MINISTERIO DE EDUCACIÓN PÚBLICA

DIRECCIÓN REGIONAL DE EDUCACIÓN DE PURISCAL

COLEGIO TÉCNICO PROFESIONAL DE TURRUBARES

DESARROLLO WEB

RIESGOS DEL USO DE REDES SOCIALES EN LOS ESTUDIANTES DE CUARTO CICLO DEL COLEGIO TÉCNICO PROFESIONAL DE TURRUBARES, DURANTE EL PRIMER PERIODO DEL AÑO 2025

Proyecto final de graduación para optar por el diploma de técnico en el nivel medio en la modalidad desarrollo web

IGNACIO JOSÉ APUY ANCHÍA

ESTELA IVETTE SOTO RIVERA

TURRUBARES, NOVIEMBRE, 2025

Tabla de contenidos

Planteamiento del problema

Las redes sociales digitales (RSD) se han integrado plenamente en la vida cotidiana de la sociedad contemporánea. Plataformas como Instagram, TikTok, Facebook y X (anteriormente Twitter) han redefinido las formas de comunicación, interacción y consumo de información. Para la población adolescente, esta integración es aún más profunda; constituyen la primera generación de "nativos digitales" que ha crecido con estas herramientas como pilar fundamental de su socialización.

Sin embargo, esta inmersión digital constante no está exenta de peligros. La misma naturaleza abierta y conectada de las RSD expone a los usuarios, y en especial a los menores de edad, a una multitud de amenazas que pueden tener consecuencias psicológicas, sociales y económicas. Los estudiantes de secundaria, en pleno desarrollo de su identidad y juicio crítico, son un grupo especialmente vulnerable.

Los riesgos van desde el ciberacoso (cyberbullying) y el acoso digital (stalking), hasta amenazas más técnicas como el phishing (suplantación de identidad para robar credenciales), estafas en línea (ofertas fraudulentas, robos de datos), y la exposición a contenido inapropiado o a depredadores en línea (grooming).

En el contexto del Colegio Técnico Profesional de Turrubares, se observa prácticamente un uso generalizado de dispositivos móviles y redes sociales por parte del estudiantado. No obstante, se desconoce el nivel real de percepción y experiencia que tienen los estudiantes de cuarto ciclo frente a estas amenazas. ¿Saben identificar un intento de phishing? ¿Han sido víctimas de estafas o acoso? ¿Qué medidas de seguridad implementan?

La ausencia de un diagnóstico claro sobre cómo esta población específica interactúa con los riesgos digitales impide a la institución, a los docentes y a los padres de familia diseñar estrategias preventivas eficaces. Este proyecto busca llenar ese vacío de información, respondiendo a la pregunta: ¿Cuáles son los principales riesgos (phishing, estafas, acosadores) asociados al uso de redes sociales, según la percepción y experiencia de los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares?

Justificación del proyecto

La realización de esta investigación se justifica primordialmente por su pertinencia institucional y social. El Colegio Técnico Profesional de Turrubares, como entidad educativa, tiene la responsabilidad de formar integralmente a sus estudiantes, lo cual, en el siglo XXI, incluye necesariamente la competencia de ciudadanía digital. Este proyecto proveerá a la institución datos concretos y actualizados sobre su propia población estudiantil. Esta información es vital para justificar y desarrollar programas de alfabetización digital, talleres de ciberseguridad y protocolos de actuación eficaces frente a casos de acoso en línea, moviendo a la institución de una postura reactiva a una proactiva.

Socialmente, los hallazgos benefician directamente a los actores más vulnerables: los estudiantes y sus familias. Al generar conciencia sobre peligros que quizás subestiman, el estudio actúa como un primer paso preventivo. Además, ofrece a los padres de familia un panorama claro de los riesgos que enfrentan sus hijos, dándoles herramientas para guiar y fomentar un diálogo abierto sobre el uso seguro de la tecnología.

Finalmente, el proyecto posee una alta relevancia formativa para el investigador. Dentro de la especialidad de Desarrollo Web, la seguridad informática (ciberseguridad) es un pilar fundamental. Un desarrollador no solo debe proteger el software (backend) y la infraestructura (servidores), sino también comprender las vulnerabilidades del "factor humano". Entender cómo operan el phishing, la ingeniería social y las estafas desde la perspectiva del usuario final permite al futuro profesional diseñar aplicaciones más seguras, intuitivas y centradas en la protección del usuario.

Descripción del proyecto

El presente proyecto es una investigación de tipo descriptivo con un enfoque cuantitativo. Se centra en diagnosticar la situación actual de los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares respecto a su exposición y percepción de riesgos en redes sociales, específicamente los relacionados con phishing, estafas en línea y acosadores.

La investigación se llevará a cabo mediante la aplicación de un instrumento tipo encuesta, diseñado específicamente para este estudio. Dicha encuesta explorará tres dimensiones principales: 1) Hábitos de uso de RSD; 2) Percepción de riesgo frente a las amenazas mencionadas; y 3) Experiencias personales con dichos riesgos y las medidas de seguridad que aplican.

Se espera que los beneficios de esta investigación radiquen en la generación de un diagnóstico base. Los datos recopilados serán tabulados, analizados estadísticamente y presentados de forma gráfica. El resultado esperado es un informe final que no solo describa la situación, sino que ofrezca recomendaciones accionables para la comunidad educativa, sirviendo como insumo para el desarrollo de futuras intervenciones pedagógicas.

Objetivos del proyecto

Objetivo general

- Analizar los principales riesgos vinculados al uso de redes sociales que enfrentan los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares, para la implementación de una estrategia contra estas amenazas durante el primer periodo del año 2025.

Objetivos específicos

- Identificar los hábitos de uso y las plataformas de redes sociales predominantes que emplean los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares.
- Analizar el entorno de riesgo en redes sociales utilizadas por los estudiantes, en cuanto a amenazas específicas de phishing, estafas en línea y acosadores.
- Proponer estrategias educativas que fomenten un uso responsable y seguro de las redes sociales entre los estudiantes.

Marco teórico

Este estudio se fundamenta en la intersección de la sociología digital, la psicología evolutiva del adolescente y la ciberseguridad.

Definiciones fundamentales del ecosistema digital

Para analizar los riesgos, primero se deben desglosar las herramientas y mecánicas que los estudiantes utilizan a diario.

¿Qué es una red social digital (RSD)?

En su nivel más básico, una Red Social Digital (RSD) o Social Network Site (SNS), es una plataforma en línea (un sitio web o una aplicación) diseñada para facilitar la creación y el mantenimiento de lazos sociales entre personas. Los teóricos pioneros en este campo, Boyd y Ellison (2007), las definen por tres características técnicas:

1. Construcción de un Perfil: Permiten al usuario crear una página personal (un "perfil") que es pública o semipública, donde se describe a sí mismo.

2. Lista de Conexiones: Permiten al usuario articular una "lista de amigos" o "seguidores", es decir, otros usuarios con los que comparte una conexión visible.

3. Navegación de Conexiones: Permiten al usuario ver y navegar no solo su propia lista de conexiones, sino también las listas de conexiones de los demás.

Lo que define a una red social no es solo la capacidad de conectar, sino la capacidad de hacer públicas esas conexiones.

La Interacción: El "Like", el "Share" y el "Comentario"

La socialización dentro de estas plataformas se basa en unidades de interacción cuantificables.

El "Like" (Me Gusta): Es la unidad de retroalimentación social más fundamental del ecosistema digital. Se representa comúnmente con un ícono de corazón o un pulgar hacia arriba. Su función es triple:

1. Función Social: Es una señal de aprobación social no verbal. Indica al creador del contenido "te vi y apruebo esto".

2. Función Psicológica: Para el receptor, cada "like" funciona como una micro dosis de dopamina, un neurotransmisor asociado al placer y la recompensa. Esto crea un ciclo de refuerzo positivo que incentiva al usuario a publicar más contenido.

3. Función Algorítmica: Para la plataforma, cada "like" es un punto de datos. Le enseña al algoritmo "a este usuario le gusta este tipo de contenido", permitiéndole personalizar las recomendaciones del usuario para mantenerlo conectado por más tiempo.

El "Share" (Compartir): Es la acción de tomar un contenido y publicarlo para la propia red de contactos. Es una interacción de mayor valor que el "like", pues implica que el usuario se identifica con el contenido al punto de convertirlo en parte de su propia identidad digital. Es el motor de la "viralidad".

El "Comentario": Es una interacción de alto esfuerzo que abre un diálogo público. Puede ser una fuente de conexión social (comentarios positivos) o un vector de ataque directo (ciberacoso).

El "Algoritmo": El curador de contenido

El "algoritmo" es un término popular para referirse a los sistemas de recomendación automatizados que deciden qué contenido ve un usuario y en qué orden. Ningún usuario ve la totalidad de lo que publican sus contactos. En su lugar, la plataforma utiliza un software complejo que analiza miles de puntos de datos (qué se mira, a qué se le da "like", cuánto tiempo se pasa en cada video, la ubicación, etc.) para crear un feed (flujo de contenido) personalizado y adictivo. El objetivo del algoritmo no es informar al usuario, sino retener su atención el mayor tiempo posible para mostrarle más anuncios.

Plataformas en relevancia

TikTok: Es una plataforma de origen chino (propiedad de ByteDance) centrada exclusivamente en videos de formato corto y vertical. Su principal innovación no es el video, sino su algoritmo, conocido como "For You Page" (FYP) o "Para Ti". A diferencia de otras redes que prioriza a quienes "sigues", el FYP de TikTok te muestra contenido de perfectos desconocidos que el algoritmo cree que te gustarán. Es un sistema de descubrimiento de contenido extremadamente eficaz y adictivo, lo que explica su rápida penetración en el mercado adolescente.

Instagram: Propiedad de Meta (Facebook), Instagram comenzó como una plataforma de fotografía (imágenes estáticas con filtros). Ha evolucionado para competir directamente con sus rivales, absorbiendo sus funciones: introdujo las "Stories" (historias efímeras de 24 horas) para competir con Snapchat, y los "Reels" (videos cortos verticales algorítmicos) para competir con TikTok. Actualmente, es un híbrido que combina perfiles basados en imágenes, mensajería directa (DM) e historias efímeras.

Facebook: Propiedad de Meta, es la red social generalista y fundacional por excelencia, con el mayor número de usuarios activos a nivel global. Su enfoque principal es la conexión personal a largo plazo entre amigos y familiares, así como la gestión de grupos e intereses comunitarios. Aunque ha integrado funciones como videos y “Stories”, su propuesta de valor se mantiene en la sección de noticias personalizada, la creación de eventos y su robusta estructura para la gestión de páginas de marcas y negocios. Es una plataforma con un amplio espectro demográfico, siendo popular en generaciones mayores (Generación X y Millennials).

Snapchat: Desarrollada por Snap Inc., fue pionera en el concepto de contenido efímero. Su característica principal son los "snaps", mensajes (fotos o videos cortos) que desaparecen automáticamente después de ser vistos. Su foco está en la interacción personal y divertida, utilizando filtros de realidad aumentada (Lenses), mapas de localización en tiempo real (Snap Map) y una interfaz centrada en la cámara. Aunque introdujo las Stories (copiadas luego por Instagram), su principal fortaleza reside en la mensajería instantánea y las herramientas creativas en tiempo real. Es especialmente popular entre la Generación Z.

WhatsApp: Propiedad de Meta, es la aplicación de mensajería instantánea líder a nivel mundial, más que una red social tradicional. Su valor se centra en la comunicación privada, directa y cifrada de extremo a extremo entre individuos o pequeños grupos. Permite el envío de mensajes de texto, notas de voz, llamadas, videollamadas y archivos multimedia. Sus funciones secundarias, como los "Estados" (contenido efímero similar a las Stories) y WhatsApp Business (para la interacción entre empresas y clientes), complementan su rol primario de comunicación.

X (Twitter): Anteriormente conocida como Twitter, es una plataforma de microblogging cuyo formato principal se basa en mensajes cortos (posts o tweets). Se distingue por su velocidad y su rol como altavoz de noticias de última hora, debates públicos, tendencias y conversaciones en tiempo real (“trending topics”). La interacción se basa en la publicación, el “retuit” (republicar) y el uso de hashtags para agrupar temas. A diferencia de otras redes, el contenido es a menudo más enfocado en lo que está sucediendo "ahora" y en la opinión pública.

Telegram: Es un servicio de mensajería instantánea en la nube (lo que permite su uso en múltiples dispositivos simultáneamente) y una plataforma de distribución de contenido a través de canales y grupos masivos (con capacidad para cientos de miles de miembros). Se destaca por su velocidad, seguridad y su enfoque en la privacidad (incluyendo chats secretos y la opción de autodestrucción de mensajes). Sus canales funcionan como herramientas de transmisión unidireccional para grandes audiencias, siendo popular para la difusión de noticias, comunidades de nicho y contenido sin la moderación de otras plataformas.

