Estrategias para la mitigación de la exposición de datos personales de estudiantes universitarios en Bogotá en el contexto del internet de las personas

Yulian Savino Fonseca Cortés

Asesora

Jenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Resumen

En la era digital actual, la interacción de los estudiantes de educación superior en los entornos digitales ha aumentado considerablemente, sobre todo por la migración a la virtualidad, conectividad y el uso de diversas plataformas como redes sociales, foros, juegos, servicios en línea, entre otros. Sin embargo, al estar más interconectados, se presentan e incrementan a diario riesgos cibernéticos, como, por ejemplo, el robo de identidad, el uso indebido de datos y el acoso digital. A pesar de la existencia de normativas como la Ley 1581 de 2012 en Colombia, la falta de conocimiento sobre estas regulaciones y la escasa adopción de prácticas seguras incrementan la vulnerabilidad de este grupo poblacional.

Esta monografía tiene como objetivo proponer estrategias para mitigar la exposición de datos personales de estudiantes universitarios en la ciudad de Bogotá D.C. en el contexto del Internet de las Personas. Para ello, se identifican los riesgos inherentes a la interacción digital, adicionalmente, se evalúa la percepción y conciencia de los estudiantes frente a temas de privacidad en entornos digitales y se analiza el aporte de algunos marcos legales tanto nacionales e internacionales. Con base en estos análisis, se diseñan recomendaciones para fomentar una cultura de protección de datos, destacando la necesidad de un enfoque integral que promueva la seguridad en entornos digitales, fortaleciendo la privacidad y la seguridad en un entorno cada vez más interconectado.

Palabras clave: Datos personales, internet de las personas, protección de datos, entornos digitales, privacidad.

Abstract

In today's digital age, the interaction of higher education students in digital environments has increased, especially due to the migration to virtuality, connectivity, and the use of various platforms such as social networks, forums, games, online services, among others. However, as we become more interconnected, cyber risks, such as identity theft, data misuse and digital abuse increase daily. Despite the existence of regulations such as Law 1581 of 2012 in Colombia, the lack of knowledge about these regulations and the poor adoption of safe practices increases the vulnerability of this population group.

This monograph aims to propose strategies to mitigate the exposure of personal data of university students in the city of Bogotá D.C. in the context of the Internet of People. To this purpose, the risks inherent to digital interaction are identified, additionally, the perception and awareness of students regarding privacy issues in digital environments is evaluated and the contribution of some national and international legal frameworks is analyzed. Based on these analyses, recommendations are designed to foster a culture of data protection, highlighting the need for a comprehensive approach that promotes security in digital environments, strengthening privacy and security in an increasingly interconnected environment.

Keywords: Personal data, internet of people, data protection, digital environments, privacy.

Tabla de Contenido

Lista de Tablas

Lista de Ilustraciones

Lista de Apéndices

Glosario

Datos personales: Información que identifica o puede identificar a una persona natural, como nombre, correo electrónico, número de documento, ubicación, entre otros.

Privacidad: Derecho de los individuos a controlar cuándo, cómo y en qué medida se recopila, usa y comparte su información personal.

Internet de las Personas (IoP): Extensión del internet que se enfoca en la conectividad entre individuos y plataformas digitales mediante la recopilación, análisis y uso intensivo de datos personales.

Riesgo: Posibilidad de que una amenaza o vulnerabilidad se materialice y cause un impacto negativo en la información o los sistemas.

Vulnerabilidad: Debilidad en un sistema, procedimiento o comportamiento que puede ser explotada por una amenaza para comprometer la seguridad de los datos.

Amenaza: Evento potencial (como un ataque cibernético, ingeniería social o malware) que puede comprometer la seguridad o privacidad de los datos personales.

Ciberacoso: Forma de acoso o intimidación que se produce a través de medios digitales, afectando la integridad, reputación o bienestar de la persona.

Phishing: Técnica de ingeniería social que busca engañar al usuario para obtener sus datos personales o credenciales a través de correos o sitios falsos.

Entornos digitales: Espacios en línea, como redes sociales, aulas virtuales, sistemas académicos o herramientas colaborativas, que requieren interacción activa y muchas veces almacenamiento de datos personales.

Introducción

En el contexto actual de creciente digitalización, el Internet de las Personas ha transformado la forma en la que los individuos interactúan, acceden a servicios, comparten información y construyen vínculos personales, académicos y profesionales. Como parte de esta transformación, están cada vez más inmersos en plataformas digitales que demandan una constante provisión de datos personales. Esta situación, aunque facilita la inmediatez y personalización de los servicios, también expone a los usuarios a riesgos considerables asociados a la privacidad, la seguridad de la información y el uso indebido de los datos.

En este escenario, la protección de los datos personales se convierte en un desafío crítico, no solo desde lo técnico y legal sino también desde lo educativo. Pese a la existencia de normativas nacionales y estándares internacionales, gran parte de los usuarios, especialmente los estudiantes universitarios, desconocen sus derechos, las implicaciones de sus decisiones digitales y los mecanismos para mitigar la exposición innecesaria de información.

Esta monografía se enfoca en identificar riesgos, analizar el nivel de concientización y diseñar estrategias educativas, normativas y tecnológicas que contribuyan a reducir la exposición de datos personales en los entornos digitales por parte de estudiantes universitarios. El propósito es brindar herramientas prácticas que fomenten un uso más responsable, ético y seguro de las plataformas digitales en el marco del Internet de las Personas.

Planteamiento del Problema

En la actualidad, la conectividad ha avanzado significativamente, especialmente tras la pandemia del COVID-19, transformando la forma en que las personas interactúan en los nuevos entornos digitales, permitiendo establecer vínculos comunicativos, de aprendizaje y con intereses comunes. Sin embargo, esta conexión también implica riesgos, ya que, para formar parte de esta red, se requiere compartir información personal, lo que puede llevar a que dicha información sea utilizada indebidamente por los ciberdelincuentes (Yocupicio Sanay, 2020). En Bogotá D.C., los estudiantes universitarios constituyen un grupo altamente activo e interconectado en plataformas digitales y redes sociales, lo que los hace especialmente vulnerables a riesgos como suplantación de identidad, robo de datos e incluso acoso digital (Bartolomé, 2021).

En Colombia, la protección de los datos personales ha ganado mucha relevancia y a su vez, ha sido implementada a todos los sectores empresariales (Cabezas, 2023) por medio de leyes como la ley 1581 de 2012 de proyección de datos personales, la ley 1266 del 2008 de Habeas Data y otras disposiciones para sectores o servicios en específico (Barrera, 2024); sin embargo, fueron diseñadas para las necesidades de las fechas en que fueron puestas en vigencia y disponen de lineamientos no tan fáciles de entender para los jóvenes, así mismo, existe una débil cultura de concientización digital frente a la privacidad, especialmente en lo que respecta al manejo de la información en plataformas digitales.

Esta problemática se acentúa en el entorno universitario en donde los estudiantes están en la etapa de formación superior, generación del conocimiento y pensamiento crítico, por otra parte, las instituciones de educación superior generan un ambiente más conectado y en línea adquiriendo nuevas plataformas, herramientas y avances tecnológicos con el fin de estar a la vanguardia, obtener la atención de sus estudiantes y mantener una cultura de desarrollo; sin

embargo, las instituciones no cuentan con planes o campañas para generar una cultura de seguridad y privacidad de la información personal. Así mismo, la necesidad de inmediatez, la búsqueda constante de la innovación y la familiaridad con la tecnología han hecho que los jóvenes normalicen la exposición de su información personal sin establecer filtros de seguridad o sin conocer las posibles consecuencias. Según Hernández (Hernández, 2018), los jóvenes, al construir su identidad digital, se enfrentan a múltiples dimensiones de privacidad como la informacional, la psicológica y la relacional que pueden resultar comprometidas si no se ejecuta una adecuada gestión de los datos personales.

Teniendo en cuenta la problemática, se plantea la siguiente pregunta: ¿Cómo afecta la baja concienciación sobre la privacidad de los datos personales a la seguridad digital de los estudiantes universitarios en entornos digitales, y qué estrategias pueden diseñarse para mitigar los riesgos de exposición en el contexto del Internet de las Personas?

Justificación

Los estudiantes universitarios, en su constante interacción con plataformas en línea para actividades académicas, laborales y de ocio, comparten grandes cantidades de información personal de forma inconsciente con el fin de crear entornos para el desarrollo de nuevas formas de comunicación, aprendizaje y colaboración. Sin embargo, esta expansión también ha traído consigo riesgos y retos considerables relacionados con la privacidad y seguridad de los datos (Vera Navas, 2021).

Aunque en Colombia existen normas como la Ley 1581 de 2012 para la protección de datos, su alcance es limitado debido al desconocimiento generalizado entre los jóvenes sobre sus derechos digitales y las medidas de autoprotección. Esta falta de concienciación, unida a la creciente dependencia de tecnologías interconectadas (De la Rosa Rodríguez, 2021), incrementa significativamente su vulnerabilidad ante riesgos como la suplantación de identidad, el ciberacoso o la fuga de información.

Ante este panorama, es fundamental comprender cómo la escasa alfabetización digital y la baja percepción del riesgo afectan la privacidad y seguridad de los estudiantes . Esta investigación busca aportar soluciones prácticas y efectivas, mediante la formulación de estrategias integrales que mitiguen la exposición de datos personales en el IoP.

Objetivos

Objetivo General

Proponer estrategias para mitigar la exposición de datos personales de estudiantes universitarios en los entornos digitales, mediante una revisión sistémica y un análisis de riesgos derivados del internet de las personas.

Objetivos Específicos

Identificar los riesgos derivados al internet de las personas que enfrentan los estudiantes universitarios en los entornos digitales.

Determinar el nivel actual de concientización y las prácticas de protección de datos en estudiantes universitarios en Bogotá D.C.

Analizar las contribuciones de leyes y normativas nacionales e internacionales frente a la protección de datos personales en los entornos digitales.

Diseñar estrategias integrales orientadas a mitigar la exposición de datos personales de estudiantes universitarios en entornos digitales.

Marco Conceptual

Internet de las Personas

El internet de las personas busca la interconexión entre las personas usando su información a través de los dispositivos o a través del internet de las cosas (Armayones Ruiz, 2015). Esta información entregada favorece a que los dispositivos y plataformas puedan predecir nuestros comportamientos, darnos información sobre nuestro estado de salud (Guirado, 2020), recomendarnos personas que tengan intereses en común o hasta incluso, dar recomendaciones de trabajo.

Datos Personales

Es toda la información asociada a una persona y que la hace única frente a las demás como individuo. Esta identificación única permite a la persona poder interactuar con las demás en una sociedad. Los datos de dicha persona se clasifican a partir de la aceptabilidad de divulgación (García González, 2007):

- Público: Pueden ser compartidos libremente determinados por la constitución política.
- Semiprivado: Son datos que pueden interesar a un cierto grupo de personas.
- Privado: Datos que son relevantes únicamente para su dueño.
- Sensible: Datos que afectan a la intimidad y reputación del dueño y su exposición indebida puede generar discriminación(Congreso de Colombia, 2022).

Entornos Digitales

Son espacios en internet, en donde se pueden desarrollar todo tipo de actividades de interacción entre múltiples personas con múltiples fines como el aprendizaje, la creación de contenido (Medina Orozco, 2022), oferta de productos y servicios, entre otros. Para la creación

de estos espacios es necesaria la conectividad, los participantes y la información a compartir o transmitir.

Riesgos

Definen todas aquellas acciones que impliquen una consecuencia negativa o que afecten la integridad de una persona (Yocupicio Sanay, 2020). Del lado digital o cibernético, los riesgos pueden ser acciones o circunstancias que afecten la integridad de una persona o de su información (Vida Fernández, 2022). Algunos riesgos pueden ser: Entrar a páginas de origen sospechoso, el contacto con desconocidos, el uso indebido de la información, opiniones o comentarios que afecten a una persona psicológicamente, entre otros.

Gestión de Riesgos Digitales

La gestión de riesgos en el contexto de la seguridad digital es el proceso sistemático de identificar, analizar, evaluar, tratar y monitorear los riesgos (MINTIC, 2021) que puedan comprometer la confidencialidad, integridad o disponibilidad de la información. Para ejecutarlo, se usan herramientas y metodologías que permiten reducir la probabilidad de amenazas y minimizar su impacto, lo que facilita la toma de decisiones que permiten proteger la información (MINTIC, 2021).

