 333-338.

Arnd-Caddigan, M. (2015). Sherry Turkle: Alone Together: Why We Expect More from Technology and Less from Each Other: Basic Books, New York, 2011, 348 pp, ISBN 978-0465031467 (pbk).

Arthur, C. (2013, August 23). Tech giants may be huge, but nothing matches big data. The Guardian; The Guardian. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

Asociación Nacional de Universidades e Instituciones de Educación Superior de Estados Unidos (NASPA). (2021). Navigating the Fourth Industrial Revolution: Implications for Higher Education. NASPA.

Banco Interamericano de Desarrollo (BID). (2019). El futuro del trabajo y la educación en México. BID.

BBVA. (2018, April 17). Kai- Fu Lee, el "rockstar" chino de la IA. BBVA NOTICIAS. https://www.bbva.com/es/kai-fu-lee-rockstar-chino-inteligencia-artificial/

Boroumand, M. R., Esmaeilpour, L., & Khoshkam, M. (2018). Investigating the privacy attitude of Iranian university students towards online social networks. Telematics and Informatics, 35(7), 1963-1976. doi: 10.1016/j.tele.2018.06.002

Buckner, K., Wittmer, D., & Murphy, K. (2018). Digital literacy training and online privacy protection: An evaluation of the use of the teaching privacy curriculum in California public libraries. Journal of Education for Library and Information Science, 59(4), 326-341. doi: 10.3138/jelis.59.4.326

Cámara de Diputados del H. Congreso de la Unión. (2020). Ley Federal de Protección de Datos Personales en Posesión de Particulares. Diario Oficial de la Federación, 12 de julio de 2020. https://www.dof.gob.mx/nota_detalle.php?codigo=5591379&fecha=05/07/2020

Capurro, R. (2000). Perspectivas de una cultura digital en Latinoamérica. Revista de Ciência da Informação, 3(2).

Caro, M. Á. (2015). Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital. Editorial Reus. https://www.torrossa.com/it/resources/an/4402696

Carrillo, M. (2003). El derecho a no ser molestado. Navarra Thomson-Aranzadi, p. 44.

Casa, de A. [@casamerica]. (2021, September 10). IA y Ética. Youtube. https://www.youtube.com/watch?v=Qb0ibq-GMGw&list=PL7nmfM2AAhjg19HiEKuMjp5uIYNJkLc2U&index=33

Castells, M. (2015). Redes de indignación y esperanza. Alianza Editorial.

Cate, F. H. (2019). Privacy and data protection. In D. L. Rhode, C. E. Cohen, & K. D. Aspen (Eds.), The Routledge Handbook of the Public Law of Gender (pp. 145-161). Routledge.

Centro de Investigaciones Sociológicas. (2020). Juventud y Redes Sociales. Madrid: Centro de Investigaciones Sociológicas.

Centro Nacional de Estadísticas Educativas. (2018). Privacidad de los datos de los estudiantes: ¿Cuál es la responsabilidad de las escuelas? Obtenido de https://nces.ed.gov/blogs/nces/post/student-data-privacy-what-is-the-schools-responsibility

Colegio de Tamaulipas. (2022). Política en Red: Acción social y agenda pública en la era digital [Network Politics: Social Action and Public Agenda in the Digital Age]. Retrieved from http://www.coltam.edu.mx/wp-content/uploads/2022/09/politica-en-red.pdf

Comisión Europea. (2021). ¿Qué es la economía digital? https://ec.eu

Comisión Interamericana de Derechos Humanos (CIDH). (2019). Informe sobre el impacto de internet en el ejercicio de los derechos humanos. Recuperado de https://www.oas.org/es/cidh/informes/pdfs/ImpactointernetDH.pdf

Comisión Nacional de los Derechos Humanos. (2015). Recomendaciones generales sobre protección de datos personales. https://www.cndh.org.mx/sites/default/files/doc/Estudios/2015/Estudio_proteccion_datos_personales.pdf

Competencias digitales México 2022. (2022). Www.metared.org. Retrieved February 23, 2023, from https://www.metared.org/mx/competencias_digitales_mexico_2022.html

Cortina Orts, A. (2019). Ética de la Inteligencia Artificial. In Anales de la Real Academia de Ciencias Morales y Políticas (pp. 379-394). Ministerio de Justicia.