Formatos fundamentales: Blog y microblogging

Antes de la explosión de las redes sociales visuales, dos formatos de contenido sentaron las bases para la publicación de contenido personal en línea:

Blog: Es el antecesor directo de la publicación en redes sociales. Un blog (abreviatura de web log o "bitácora web") es un sitio web que recopila cronológicamente artículos o publicaciones de uno o varios autores. El contenido suele ser más extenso y reflexivo. Aunque han perdido popularidad frente a la inmediatez de las RSD, siguen siendo fundamentales para el contenido de nicho y profesional.

Microblogging: Es una evolución del blog que se centra en la brevedad y la frecuencia. Como se mencionó en la definición de X (Twitter), las plataformas de microblogging permiten a los usuarios compartir actualizaciones cortas de texto, imágenes o enlaces. Estas publicaciones ("posts") son fáciles de consumir y compartir, lo que fomenta la conversación en tiempo real y la rápida difusión de información.

La sociedad red y el adolescente conectado

El sociólogo Manuel Castells (2010) argumenta que vivimos en una "Sociedad Red", donde las estructuras sociales y el poder se organizan en torno a redes de información digitales. Las RSD son la manifestación más personal de esta estructura. Para el adolescente, estas plataformas no son un "mundo virtual" separado del "mundo real". Son simplemente una extensión de su realidad social. Lo que ocurre en línea (un comentario, un "like", una exclusión) tiene repercusiones emocionales y sociales reales e inmediatas en el colegio al día siguiente.

El contexto entre generaciones

Comprender la simbiosis entre el adolescente y la red exige diferenciar su cohorte demográfica de la de sus predecesores. La distinción entre las experiencias de la Generación Z y la Generación Millennial es clave, ya que los riesgos y la percepción de la tecnología no son universales; están mediados por la época en que cada grupo la adoptó.

Por un lado, los Millennials (nacidos aprox. 1981-1996) son los "pioneros digitales". No nacieron con internet, sino que su adolescencia transcurrió en paralelo a la masificación de las computadoras de escritorio, el email y las primeras redes sociales. Tuvieron que aprender y adoptar la tecnología, y para ellos existió durante mucho tiempo una clara división entre la vida "online" y la "offline".

En contraste, la Generación Z (nacidos aprox. 1997-2012), que compone el grupo de adolescentes actual, son los verdaderos "nativos digitales". Es la primera generación que no conoce un mundo sin internet, smartphones o redes sociales. Para ellos, no existe una división entre lo real y lo virtual; es una única realidad híbrida, tal como lo expone Castells. Su socialización, identidad y aprendizaje están intrínsecamente mediados por la conectividad móvil, visual e instantánea.

Construcción de la identidad en la adolescencia digital

El psicólogo Erik Erikson (1968) definió la adolescencia como la etapa vital marcada por la crisis de "Identidad vs. Confusión de Roles". El joven busca responder a la pregunta "¿Quién soy yo?". Las RSD actúan como un laboratorio 24/7 para esta experimentación. El "perfil" es un escenario donde el adolescente actúa como actor, director y curador de su propia imagen.

Esta "identidad digital" curada se enfrenta a la retroalimentación constante y cuantificable (likes, seguidores). Esto puede exacerbar la "audiencia imaginaria", un concepto psicológico donde el adolescente siente que está constantemente siendo observado y juzgado. La búsqueda de esta validación social cuantificable puede llevar a los jóvenes a asumir conductas de riesgo, como la sobreexposición de información personal o la priorización de la popularidad sobre la seguridad.

Taxonomía de riesgos digitales

Los peligros en este entorno se pueden clasificar en función de la naturaleza de la amenaza. Para este proyecto, nos centramos en dos categorías principales: riesgos de ciberseguridad (el engaño técnico) y riesgos de interacción (el depredador humano).

Riesgos de ciberseguridad (El engaño técnico)

Estos riesgos involucran engaños técnicos y exposición a contenido malicioso, cuyo objetivo principal suele ser el beneficio económico o la vulneración de datos.

Ingeniería Social: Es el concepto clave que unifica esta categoría. Se define como el arte de la manipulación psicológica para engañar a las personas y que realicen acciones que no deberían (como revelar información confidencial) o quebrar procedimientos de seguridad. El ataque no va dirigido al software, sino al usuario. Se explota la confianza, la curiosidad, el miedo o la urgencia.

Phishing (Suplantación de Identidad): Es la forma más común de ingeniería social:

Definición: Es el envío de comunicaciones fraudulentas (usualmente correos electrónicos, pero también mensajes directos o “Smishing” vía SMS) que suplantan la identidad de una entidad legítima (un banco, Netflix, Instagram, el MEP, etc.).

El Ataque: El mensaje busca generar urgencia o miedo. Ejemplos comunes: "Tu cuenta ha sido comprometida, haz clic aquí para verificarla", "Detectamos un inicio de sesión sospechoso", "Ganaste un premio".

El Gancho: El mensaje contiene un enlace (el "gancho"). Al hacer clic, la víctima es redirigida a un sitio web falso que es visualmente idéntico al real (una "página espejo").

El Robo: La víctima, creyendo estar en el sitio legítimo, introduce sus credenciales (usuario y contraseña). Esos datos no inician sesión, sino que se envían directamente al atacante. El atacante ahora tiene control total de la cuenta.

Estafas en Línea (Scams): Es un término más amplio para cualquier tipo de fraude en línea que busca un beneficio económico directo. En el contexto adolescente, estas estafas se adaptan a sus intereses:

Estafas de Videojuegos: Promesas de moneda virtual gratuita (V-Bucks en Fortnite, Robux en Roblox, "skins" en CS: GO) a cambio de ingresar los datos de la cuenta o completar "encuestas" que roban información.

Falsos Premios y Sorteos (Giveaways): Notificaciones de que han ganado un premio (un iPhone, una tarjeta de regalo de SHEIN) que requiere un pequeño pago de "gastos de envío" o el registro de datos bancarios.

Estafas de Inversión Falsas: Crecientemente dirigidas a jóvenes, promesas de "dinero fácil" invirtiendo en criptomonedas o esquemas piramidales.

Tiendas Fraudulentas: Publicidad en Instagram o TikTok de productos (zapatillas, ropa, tecnología) a precios irreales. La víctima paga y el producto nunca llega.

Riesgos de interacción y conducta (El depredador humano)

Estos riesgos surgen de la interacción social con otros usuarios malintencionados.

Acoso Digital (Stalking): Implica una persecución u observación obsesiva y no deseada mediante medios digitales que genera miedo o angustia. Puede incluir el monitoreo constante de todas las publicaciones, la creación de perfiles falsos para interactuar, el envío masivo de mensajes y amenazas directas.

Grooming (Acoso Sexual de Adultos a Menores): Es el riesgo de interacción más severo. No es un evento, es un proceso deliberado que sigue etapas predecibles:

1. Etapa de Identificación: El acosador (que a menudo usa un perfil falso, fingiendo ser un par) busca víctimas en espacios públicos (comentarios de TikTok, juegos en línea, chats de Instagram). Busca jóvenes que expresan vulnerabilidad, soledad o baja autoestima.

2. Etapa de Ganar Confianza: El acosador inicia una conversación. Se muestra como un amigo comprensivo, comparte "secretos", ofrece apoyo emocional y valida los sentimientos del menor. Construye un lazo de confianza y dependencia.

3. Etapa de Aislamiento: El acosador intenta aislar al menor de su red de apoyo. Le dice "tus padres no te entienden, yo sí", "no le cuentes a tus amigos, esto es solo nuestro". Mueve la conversación de una plataforma pública (comentarios de TikTok) a una privada (Mensaje Directo de Instagram, luego a WhatsApp).

4. Etapa de Normalización y Petición: Una vez construida la confianza y el aislamiento, el acosador normaliza la conversación sexual, primero con insinuaciones y luego pidiendo explícitamente fotos o videos íntimos (sexting).

5. Etapa de Extorsión (Sextorsión): Si el menor accede, el acosador usa ese material para extorsionar, pidiendo más material o dinero a cambio de no hacer públicas las imágenes.

Riesgos psicológicos y de conducta

Aunque no son el foco principal (phishing/estafas), estos riesgos forman parte del contexto.

Ciberacoso (Cyberbullying): A diferencia del grooming (adulto a menor) o stalking (persecución), el ciberacoso es una agresión intencional, repetitiva y mantenida en el tiempo, perpetrada por pares (otros estudiantes) utilizando medios digitales. Sus características (anonimato, viralidad y persistencia 24/7) lo diferencian del acoso tradicional.

Sexting (Envío de Contenido Íntimo): Es un neologismo que surge de la unión de "sex" (sexo) y "texting" (enviar mensajes). Describe el acto de enviar, recibir o reenviar mensajes, fotografías o videos de contenido sexualmente explícito o erótico a través de dispositivos digitales (principalmente smartphones). Aunque a veces ocurre de forma consensuada entre pares, el sexting presenta dos riesgos principales. Primero, la pérdida total de control sobre el contenido; una vez enviado, el material puede ser enviado, publicado o robado, volviéndose permanente e imposible de eliminar de internet. Segundo, es la herramienta fundamental de coerción en la Sextorsión: un atacante (sea un par o un adulto) utiliza material de sexting que obtuvo (ya sea por coerción, engaño o confianza rota) para extorsionar a la víctima.

Alfabetización digital y mediación

Frente a este complejo panorama de riesgos, la literatura académica propone dos soluciones complementarias: alfabetización y mediación.

Alfabetización Digital (Resiliencia): Es un concepto que trasciende el simple "saber usar" un dispositivo. Implica la capacidad de acceder, analizar, evaluar y crear contenido de forma crítica y segura. Una persona digitalmente alfabetizada no solo sabe configurar la privacidad de su cuenta, sino que sabe evaluar críticamente un mensaje sospechoso de phishing, reconociendo las "banderas rojas" (red flags) como errores ortográficos, remitentes extraños o la solicitud de urgencia.

Mediación Parental: Se refiere a las estrategias que usan los padres para gestionar el uso de internet de sus hijos. Esta mediación puede ser restrictiva (prohibir plataformas, instalar software de bloqueo) o activa (conversar sobre los riesgos, enseñar a evaluar contenido, establecer reglas consensuadas). Los estudios sugieren que la mediación activa es más efectiva a largo plazo para construir resiliencia digital en los adolescentes.

Metodología

Enfoque y tipo de investigación

La investigación utilizará un enfoque cuantitativo, ya que busca medir la frecuencia, prevalencia y percepción de los riesgos a través de la recolección y análisis de datos numéricos. El tipo de estudio es descriptivo, pues busca especificar las propiedades y características del fenómeno estudiado (los riesgos percibidos y experimentados) en la población seleccionada. Asimismo, es de corte transeccional, ya que los datos se recopilan en un único momento (el primer periodo lectivo de 2025).

Población y muestra

Población: La población objeto de estudio está constituida por la totalidad de los estudiantes matriculados en el cuarto ciclo del Colegio Técnico Profesional de Turrubares durante el curso lectivo 2025. Durante el presente año, según datos obtenidos de la matrícula, hay un total de 108 estudiantes en cuarto ciclo, donde 42 son de décimo grado, 34 son de undécimo grado, 29 son de duodécimo grado, y 3 son de plan nacional (Apéndice 1).

Muestra: Se utilizará un muestreo parcial de la población. Se estima que el porcentaje aproximado para obtener resultados favorables es de al menos el 50% de la población, que en este caso serían al menos 54 estudiantes.

Instrumento de recolección de datos

Se diseñará y aplicará un cuestionario (encuesta) estructurado como instrumento principal. El instrumento será validado mediante juicio de expertos (revisión por parte de la tutora) antes de su aplicación. Se estructurará en las siguientes secciones:

1. Datos Sociodemográficos: (Edad, género).

2. Patrones de Uso de RSD: (Tiempo diario de conexión, plataformas más usadas).

3. Percepción de Riesgos: (Usando una escala del 1 al 5 para medir qué tan peligrosos perciben el phishing, las estafas y los acosadores).

4. Experiencia Directa con Riesgos: (Preguntas Sí/No) sobre si han recibido mensajes de phishing, si han sido víctimas de estafas o si han sido contactados por acosadores).

5. Medidas de Seguridad: (Preguntas de opción múltiple sobre las prácticas de seguridad que implementan, ej. uso de contraseñas, configuración de perfil privado, verificación en dos pasos).

El instrumento final se incluirá en la sección de apéndices (Apéndice 2).