Privacidad

Es un derecho fundamental en donde las personas deciden qué datos pueden ser adquiridos libremente (M. R. Martínez & Pincay-Ponce, 2024) o, en otras palabras, pueden ser de acceso público y pueden ser usados de cualquier forma. La privacidad de los datos va determinada según su aceptabilidad de exposición, estos son, públicos, semiprivados, privados y sensibles (Congreso de Colombia, 2022). Por lo que, si un dato compromete o vulnera a una persona en cualquier sentido, se considera como una violación a la privacidad.

Suplantación de Identidad

Es el acto de hacerse pasar por otra persona, utilizando su información personal, como nombres, contraseñas, documentos o imágenes, con fines maliciosos y para obtener beneficios ilegítimos o causar daño (SIC, 2022). En los entornos digitales, esta práctica es común en fraudes electrónicos, estafas en redes sociales y accesos no autorizados a cuentas, y representa una amenaza directa a la seguridad y privacidad de los usuarios.

Ciberacoso

El ciberacoso es una forma de violencia digital en la que una persona o grupo utiliza medios electrónicos como redes sociales, correo, foros o mensajería instantánea para hostigar, intimidar, humillar o amenazar (Unicef, 2025) de manera repetida o frecuente a otra persona. Esto genera consecuencias graves que afectan la salud mental, la reputación y la seguridad de las víctimas (Unicef, 2025), por lo que, requiere tanto de una intervención educativa como jurídica .

Inteligencia Artificial

Consiste en una tecnología, la cual se destaca por simular a la inteligencia humana y su capacidad para la resolución de problemas (Murrugarra Retamozo, 2024), esto debido a que, es capaz de aprender de la información que se le proporciona para funcionar, a este proceso se le llama inteligencia generativa. En la actualidad, la IA generativa es capaz de aprender no solo el lenguaje humano, sino que también otro tipo de datos como imágenes, vídeos, códigos, música, entre muchos otros (Ruschemeier, 2025).

Big Data

Consiste en un conjunto de datos en cantidades masivas, los cuales no pueden ser procesados y analizados sin que se necesite utilizar una herramienta o software. Para el

tratamiento y procesado de la información, se suelen utilizar información estructurada (Armayones Ruiz, 2015) y, por lo tanto, es necesaria la presencia de una inteligencia artificial para su gestión y el análisis predictivo: Gracias a esto, es posible identificar y analizar patrones que permitan la toma de decisiones frente a una tendencia o comportamiento (Zhang, Yang, & Shuaishuai, 2022).

Concienciación Digital.

Hace referencia al nivel de conocimiento, comprensión y responsabilidad que tiene una persona sobre su comportamiento en internet (Ostec, 2022), incluyendo el uso seguro, ético y responsable de la tecnología. Esta concienciación implica reconocer riesgos como el robo de datos, fraudes cibernéticos o la desinformación, así como adoptar prácticas que protejan su privacidad e identidad digital (Ostec, 2022), por lo que, es clave en la formación de ciudadanos digitales.

Alfabetización Digital

La alfabetización digital es la capacidad de una persona para utilizar tecnologías de la información y la comunicación (también llamadas TICs) de manera efectiva, crítica y segura. Esta alfabetización incluye competencias como buscar, analizar y crear contenido digital (Unesco, 2025), interactuar en redes sociales, proteger la información personal y reconocer amenazas cibernéticas (Unesco, 2025). Por lo que, es fundamental para el desarrollo de habilidades ciudadanas y así reducir brechas digitales.

Marco Teórico

Ley 1581 de 1012

Esta ley protege el derecho de todas las personas en el territorio colombiano a poder conocer, actualizar y rectificar la información que se haya recolectado en cualquier base de datos por alguna organización pública o privada (Congreso de Colombia, 2022). En esta se define qué son los datos personales, cómo se clasifican, cómo debe ser su recolección, el principio de transparencia, el tratamiento que se les debe hacer, los deberes de los responsables, mecanismos de vigilancia, etc.

Ley 1266 de 2008

La Ley 1266 de 2008 es una norma colombiana que establece disposiciones generales sobre el hábeas data, es decir, el derecho que tienen los ciudadanos a conocer, actualizar y rectificar la información que sobre ellos reposa en bancos de datos financieros, crediticios, comerciales o de cualquier tipo de servicios. Esta ley regula el tratamiento de datos personales relacionados con la actividad financiera, crediticia y de cobranzas, y fija principios como la veracidad, la seguridad, la confidencialidad, el acceso restringido, y la circulación restringida. Asimismo, otorga a los titulares el derecho de conocer y solicitar la corrección o supresión de información inexacta o desactualizada en centrales de riesgo.

Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio

La Circular Externa No. 002 de 2024, emitida por la Superintendencia de Industria y Comercio (SIC), establece directrices específicas para el tratamiento de datos personales en sistemas de inteligencia artificial (IA) en Colombia. Esta circular busca garantizar el respeto a los principios y derechos establecidos en el régimen de protección de datos, particularmente

frente a tecnologías emergentes como el aprendizaje automático, la analítica de datos y los algoritmos automatizados.

Modelo de Gestión de la Seguridad de la Información SGSI

El SGSI o modelo de gestión de seguridad de la información es un conjunto de políticas, procedimientos y controles que buscan proteger la información ante cualquier tipo de amenaza que vulnere su disponibilidad, integridad y confidencialidad (ISO, 2023), es decir, riesgos como fuga de información, accesos no autorizados, modificaciones o destrucción. El SGSI está enfocado a las organizaciones que quieren proteger sus activos de información, bien sean datos internos como de las partes interesadas de atacantes cibernéticos.

Reglamento General de Protección de Datos RGPD

El reglamento general de protección de datos o el RGPD establece un conjunto de políticas y requisitos específicos para las empresas al momento de recoger, almacenar y usar los datos de las personas o datos personales. Este reglamento busca que las personas tengan un mejor control sobre sus datos recolectados por alguna entidad pública o privada (Parlamento europeo y el consejo de la unión europea, 2016) y que sus procesos se ejecuten de forma legítima y segura. Cabe resaltar que, el RGPD aplica a cualquier organización que use datos personales de individuos localizados en la unión europea.

Diseño Metodológico

El presente trabajo de grado adopta un enfoque mixto de investigación en el que, se utilizan herramientas cuantitativas y cualitativas para alcanzar una comprensión integral del fenómeno investigado.

Por una parte, la dimensión cuantitativa se centra en la aplicación de una encuesta estructurada con preguntas cerradas, diseñada para medir el nivel de concientización, las prácticas digitales y el conocimiento normativo en torno a la protección de datos personales.

Por otra parte, el componente cualitativo contempla un análisis documental de las normativas legales nacionales e internacionales relacionadas con la protección de datos personalesPara ello, se utilizará una técnica de análisis de contenido temático, a fin de identificar los principios, derechos, deberes y lineamientos clave que servirán como base para la formulación de estrategias educativas, normativas y tecnológicas.

Metodológicamente, esta investigación se enmarca como un estudio de tipo descriptivo-analítico. Es descriptiva, debido a que, permite caracterizar el conocimiento, las prácticas y la percepción de los estudiantes universitarios frente al manejo de su información personal en redes sociales; y a su vez, es analítica, al interpretar los aportes normativos y conceptuales desde una perspectiva crítica, orientada a la construcción de propuestas estratégicas aplicables en el contexto del Internet de las Personas (IoP).

Cabe resaltar que, la población objetivo de este trabajo de grado está centrado en estudiantes universitarios mayores de 18 años, residentes en Bogotá D.C., que estén cursando actualmente programas de educación superior. Estos criterios de inclusión se establecen con el fin de garantizar la homogeneidad del grupo en relación con el contexto educativo y legal aplicable a mayores de edad.

Identificación de los Riesgos Derivados del Internet de las Personas que Enfrentan los Estudiantes Universitarios en los Entornos Digitales.

El crecimiento del internet de las personas ha transformado radicalmente la forma en la que las personas se informan e interactúan entre sí a través de las tecnologías digitales, facilitando la integración de nuevos hábitos en línea. Así mismo, las personas están dependiendo cada vez más de estas tecnologías de información y comunicación (Sánchez, 2021), lo que quiere decir que, utilizan múltiples plataformas digitales para múltiples fines.

En el caso de los estudiantes universitarios, estos han adoptado una dinámica digital en la que esperan que todo esté disponible de forma digital, desde recursos académicos hasta actividades de ocio como juegos en comunidad. Esta nueva necesidad de inmediatez y facilidad de acceso les permite registrarse en nuevas plataformas o vincular sus cuentas personales para acceder a contenidos y servicios. (Navarrez, 2023). En este proceso, muchas veces no se detienen a leer las políticas de privacidad o en el peor de los casos, si las leen, no las comprenden ni entienden su alcance en términos de permisos. Por lo que, se sumergen en un ecosistema digital en el que pierden el control sobre el acceso a su información y aparecen los riesgos (Navarrez, 2023).

Cabe aclarar que, estos riesgos digitales no van enfocados al entorno digital, sino a todo tipo de información que pueda ser vinculada a una persona y que vulnere sus derechos y su dignidad, así como lo declara José Fernández en su artículo de la gobernanza de los riesgos digitales (Fernández, 2022). Así mismo, si se presenta un caso en donde se vulnere algún derecho de privacidad e intimidad puede llegar a verse minimizado de forma no intencional dado que no representa un daño físico y hasta en algunos casos, psicológico, sin embargo, esa vulneración permanece vigente.

Alimentando a las Plataformas Digitales con Información en el Día a Día

Como se ha venido mencionando, la inmediatez de los servicios en línea y la necesidad conectividad permite que un estudiante universitario proporcione su información a diversas plataformas digitales, muchas veces sin tener plena conciencia de ello (Sánchez, 2021). Teniendo en cuenta lo anterior y para poder determinar los riesgos, es necesario establecer tipos de entornos digitales en donde exista el internet de las personas o, en otras palabras, entornos de comunicación o de interacción entre personas; estas son:

a) Entorno de Aprendizaje

Desde el momento en que se matriculan, las instituciones de educación superior o plataformas de educación y aprendizaje recopilan información básica de los estudiantes como nombres, documento de identidad, correo electrónico, direcciones y hasta historiales de salud. A ello se suma la utilización cotidiana de plataformas educativas internas y externas, servicios en la nube, aplicaciones de colaboración e incluso herramientas basadas en inteligencia artificial, las cuales solicitan la creación de una cuenta para almacenar la información académica, pero para poder acceder a dicha cuenta, necesitan proporcionar datos como nombres, institución a la que pertenecen, correo y, en algunos casos, hasta la ubicación geográfica en tiempo real (Hernández, 2021). Esta exposición constante crea una serie de rastros de comportamiento del usuario en internet o también llamado, “la huella digital del estudiante” (Hernández, 2021).

b) Entorno Social

Por otra parte, se tienen a las redes sociales como plataformas primordiales en el entorno social, las cuales representan uno de los escenarios de mayor exposición, dado que, estas plataformas no solo recopilan información obligatoria solicitada a los usuarios, como nombre, edad, ubicación y centro educativo, sino que también rastrean su comportamiento digital,

interacciones, preferencias y hasta rasgos de su personalidad (Yocupicio Sanay, 2020). Por lo que, las redes como Instagram, TikTok, o X, permiten una exposición involuntaria o voluntaria de aspectos personales.

c) Entorno de Ocio

Finalmente, tenemos a los videojuegos en línea como pilar en el entorno de ocio, en donde los estudiantes también enfrentan riesgos significativos para su privacidad. Al registrarse en estas plataformas, es común que se soliciten datos como el correo electrónico, alias vinculados a un nombre y en algunos casos, información financiera para realizar compras, por lo que, se convierten en vectores de riesgo adicionales. Además, la socialización dentro del juego puede implicar la divulgación no intencional de información personal a través de canales de voz o de chat.

Riesgos y Consecuencias de la Exposición Digital

La exposición constante de los datos personales en los entornos académicos, de comunicación y ocio puede generar un conjunto de riesgos que una vez materializados, en la mayoría de las ocasiones, pueden generar un impacto potencial en el estudiante.