Cortina, A. (2021,Septiembre 23). "Ética de la Inteligencia Artificial." [Video] Youtube. https://www.youtube.com/watch?v=S4qIQd8wqnk&t=1s

Cortina, A. (2022). Los desafíos éticos del transhumanismo. Pensamiento. Revista de Investigación e Información Filosófica, 78(298 S. Esp), 471-483.

De Hert, P., Papakonstantinou, V., & Schaar, P. (2018). Fundamentals of EU data protection law. Springer.

de Prensa UV, D. (n.d.). UV, primera en integrarse a la Iniciativa de Contrataciones Abiertas en el país. Universo - Sistema de noticias de la UV. Retrieved January 20, 2023, from https://www.uv.mx/prensa/banner/uv-primera-en-integrarse-a-la-iniciativa-de-contrataciones-abiertas-en-el-pais/

Deloitte. (2019). The Industry 4.0 paradox: Overcoming disconnected data in a connected world.

Departamento de Educación de los Estados Unidos. (2019). Proteger la privacidad de los estudiantes. Obtenido de https://www.ed.gov/student-privacy

Diario Oficial de la Federación (2013). Norma Oficial Mexicana NOM-024-SSA3-2013, "Sistema Nacional de Vigilancia Epidemiológica". Recuperado de http://www.salud.gob.mx/unidades/cdi/nom/compi/ssa3_noms_024.html

Diario Oficial de la Federación. (2019). Decreto por el que se crea el Consejo de la Estrategia Digital Nacional. Diario Oficial de la Federación, 28 de diciembre de 2019. https://www.dof.gob.mx/nota_detalle.php?codigo=5580136&fecha=28/12/2019

Drummond, V. (2004). internet, privacidad y datos personales. Editorial Reus.

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin 's Press

European University Association (EUA). (2018). EUA trends 2018: Learning and teaching in the European higher education area.

Ford, M. (2015). Rise of the Robots: Technology and the Threat of a Jobless Future. Basic Books.

Foresight and STI Governance, 11(4), 6-8. https://doi.org/10.17323/2500-2597.2017.4.6.8.

Foro Económico Mundial. (2019). Platforms and Ecosystems: Enabling the Digital Economy. https://www.weforum.org/reports/platforms-and-ecosystems-enabling-the-digital-economy

Foro Económico Mundial. (2020). The Future of Jobs Report 2020. World Economic Forum.

Fuentes, M. C. (2023, February 15). Robo sigiloso en 2023: así sustraen nuestros datos sin que nos demos cuenta. La Tercera. https://www.latercera.com/piensa-digital/noticia/robo-sigiloso-en-2023-asi-sustraen-nuestros-datos-sin-que-nos-demos-cuenta/WQ3WC6V7BNCMJPVEBYHFYRWO5I/

García Macías, J. A. (2019). Composición de políticas basada en el contexto de uso de datos. Ingeniería, Investigación y Tecnología, 20(1), 1-10.

German Politician Wins Battle for Cellphone Data" - The New York Times (2013): https://www.nytimes.com/2013/02/28/technology/german-politician-wins-battle-for-cellphone-data.html

González Guerrero, L. D. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. Estudios Socio-Jurídicos, 21(1), 209-244.

Gutiérrez-Maldonado, V. M., & Reyes-López, S. (2021). La economía de los datos en la educación superior mexicana: una revisión crítica. Revista de la Educación Superior, 50(198), 1-20.

Hernández-Fuentes, J. L., & Ortiz-López, J. J. (2020). La educación superior ante los desafíos de la Cuarta Revolución Industrial: reflexiones desde la perspectiva de la ética y la responsabilidad social. Revista Mexicana de Investigación Educativa, 25(85), 73-93.
https://www.cide.edu/wp-content/uploads/2021/03/LFPDPPP-Comentada_digital.pdf

INEGI (2019). Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en Hogares (MODUTIH). Recuperado de https://www.inegi.org.mx/programas/modutih/2019/default.html

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, & Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California. (2021). Informe sobre la situación que

guarda el derecho de acceso a la información y la protección de datos personales en el Estado de Baja California. Recuperado de https://www.inai.org.mx/sites/default/files/2021-03/Informe_Situacion_Baja_California_2020.pdf

Instituto Tecnológico de Tijuana (ITT). (2022). Maestría en Ingeniería en Sistemas de Manufactura.

Jackson, T. (2016). Prosperity without growth: Foundations for the economy of tomorrow. Routledge.

Jara, C. A., Fernandez-Llatas, C., & Ibanez-Sanchez, G. (2018). The role of Industry 4.0 in the education of the future. International Journal of Advanced Computer Science and Applications, 9(1), 239-246.