Procesamiento de datos

Los datos recopilados de la encuesta serán analizados y representados en tablas. Se aplicará estadística descriptiva para obtener frecuencias absolutas, porcentajes y promedios. Los resultados serán visualizados mediante gráficos (de barras y circulares) para facilitar su interpretación, los cuales se presentarán en la sección de Resultados y los datos en tablas serán presentados en la sección de apéndices (Apéndices 3-16).

Estrategia de concientización

Se elaborará una Estrategia de Concientización y Transferencia del Conocimiento dirigida a la población meta (estudiantes del cuarto ciclo) y al cuerpo docente, basándose directamente en los resultados del estudio descriptivo.

El propósito de esta estrategia es transformar los datos descriptivos en acciones de prevención específicas. No se presentará información general sobre ciberseguridad, sino que se abordarán y priorizarán los riesgos que hayan mostrado mayor prevalencia (experiencia directa) y menor percepción de peligro en la población encuestada.

Cronograma de actividades

Cronograma del proyecto final de graduación

Curso lectivo 2025

Centro educativo: CTP Turrubares **Tipo de proyecto:** Investigación

Nombre completo del estudiante (s): Ignacio José Apuy Anchía

Nombre completo de la persona tutora: Estela Ivette Soto Rivera

Nombre del proyecto: Riesgos del uso de redes sociales en los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares, durante el primer periodo del año 2025

			Meses								
N°	**Descripción de la tarea**	**Responsable**	**Semana**				**Semana**				**N° horas**
			1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
1	Análisis del contexto en la institución. Propuesta de tema de proyecto en base a problemáticas encontradas.	• Ignacio Apuy Anchía	X								35
2	Discusión y aprobación del tema. Creación y revisión de objetivos.	• Ignacio Apuy Anchía		X							32
3	Estructuración inicial del documento. Redacción de secciones (Planteamiento, Justificación, Descripción)	• Ignacio Apuy Anchía			X						28
4	Desarrollo del marco teórico, marco metodológico y búsqueda de referencias.	• Ignacio Apuy Anchía				X					43
5	Creación y aplicación de encuesta a estudiantes de manera presencial.	• Ignacio Apuy Anchía					X				42
6	Procesamiento de datos. Creación de gráficos, redacción de resultados, conclusiones y recomendaciones.	• Ignacio Apuy Anchía						X			51
7	Elaboración de estrategia (Planteo, contenido, código, pruebas). Redacción y revisión final del proyecto.	• Ignacio Apuy Anchía							X		58
8	Revisiones adicionales. Presentación final.	• Ignacio Apuy Anchía								X	31
										Total de horas	320

Lista de materiales, productos y servicios utilizados

Equipo físico

- Computadora de escritorio.
- Computadora portátil.
- Smartphone.

Servicios adicionales contratados

- Acceso a Internet.

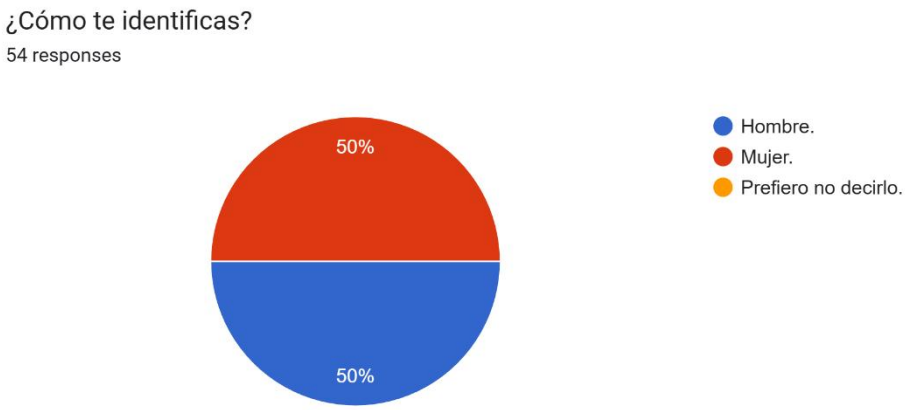
Plataformas digitales (Software)

- Microsoft Word.
- Microsoft Excel.
- Google Drive.
- Google Docs.
- Google Forms.
- Canva.
- Microsoft Visual Studio Code.

Resultados

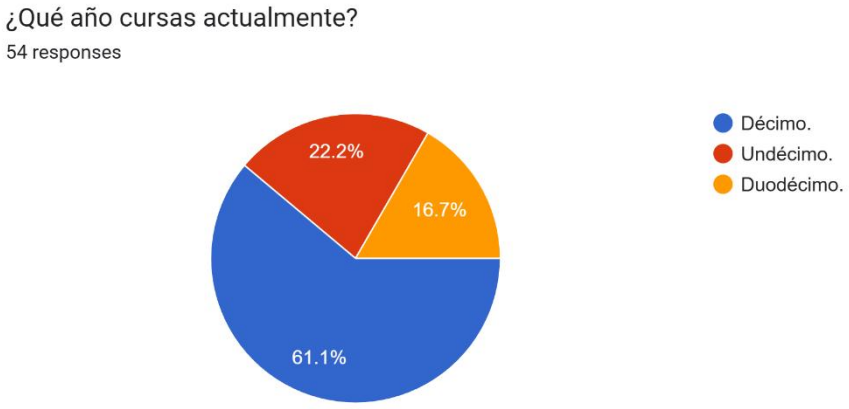
En esta sección se presentan los resultados obtenidos de la encuesta aplicada a 54 estudiantes (50% del total de 108 estudiantes) del cuarto ciclo del Colegio Técnico Profesional de Turrubares.

Gráfico 1: Identificación por género



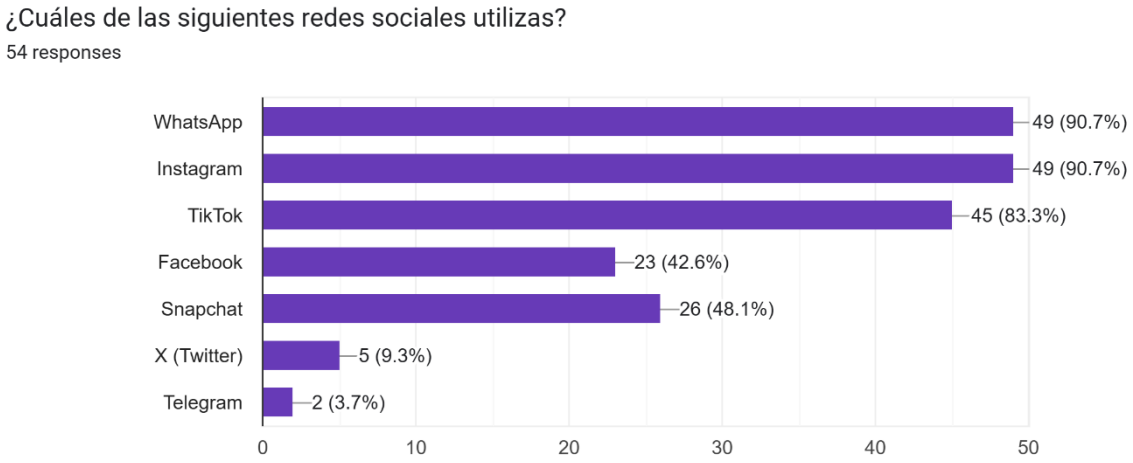
Como muestra el Gráfico 1, una mitad de la población encuestada es hombre, mientras que la otra mitad es mujer. Esto quiere decir que, aunque no se tomó en cuenta a toda la población (108 estudiantes), sí se obtuvo un resultado balanceado, lo que favorece los siguientes resultados ya que existe equidad entre percepciones.

Gráfico 2: Identificación por sección



Según los datos obtenidos a partir del Gráfico 2, la mayoría con un 61.1% de los encuestados se encuentra cursando décimo año, seguido de undécimo año con un 22.2%, y finalmente duodécimo año siendo la menor cantidad con un 16.7%. Estos datos coinciden con la distribución de estudiantes matriculados de cuarto ciclo, los cuales se ordenan de mayor a menor de la misma forma.

Gráfico 3: Redes sociales según su uso

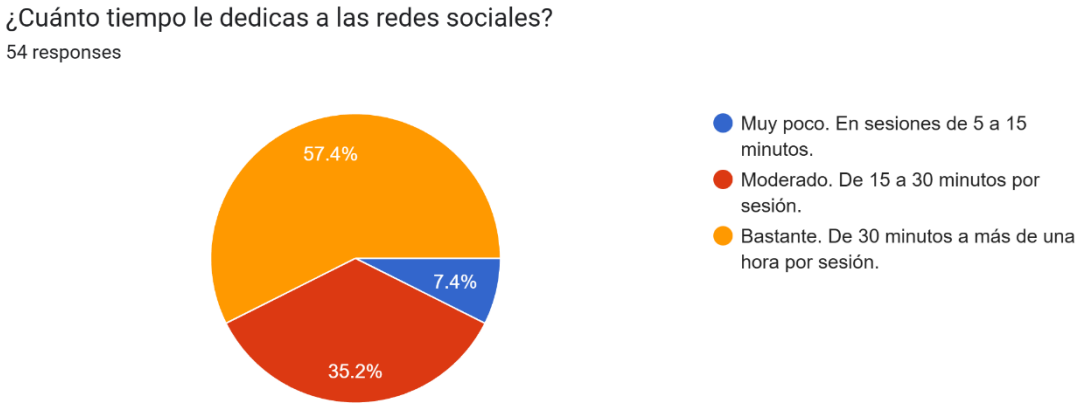


De los resultados del Gráfico 3 se puede destacar que las redes sociales más utilizadas por los estudiantes encuestados son WhatsApp, Instagram y TikTok, donde WhatsApp e Instagram poseen 49 votos cada una, mientras que TikTok se acerca con 45 votos. Seguidamente se encuentran Facebook y Snapchat con 23 y 26 votos respectivamente, situándose entre las redes que no todos usan, pero sí siguen siendo relevantes.

Finalmente, X (anteriormente Twitter) y Telegram se ubican como las apps menos utilizadas por los estudiantes encuestados, demostrando que, debido a su formato y/o contenido, no llegan a generar el mismo interés que otras redes sociales.

De la información anterior se demuestra no solo un mayor enfoque en la mensajería como tal, presentes en WhatsApp e Instagram, sino también en el entretenimiento rápido y efectivo que ofrecen principalmente TikTok e Instagram, gracias a sus videos cortos.

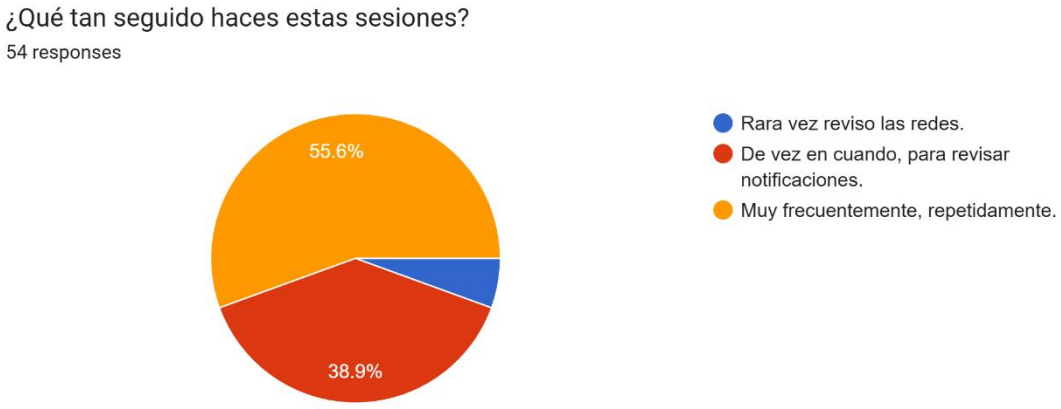
Gráfico 4: Tiempos por sesión en redes



A partir del Gráfico 4, se obtiene que un 57.4% de los estudiantes encuestados dedican gran parte de su tiempo a largas sesiones en redes sociales, alcanzando más de media hora de dicho tiempo, e incluso horas. Luego, con un 35.2%, se obtiene a aquellos estudiantes que no dedican mucho ni poco tiempo a las redes sociales, o sea un intermedio. Finalmente, con una pequeña cantidad de 7.4%, se encuentran a aquellos estudiantes que se limitan a participar poco tiempo por sesión.

Estos datos nos indican que una gran parte de los estudiantes invierten su tiempo en redes sociales en sesiones extensas, lo que puede llegar a afectar otras tareas de su día a día, pero también los expone a amenazas presentes en las mismas redes dada su participación.