Para empezar, se toma como referencia el artículo de Lorena García sobre la Perspectiva de los Jóvenes sobre privacidad en las redes sociales (García, 2015), un artículo de Roberto Vega sobre los riesgos en las redes sociales (Vega, 2017), un estudio de Emiko Yocupicio sobre la facilidad de presencia de los riesgos digitales (Yocupicio, 2020), un análisis de riesgos de autorrepresentación digital por María Hernández (Hernández, 2021) y el proceso de identificación y clasificación de riesgos de la norma ISO/IEC 27005:2022 (ISO/IEC, 2022) para identificar y determinar las vulnerabilidades y amenazas presentes en los entornos digitales, estos se presentan a continuación.

a) Vulnerabilidades

- Contraseñas débiles o compartidas.
- Falta de conciencia sobre seguridad y privacidad.
- Configuración inadecuada de privacidad o seguridad en plataformas digitales.
- Exposición excesiva de información personal en redes sociales.
- Plataformas digitales sin seguridad.
- Conexión a redes no seguras.

b) Amenazas

- Suplantación de identidad.
- Acceso no autorizado.
- Ingeniería social.
- Malware en sitios inseguros.
- Ciberacoso.
- Vigilancia.

Luego de esto, se crea una tabla que combine las 6 vulnerabilidades con las 6 amenazas identificadas y para evaluarlas se tienen en cuenta los siguientes criterios para la probabilidad e impacto tomando como referencia una versión simplificada de las tablas A.1 y A.2 de la ISO/IEC 27005:2022:

- Probabilidad: Improbable (1), Probable (2), Muy Probable (3)
- Impacto: Menor (1), Significativo (2), Grave (3)
- Nivel de Riesgo: $Probabilidad \times Impacto$
- Criticidad del riesgo: Bajo (1–3), Medio (4–6), Alto (7–9)

Tabla 1

Calificación de Riesgos en Entornos Digitales

Código	Vulnerabilidad	Amenaza asociada	Probabilidad	Impacto	Riesgo	Criticidad
R01	Contraseñas débiles o compartidas.	Acceso no autorizado	2	3	6	Medio
R02	Falta de conciencia sobre seguridad y privacidad.	Ingeniería social.	3	2	6	Medio
R03	Configuración inadecuada de privacidad o seguridad en plataformas digitales.	Suplantación de identidad	3	3	9	Alto
R04	Exposición excesiva de información personal en redes sociales.	Ciberacoso	3	3	9	Alto
R05	Plataformas digitales sin seguridad	Malware en sitios inseguros.	2	3	6	Medio
R06	Conexión a redes no seguras	Vigilancia.	3	2	6	Medio

Teniendo en cuenta la tabla 1, se identifica 1 riesgo bajo, 3 riesgos de nivel medio y 2 riesgos de alto nivel, los cuales van a ser tratados en los siguientes apartados del documento.

Determinación del Nivel Actual de Concientización y las Prácticas de Protección de Datos en Estudiantes Universitarios en Bogotá D.C.

Con el propósito de establecer un diagnóstico real y contextualizado sobre la situación actual en el nivel de concientización en cuanto a la protección de los datos personales en estudiantes universitarios de Bogotá D.C., se diseñaron y ejecutaron dos instrumentos de recolección de información mediante encuestas estructuradas. Dichas encuestas fueron aplicadas de manera virtual o digital y de forma anónima, teniendo como base de población a estudiantes activos en instituciones de educación superior dentro de la ciudad de Bogotá.

La decisión de implementar dos encuestas obedece a la necesidad de abordar dos problemas principales como razones de peso para que exista una exposición de datos personales. Por una parte, están las prácticas de seguridad relacionadas con la privacidad y el uso seguro de los entornos digitales y, por otro lado, el nivel de conocimiento y comprensión que los estudiantes poseen respecto a las normativas legales y vigentes, tanto a nivel nacional como internacional que rigen la protección de datos personales.

La primera encuesta titulada “Prácticas para la Privacidad en Entornos Digitales”, indaga el comportamiento cotidiano de los estudiantes frente a su privacidad en línea, es decir, aspectos como el uso de contraseñas, la configuración de privacidad en plataformas sociales, la conexión a redes públicas o abiertas, y el entendimiento de tecnologías emergentes como la inteligencia artificial. Este instrumento busca no solo obtener datos cuantitativos, sino también promover un proceso de autoevaluación y reflexión en los encuestados, permitiéndoles identificar posibles áreas de mejora en sus hábitos digitales.

La segunda encuesta, bajo el nombre “Conocimiento en Normativas de Protección de Datos Personales”, tiene como objetivo identificar si los estudiantes reconocen las leyes

colombianas como la Ley 1581 de 2012, la Ley 1266 de 2008 o la Circular Externa No. 002 de 2024, así como normativas internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea o cualquier otra. Esta encuesta permite evaluar el grado de "alfabetización" normativa y jurídica de los estudiantes en materia de privacidad digital nacional e internacional.

Justificación Metodológica

El enfoque cuantitativo de esta fase permite obtener información medible, comparable y estadísticamente significativa sobre los hábitos y el conocimiento normativo de los estudiantes. Para la ejecución de las encuestas, se crearon formularios en línea con la herramienta Microsoft Forms y se mantuvieron abiertas durante un periodo de 3 semanas. La población objetivo estuvo compuesta por estudiantes universitarios activos en Bogotá D.C., alcanzando una participación total de 120 personas. En la primera encuesta se obtuvieron 124 respuestas válidas, y en la segunda 121 respuestas, lo que demuestra un alto nivel de participación y relevancia del tema entre la comunidad estudiantil.

Resultados de la Encuesta 1: Prácticas para la Privacidad en Entornos Digitales

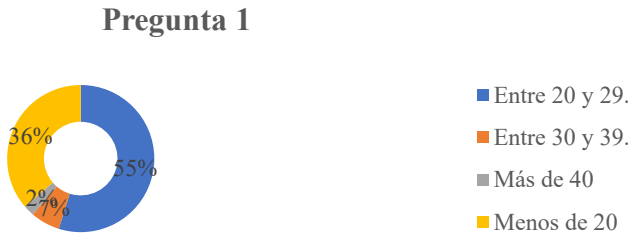
A continuación, se presentan las preguntas aplicadas junto con sus respectivos resultados en formato gráfico. Estas visualizaciones permiten evidenciar el comportamiento digital de los estudiantes, su exposición y el nivel de autoprotección que aplican a su información personal.

Pregunta 1. Rango de edad.

- Menos de 20.
- Entre 20 y 30.
- Entre 30 y 40.
- Más de 40.

Figura 1

Pregunta 1 de la Encuesta de Prácticas de Seguridad

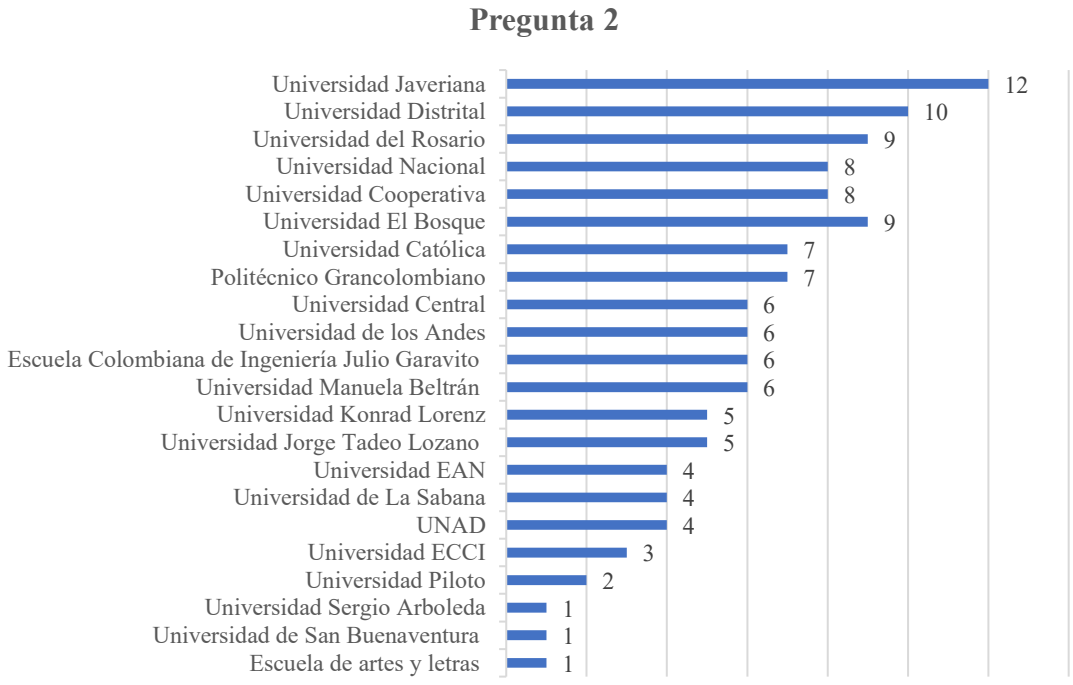


Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 2. Nombre de la universidad en la que estudia.

Figura 2

Pregunta 2 de la Encuesta de Prácticas de Seguridad



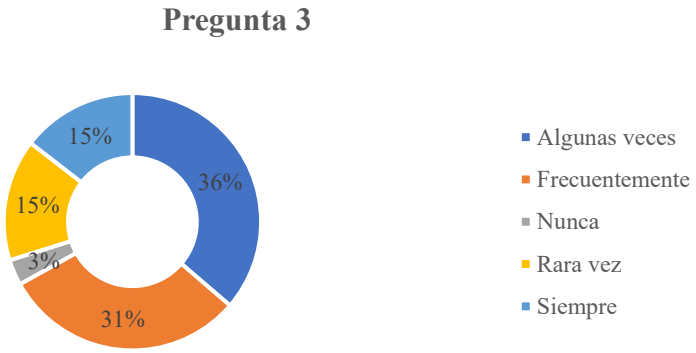
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 3. ¿Con qué frecuencia compartes información personal (nombre, ubicación, correo, número de documento, etc.) en plataformas digitales?

- Nunca
- Rara vez
- Algunas veces
- Frecuentemente
- Siempre

Figura 3

Pregunta 3 de la Encuesta de Prácticas de Seguridad



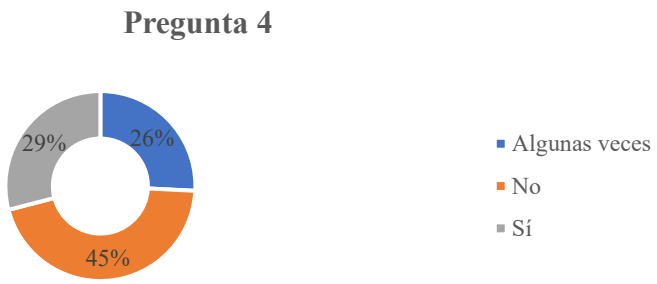
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 4. ¿Sueles leer las políticas de privacidad de las plataformas antes de aceptarlas?

- Sí
- No
- Algunas veces

Figura 4

Pregunta 4 de la Encuesta de Prácticas de Seguridad



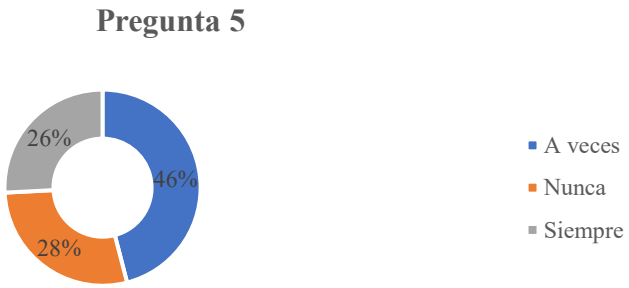
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 5. ¿Revisas o modificas las configuraciones de privacidad de tus redes sociales?

- Siempre
- A veces
- Nunca

Figura 5

Pregunta 5 de la Encuesta de Prácticas de Seguridad



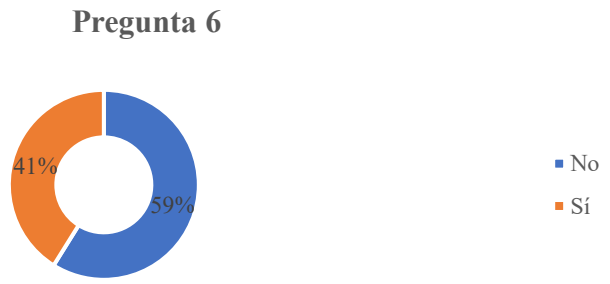
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 6. ¿Compartes contraseñas con otras personas?

- Sí
- No

Figura 6

Pregunta 6 de la Encuesta de Prácticas de Seguridad



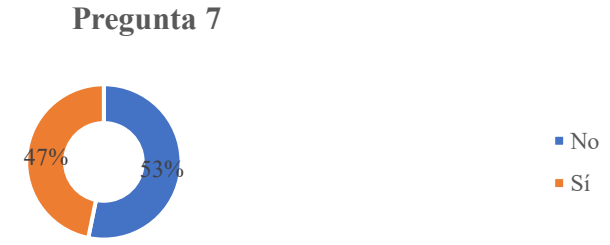
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 7. ¿Utilizas la misma contraseña en varias plataformas?