Jarosz, S., Soltysik, M., & Zakrzewska, M. (2020). The fourth industrial revolution in the light of social and competence changes.

Johnson, K. (2017). Big Data's Impact on Privacy, Security and Consumer Welfare. European Journal of Law and Technology, 8(2), 1-18.

Kalaitzidis, T. J., & Lian, J. W. (2019). Industry 4.0 and the Digital Transformation of Higher Education. In Proceedings of the 7th International Conference on Information Technology and Science (pp. 1-6).

Kang, H., & Stein, J. (2019). University students' knowledge, attitudes, and behaviors on digital citizenship. Education and Information Technologies, 24(5), 2707-2721. doi: 10.1007/s10639-019-09895-8

Kaspersky. (2019). Global privacy report. Recuperado de https://www.kaspersky.com/blog/global-privacy-report/24221/

Kergroach, S. 2017. Industria 4.0: Nuevos retos y oportunidades para el mercado laboral.

Kernaghan, K. (2019). The importance of digital literacy and the protection of privacy rights.

Information Management Journal, 53(6), 22-27. https://doi.org/10.1177/0894439319886096

Klaus Schwab. (2016). The Fourth Industrial Revolution. World Economic Forum.

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Cyberbullying: Bullying in the digital age. John Wiley & Sons.

Lee, S. (Producer & Director). (2020). Code for bias [Streaming service]. Retrieved from https://www.netflix.com/watch/81437323

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, art. 37 (2020).

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (n.d.). Www.diputados.gob.mx. https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017). Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5480033&fecha=26/01/2017

Li, X., Huang, D., Sung, M., & Zhang, X. (2016). Privacy risks and benefits of mobile location-based services. Information Systems Frontiers, 18(2), 291-307.

Linares, A. M., Nava-Fernández, M., & Aguirre-Castro, L. A. (2018). La 4RI y la formación de profesionistas en la educación superior. Revista Iberoamericana de Educación Superior, 9(26), 38-59.

Locke, M. (2021, May 15). Data isn’t oil, so what is it? Howtomeasureghosts.substack.com. https://howtomeasureghosts.substack.com/p/data-isnt-oil-so-what-is-it

Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. Pew Research Center.

Mañas, J. L. P., Ornelas Núñez, L. y. S. L. A., de Marcos, I. D. F., Mariscal, J. P., Lujambio Irazábal, A. y. L. O. N., Ornelas Núñez, L. y. E. M. R., Navarrete, J. R., & Xopa, J. R. (2010).

Malte Spitz's six-month journey with his mobile phone data" - The Guardian (2011): https://www.theguardian.com/world/interactive/2011/apr/01/mobile-phone-data-malte-spitz

Protección de datos personales. México: Tiro Corto Editores. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/31.pdf

Maqueo Ramírez, María Solange, Moreno González, Jimena, & Recio Gayo, Miguel. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de derecho (Valdivia), 30(1), 77-96. https://dx.doi.org/10.4067/S0718-09502017000100004

Martínez Devia, A. (2019). La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. Rev. Prop. Inmaterial, 27, 5.

McKinsey Global Institute. (2019). The age of analytics: Competing in a data-driven world. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world

Miguel de Bustos, J. C., & Izquierdo-Castillo, J. (2019). ¿ Quién controlará la Comunicación? El impacto de los GAFAM sobre las industrias mediáticas en el entorno de la economía digital.

National Center for Education Statistics. (1997). Projections of Education Statistics to 2006 (NCES 97-949) [PDF file]. Retrieved from https://nces.ed.gov/pubs97/97949.pdf

Nations, U. (2016). Human Rights in the Digital Age. Recuperado de https://www.ohchr.org/Documents/Issues/DigitalAge/DigitalAgeReport.pdf

Naughton, J. (2021, May 29). Data isn't oil, whatever tech commentators tell you: it's people's lives | John Naughton. The Guardian. https://www.theguardian.com/commentisfree/2021/may/29/data-oil-metaphor-tech-companies-surveillance-capitalism

OCDE. (2019). La economía digital en transformación: Una oportunidad y un desafío. https://www.oecd.org/internet/la-economia-digital-en-transformacion-esp.pdf

Office of the High Commissioner for Human Rights. (2014). The right to privacy in the digital age. Recuperado de https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session27/A.HRC.27.37_en.pdf

OpenAI. (2022, November 30). ChatGPT: Optimizing language models for dialogue. OpenAI. https://openai.com/blog/chatgpt/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2015). Repensando la educación: ¿Hacia un bien común global? Obtenido de https://unesdoc.unesco.org/ark:/48223/pf0000232417

Organización para la Cooperación y el Desarrollo Económico. (2015). Privacy Online: OECD Guidance on Policy and Practice. París: Organización para la Cooperación y el Desarrollo Económico.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2018). La La Cuarta Revolución Industria y el futuro del trabajo en México. OCDE.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2019). Education in the Digital Age: Policy Brief. OCDE.