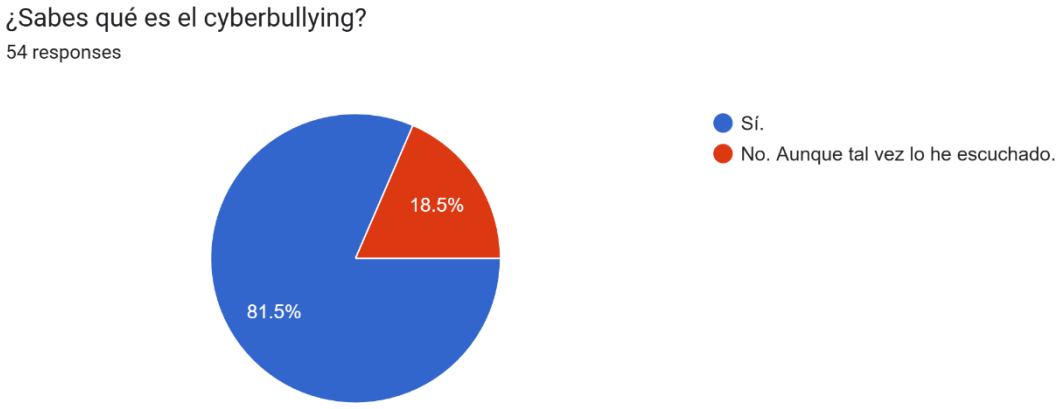
Gráfico 5: Intervalos entre sesiones en redes



Según los datos del Gráfico 5, una gran parte con un 55.6% de los estudiantes se encuentran activamente en redes sociales, en sesiones bastante frecuentes. Luego se encuentra un 38.9% de los estudiantes en términos intermedios, utilizando las redes sociales casualmente, principalmente para obtener nuevas actualizaciones de diversos sucesos. En último lugar se encuentra una mínima cantidad de 5.6% de estudiantes que rara vez utilizan redes sociales.

De acuerdo con estos datos, se puede destacar que existe un gran apego por parte de la población estudiantil a estar conectado en redes sociales, lo que se puede complementar con el Gráfico 4 que nos indica que un gran número participan en largas sesiones, indicando aún más interés en la interacción activa en redes.

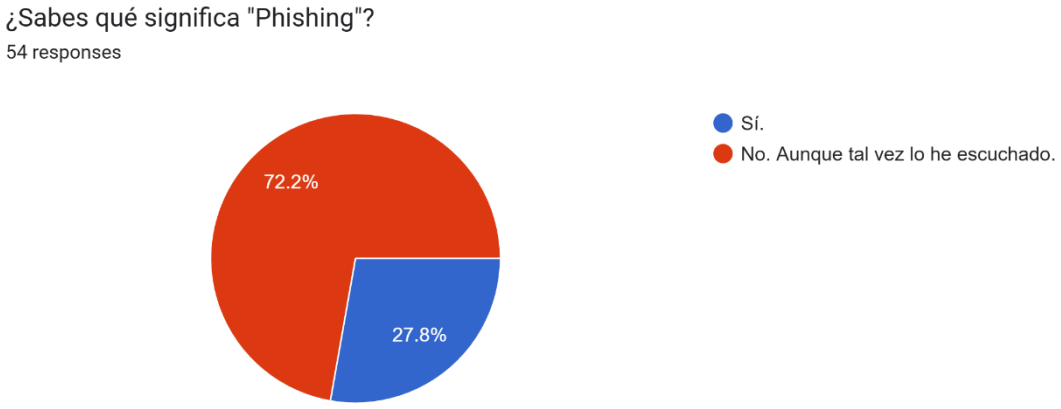
Gráfico 6: Conocimiento sobre el cyberbullying



El Gráfico 6 nos indica que más de la mitad de los estudiantes, con un 81.5%, tienen conocimiento sobre el término de cyberbullying, siendo uno de los factores más relevantes en cuanto a riesgos en redes sociales. El otro 18.5% de los estudiantes no conoce el significado de este término, aunque no se descarta que lo hayan podido escuchar anteriormente.

Esto nos resulta en que gran parte de la población de estudiantes está consciente sobre el significado del término cyberbullying y sus efectos.

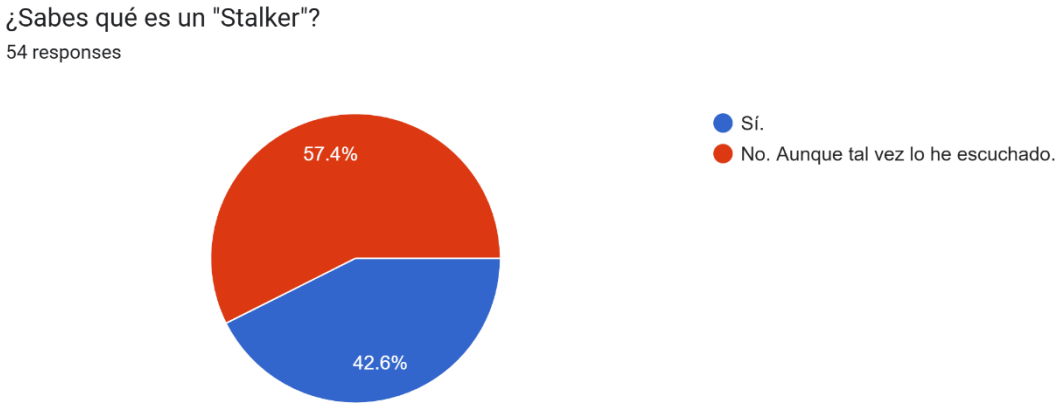
Gráfico 7: Conocimiento sobre el “Phishing”



El Gráfico 7 nos destaca que un 72.2% de la población desconoce el término “Phishing”, que, aunque utilizado técnicamente en gran parte, es importante para saber identificar estafas y riesgos similares. El otro 27.8% de los estudiantes sí logró identificar correctamente el término.

Esta información nos indica que un menor número de estudiantes realmente asocia correctamente el término, lo que no significa un mayor problema si aun así se identifican los riesgos, pero puede aplicarse mayor concientización.

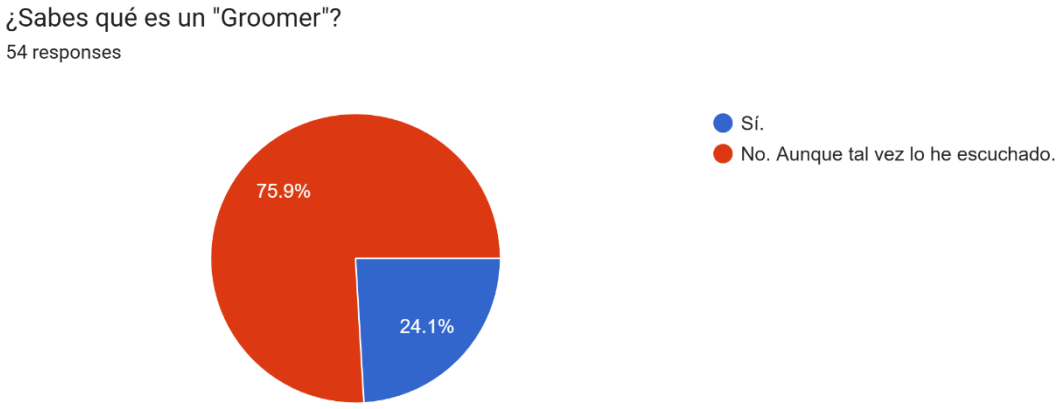
Gráfico 8: Conocimiento sobre los “Stalker”



A partir del Gráfico 8 se obtiene que un 57.4% de los estudiantes desconoce el término “Stalker”, pero no quiere decir que no se sepa de qué trata. Por otro lado, un fuerte 42.6% de los estudiantes conoce sobre el término, lo que se aproxima a la mitad, pero sigue sin alcanzarla.

Estos datos resultan en casi la igualdad entre aquellos estudiantes que conocen y los que desconocen el término. A diferencia del término “Phishing”, al menos aquí se encuentra que casi la mitad de la población sí logra identificar a los “Stalker”, pero sigue siendo un número bajo.

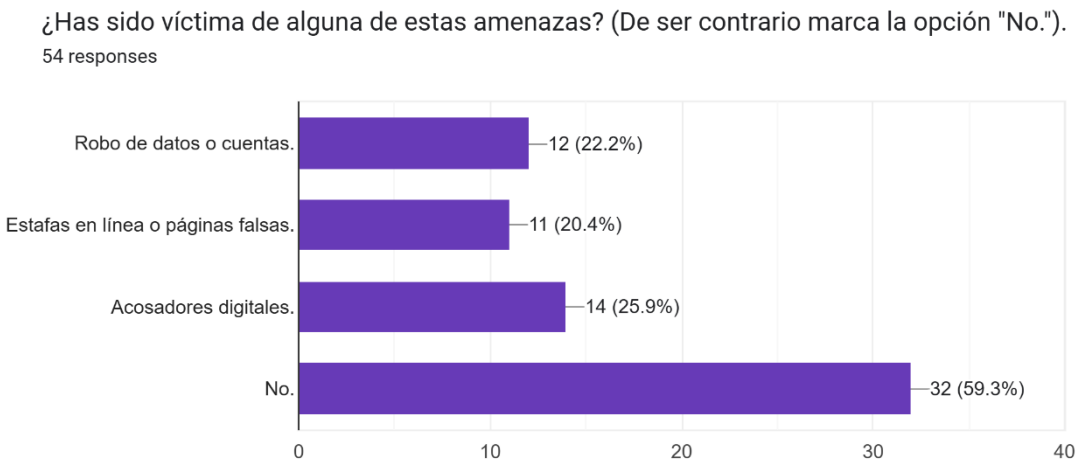
Gráfico 9: Conocimiento sobre los “Groomer”



A partir del Gráfico 9 se obtiene que un 75.9% de la población no logró identificar el término “Groomer”, aunque no se descarta completamente que lo hayan escuchado anteriormente. El otro 24.1% de los estudiantes sí conocen el término y su significado.

Este resultado quiere decir que son medianamente pocos los estudiantes que saben sobre el significado y las acciones de un “Groomer”, lo que sí puede generar cierta preocupación ya que son actores de suma relevancia en cuanto a los riesgos que se presentan en redes sociales.

Gráfico 10: Índices de amenazas y población afectada

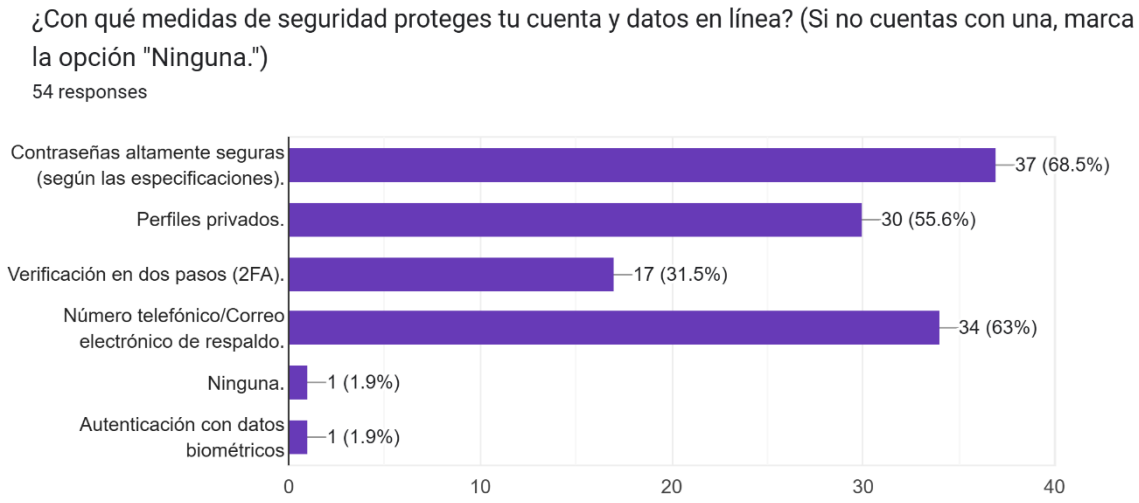


Según el Gráfico 10, un gran porcentaje de la población encuestada no ha sido víctima de alguna de las amenazas sugeridas, dicho porcentaje de un 59.3%. Un 22.2% de los estudiantes encuestados se ha enfrentado a robo de datos personales o de autenticación y por lo tanto cuentas. Otro 20.4% de la población se ha encontrado y ha sido víctima a causa de alguna página falsa, estafa o engaño a través de redes sociales. Situándose por encima de las demás amenazas indicadas, se encuentra un 25.9% de la población que ha sido afectada por acosadores en línea.

Dados los datos anteriores, se detalla que, aunque muchos no han sido afectados por alguna estafa, acoso, etc., sigue existiendo el riesgo y las víctimas a causa de estos y otras amenazas.