- Sí
- No

Figura 7

Pregunta 7 de la Encuesta de Prácticas de Seguridad



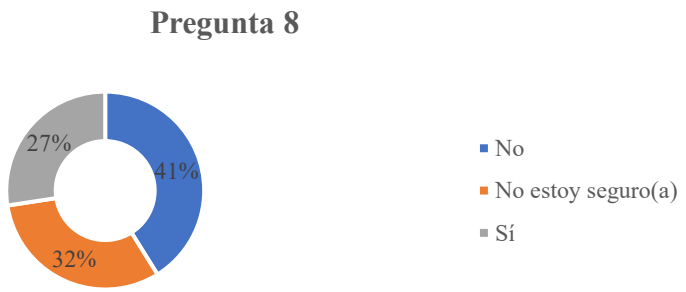
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 8. ¿Has publicado en línea fotos que podrían revelar información privada (como tu casa, universidad, rutinas)?

- Sí
- No
- No estoy seguro(a)

Figura 8

Pregunta 8 de la Encuesta de Prácticas de Seguridad



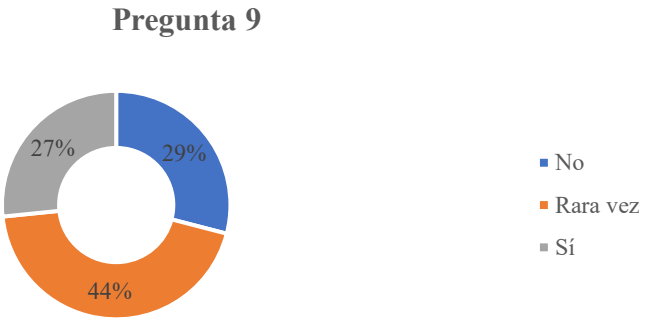
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 9. ¿Utilizas redes Wi-Fi públicas para ingresar a cuentas personales o académicas?

- Sí
- No
- Rara vez

Figura 9

Pregunta 9 de la Encuesta de Prácticas de Seguridad



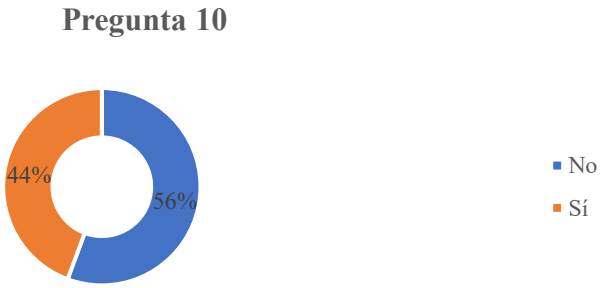
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 10. ¿Has recibido correos o mensajes sospechosos pidiéndote información personal?

- Sí
- No

Figura 10

Pregunta 10 de la Encuesta de Prácticas de Seguridad



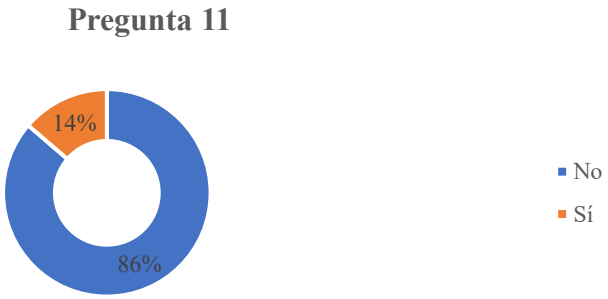
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 11. ¿Has sufrido de alguna suplantación de identidad?

- Si
- No

Figura 11

Pregunta 11 de la Encuesta de Prácticas de Seguridad



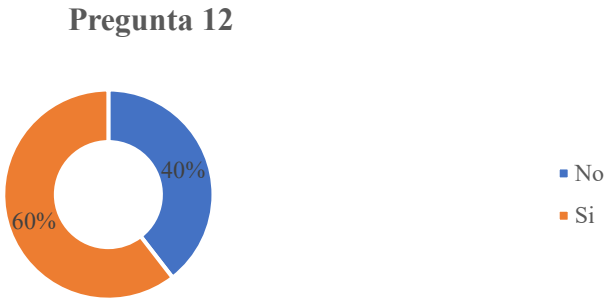
Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Pregunta 12. ¿Eres consciente de los riesgos digitales al compartir información personal?

- Si
- No

Figura 12

Pregunta 12 de la Encuesta de Prácticas de Seguridad



Nota. Gráfica de resultados de la pregunta de la encuesta 1, de elaboración propia en Excel.

Teniendo en cuenta los resultados, se encuentra por una parte que, el 55% de los estudiantes encuestados corresponden a una población entre los 20 y 30 años, en otras palabras, a la población más grande, mientras que el 36% corresponden a estudiantes entre 18 y 20 años y un 2% a una población de más de 40 años. Por otra parte, un 82% de los encuestados comparte información por internet, bien sean nombres, correos, identificaciones, entre otro tipo de datos.

El 45% de las personas no leen las políticas de privacidad de las plataformas digitales, sin embargo, solo el 28% no modifican sus preferencias de privacidad, es decir, utilizan las configuradas de forma predeterminada, sin embargo, el 60% de los encuestados están conscientes o al tanto de los riesgos que pueden existir al compartir datos personales. Adicionalmente, el 41% de las personas comparten su contraseña y de ese porcentaje, el 45% utiliza las mismas contraseñas en múltiples plataformas digitales. Finalmente, el 44% de los encuestados ha recibido o recuerda haber algún tipo de correo con intenciones fraudulentas o malignas, mientras que el 14% ha sufrido de algún tipo de suplantación en algún tipo de plataforma digital en el marco del internet de las personas.

Resultados de la Encuesta 2: Conocimiento sobre Normativas de Protección de Datos en Entornos Digitales

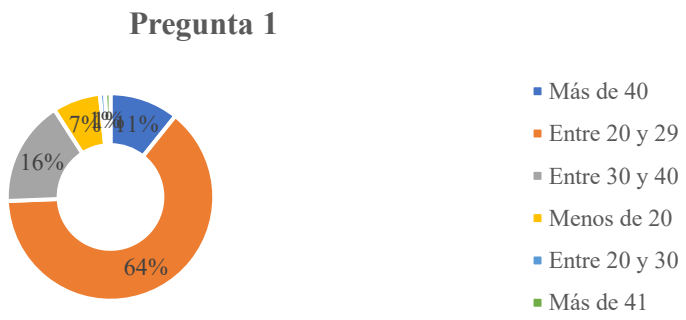
La segunda encuesta buscó evaluar el nivel de alfabetización legal y digital en torno a la protección de datos personales. A continuación, se detallan las preguntas realizadas y las respuestas obtenidas por los participantes.

Pregunta 1. Rango de edad.

- Menos de 20.
- Entre 20 y 30.
- Entre 30 y 40.
- Más de 40.

Figura 13

Pregunta 1 de la Encuesta de Normativas

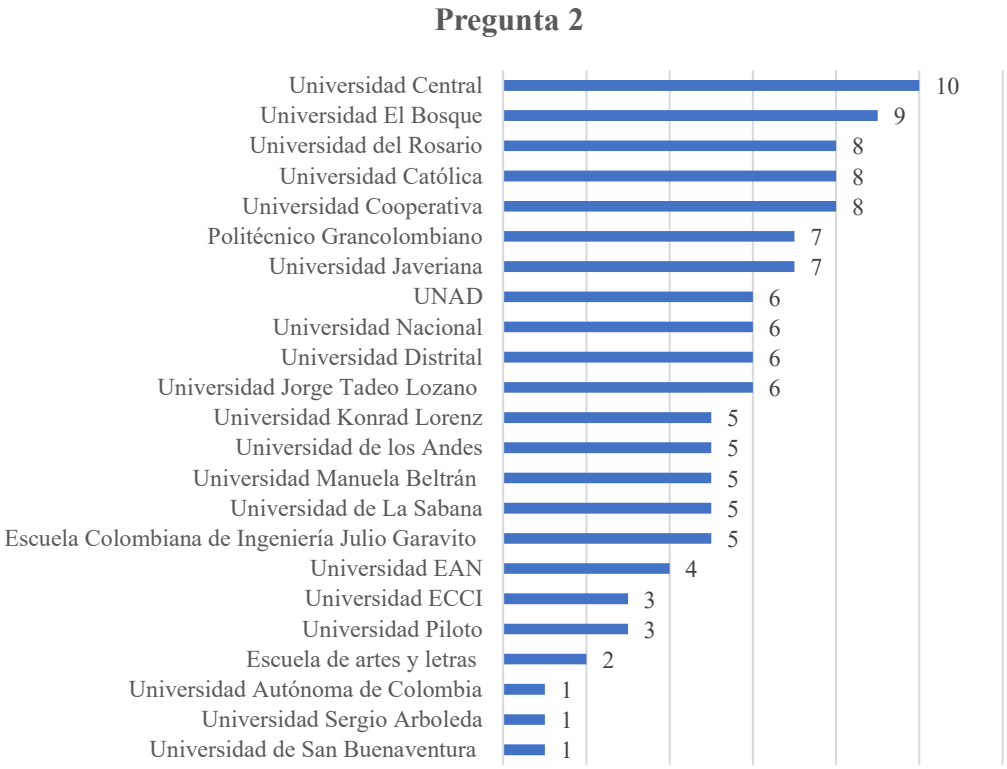


Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 2. Nombre de la universidad en la que estudia.

Figura 14

Pregunta 2 de la Encuesta de Normativas



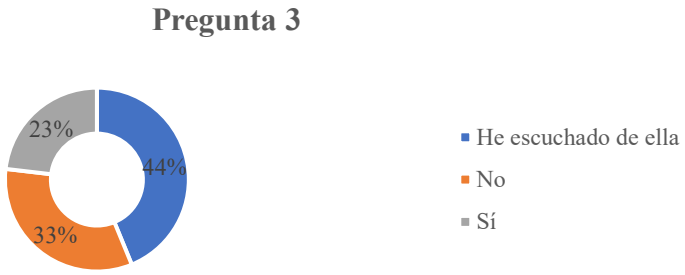
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 3. ¿Conoces la Ley 1581 de 2012 sobre protección de datos personales en Colombia?

- Sí
- No
- He escuchado de ella

Figura 15

Pregunta 3 de la Encuesta de Normativas



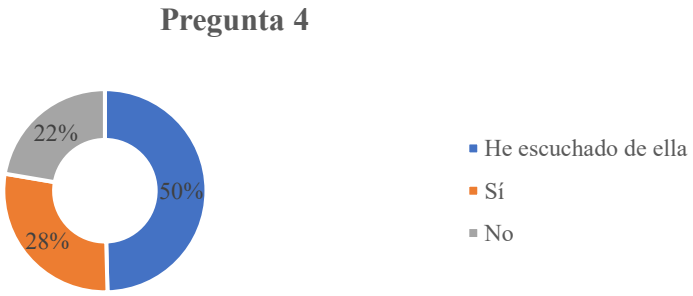
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 4. ¿ Conoces la Ley 1266 de 2008 o hábeas data y regulación del manejo de información en Colombia?

- Sí
- No
- He escuchado de ella

Figura 16

Pregunta 4 de la Encuesta de Normativas



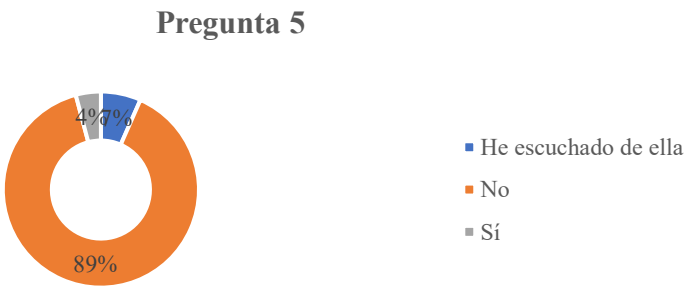
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 5. ¿Conoces la Circular Externa No. 002 de 2024 para el tratamiento de datos en sistemas de IA en Colombia?