Orozco, J. F. (2019). La Cuarta Revolución Industrial: Desafíos y oportunidades en la educación superior. Comunicar, 27(60), 9-18. https://doi.org/10.3916/C60-2019-01

Pérez-Montoro, M., & Minguillón, J. (2016). Los jóvenes y la privacidad en internet: Comportamientos, actitudes y educación. El profesional de la información, 25(4), 619-626. doi: 10.3145/epi.2016.jul.08

Piñar Mañas, J. L. (2010). "¿Existe privacidad?", en Protección de Datos Personales. Compendio de Lecturas y Legislación.

Ponce-López, J.L., Vicario-Solórzano, C.M. & López-Valencia, F. (Coords.). (2021). Competencias Digitales Docentes Metared México, estudio 2021. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.

Prescencion, A. (2022, May 22). INSTALAN RED ESTATAL DE DATOS ABIERTOS EN BC. ItaipBC; Instituto de Transparencia Baja California. https://www.itaipbc.org.mx/itaipBC-2019/instalan-red-estatal-de-datos-abiertos-en-bc/

Presidencia de la República. (2020). Programa de Cultura Ciudadana Digital. https://www.gob.mx/estrategia-digital-nacional/acciones-y-programas/programa-de-cultura-ciudadana-digital

PwC. (2018). Higher education in the digital age. PwC.

Ramírez-Alvarez, M., Rodríguez-Gómez, G., & Vázquez-Cano, E. (2020). ¿Cómo protegen los usuarios sus datos personales en redes sociales? Un estudio de caso en México. El profesional de la información, 29(4), e290401. https://doi.org/10.3145/epi.2020.jul.01

Rabelo Ramírez, J. (2018). Política digital y gobernanza en México. Revista Mexicana de Política Digital, 7(1), 4-21.

Raworth, K. (2017). Doughnut economics: seven ways to think like a 21st-century economist. Chelsea Green Publishing.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (2011, December 21). Www.ordenjuridico.gob.mx. http://www.ordenjuridico.gob.mx/Documentos/Federal/html/wo88475.html

Reglamento de Protección de Datos Personales de la Universidad de Guadalajara. (2018).

Romo-Rodríguez, J. M., & García-Rodríguez, R. (2019). Los desafíos de la Cuarta Revolución Industrial en la educación superior mexicana. Revista de Investigación Académica, 17, e278.

Rosen, L. D., Whaling, K., Rab, S., Carrier, L. M., & Cheever, N. A. (2013). Is Facebook creating "iDisorders"? The link between clinical symptoms of psychiatric disorders and technology use, attitudes and anxiety. Computers in Human Behavior, 29(3), 1243-1254.

Sánchez-García, J. A., & Rojas-López, M. (2018). La 4RI y su impacto en la educación superior en México. Revista Internacional de Investigación en Educación, 11(1), 1-10.

Sánchez, M. A. G. (2020). La protección de datos personales en México: cambios evolutivos a 10 años de su inclusión a nivel constitucional. Revista Mexicana de Ciencias Penales, 3(10), 47-58.

Sánchez, M. A. G. (2020). La protección de datos personales en México: cambios evolutivos a 10 años de su inclusión a nivel constitucional. Revista Mexicana de Ciencias Penales, 3(10), 47-58.

Schneier B. (2015). Secrets and lies : digital security in a networked world (15th Anniversary). John Wiley & Sons.

Schneier, B. (2018). Click here to kill everybody: Security and survival in a hyper-connected world. WW Norton & Company.

Schwab, K. (2016). La Cuarta Revolución Industrial. Barcelona: Penguin Random House.

Secretaría de Economía. (2010). Ley federal de protección de datos personales en posesión de particulares. Diario Oficial de la Federación, 6 de julio de 2010. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5149607&fecha=05/07/2010

Secretaría de Educación Pública (SEP). (2018). Plan Nacional de Desarrollo 2018-2024. Gobierno de México.