Aunque no se tomó en cuenta individualmente el género de los encuestados, es importante destacar que estudios globales de entidades como ONU Mujeres y la OEA (Organización de los Estados Americanos) demuestran que las mujeres jóvenes y adolescentes sufren acoso en línea (especialmente de tipo sexual y stalking) de manera desproporcionada. Este estudio se debe tomar en cuenta ya que el acoso sigue siendo uno de los rubros muy altos, y un punto que vulnera principalmente a las mujeres jóvenes.

Gráfico 11: Aplicación de medidas de seguridad



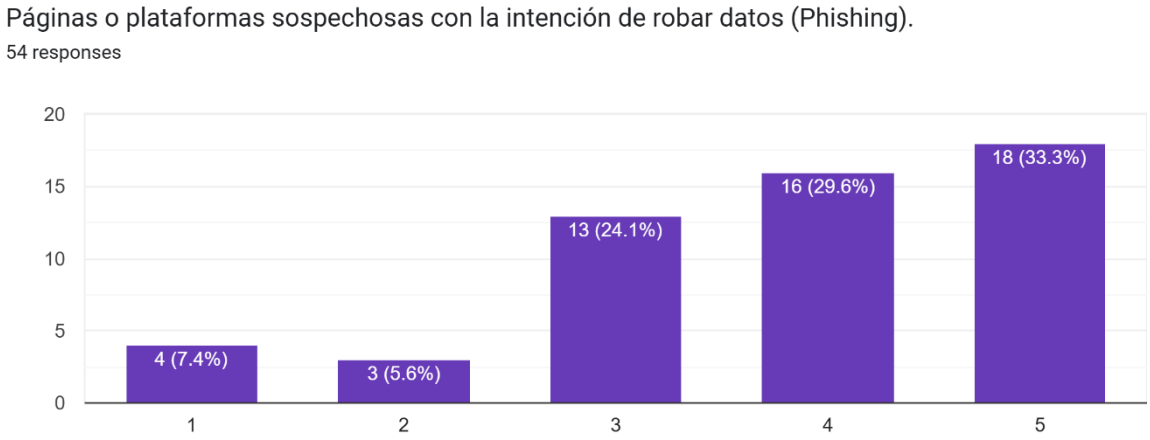
De acuerdo a los datos obtenidos en el Gráfico 11, se obtiene que una mayoría del 68.5% de los estudiantes utiliza contraseñas altamente seguras según especificaciones estándar como el uso de caracteres alfanuméricos, símbolos, entre otros. Otra mayoría de estudiantes con un 63% utiliza correos y/o números de teléfono alternativos como respaldo en caso de que su cuenta principal se vea afectada.

Un porcentaje de 55.6% estudiantes utiliza perfiles privados para asegurar su privacidad y mantener sus datos y hábitos personales lejos de todo público. Seguidamente, un 31.5% de los estudiantes utilizan verificación en dos pasos, método que genera una protección extra además de la contraseña.

Finalmente, una mínima parte de la población, un 1.9%, no cuenta con ninguna de los métodos de seguridad anteriormente mencionados. Adicionalmente, un estudiante sugiere la autenticación con datos biométricos como método alternativo, que es de gran importancia ya que provee una protección extra además de la habitual contraseña, pero ya cuenta como un método de verificación en dos pasos, que fue sugerido anteriormente.

Los datos anteriores son de gran importancia y representan a una población segura y preventiva contra los riesgos de seguridad en redes sociales en casi su totalidad. Gran parte de la misma utilizan los métodos habituales en cuanto a protección en línea, aunque se refleja la falta de métodos aún más seguros y eficientes como la verificación de doble factor, altamente recomendada por organizaciones a nivel mundial (Microsoft, 2022), y herramienta importante para aumentar la seguridad drásticamente contra ataques en línea.

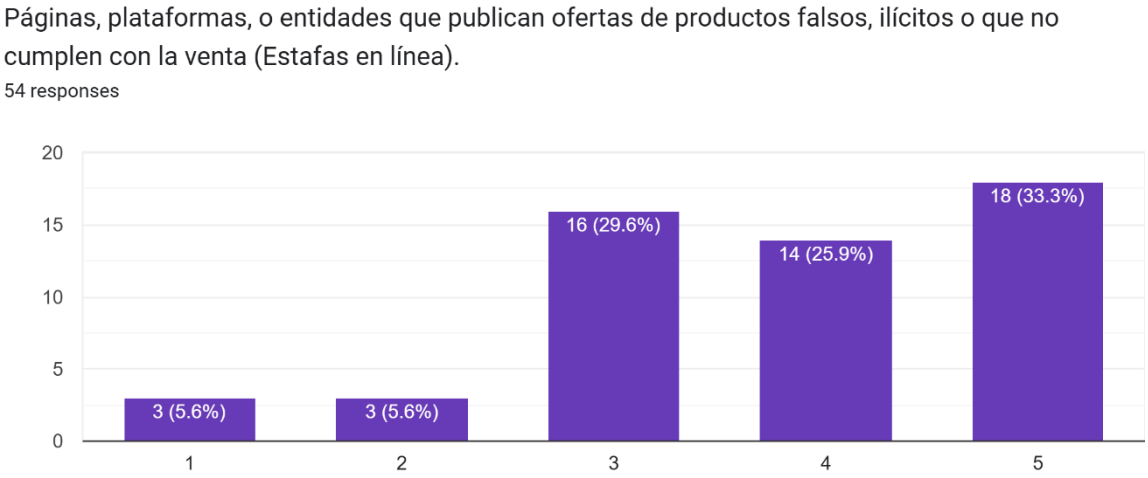
Gráfico 12: Percepción de riesgo sobre el “Phishing”



Según los datos obtenidos en el Gráfico 12, gran parte de la población percibe el “Phishing” como una amenaza mayor. En una escala del 1 (Poco peligroso) al 5 (Muy peligroso), se ubican porcentajes de 33.3% y 29.6% de la población en los puntajes 5 y 4 respectivamente, mientras que se presenta un 24.1% de la población en la escala 3 como medianamente peligroso, y finalmente se encuentran los porcentajes 5.6% y 7.4% en los términos menos peligrosos 2 y 1 respectivamente.

Dados los datos recopilados, se destaca que hay una buena conciencia y percepción en general de qué tan graves son las estafas en línea y otras amenazas del “Phishing” en general. Poca parte de la población estudiantil lo considera poco peligroso, lo que puede requerir mayor énfasis.

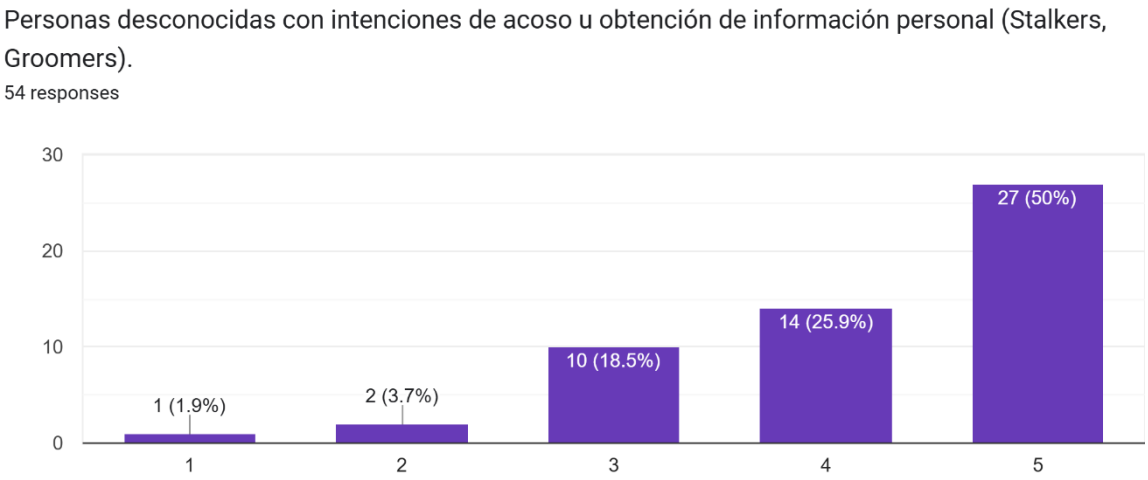
Gráfico 13: Percepción de riesgo sobre las estafas en línea



A partir del Gráfico 13 se destaca una fuerte percepción sobre lo peligrosas que pueden llegar a ser las estafas en línea. En una escala del 1 (Poco peligroso) al 5 (Muy peligroso), se detalla que la gran mayoría de la población afirma que tales estafas son altamente peligrosas, con un 33.33% de la población estudiantil encuestada, mientras que otra gran mayoría con un 29.6% afirma que, en su lugar, son medianamente peligrosas. Seguidamente, un 25.9% de los estudiantes califica con un 4 a tales amenazas, resultando en una percepción de que no es tan peligroso, pero sí bastante preocupante. Finalmente, con porcentajes de 5.6%, se presentan los rubros que califican a las estafas como poco peligrosas, tanto en la calificación 2 como la 1.

Los datos anteriores representan una percepción generalmente acertada en cuanto al riesgo que presentan las estafas en línea, aunque también se aproxima una gran parte de la población a afirmar que es medianamente peligroso, lo que puede generar incertidumbre sobre el tema y puede requerir concientización.

Gráfico 14: Percepción de riesgo sobre acosadores en línea



A partir de la información recopilada en el Gráfico 14, se puede visualizar cómo percibe la población el riesgo de los acosadores que afectan a los usuarios en línea. En una escala del 1 (Poco peligroso) al 5 (Muy peligroso), se presenta la mayoría con un 50% de los estudiantes encuestados con un puntaje de 5 (Muy peligroso) en cuanto a qué tan peligrosos pueden llegar a ser los acosadores. Seguidamente con un 25.9% de la población, se encuentran aquellos que calificaron con un 4, o bien una amenaza grave pero no tan preocupante. Luego, con un 18.5%, los estudiantes califican con un 3 (Medianamente peligroso) a los acosadores y sus hábitos. Finalmente, en las escalas más bajas de 2 y 1, se encuentran los porcentajes de 3.7% y 1.9% respectivamente, indicando una pequeña parte de la población estudiantil que percibe a los acosadores como algo poco peligroso.

Según la información anterior, se representa a una población con una percepción inclinada a indicar que los acosadores en línea sí son un riesgo bastante grave y que se debe tener cuidado con ellos. Poca parte de la población los considera poco peligrosos, por lo que se puede aplicar una orientación en cuanto a su percepción.

Conclusiones y recomendaciones

La presente investigación ha permitido trazar un diagnóstico claro sobre la interacción de los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares con las redes sociales digitales. Los resultados revelan una población estudiantil profundamente inmersa en el ecosistema digital; la vida social de los jóvenes se articula predominantemente a través de plataformas como WhatsApp, Instagram y TikTok, a las cuales no solo acceden de forma casi universal (con más del 83% de uso en las tres plataformas), sino que también dedican una cantidad de tiempo considerable. Los datos indican que una mayoría (57.4%) invierte largas sesiones de más de 30 minutos y lo hace con una frecuencia notable (55.6% revisa "muy frecuentemente"), confirmando una alta y constante exposición al entorno digital.

Esta inmersión constante, sin embargo, coexiste con paradójicas brechas de conocimiento que constituyen el núcleo de la vulnerabilidad detectada. Si bien los estudiantes demuestran una percepción de riesgo acertada y elevada frente a amenazas visibles (por ejemplo, el 50% calificó a los acosadores con la peligrosidad más alta (5/5) y un 33.3% hizo lo mismo con el Phishing), este entendimiento intuitivo no se corresponde con un conocimiento técnico de las amenazas. Resulta alarmante que, a pesar de temer al Phishing, un 72.2% de los estudiantes desconoce el significado del término, y un 75.9% desconoce por completo el concepto de "Groomer", uno de los actores más peligrosos en el acoso sexual a menores. Esta disonancia es crítica: los estudiantes saben que existen peligros, pero no poseen el vocabulario ni el conocimiento estructurado para identificar, nombrar y, por ende, gestionar las amenazas específicas.

El análisis de las experiencias directas refuerza esta preocupación. Los "Acosadores digitales" se posicionaron como la amenaza más reportada por la población (25.9%), superando al robo de datos y las estafas. Este dato, sumado al hecho de que la muestra estaba equitativamente balanceada por género, sugiere una problemática de stalking y acoso que, como indica la literatura especializada, suele afectar de manera desproporcionada a las jóvenes.