- Sí
- No
- He escuchado de ella

Figura 17

Pregunta 5 de la Encuesta de Normativas



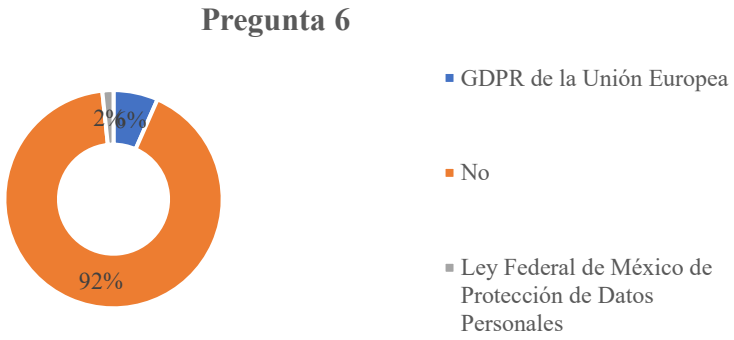
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 6. ¿Conoces Reglamentación, normativas o leyes de otros países?

- No
- Si, ¿Cuáles?

Figura 18

Pregunta 6 de la Encuesta de Normativas



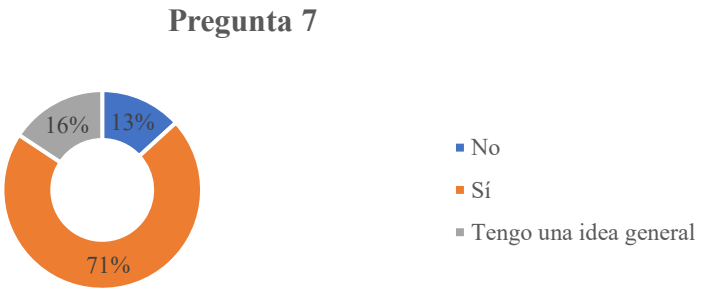
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 7. ¿Sabías que algunas plataformas recopilan información personal mediante inteligencia artificial?

- Sí
- No
- Tengo una idea general

Figura 19

Pregunta 7 de la Encuesta de Normativas



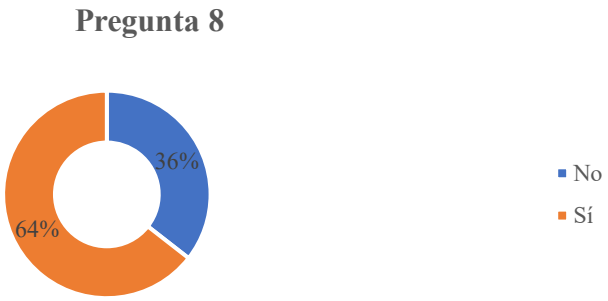
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 8. ¿Entiendes cómo funciona la recopilación de datos personales por IA (por ejemplo, en redes sociales o asistentes virtuales)?

- Sí
- No

Figura 20

Pregunta 8 de la Encuesta de Normativas



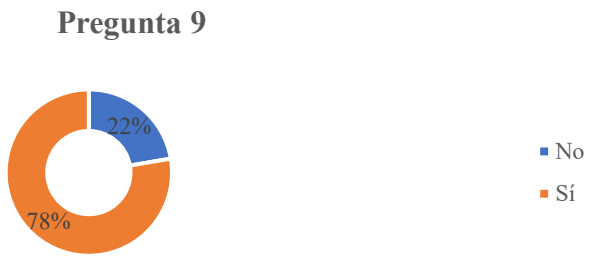
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 9. ¿Sabes qué tipo de información recolectan las plataformas que usas a diario?

- Sí
- No

Figura 21

Pregunta 9 de la Encuesta de Normativas



Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 10. ¿Sabes si puedes solicitar la eliminación o rectificación de tus datos personales en las plataformas?

- Sí
- No
- No estoy seguro(a)
- Lo he hecho

Figura 22

Pregunta 10 de la Encuesta de Normativas

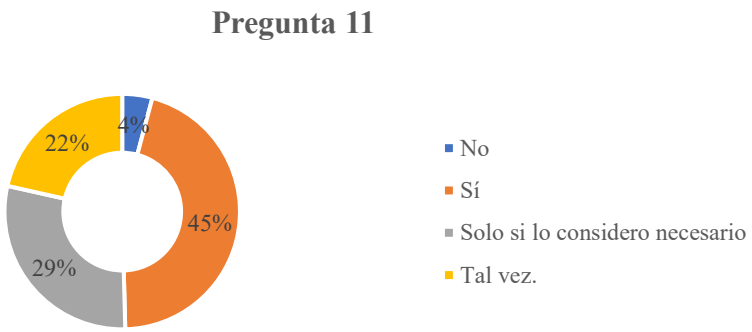
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 11. Si se creara un manual con lenguaje sencillo y estrategias para mitigar la exposición de datos personales, ¿estarías dispuesto(a) a leerlo?

- Sí
- Tal vez.
- Solo si lo considere necesario.
- No

Figura 23

Pregunta 11 de la Encuesta de Normativas



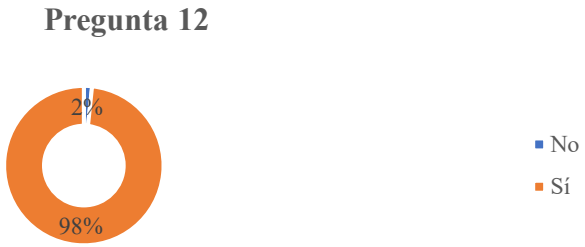
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 12. ¿Consideras necesario que existan guías o manuales adaptados para comprender cómo proteger los datos personales en internet?

- Sí
- No

Figura 24

Pregunta 12 de la Encuesta de Normativas



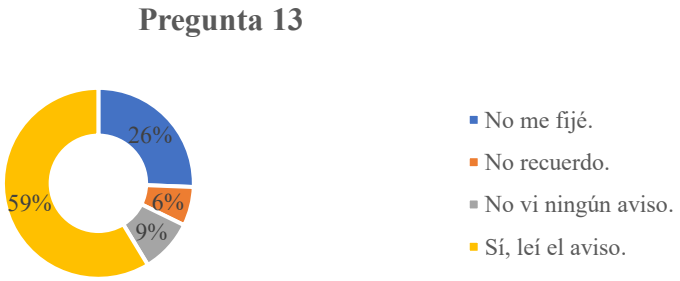
Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

Pregunta 13. Al responder este cuestionario, ¿te fijaste en cuál sería el uso de la información que se te solicitó?

- Sí, leí el aviso.
- No me fijé.
- No recuerdo.
- No vi ningún aviso.

Figura 25

Pregunta 13 de la Encuesta de Normativas



Nota. Gráfica de resultados de la pregunta de la encuesta 2, de elaboración propia en Excel.

En los resultados de la encuesta, se encuentra que, 23% de los encuestados conoce la ley 1581 de 2012, un 28% conoce la ley 1266 de 2018 y un 4% conoce la circular externa No. 002 de 2024, lo que indica que, en promedio, un 18,3% de los encuestados conoce al menos una de las leyes colombianas más reconocidas para la protección de los datos personales.

Por otra parte, el 71% de las personas entiende o cree entender cómo funciona el tratamiento de los datos personales en las plataformas, así mismo, el 64% sabe qué existen plataformas de IA que recolectan información de forma masiva y el 66% de los encuestados saben que pueden hacer reclamaciones sobre sus derechos como usuarios de las plataformas.

Resumen de los Resultados

Los resultados obtenidos permiten observar que existe una diversidad en los niveles de concientización de los estudiantes universitarios respecto a la protección de sus datos personales. Si bien muchos manifiestan preocupación por su seguridad digital, aún persisten comportamientos de riesgo, como el uso de contraseñas poco robustas, la conexión a redes públicas sin protección y la publicación de datos sensibles en plataformas digitales. Del mismo modo, la encuesta sobre normativas reveló un desconocimiento generalizado sobre leyes fundamentales de protección de datos, especialmente en lo que respecta al uso de tecnologías como la inteligencia artificial (circular de la superintendencia de industria y comercio) y las decisiones automatizadas.

Estos hallazgos evidencian la necesidad de diseñar e implementar estrategias educativas, informativas y tecnológicas para mitigar la exposición de datos personales, así como fortalecer la formación jurídica básica sobre el tratamiento adecuado de información en los entornos digitales. Cabe resaltar que, también ofrece un panorama actual de las fortalezas, debilidades, desconocimientos y percepciones que tienen los jóvenes sobre su privacidad en línea. Además,

permite establecer líneas base para comparar futuros avances tras campañas de concientización, educación digital o intervención normativa.

Análisis de las Contribuciones de Leyes y Normativas Nacionales e Internacionales Frente a la Protección de Datos Personales en los Entornos Digitales

La protección de los datos personales es una preocupación muy grande teniendo en cuenta los resultados y las estadísticas de las encuestas ejecutadas anteriormente, sobre todo teniendo en cuenta que la población de cada encuesta representa un porcentaje pequeño con respecto a todos los estudiantes en la ciudad de Bogotá.

A medida que los datos se han estado convirtiendo en uno de los activos más valiosos, los riesgos asociados a su tratamiento indebido se han incrementado significativamente, por lo que es necesario recurrir a algunos marcos legales y normativos tanto a nivel nacional como internacional que, permitan garantizar su seguridad y privacidad. A continuación, se presenta un análisis, el cual se centra en evaluar las contribuciones de algunas normativas relevantes, tanto a nivel internacional como nacional. En este caso, se revisará la norma ISO/IEC 27001:2022, la Ley 1581 de 2012 de protección de datos personales, la Ley 1266 de 2008 de habeas data, la Circular Externa No. 002 de 2024 de la Superintendencia de Industria y Comercio y el Reglamento General de Protección de Datos o GDPR–UE 2016/679. Con dicha información extraída, se pretende obtener lineamientos y elementos fundamentales que contribuyan a la construcción de estrategias efectivas de protección de datos personales en los entornos digitales.

ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 establece un sistema de gestión de seguridad de la información o también llamado SGSI, el cual puede ser aplicado por cualquier tipo de organización. Esta norma internacional proporciona un marco robusto para identificar riesgos (ISO/IEC, 2022) y establecer controles que protejan los activos de información, otras palabras, se

considera la base o los cimientos para establecer la seguridad de la información y la protección de los datos personales.

En esta norma se establece el control A.5.12 para la clasificación de la información (ISO/IEC, 2022), el cual menciona la necesidad de clasificar la información según las necesidades de la organización con el fin de mantener la integridad, disponibilidad y confidencialidad de la información. El control A.5.14 establece la necesidad de las reglas para poder mantener un adecuado proceso de transferencia de información (ISO/IEC, 2022) y para esto, se pueden definir métodos como el cifrado o hashes para proteger la información durante su transmisión. El control A.5.27 establece que se debe aprender de los incidentes de seguridad de la información (ISO/IEC, 2022), es decir, recopilar toda la información que sea necesaria para reforzar y mejorar la seguridad de la información. El control A.5.33 establece la protección de los registros de información o registros de auditoría de riesgos como la pérdida (ISO/IEC, 2022), alteración, falsificación y acceso no autorizado.

Por otra parte, se tiene el control A.8.5, el cual establece que se deben implementar tecnologías o procedimientos que permitan una autenticación segura al momento de acceder a un sistema de información o a la misma información (ISO/IEC, 2022). El control A.8.10 establece la necesidad de eliminar la información de cualquier sistema o cualquier medio de almacenamiento (ISO/IEC, 2022) cuando ya no esté en uso o no sea necesario. El control A.8.13 establece que se debe mantener una copia de seguridad sobre la información (ISO/IEC, 2022) y debe ser actualizada periódicamente. El control A.8.23 establece la necesidad de gestionar los sitios web a los que se accede con el fin de reducir la exposición a contenidos con intenciones maliciosas. Finalmente, el control 8.24 establece la necesidad de establecer modelos

criptográficos (ISO/IEC, 2022) con el fin de mantener protegida la información en momentos específicos.

Ley 1581 de 2012 – Protección de Datos Personales en Colombia

La Ley 1581 de 2012 ejerce como "norma" principal y fundamental en Colombia en temas de la protección de los datos personales. Con esta ley, se establecen los principios base del tratamiento de datos y define los derechos de los titulares y las obligaciones de los responsables y encargados del tratamiento (Función pública, 2022). Dentro de sus aportes más relevantes, se encuentran:

El principio de seguridad, que establece la obligación de implementar medidas técnicas, humanas y administrativas para garantizar la protección de los datos de su robo, pérdida de integridad o acceso no autorizado(Función pública, 2022). El principio de finalidad señala el tratamiento de datos de forma legítima, es decir, para obtener los datos personales, se debe contar con una autorización informada de manera previa, clara y explícita al titular (Función pública, 2022), por tanto, ninguna organización puede utilizar datos personales con fines no autorizados por el titular. Por otra parte, el principio de acceso y circulación restringida prohíbe que datos personales salvo los públicos, estén disponibles sin medidas de seguridad que controlen su acceso.