Secretaría de Educación Pública (SEP). (2020). Tecnologías emergentes en educación superior: desafíos y oportunidades para México. Gobierno de México.

Secretaría de Educación Pública. (2020). Estrategia Digital Nacional para la Educación. https://www.gob.mx/sep/acciones-y-programas/estrategia-digital-nacional-para-la-educacion

Secretaría de Gobernación (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Serrano-Santoyo, A. (2016). El proceso de convergencia digital: una propuesta estratégica para promover su adopción. Comunicación y Sociedad, (26), 155-184.

Serrano Santoyo, A. (2018). Retos de la protección de datos personales en México. Cuadernos de información, 43, 47-60.

Shariff, S. (2009). Confronting Cyber-Bullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences. Cambridge University Press. 32 Avenue of the Americas, New York, NY 10013.

Silva-Ayala, D., Valencia-García, R., & Padilla-Meléndez, A. (2019). Competencias en la educación superior ante la Cuarta Revolución Industrial. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (E25), 236-249.

Sociedad Internacional para la Tecnología en la Educación. (2017). Estándares ISTE para estudiantes. Obtenido de https://www.iste.org/standards/for-students

Solove, D. J. (2008). Understanding privacy.

Sujetos obligados. (n.d.). Gob.mx. Retrieved January 25, 2023, from https://edomex.gob.mx/sujetos_obligados

Tapscott, D., & Osorio, M. B. (1997). La economía digital. Bogotá: McGraw-Hill.

Tegmark, M. (2018). Vida 3.0. Taurus.

The Importance of Malte Spitz's Data" - The New Yorker (2013): https://www.newyorker.com/news/news-desk/the-importance-of-malte-spitzs-data

Tenorio Cueto, G. A. (2019). Ley Federal de Protección de Datos Personales en Posesión de los Particulares, comentada.

Tenorio Cueto, G. A. (2021). El derecho a una vida libre de algoritmos. Revista IUS, 15(48), 115-135.

Tenorio, G. A. (2019). Ley Federal De Protección De Datos Personales En Posesión De Los Particulares, Comentada. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

UABC. (2022). Ingeniería en Ciencias de Datos. Recuperado el 2 de mayo de 2023, de https://www.uabc.mx/ingenieria-en-ciencias-de-datos

UNCTAD. (2019). The Digital Economy Report 2019. https://unctad.org/system/files/official-document/der2019_en.pdf

UNCTAD. (2020). World Trade Report 2020. https://unctad.org/system/files/official-document/wir2020_en.pdf

UNESCO. (2020). Educación en derechos digitales: Guía para la formación de formadores. https://unesdoc.unesco.org/ark:/48223/pf0000373991

Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Unión Internacional de Telecomunicaciones (2017). Medición de la Sociedad de la Información y el Conocimiento. Recuperado de https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2017-PDF-E.pdf

Vakulenko, E., Golubtsov, S., & Stepanova, E. (2021). Digital privacy awareness in Russia and Ukraine. Telematics and Informatics, 58, 101529. doi: 10.1016/j.tele.2020.101529

Vega-Rivera, S., & Martínez-Rodríguez, L. (2020). La formación en habilidades digitales ante la Cuarta Revolución Industrial en el ámbito universitario de Baja California, México.

En Congreso Internacional de Innovación y Tecnología Educativa (CIITE) (pp. 59-65). Universidad Nacional Autónoma de México.

Yudkowsky, E. (2007). The hidden complexity of wishes. Retrieved from Less Wrong: http://lesswrong. com/lw/ld/the_hidden_complexity_of_wishes.

ANEXOS

Preguntas de encuesta para el diagnóstico del nivel de conocimiento sobre los derechos ARCO y la privacidad y protección de datos en los estudiantes universitarios de FEyRI UABC

Este cuestionario se aplicará en *Google Forms*, será por bloques temáticos en el contexto de Privacidad y Protección de Datos Personales, consta de 28 preguntas, cuatro preguntas por bloque, de opción múltiple; sucesivamente, la respuesta Si, será en la categoría de "informado", la respuesta NO, sera "no informado" y la respuesta Tal vez, será "poco informado"; en la respuesta de control (opcional) solo se tomara la opción correcta y será "informado"