Finalmente, la brecha más significativa se encontró en la praxis de la ciberseguridad. Aunque la mayoría aplica medidas básicas (contraseñas seguras 68.5%, perfiles privados 55.6%), fallan en la implementación de las barreras más efectivas. El hallazgo de que solo un 31.5% de los estudiantes utiliza la Verificación en Dos Pasos (2FA) es, quizás, la conclusión más notable del estudio. En una era donde el robo de credenciales mediante phishing es el principal vector de ataque, la baja adopción de 2FA (una medida que, según expertos de la industria, bloquea el 99.9% de los ataques automatizados) deja a la gran mayoría de los estudiantes innecesariamente expuestos, a pesar de sus buenas intenciones de seguridad.

A partir de estas conclusiones, y en estricto cumplimiento del objetivo de proponer estrategias educativas y la metodología de concientización, se establece la siguiente recomendación central: la creación y difusión de un blog informativo diseñado como una estrategia de transferencia de conocimiento directa y permanente para la comunidad del CTP Turrubares.

Este blog se propone como un recurso digital vivo, alineado con los hábitos de consumo de información de la Generación Z. El blog funcionará como el eje central de la alfabetización digital de la institución y deberá estructurarse para responder directamente a las vulnerabilidades detectadas en esta investigación.

Para ello, el contenido del blog deberá priorizar:

1. Traducción de Riesgos: Crear artículos claros y directos que cierren la brecha terminológica. Se deben desarrollar guías visuales bajo títulos como: "¿Qué es el 'Phishing' y cómo luce uno en Instagram?", "¿Qué es un 'Groomer' y cuáles son sus etapas de engaño?". El objetivo es tomar los riesgos que hoy desconocen y hacerlos reconocibles.

2. Promoción de Medidas Críticas: Dado el alarmante bajo uso de la 2FA, el blog debe incluir tutoriales sencillos (paso a paso con capturas de pantalla) sobre cómo activar la Verificación en Dos Pasos en WhatsApp, Instagram y TikTok, las plataformas más usadas por esta población.

3. Respuesta a Amenazas Prevalentes: Al ser los "Acosadores digitales" la amenaza más reportada, se debe generar contenido enfocado en la gestión de la privacidad, cómo bloquear y reportar eficazmente a un acosador, y la importancia de documentar las pruebas sin interactuar con el agresor.

Al entregar este blog a la Dirección y al cuerpo docente, el CTP Turrubares contará con una herramienta pedagógica específica, basada en evidencia propia y diseñada a la medida de su población estudiantil, transformando los datos de esta investigación en una acción preventiva concreta y sostenible.

Referencias

Agencia Española de Protección de Datos (AEPD). (2019). *Guía de protección de datos para centros educativos*. https://www.aepd.es/guias/guia-centros-educativos.pdf

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. https://academic.oup.com/jcmc/article/13/1/210/4583062

Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

Erikson, E. H. (1968). *Identity: Youth and crisis*. W. W. Norton & Company.

Instituto Nacional de Ciberseguridad de España (INCIBE). (2020). *Guía de ciberataques*. https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Livingstone, S., & Haddon, L. (Eds.). (2009). *Kids online: Opportunities and risks for children*. Policy Press (Bristol University Press). https://academic.oup.com/policy-press-scholarship-online/book/22399

Microsoft. (2022). *The importance of two-factor authentication*. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/importance-of-two-factor-authentication

Morales, K. N. (s.f.). *La violencia de género en línea contra las mujeres y niñas*. Organización de los Estados Americanos (OEA). https://www.oas.org/es/sms/cicte/docs/Manual-practico-de-seguridad-digital-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

Sánchez, R. P. (2024). *Niñas, niños y adolescentes en la Internet* (Reporte completo KO-Costa Rica 2023). Kids Online. http://globalkidsonline.net/wp-content/uploads/2024/02/KO-Costa-Rica-2023-full-report-spanish.pdf

UNICEF. (2017). *El estado mundial de la infancia 2017: Niños en un mundo digital*. https://www.unicef.org/dominicanrepublic/media/656/file/El%20Estado%20Mundial%20de%20la%20Infancia%202017:%20Ni%C3%B1os%20en%20un%20mundo%20digital.pdf

Apéndices

Apéndice 1: Población estudiantil de cuarto ciclo matriculada durante el curso lectivo presente, ordenados según su nivel y sección.

Lista de estudiantes matriculados
CTP Turrubares
Curso lectivo 2025

Cuarto ciclo	Décimo año	Undécimo año	Duodécimo año	Plan nacional	
Sección 1	20	15	13	3	
Sección 2	22	19	16		
					TOTAL CUARTO CICLO
Total	42	34	29	3	108

Apéndice 2: Instrumento de recolección de datos.

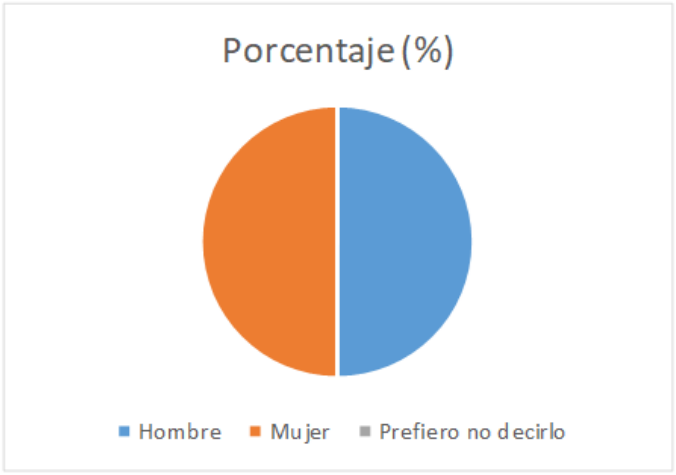
Riesgos en redes sociales

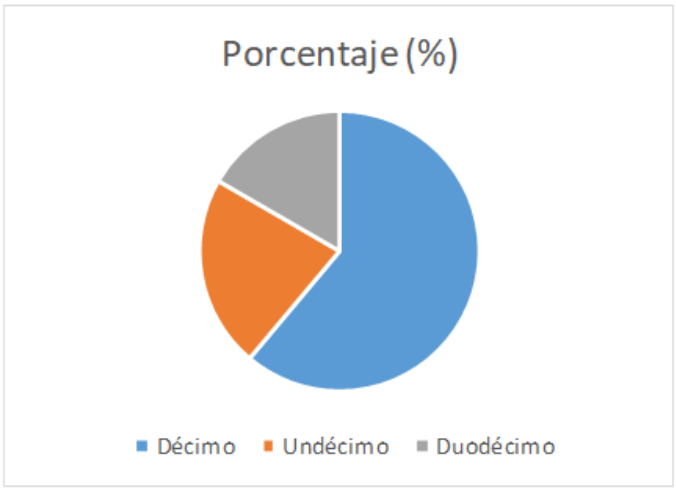
Responde a las siguientes preguntas relacionadas a los riesgos que se suelen presentar en las redes sociales comúnmente.

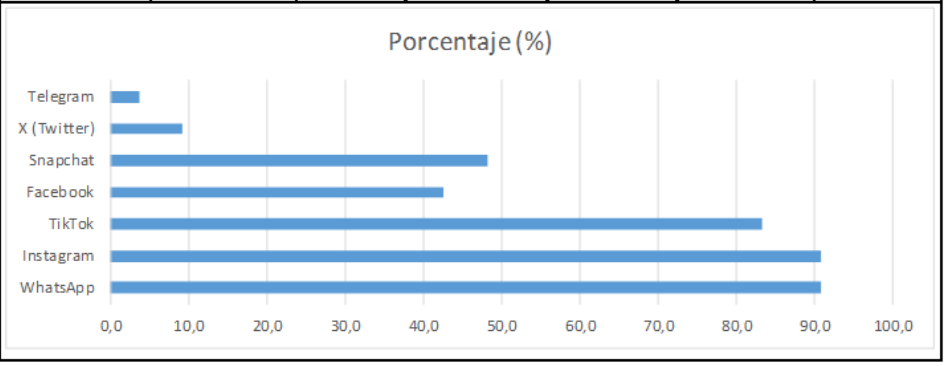
Ignacio Apuy Anchia. Noviembre 2025.

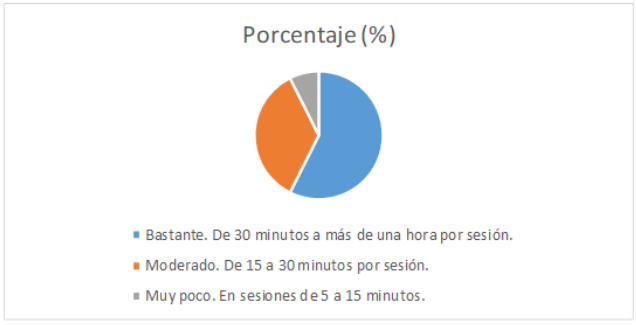
Información personal	Amenazas en redes sociales
Rellena la siguiente información. Los datos personales individuales no serán publicados, sólo utilizados generalmente como parte de una estadística amplia. ¿Cómo te identificas? ◯ Hombre. ◯ Mujer. ◯ Prefiero no decirlo. ¿Qué año cursas actualmente? ◯ Décimo. ◯ Undécimo. ◯ Duodécimo. ¿Cuáles de las siguientes redes sociales utilizas? ☐ WhatsApp ☐ Instagram ☐ TikTok ☐ Facebook ☐ Snapchat ☐ X (Twitter) ☐ Telegram ¿Cuánto tiempo le dedicas a las redes sociales? ◯ Muy poco. En sesiones de 5 a 15 minutos. ◯ Moderado. De 15 a 30 minutos por sesión. ◯ Bastante. De 30 minutos a más de una hora por sesión.	Responde conscientemente a las siguientes preguntas sobre amenazas en redes sociales. ¿Sabes qué es el cyberbullying? ◯ Sí. ◯ No. Aunque tal vez lo he escuchado. ¿Sabes qué significa “Phishing”? ◯ Sí. ◯ No. Aunque tal vez lo he escuchado. ¿Sabes qué es un “Stalker”? ◯ Sí. ◯ No. Aunque tal vez lo he escuchado. ¿Sabes qué es un “Groomer”? ◯ Sí. ◯ No. Aunque tal vez lo he escuchado.
Protección en línea	**Escala de gravedad de amenazas**
¿Has sido víctima de alguna de estas amenazas? (De ser contrario marca la opción “No.”) ☐ Robo de datos o cuentas. ☐ Estafas en línea o páginas falsas. ☐ Acosadores digitales. ☐ No. ☐ Otro:_____ ¿Con qué medidas de seguridad proteges tu cuenta y datos en línea? (Si no cuentas con una, marca la opción “Ninguna.”) ☐ Contraseñas altamente seguras. ☐ Perfiles privados. ☐ Verificación en dos pasos (2FA). ☐ Número telefónico/Correo electrónico de respaldo. ☐ Ninguna. ☐ Otro:_____	De las siguientes amenazas, ¿Cuáles consideras más o menos graves? (1= Poco peligroso, 5=Muy peligroso) Páginas o plataformas sospechosas con la intención de robar datos (Phishing). ◯ ◯ ◯ ◯ ◯ 1 2 3 4 5 Páginas o entidades con ofertas falsas o ilícitas (Estafas en línea). ◯ ◯ ◯ ◯ ◯ 1 2 3 4 5 Personas desconocidas con intenciones de acoso o robo de información (Stalkers, Groomers). ◯ ◯ ◯ ◯ ◯ 1 2 3 4 5

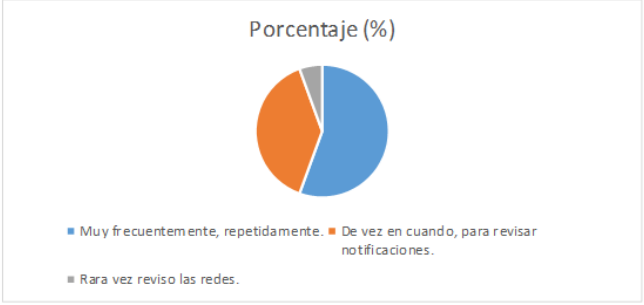
Apéndices 3-16: Procesamiento de datos de la encuesta.