Adicionalmente, se establece en el artículo 6, la necesidad de establecer una autorización explicita en todo momento para el tratamiento de los datos a obtener por un sistema (Función pública, 2022), a excepción de los casos en donde verdaderamente no se considere necesario. El artículo 8 establece como derecho fundamental de los titulares de la información a conocer, actualizar y rectificar sus datos personales en cualquier sistema en donde hayan sido almacenados sus datos, así mismo, se extiende sobre datos que estén parciales, incorrectos,

alterados o con errores (Función pública, 2022), finalmente, se establece el derecho de presentar una queja ante la Superintendencia de Industria y Comercio por el uso inadecuado de los datos almacenados por cualquier entorno digital (Función pública, 2022)..

Estos elementos son fundamentales para cualquier entorno digital, pues proporcionan el marco ético y jurídico para el manejo responsable de la información personal.

Ley 1266 de 2008 – Protección de la Información Financiera

La Ley 1266 de 2008, aunque centrada en el ámbito financiero y crediticio, establece un precedente importante sobre el derecho que tienen los ciudadanos a conocer, actualizar y rectificar la información personal en poder de terceros (Función pública, 2021) y, por tanto, se pueden extraer algunos principios como:

El principio de circulación restringida y es la de verificar que los datos personales no públicos almacenados en un sistema no estén accesibles por internet o cualquier medio de comunicación masiva (Función pública, 2021), esto con el fin de no vulnerar el principio de confidencialidad de los datos. Por otra parte, se establece en el artículo 6 el derecho del titular de la información a solicitar pruebas de la existencia de una autorización del tratamiento de datos en sistemas en los que no esté seguro o no haya proporcionado información personal (Función pública, 2021).

Circular Externa No. 002 de 2024 – Tratamiento de Datos en Sistemas de Inteligencia Artificial

Con el avance de la inteligencia artificial o IA y su uso en los sistemas de información para su recolección, tratamiento y demás funcionalidades, la Superintendencia de Industria y Comercio de Colombia establece la Circular Externa No. 002 de 2024, la cual regula el tratamiento de datos personales en los sistemas de Inteligencia Artificial (Superintendencia de

Industria y Comercio, 2024). Esta norma representa un avance significativo, ya que aborda riesgos emergentes relacionados con el uso automatizado de información personal, sobre todo teniendo en cuenta que, actualmente no existe en Colombia una ley que regule el uso de las inteligencias artificiales por parte de las entidades (Superintendencia de Industria y Comercio, 2024) y los entornos digitales. Entre sus aportes clave se destacan:

Los principios de necesidad, razonabilidad y proporcionalidad, los cuales establecen que, el tratamiento de datos mediante IA debe limitarse estrictamente a lo necesario para la finalidad definida (Superintendencia de Industria y Comercio, 2024) y no podrán vulnerar algún derecho establecido en la ley 1581 de 2012 y la ley 1266 de 2008. Por otra parte, está la necesidad de los sistemas de tratamiento de datos con IA de no utilizar datos parciales o alterados, así mismo, no pueden utilizar ningún tipo de dato (privado, semiprivado, sensible o público) en sistemas de tratamiento de datos con IA sin una autorización previa y expresa (Superintendencia de Industria y Comercio, 2024).

Esta Circular fortalece la protección de los datos personales frente a nuevas tecnologías que presentan riesgos significativos por su capacidad de recopilar y procesar grandes volúmenes de información (Superintendencia de Industria y Comercio, 2024), muchas veces de manera imperceptible para los usuarios.

Reglamento General de Protección de Datos o GDPR–UE 2016/679

El GDPR es el principal referente internacional en protección de datos personales, aplicable a cualquier entidad que trate datos de ciudadanos de la Unión Europea, y reconocido por sus principios de protección avanzada, derechos de los titulares y obligaciones estrictas para los responsables del tratamiento. Sus aportes principales son:

En el artículo 7, se establece que una vez un usuario haya dado un consentimiento o autorización del tratamiento de sus datos personales, tiene el derecho de solicitar el retiro de su consentimiento (Intersoft Consulting, 2016). Así mismo, declara la necesidad de revisar y analizar de forma previa al consentimiento el fin y el tipo de tratamiento que se va a dar sobre sus datos en cualquier sistema, plataforma o entorno digital, esto con el fin de aceptar o rechazar los términos de tratamiento de datos (Intersoft Consulting, 2016). Adicionalmente, el artículo 13 establece que, al momento de leer los términos de tratamiento de datos en un sistema, plataforma o entorno digital, se deben verificar la existencia de los siguientes apartados:

- Los datos de contacto del responsable del tratamiento.
- Los fines del tratamiento de los datos.
- La base jurídica del tratamiento.
- Los intereses del responsable.
- Los destinatarios o quienes tendrán acceso a dicha información.
- En caso de ser datos que se transfieran de forma internacional, la existencia de garantías para su buena disposición y tratamiento.
- El periodo de almacenamiento de los datos si aplica.
- La existencia del derecho a solicitar la consulta, modificación y eliminación de los datos personales o rechazo del tratamiento.
- El derecho de presentar una reclamación ante un ente de autoridad.

Por otra parte, se establece la minimización de los datos, es decir que, solo se deban recopilar los datos personales estrictamente necesarios (Intersoft Consulting, 2016), por tanto, no es válido recolectar más información de la requerida y a su vez, el titular tiene el derecho de verificar qué información se va a recolectar y tratar (Intersoft Consulting, 2016). La limitación

del plazo de conservación establece que, los datos no pueden ser almacenados indefinidamente, por lo que, deben conservarse solo por el tiempo necesario para cumplir con el propósito del tratamiento de la plataforma o entorno digital (Intersoft Consulting, 2016); esto obliga a las plataformas a tener políticas de retención de datos y a eliminarlos de manera segura una vez que ya no se requieran o estén obsoletos (Intersoft Consulting, 2016).

El GDPR representa un modelo integral de protección de datos en entornos digitales a nivel internacional, sobre todo por su enfoque en la transparencia, la minimización del riesgo, la seguridad por diseño y la autodeterminación informativa, el cual proporciona una guía sólida para cualquier estrategia de mitigación de exposición de datos personales. Si bien en Colombia no se tienen implementadas muchas medidas, se pueden extraer herramientas o artículos que aporten a la creación de estrategias para la protección de los datos personales para estudiantes universitarios en Bogotá D.C.

Diseño de Estrategias Integrales Orientadas a Mitigar la Exposición de Datos Personales de Estudiantes Universitarios en Entornos Digitales

El diseño de las estrategias para la protección de datos personales en los entornos digitales identificados requiere una aproximación integral que contemple una dimensión educativa, normativa y tecnológica y para esto, se tiene que tomar como base el análisis de riesgos en los entornos digitales, el cual fue efectuado previamente, así como los resultados de las encuestas aplicadas a estudiantes universitarios de la ciudad de Bogotá.

Para poder desarrollar las estrategias, se propone una matriz con características que permitan al estudiante poder determinar por ejemplo si alguna de las estrategias está basada en alguna norma, política o ley y a qué código de riesgo cubre.

Estrategias Educativas

Las estrategias educativas están orientadas de forma que puedan fomentar una cultura de protección de datos y cómo estas pueden incrementar el conocimiento, la reflexión crítica y la concientización sobre el estudiante universitario y cómo ser y cómo hacer uso responsable frente a sus datos personales, en otras palabras, ayudar al estudiante a que prevenga una exposición involuntaria, innecesaria y riesgosa de sus datos personales.

Con lo anterior, se pretenden abordar estrategias relacionadas con el análisis del entorno de las plataformas, el reconocimiento de situaciones riesgosas, entre otras.

Tabla 2

Estrategias educativas junto con el riesgo que mitigan

Código	Título	Descripción	Basada en	Riesgos que mitiga
EE01	Revisión antes de Aceptar	Antes de aceptar términos y condiciones de uso en plataformas digitales, dedicar tiempo a revisar qué tipo de datos serán recopilados, con qué fines y durante cuánto tiempo.	Ley 1581 de 2012	R04
EE02	Leer Alertas de seguridad	Prestar atención a los mensajes generados por el navegador, antivirus cuando se entra a entornos no seguros.	Resultados de las encuestas	R05
EE03	Sobrenombres sin nombres	Utilizar nombres alternativos en foros, videojuegos o redes en donde no sea obligatorio usar datos reales o con fines profesionales.	Resultados de las encuestas	R04
EE04	Ejecución de encuestas	Al momento de decidir llenar una encuesta, verificar qué tipo de información se está solicitando y validar si se pide información innecesaria al objetivo de la encuesta.	Resultados de las encuestas	R04
EE05	¿Qué harás con mi información?	Al momento de decidir llenar una encuesta, validar cuál va a ser el uso de la información que vas a entregar y dependiendo del caso, por cuánto tiempo se va a almacenar	Resultados de las encuestas	R04
EE06	No compartir sin pensar	Reflexionar antes de compartir fotos, ubicaciones, opiniones o datos familiares en plataformas en las que no tengas el control del público al que está destinado.	Resultados de las encuestas	R04

Código	Título	Descripción	Basada en	Riesgos que mitiga
EE07	Información fuera de la academia.	Para información relacionada con las instituciones o academias, evitar compartir datos o documentos en chats, foros o grupos fuera de los entornos no institucionales.	Resultados de las encuestas	R04
EE08	La regla del mínimo necesario	Compartir únicamente la información que sea estrictamente obligatoria o requerida para poder acceder a un servicio o entorno digital.	Resultados de las encuestas	R03, R06
EE09	Clasificación de los datos	Entiende qué datos personales se consideran públicos, semiprivados, privados y sensibles con el fin de entender qué datos puedes compartir en los entornos digitales y cuáles no.	Ley 1581 de 2012, ISO 27001:2012	R04
EE10	¿Quién soy en internet?	Realizar la búsqueda de datos como del nombre, identificación, numero de celular con el fin de, encontrar en qué entornos digitales están expuestos los datos de forma pública.	Resultados de las encuestas	R02

En este caso, se observa el diseño 10 estrategias, las cuales están identificadas por un código único, así como su nombre, definición, de dónde fueron basadas, es decir, si fueron tomadas de los resultados de las encuestas o de alguna ley, marco o normativa. Adicionalmente, se consigna a qué riesgo está relacionado y puede mitigarlo completa o parcialmente.

Estrategias Normativas

Las estrategias normativas consisten en acciones individuales que los estudiantes pueden tomar basadas en los derechos y principios legales existentes en materia de protección de datos personales. Por lo que, estas estrategias están principalmente fundamentadas en marcos normativos como las leyes colombianas 1581 de 2012 y 1266 de 2008, la circular 002 de 2024 y

el RGPD a nivel internacional, las cuales protegen el derecho a la privacidad y la autodeterminación informativa.

En este contexto, implican el conocimiento y ejercicio de derechos como el acceso, la rectificación, la revocatoria del consentimiento, el uso informado de los términos y condiciones, y la evaluación del uso de datos por sistemas automatizados o de inteligencia artificial.