Bloque 1	Bloque 2	Bloque 3	Bloque 4	Bloque 5	Bloque 6	Bloque 7
Ética	Derechos Humanos Digitales	Regulación	Seguridad de Datos	Protección y Privacidad	Generación de capacidades	Adaptación Tecnológica

#	Preguntas	Bloque
1	Puede ser que las aplicaciones digitales son un beneficio para tu vida diaria, ¿conoces la forma en como ellas recuperan su inversión o la manera de generar beneficios de estas plataformas?	B1
2	Las aplicaciones que has utilizado, ¿han solicitado tu consentimiento para el manejo de tus datos personales?	B1
3	¿Es relevante saber la cantidad de información que proporcionas voluntariamente o involuntariamente a las plataformas digitales?	B1
4	De las siguientes opciones ¿Cual es un problema ético que pudiera enfrentar la sociedad en la era digital? a) Ciberacoso b) Abandono c) Uso de credenciales	**B1**
5	¿Los derechos digitales sobre tus datos personales son parte de los derechos humanos?	B2
6	¿Es necesario saber si las apps están usando tu geolocalización?	B2
7	¿Es un derecho a tus datos personales el acto de recibir un aviso de	B2

	privacidad por parte de las plataformas, instituciones u organismos que te soliciten ingresar tus datos?	
8	¿Cuál de estas opciones es la correcta nomenclatura de los derechos ARCO? a) Acción, Rectificación, Corrección, y Objeción. **b) Acceso, Rectificación, Cancelación y Oposición.** c) Acceso, Registro, Contraposición, y Obstaculización.	**B2**
9	¿El Instituto de Transparencia, Acceso a la Información Pública de Baja California, es el órgano que se encarga de atender tus derechos digitales?	B3
10	Tu expediente clínico, ¿es un dato personal?	B3
11	Según tu conocimiento respecto a los datos personales ¿Los menores de edad, son titulares de sus datos personales?	B3
12	¿Cual de estas es la ley que protege tu privacidad de tus datos personales? a) Ley Federal de Transparencia y Acceso a la Información Pública. **b) Ley Federal de Protección de Datos Personales en Posesión de los Particulares.** c) Ley General de Protección de Datos Personales en posesión de sujetos obligados.	**B3**
13	De acuerdo a tu experiencia como estudiante de la UABC ¿Consideras que la institución académica se rige bajo los derechos de privacidad?	B4
14	¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda?	B4
15	¿Te han *hackeado* tu correo institucional o de *Blackboard* UABC?	B4
16	¿Conoces el departamento de la universidad que te de asesoría sobre tus derechos digitales en caso de ser necesario asistir por ayuda? Cual de estas opciones es el departamento correcto a) Departamento de informática y bibliotecas UABC. **b) Unidad de Transparencia y Acceso a la Información Pública de la UABC.** c) Unidad de Transparencia y Acceso a la Información Pública.	**B4**
17	¿Es diferente la privacidad de la protección?	B5
18	¿Has firmado alguna vez algún aviso de protección y privacidad de datos en tu institución?	B5
19	¿Conoces las responsabilidades de las instituciones académicas con el manejo de tus datos personales?	B5
20	¿Qué es privacidad? a) Referente a los datos personales, trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no.	**B5**

	b) **Referente a los datos personales, significa la capacidad de una persona para determinar por sí misma cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal.** c) Se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información.	
21	¿Has recibido algún tipo de capacitación o curso informativo sobre tus derechos digitales en tu facultad?	B6
22	¿Te han enseñado temas referentes a tus derechos digitales dentro de tu programa de estudio?	B6
23	¿Has tomado algún curso o capacitación sobre tecnología y/o sus implicaciones?	B6
24	¿Qué temas, de estas opciones, son sobre la privacidad y protección de tus derechos digitales a tus datos personales? a) Instituciones y la regulación de tus derechos. **b) Ciberseguridad y protección de datos personales.** c) Avisos de privacidad de los sujetos obligados	**B6**
25	¿Podrías identificar alguna implicación del uso de tus datos personales tomados sin tu consentimiento?	B7
26	¿Has creído en alguna fake new?	B7
27	¿Utilizas aplicaciones para automatizar tus tareas diarias?	B7
28	¿Podrías identificar de las siguientes opciones alguna implicación del uso de tus datos personales tomados sin tu consentimiento? **a) Teclear tu nombre en el buscador de internet, y que aparezca en una lista de asistencia de alguna clase.** b) La publicación de tu matrícula en una carta de aceptación. c) Una foto tuya en la publicación de alguien más.	**B7**