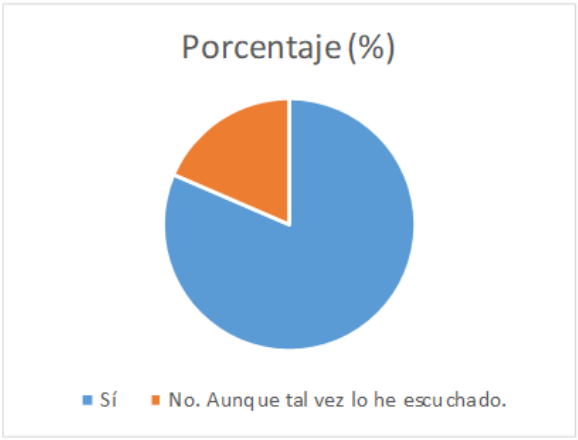
1. ¿Cómo te identificas?	Hombre	Mujer	Prefiero no decirlo
Puntaje	27	27	0
Porcentaje (%)	50	50	0
Gráfico			

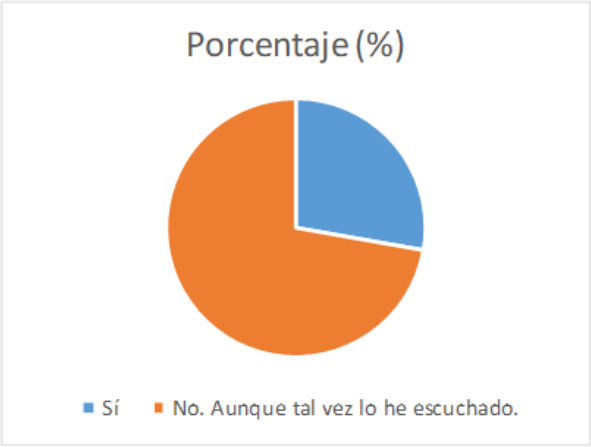
2. ¿Qué año cursas actualmente?	Décimo	Undécimo	Duodécimo
Puntaje	33	12	9
Porcentaje (%)	61,1	22,2	16,7
Gráfico			

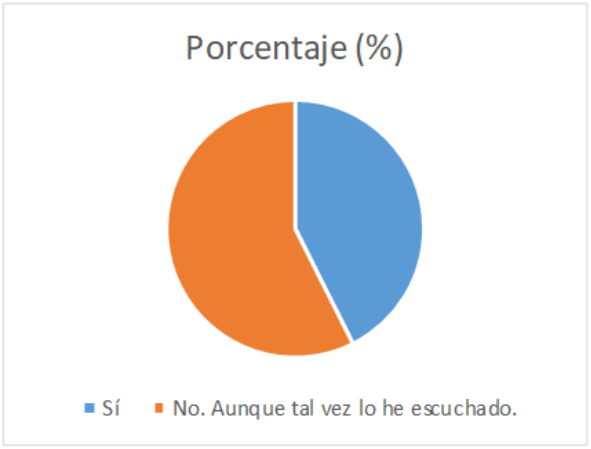
3. ¿Cuáles de las siguientes redes sociales utilizas?	WhatsApp	Instagram	TikTok	Facebook	Snapchat	X (Twitter)	Telegram
Puntaje	49	49	45	23	26	5	2
Porcentaje (%)	90,7	90,7	83,3	42,6	48,1	9,3	3,7
Gráfico							

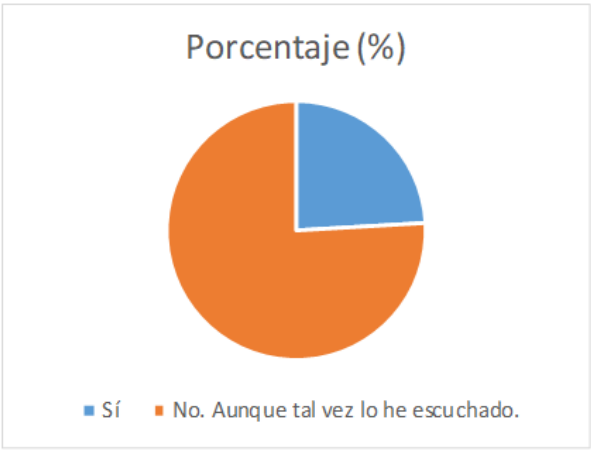
4. ¿Cuánto tiempo le dedicas a las redes sociales?	Bastante. De 30 minutos a más de una hora por sesión.	Moderado. De 15 a 30 minutos por sesión.	Muy poco. En sesiones de 5 a 15 minutos.
Puntaje	31	19	4
Porcentaje (%)	57,4	35,2	7,4
Gráfico			

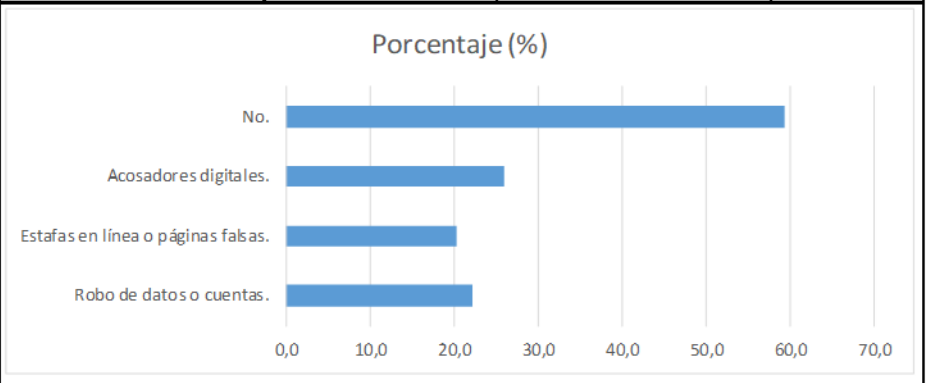
5. ¿Qué tan seguido haces estas sesiones?	Muy frecuentemente, repetidamente.	De vez en cuando, para revisar notificaciones.	Rara vez reviso las redes.
Puntaje	30	21	3
Porcentaje (%)	55,6	38,9	5,6
Gráfico			

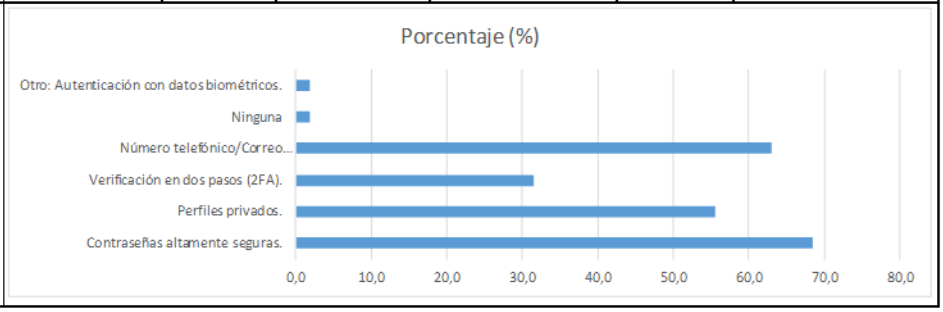
6. ¿Sabes qué es el cyberbullying?	Sí	No. Aunque tal vez lo he escuchado.
Puntaje	44	10
Porcentaje (%)	81,5	18,5
Gráfico		

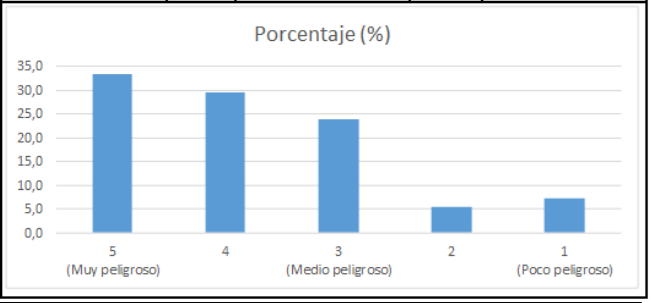
7. ¿Sabes qué significa "Phishing"?	Sí	No. Aunque tal vez lo he escuchado.
Puntaje	15	39
Porcentaje (%)	27,8	72,2
Gráfico		

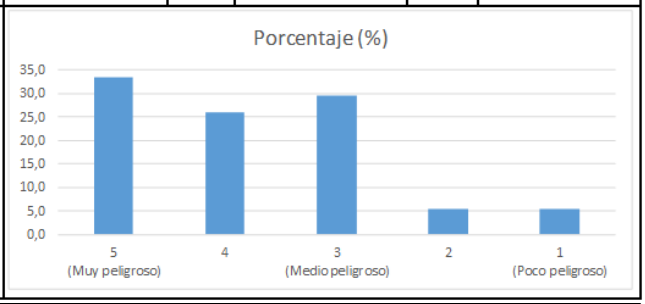
8. ¿Sabes qué es un "Stalker"?	Sí	No. Aunque tal vez lo he escuchado.
Puntaje	23	31
Porcentaje (%)	42,6	57,4
Gráfico		

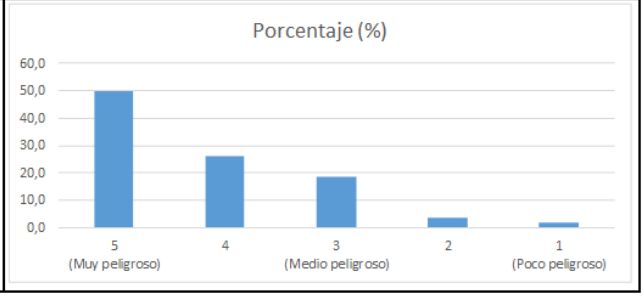
9. ¿Sabes qué es un "Groomer"?	Sí	No. Aunque tal vez lo he escuchado.
Puntaje	13	41
Porcentaje (%)	24,1	75,9
Gráfico		

10. ¿Has sido víctima de alguna de estas amenazas?	Robo de datos o cuentas.	Estafas en línea o páginas falsas.	Acosadores digitales.	No.
Puntaje	12	11	14	32
Porcentaje (%)	22,2	20,4	25,9	59,3
Gráfico				

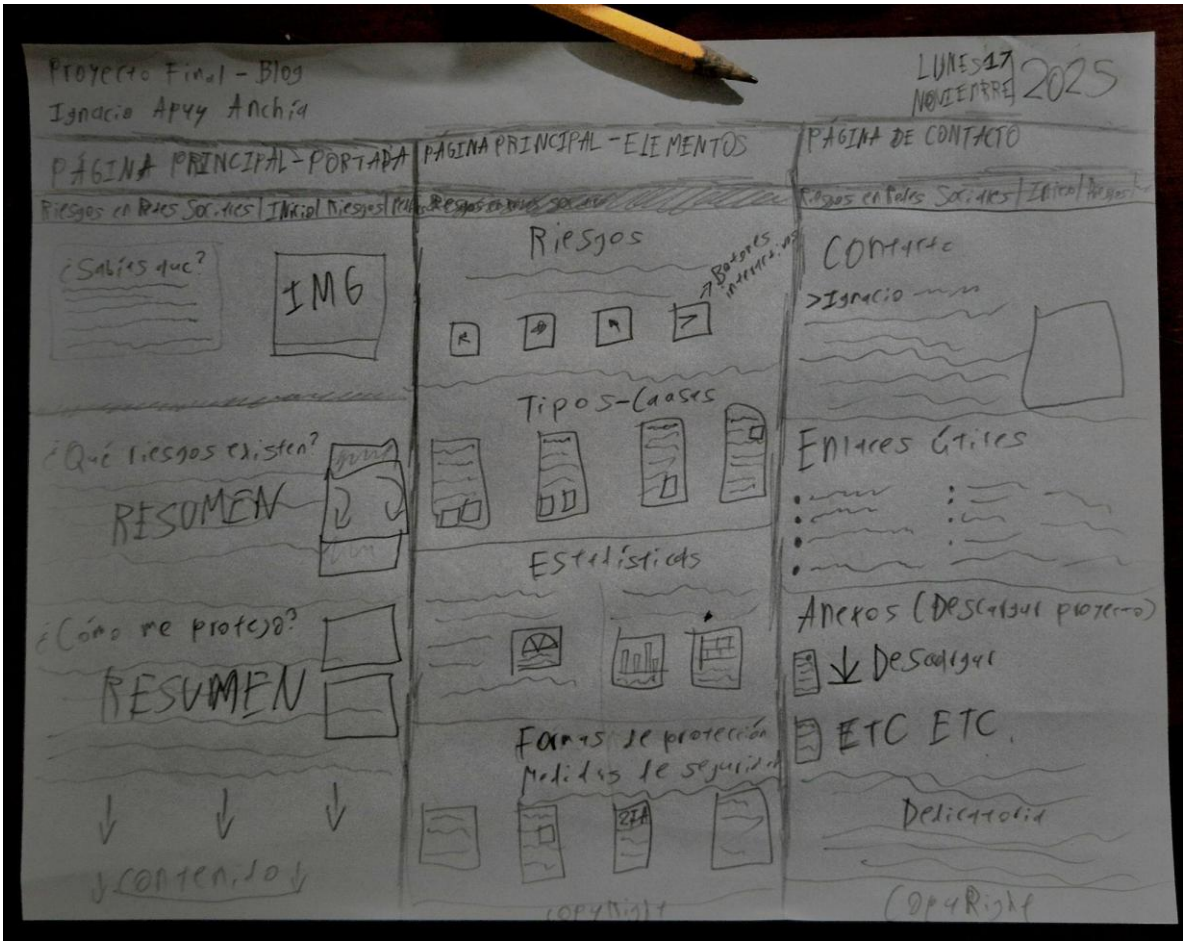
11. ¿Con qué medidas de seguridad proteges tu cuenta y datos en línea?	Contraseñas altamente seguras.	Perfiles privados.	Verificación en dos pasos (2FA).	Número telefónico/Correo electrónico de respaldo	Ninguna	Otro: Autenticación con datos biométricos.
Puntaje	37	30	17	34	1	1
Porcentaje (%)	68,5	55,6	31,5	63,0	1,9	1,9
Gráfico						