Tabla 3

Estrategias Normativas Junto con el Riesgo que Mitiga

Código	Título	Descripción	Basada en	Riesgos que mitiga
EN01	Configuración de la privacidad	Ingresar a los ajustes de cada plataforma o entorno digital y ajustar manualmente qué tantos permisos quieres conceder, algunos permisos pueden ser: El micrófono, la cámara, archivos, la ubicación, entre otros.	Resultados de las encuestas	R02, R03, R06
EN02	Revisar las políticas de los entornos digitales.	Al momento de iniciar por primera vez en un entorno digital es importante leer los siguientes apartados: * Datos de contacto del responsable del entorno digital. * Qué datos se van a recolectar. * El tratamiento que se le dará a los datos. * Quiénes tendrán acceso a los datos recolectados. * El derecho a la consulta, modificación y eliminación (si aplica) de los datos. * El derecho de presentar una reclamación.	GPRD, Resultados de las encuestas	R02, R03

Código	Título	Descripción	Basada en	Riesgos que mitiga
EN03	Privacidad con la IA	Antes de usar un entorno digital que haga uso de inteligencia artificial, revisa la política de privacidad y busca cómo se almacenan, procesan y reutilizan las conversaciones o datos que ingreses.	Circular 002 de 2024	R02
EN04	Revocar autorizaciones	Si en una plataforma en la que has concedido permisos, no estás de acuerdo sobre alguno de ellos, puedes ejercer tu derecho a revocar el consentimiento o retirarte de la plataforma y exigir la eliminación de tus datos.	Ley 1581 de 2012, GPRD, ISO 27001:2022	R03, R04
EN05	Pruebas de incidentes digitales	Si presentas algún caso de robo de datos, acoso, suplantación o cualquier tipo de uso no autorizado, toma capturas o fotos como evidencia de la situación y reporta el caso ante las autoridades.	ISO 27001:2022	R02
EN06	Cookies innecesarias	Al momento de entrar a un sitio web o entorno digital, verifica que únicamente se acepten las cookies estrictamente necesarias.	RGPD	R04, R05
EN07	Actualizar la información	Se tiene el derecho a actualizar los datos recolectados por entornos digitales y evitar problemas de identificación o la recolección de datos incompletos, alterados o con errores.	Ley 1581 de 2012	R03
EN08	Verificación de los datos	Validar que la información que aceptaste su recolección por parte de un entorno digital sea la que verdaderamente se aceptó.	Ley 1581 de 2012	R04

En este caso, se observa el diseño 8 estrategias, las cuales están identificadas por un código único, así como su nombre, definición, de dónde fueron basadas, es decir, si fueron tomadas de los resultados de las encuestas o de alguna ley, marco o normativa. Adicionalmente, se consigna a qué riesgo está relacionado y puede mitigarlo completa o parcialmente.

Estrategias Tecnológicas

Las estrategias tecnológicas consisten en acciones prácticas basadas en el uso correcto, seguro y consciente de herramientas digitales. Para esto, se tienen en cuenta las configuraciones de privacidad, de autenticación, de navegación segura, entre otras.

En este contexto, estas estrategias permiten al estudiante universitario reducir riesgos técnicos relacionados con la exposición de datos personales, mediante la protección y limitación del acceso no autorizado o el rastreo por terceros a través de prácticas tecnológicas.

Tabla 4

Estrategias Tecnológicas Junto con el Riesgo que Mitiga

Código	Título	Descripción	Basada en	Riesgos que mitiga
ET01	Autenticación en dos pasos	Habilitar el doble factor de autenticación en cuentas que lo permitan y así reforzar el acceso a la información personal.	ISO 27001:2022	R01
ET02	Usar contraseñas seguras	Evitar utilizar la misma contraseña en múltiples sitios y así mismo, utilizar combinaciones entre números, letras y símbolos no consecutivos o que se consideren predecibles.	ISO 27001:2022	R01
ET03	Gestores de contraseñas	Para evitar olvidar contraseñas largas y complejas, instalar gestores de contraseñas	ISO 27001:2022	R01

Código	Título	Descripción	Basada en	Riesgos que mitiga
		reconocidos para almacenarlas de forma segura.		
ET04	Después de compartir una contraseña	Si tuviste un caso en donde compartiste la contraseña de cualquier cuenta, actualiza inmediatamente la contraseña y cierra el acceso a todos los dispositivos que no sean de tu uso o que no reconozcas.	Resultados de las encuestas	R01
ET05	Cifrar para compartir	Al momento de compartir datos sensibles como por ejemplo datos biométricos, historiales médicos, entre otros, cifra la información y comparte la clave de cifrado únicamente con el destinatario autorizado.	ISO 27001:2022	R01
ET06	Autenticidad de la información	Al momento de compartir documentos con firmas o datos biométricos, entre otros, genera hashes por medio de herramientas instaladas (no herramientas en línea) con el fin de que el destinatario pueda verificar la autenticidad de la información que se ha compartido.	ISO 27001:2022	R03
ET07	Copias de seguridad	Genera copias de seguridad en diferentes medios de almacenamiento para documentos importantes como identificaciones, certificados, membresías y cualquier tipo de información que contenga datos personales con el fin de no perderlos en caso de sufrir algún incidente de seguridad.	ISO 27001:2022	
ET08	Redes Wifi públicas	No acceder a cuentas personales, institucionales o laborales desde redes abiertas	ISO 27001:2022, Resultados	R04, R06

Código	Título	Descripción	Basada en	Riesgos que mitiga
		o públicas, debido a que son focos de robo de credenciales por parte de ciberatacantes.	de las encuestas	
ET09	Suplantación de la identidad	Al momento de recibir un correo, mensaje de texto, llamada o cualquier intento de comunicación, verificar que quien lo envía sea verdaderamente quien dice ser. Para esto examina la redacción, errores ortográficos, logo y marca si aplica, si denota algún tipo de urgencia, el envío de enlaces a páginas de internet.	Resultados de las encuestas	R02, R03, R06

En este caso, se observa el diseño 9 estrategias, las cuales están identificadas por un código único, así como su nombre, definición, de dónde fueron basadas, es decir, si fueron tomadas de los resultados de las encuestas o de alguna ley, marco o normativa. Adicionalmente, se consigna a qué riesgo está relacionado y puede mitigarlo completa o parcialmente.

Una vez formuladas y estructuradas las estrategias educativas, normativas y tecnológicas, se procede a ejecutar una reevaluación de los riesgos previamente identificados en el primer objetivo del estudio. Este proceso tiene como propósito analizar si los riesgos asociados a la exposición de datos personales de estudiantes universitarios en entornos digitales pueden ser mitigados de manera efectiva mediante la implementación y el buen uso de las estrategias propuestas. Asimismo, esta revisión permite valorar la pertinencia, aplicabilidad y suficiencia de cada estrategia frente a los escenarios digitales actuales, considerando la realidad del contexto universitario y el comportamiento digital de los estudiantes.

Para evaluarlas se tienen en cuenta los siguientes criterios para la probabilidad e impacto tomando como referencia una versión simplificada de las tablas A.1 y A.2 de la ISO/IEC 27005:2022:

- Probabilidad: Improbable (1), Probable (2), Casi seguro (3)
- Impacto: Menor (1), Significativo (2), Grave (3)
- Nivel de Riesgo: $Probabilidad \times Impacto$
- Criticidad del riesgo: Bajo (1–3), Medio (4–6), Alto (7–9)

Tabla 5

Calificación de Riesgos en Entornos Digitales

Código	Vulnerabilidad	Amenaza asociada	Probabilidad	Impacto	Riesgo	Criticidad
R01	Contraseñas débiles o compartidas.	Acceso no autorizado	2	1	**2**	**Bajo**
R02	Falta de conciencia sobre seguridad y privacidad.	Ingeniería social.	2	2	**4**	**Medio**
R03	Configuración inadecuada de privacidad o seguridad en plataformas digitales.	Suplantación de identidad	2	2	**4**	**Medio**
R04	Exposición excesiva de información personal en redes sociales.	Ciberacoso	1	2	**2**	**Bajo**

Código	Vulnerabilidad	Amenaza asociada	Probabilidad	Impacto	Riesgo	Criticidad
R05	Plataformas digitales sin seguridad	Malware en sitios inseguros.	2	2	**4**	**Medio**
R06	Conexión a redes no seguras	Vigilancia.	2	1	**2**	**Bajo**

Para evaluar las diferencias, se crea la tabla 6, la cual representa los niveles de riesgo y criticidad antes y después de aplicar las estrategias de mitigación.

Tabla 6

Comparación de la Criticidad de los Riesgos

Código de Riesgo	Evaluación inicial (Riesgo inherente)		Evaluación Final (Riesgo residual)	
	Riesgo	Criticidad	Riesgo	Criticidad
R01	6	Medio	2	Bajo
R02	6	Medio	4	Medio
R03	9	Alto	4	Medio
R04	9	Alto	2	Bajo
R05	6	Medio	4	Medio
R06	6	Medio	2	Bajo

En este caso, los resultados reflejan una reducción significativa en la criticidad de tres de los seis riesgos analizados, particularmente en los códigos R01, R04 y R06, los cuales pasaron de un nivel medio o alto a un nivel bajo tras la aplicación de las medidas sugeridas; en el caso del

riesgo R03, la criticidad se redujo de alta a media; mientras que, R02 y R05 mantuvieron su nivel de riesgo medio, aunque con una disminución en el puntaje cuantitativo.

Conclusiones

El comportamiento digital actual de los estudiantes universitarios en la ciudad de Bogotá D.C. revela altos niveles de exposición de datos personales, motivado por la creciente necesidad de acceder y participar en múltiples entornos digitales desde plataformas académicas, redes sociales, foros y comunidades hasta herramientas basadas en inteligencia artificial.

Así mismo, las encuestas aplicadas confirmaron que muchos estudiantes no identifican claramente los riesgos asociados a sus prácticas digitales cotidianas, ni comprenden en su totalidad el alcance del uso de su información personal.

Adicionalmente, una porción significativa de los estudiantes no ha leído o no comprende en profundidad leyes como la Ley 1581 de 2012, la Ley 1266 de 2008 o el RGPD y desconoce aspectos fundamentales sobre sus derechos en la privacidad en entornos digitales, por lo que, limita su capacidad para ejercer derechos fundamentales como el acceso, la rectificación o la revocatoria del consentimiento.

Por otra parte, la identificación de riesgos relacionados con el Internet de las Personas permitió caracterizar amenazas y vulnerabilidades concretas, como el uso contraseñas débiles y compartidas, la exposición excesiva de información, desconocimiento de normas de privacidad y uso de redes inseguras, las cuales permiten el acceso no autorizado, la suplantación de identidad, el ciberacoso o la vigilancia digital.

La revisión de leyes como la Ley 1581 de 2012 y otras normativas de protección de datos nacionales e internacionales evidencia su papel fundamental en la formulación de estrategias de mitigación, dado que, estas normas proporcionan un marco legal sólido que orienta el diseño de acciones educativas, tecnológicas y de concienciación para proteger la privacidad de los estudiantes en entornos digitales.

A partir del diagnóstico cuantitativo y cualitativo, se diseñaron estrategias educativas, normativas y tecnológicas enfocadas para la fácil comprensión en estudiantes universitarios, además, estas estrategias están orientadas a promover un cambio en las decisiones cotidianas de los usuarios, generando conciencia, promoviendo buenas prácticas y fortaleciendo su capacidad de decisión frente al tratamiento de sus datos.

Finalmente, la reevaluación de los riesgos iniciales tras la propuesta de estrategias educativas, normativas y tecnológicas mostró una reducción significativa en la criticidad de los riesgos en la mayoría de los casos, lo que demuestra que, la aplicación combinada de estrategias basadas en normativas existentes y la situación actual de los estudiantes permiten generar un impacto real y positivo en la disminución de la exposición digital de los estudiantes universitarios en la ciudad de Bogotá D.C.

Referencias Bibliográficas

Agreda-Montoro, M. (2024). *Perfil Competencial del Profesorado Andaluz en Seguridad Digital: Evaluación de la Protección de Datos y Privacidad de acuerdo con el Marco de Competencias Digitales para la Ciudadanía (DigComp 2.2).* Pixel-Bit, Revista de Medios y Educación, 70, pp. 123 - 142. Retrieved from: https://institucional.us.es/revistas/PixelBit/70/7_104153.pdf

Armayones Ruiz, M. (2015). Big Data y Psicología: ¿una oportunidad para el Internet de las Personas? Aloma: Revista de Psicologia, Ciències de l'educació i de l'esport Blanquerna, 33, 21–29. Retrieved 9 January 2025 from https://raco.cat/index.php/Aloma/article/view/301479.

Barrios, M. (2022). Necesidad de Proteger los datos personales y privados en las redes sociales. Revista Jurídica Jalisciense, 2, 191–210. Retrieved from https://doi.org/10.32870/rjj.v2i4.130

Barrón, P. (2019). *La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales.* Cuadernos Europeos de Deusto, (61), pp. 29 - 65. Retrieved from: https://ced.revistas.deusto.es/article/view/1644/1996

Bartolomé, M. (2021). Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. Revista de Estudios En Seguridad Internacional, 7(2), 167–185. Retrieved from https://doi.org/10.18847/1.14.9

Berdote E.B. (2022). *The fragility of the fundamental right to the protection of minors' personal data when faced with the exposure of their personal and family life on the internet: The*

need for new mechanisms and legal safeguards. Estudios de Deusto, 70 (2), pp. 49 – 76. Retrieved from: https://revista-estudios.revistas.deusto.es/article/view/2646/3124

Cabezas Azuero, J. (2023). *Tratamiento de datos personales y compliance en Colombia.* Revista de la Facultad de Derecho y Ciencias Politicas, 53 (138), pp. 1 – 25. Retrieved from: https://revistas.upb.edu.co/index.php/derecho/article/view/6778/7038

Castaño, S. (2025). *La inteligencia artificial en Salud Pública: oportunidades, retos éticos y perspectivas futuras.* Revista española de salud pública, 99. Retrieved from: https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2-s2.0-105002541338&origin=resultslist&sort=plf-f&src=s&sid=b2744c6e6f8f0ce6a33f29e6a4e5fde7&sot=a&sdt=a&s=TITLE-ABS-KEY%28datos+AND+privacidad+AND+%28digital+OR+internet%29%29&sl=61&sessionSearchId=b2744c6e6f8f0ce6a33f29e6a4e5fde7

Congreso de Colombia. (2022). Ley 1581 de 2012. Retrieved 12 December 2024, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

David, A., Gomathi Sankar, J., & Azam, M. (2023). Internet Users Top Concerns Ensuring Data Privacy, Security, and Protection.

De la Rosa Rodríguez, P. I. (2021). Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. RIDE Revista Iberoamericana Para La Investigación y El Desarrollo Educativo, 12(23). Retrieved 12 December 2024 from https://doi.org/10.23913/ride.v12i23.980

Función pública (2021). Ley 1266 de 2008. Retrieved from: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Función pública (2022). Ley 1581 de 2012. Retrieved from: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

García González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado*. Boletín Mexicano de Derecho Comparado. Retrieved 9 January 2025 from https://www.scielo.org.mx/scielo.php?pid=S0041-86332007000300003&script=sci_arttext

García, L. (2015). *Perspectiva de los jóvenes sobre seguridad y privacidad en las redes sociales*. Icono 14, volumen (14), pp. 24-49. doi: 10.7195/ri14.v14i1.885. Retrieved from: https://dialnet.unirioja.es/servlet/articulo?codigo=5345626

Guirado, J. (2020). El Internet de las cosas y el Internet de las personas. Retrieved 9 January 2025, from https://www.mundodeportivo.com/urbantecno/android/internet-de-las-cosas-y-personas

Hernández, M.; Renés, P. (2021). *Privacidad en redes sociales: Análisis de los riesgos de auto-representación digital de adolescentes españoles.* Revista Latina de Comunicación Social, (79), pp. 133 - 154. Retrieved from: https://nuevaepoca.revistalatinacs.org/index.php/revista/article/view/1518/3454

Hidalgo, G., Cando, J., Quezada, G., & Granda, J. (2023). Análisis de la protección de datos personales en las redes sociales. Dilemas Contemporáneos: Educación, Política y Valores. Retrieved from https://doi.org/10.46377/dilemas.v2i10.3487

Indriasari, D., & Karman, K. (2023). Privacy, Confidentiality, and Data Protection: Ethical Considerations in the Use of the Internet. International Journal of Islamic Education, Research and Multiculturalism (IJIERM), 5, 431–450. Retrieved from https://doi.org/10.47006/ijierm.v5i2.239

Intersoft Consulting (2016). General Data Protection Regulation GDPR. Retrieved from: https://gdpr-info.eu/

ISO/IEC, SGS. (2022). *ISO 27005:20222*. Retrieved from: https://es.scribd.com/document/708584609/ISO-27005-2022

ISO/IEC. (2023). Sistema de Gestión y Seguridad de la Información (SGSI). Retrieved 9 January 2025 from https://www.iso27000.es/sgsi.html

Kishalay, A. (2018). *Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks.* Journal of Global Marketing, Volume 31, Issue 2, Pages 96 - 110. Retrieved from: https://www-tandfonline-com.bibliotecavirtual.unad.edu.co/doi/full/10.1080/08911762.2017.1412552#abstract

Martínez, M. R., & Pincay-Ponce, J. I. (2024). Buenas Prácticas de Seguridad para la Protección de la Privacidad con Datos Abiertos. Revista Científica de Informática ENCRIPTAR, 7(14), 187–205. Retrieved 9 January 2025 from https://doi.org/10.56124/encriptar.v7i14.010

Martínez, W. (2021). Ciberseguridad en las redes sociales. Una revisión teórica. Revista UNIANDES Episteme. Retrieved 12 December 2024 from https://dialnet.unirioja.es/servlet/articulo?codigo=8298208

Mayorga-Veloz, A., Noboa-Avalos, E., Pajuña-Inchiglema, C., & Mosquera-Endara, M. (2024). Las redes sociales y la violación al derecho de intimidad [Social media and the violation of privacy rights]Social media and the violation of privacy rights [Las redes sociales y la violación al derecho de intimidad]. Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales, 3, 230–241. Retrieved from https://doi.org/10.62574/t2gt9v96

Medina Orozco, L. A. (2022). Entornos digitales. Descripción de hábitos y tendencias de uso de las herramientas tecnológicas. Revista Investigium IRE Ciencias Sociales y Humanas, 13(2), 124–137. Retrieved 9 January 2025 from https://doi.org/10.15658/INVESTIGIUMIRE.221302.09

Meier, Y; Krämer, N. (2025). *Differences in access to privacy information can partly explain digital inequalities in privacy literacy and self-efficacy.* Social Psychology: Media and Communication, 44 (6), pp. 1183 - 1198. Retrieved from: https://www.tandfonline.com/doi/pdf/10.1080/0144929X.2024.2349183?utm_source=scopus&getft_integrator=scopus

MINTIC (2021). ¿Qué es el MGRSD? Retrieved from: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MGRSD/

Montoya, H., & Guzmán, F. (2024). Gamificación: Estrategia preventiva de ciberseguridad para sexting y grooming. Revista Logos, Ciencia & Tecnología, 16, 95–117. Retrieved from https://doi.org/10.22335/rlct.v16i2.1919

Murrugarra Retamozo, B. I. (2024). Inteligencia artificial y privacidad en internet: amenazas para los datos personales de los usuarios Artificial intelligence and privacy on the Internet: threats to users' personal data, 3, 30–48. Retrieved from https://doi.org/10.69516/9dp8ap45

Navarrez, F. (2023). Guía de prevención de riesgos de ciberseguridad derivado del uso del internet y las redes sociales en niños y adolescentes del cantón Cañar. UNIVERSIDAD CATÓLICA DE CUENCA, Quito. Retrieved 12 December 2024 from https://dspace.ucacue.edu.ec/bitstreams/c8e8b114-bd81-41b9-ba6f-6e5fea1fd477/download

Nešić, A. (2023). Data protection about children on the Internet. Savremene Studije Bezbednosti, 29–48. Retrieved from https://doi.org/10.5937/ssb202301029N

Ostec (2022). Concientización de seguridad digital: ¿Qué enseñar a los empleados exactamente? Retrieved from: https://ostec.blog/es/seguridad/concientizacion-de-seguridad-digital-que-ensenar-a-los-empleados-exactamente/

Parlamento europeo y el consejo de la unión europea. (2016). Reglamento general de protección de datos.

Ruschemeier, H. (2025). Generative AI and data protection. Cambridge Forum on AI: Law and Governance, 1. Retrieved from https://doi.org/10.1017/cfl.2024.2

Sánchez Quintero, C. (2021). Redes sociales y gestión de crisis, en entornos de ciberseguridad y ciberdefensa. Seguridad, Ciencia & Defensa, 5, 47–55. Retrieved from https://doi.org/10.59794/rscd.2019.v5i5.pp47-55

Shen, N. (2025). *Canadians and Digital Health Data: Privacy Experiences and Perspectives.* Studies in Health Technology and Informatics, 322, pp. 32 - 36. Retrieved from: https://ebooks.iospress.nl/doi/10.3233/SHTI250009

SIC (2022). Indebido Tratamiento de Datos Personales por casos de suplantación de identidad. Retrieved from: https://www.sic.gov.co/boletin/juridico/habeas-data/indebido-tratamiento-de-datos-personales-por-casos-de-suplantaci%C3%B3n-de-identidad

Superintendencia de Industria y Comercio. (2024). Circular Externa No. 002 de 2024 del 21 de agosto de 2024 “Lineamientos sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial”. Retrieved from: https://sedeelectronica.sic.gov.co/transparencia/normativa/circular-externa-no-002-de-

2024-del-21-de-agosto-de-2024-lineamientos-sobre-el-tratamiento-de-datos-personales-en-sistemas-de

Unesco (2025). Qué debe saber sobre la alfabetización. Retrieved from: https://www.unesco.org/es/literacy/need-know

Unicef (2025). Ciberacoso: qué es y cómo detenerlo. Retrieved from: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Vega, R. (2017). *Redes sociales: riesgos y amenazas*. Cuaderno Jurídico y Político. Volumen2, No.7. Retrieved from: https://revistasnicaragua.cnu.edu.ni/index.php/cuadernojurypol/article/view/6661/8137

Vera Navas, N. A. (2021). Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales. Universidad Politécnica Salesiana, Quito.

Vida Fernández, J. (2022). La gobernanza de los riesgos digitales. CUADERNOS DE DERECHO TRANSNACIONAL, 14(1), 489–503. Retrieved 9 January 2025 from https://doi.org/10.20318/cdt.2022.6695

Yalid. (2025). The Concept Of Legal Norms Of Personal Data Protection Related To Data Processing In The Form Of Artificial Intelligence. Jurnal Riset Multidisiplin Edukasi, 2, 471–496. Retrieved from https://doi.org/10.71282/jurmie.v2i1.75

Yocupicio Sanay, E. (2020). Riesgos cibernéticos a un clic de distancia. Tamma Dalama, 2. Retrieved 9 January 2025 from https://universidadmundial.edu.mx/wp-content/uploads/2020/04/riesgos-ciberneticos-a-un-clicl-de-distancia.pdf

Zhang, J., Yang, A., & Shuaishuai, F. (2022). Data Protection of Internet Enterprise Platforms in the Era of Big Data. Journal of Web Engineering. Retrieved from https://doi.org/10.13052/jwe1540-9589.21314

Apéndices

Apéndice A

Vídeo Presentación de la Propuesta

Video de la presentación de la propuesta inicial: https://youtu.be/3fIodxs_Gx8

Apéndice B

Vídeo de la Sustentación Final

Video de la sustentación final: https://youtu.be/VsaiKP7RYC8

Apéndice C

Variables Clave

- *Nivel de concientización sobre la protección de datos personales:* Se refiere al grado de percepción, comprensión y valoración que tienen los estudiantes universitarios sobre la importancia de proteger sus datos personales en entornos digitales.
- *Justificación:* Esta variable permite evaluar el punto de partida para el diseño de estrategias educativas. Medir el nivel de concientización ayuda a identificar vacíos en la cultura digital preventiva y a proponer intervenciones efectivas para reducir los riesgos de exposición indebida.
- *Prácticas de protección de datos personales:* Se refiere al conjunto de acciones y comportamientos adoptados por los estudiantes universitarios en relación con el uso, almacenamiento y compartición de su información personal en plataformas digitales.
- *Justificación:* Esta variable permite identificar qué tan coherente es el comportamiento digital de los estudiantes con las recomendaciones básicas de ciberseguridad. Este análisis proporciona evidencia empírica sobre las debilidades prácticas que deben abordarse desde una estrategia pedagógica y normativa.
- *Porcentaje de conocimiento sobre normativas de protección de datos:* Se refiere al grado de familiaridad, comprensión y aplicación que los estudiantes poseen respecto a las leyes, normas y lineamientos nacionales e internacionales sobre protección de datos personales, como la Ley 1581 de 2012, la Ley 1266 de 2008, la Circular 002 de 2024, la ISO 27001:2022 y el GDPR.
- *Justificación:* Esta variable es fundamental para diagnosticar la brecha normativa en el entorno universitario. Permite identificar si los estudiantes reconocen sus derechos y

obligaciones en relación con el uso de su información, tanto en instituciones educativas como en plataformas digitales.

- *Nivel Exposición de datos personales en entornos digitales:* Se refiere al nivel en el que los estudiantes hacen pública o comparten su información personal (como ubicación, contactos, fotos, hábitos o datos académicos) a través de redes sociales, plataformas educativas o aplicaciones sin tomar medidas de protección adecuadas.

- *Justificación:* Esta variable permite medir el riesgo real de vulnerabilidad y exposición, sirviendo como base para identificar conductas de alto riesgo que requieren intervención educativa inmediata.

- *Reflexión sobre uso de datos en formularios:* Se refiere al nivel de atención que presta el estudiante al aviso de privacidad o condiciones del uso de sus datos en formularios digitales.

- *Justificación:* Con esta variable se mide el pensamiento crítico digital y la comprensión de los datos personales entregados online.