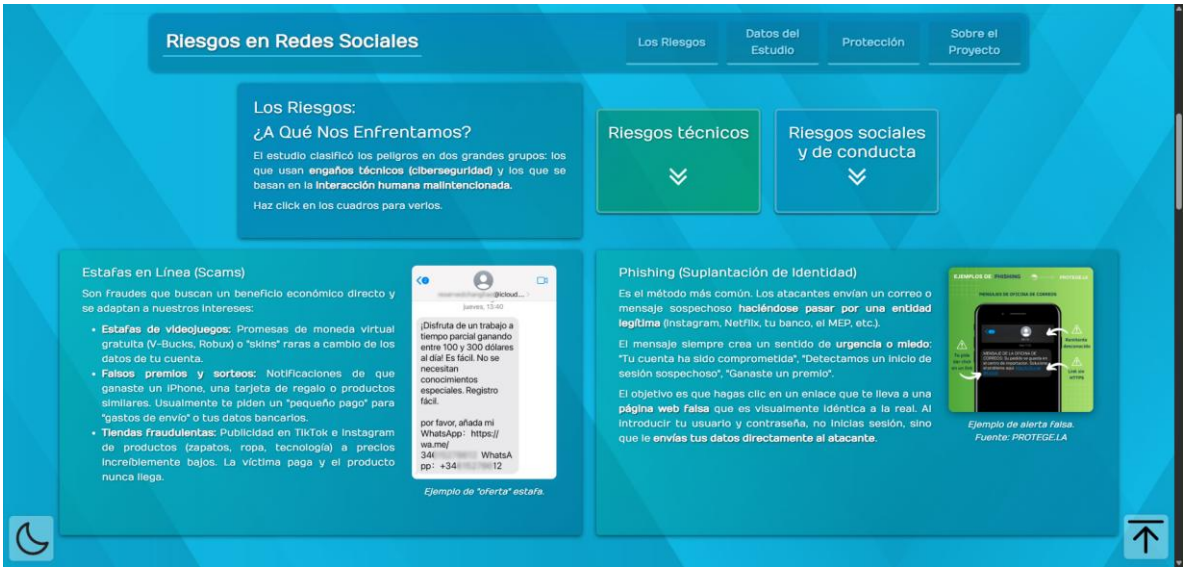
12. Nivel de peligro en páginas o plataformas sospechosas con la intención de robar datos (Phishing).	5 (Muy peligroso)	4	3 (Medio peligroso)	2	1 (Poco peligroso)
Puntaje	18	16	13	3	4
Porcentaje (%)	33,3	29,6	24,1	5,6	7,4
Gráfico					

13. Nivel de peligro en páginas, plataformas, o entidades que publican ofertas de productos falsos, ilícitos o que no cumplen con la venta (Estafas en línea).	5 (Muy peligroso)	4	3 (Medio peligroso)	2	1 (Poco peligroso)
Puntaje	18	14	16	3	3
Porcentaje (%)	33,3	25,9	29,6	5,6	5,6
Gráfico					

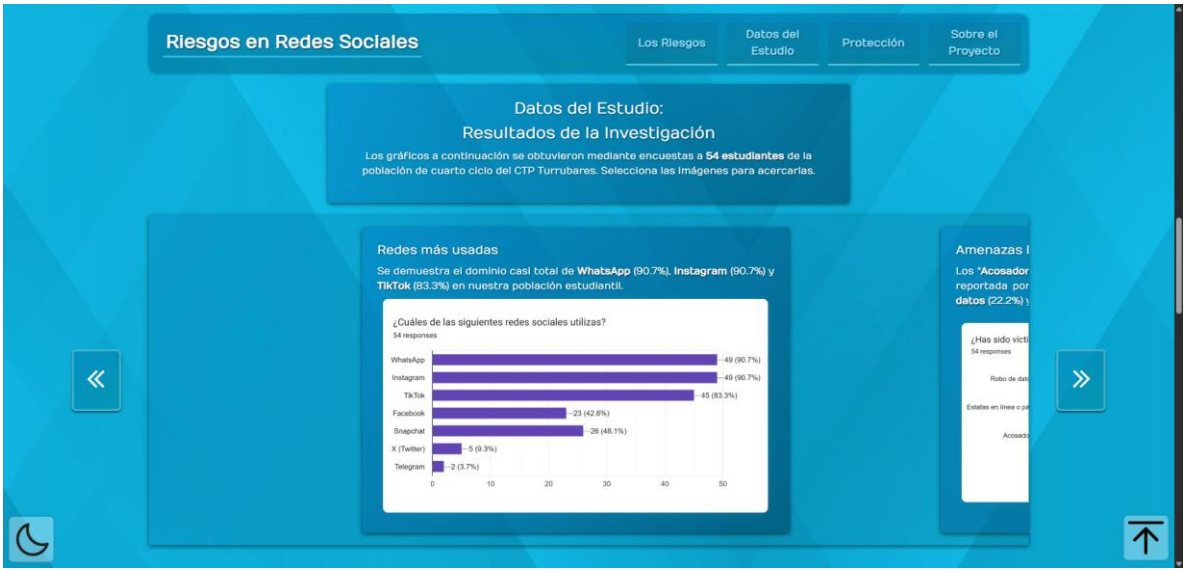
14. Nivel de peligro de personas desconocidas con intenciones de acoso u obtención de información personal (Stalkers, Groomers).	5 (Muy peligroso)	4	3 (Medio peligroso)	2	1 (Poco peligroso)
Puntaje	27	14	10	2	1
Porcentaje (%)	50,0	25,9	18,5	3,7	1,9
Gráfico					

Apéndices 17-20: Estrategia de concientización (Blog informativo)

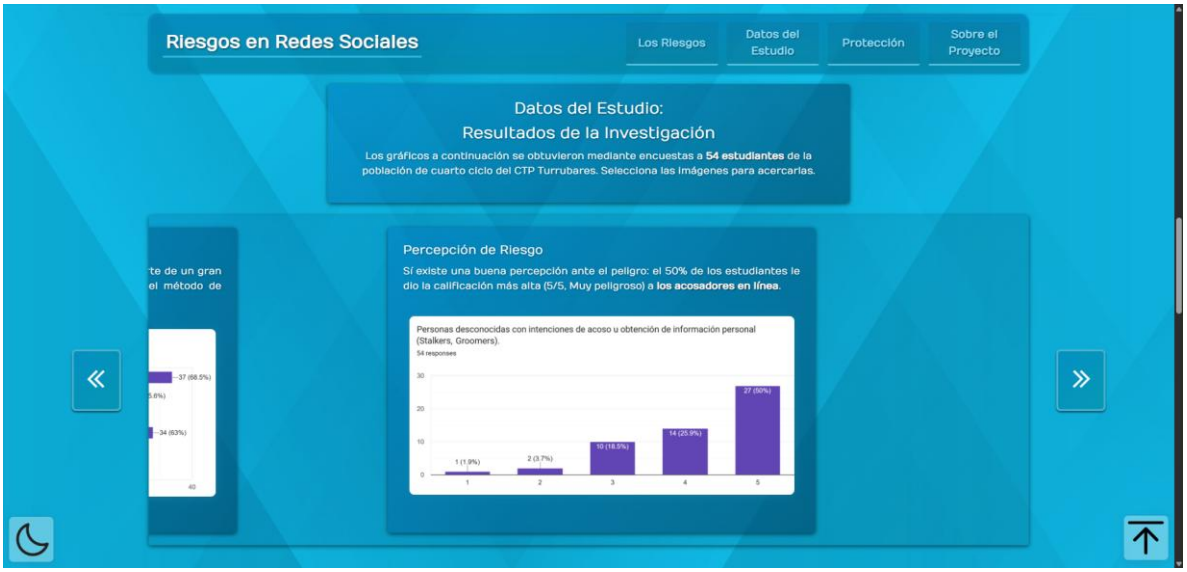



Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Los Riesgos:
¿A Qué Nos Enfrentamos?
El estudio clasificó los peligros en dos grandes grupos: los que usan engaños técnicos (ciberseguridad) y los que se basan en la interacción humana malintencionada.
Haz click en los cuadros para verlos.
Riesgos técnicos
Riesgos sociales y de conducta
Estafas en Línea (Scams)
Son fraudes que buscan un beneficio económico directo y se adaptan a nuestros intereses:
Estafas de videojuegos: Promesas de moneda virtual gratuita (V-Bucks, Robux) o "skins" raras a cambio de los datos de tu cuenta.
Falsos premios y sorteos: Notificaciones de que ganaste un iPhone, una tarjeta de regalo o productos similares. Usualmente te piden un "pequeño pago" para "gastos de envío" o tus datos bancarios.
Tiendas fraudulentas: Publicidad en TikTok e Instagram de productos (zapatos, ropa, tecnología) a precios increíblemente bajos. La víctima paga y el producto nunca llega.
¡Disfruta de un trabajo a tiempo parcial ganando entre 100 y 300 dólares al día! Es fácil. No se necesitan conocimientos especiales. Registro fácil.
por favor, añada mi WhatsApp: https://wa.me/
Ejemplo de "oferta" estafa.
Phishing (Suplantación de Identidad)
Es el método más común. Los atacantes envían un correo o mensaje sospechoso haciéndose pasar por una entidad legítima (Instagram, Netflix, tu banco, el MEP, etc.).
El mensaje siempre crea un sentido de urgencia o miedo: "Tu cuenta ha sido comprometida", "Detectamos un inicio de sesión sospechoso", "Ganaste un premio".
El objetivo es que hagas clic en un enlace que te lleva a una página web falsa que es visualmente idéntica a la real. Al introducir tu usuario y contraseña, no inicias sesión, sino que le envías tus datos directamente al atacante.
Ejemplo de alerta falsa.
Fuente: PROTEGE.LA


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Los Riesgos:
¿A Qué Nos Enfrentamos?
El estudio clasificó los peligros en dos grandes grupos: los que usan engaños técnicos (ciberseguridad) y los que se basan en la interacción humana malintencionada.
Haz click en los cuadros para verlos.
Riesgos técnicos
Riesgos sociales y de conducta
Acoso Digital (Stalking)
El acoso digital consiste en una persecución virtual y conducta intrusiva que busca afectar la integridad del individuo mediante el seguimiento obsesivo y otras características:
Monitoreo y vigilancia: Observación constante de la actividad de la víctima, registrando publicaciones para construir un perfil de vulnerabilidad.
Evasión y suplantación: Creación de identidades falsas para evitar bloqueos y mantener el contacto.
Contacto invasivo: Envío persistente de mensajes o correos para forzar la interacción y mantener a la víctima en estado de alerta.
Ataque: Amenaza o publicación de información, personal de la víctima, buscando la humillación.
Los "Stalker" se suelen camuflar en internet para no ser descubiertos.
Grooming (Acoso Sexual de Adultos a Menores)
Es el riesgo de interacción más severo y no es un evento, sino un proceso deliberado de engaño. El "Groomer" suele seguir estas etapas para manipular a un menor:
1. Identifica: Busca víctimas en redes sociales y detecta vulnerabilidades o soledad.
2. Gana confianza: Finge ser un par o un amigo comprensivo y se gana la confianza del menor.
3. Aísla: Intenta aislar al menor de su red de apoyo y mueve la conversación a un chat privado.
4. Accede: Normaliza la conversación sexual y pide fotos o videos íntimos (Sexting).
5. Extorsiona: Usa el material para extorsionar, pidiendo más o incluso dinero a cambio de no hacerlo público.
Debemos tener cuidado con quienes conversamos en redes sociales.


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Datos del Estudio:
Resultados de la Investigación
Los gráficos a continuación se obtuvieron mediante encuestas a 54 estudiantes de la población de cuarto ciclo del CTP Turrubares. Selecciona las imágenes para acercarlas.
Redes más usadas
Se demuestra el dominio casi total de WhatsApp (90.7%), Instagram (90.7%) y TikTok (83.3%) en nuestra población estudiantil.
¿Cuáles de las siguientes redes sociales utilizas?
54 responses
WhatsApp
Instagram
TikTok
Facebook
Snapchat
X (Twitter)
Telegram
49 (90.7%)
49 (90.7%)
45 (83.3%)
23 (42.6%)
26 (48.1%)
5 (9.3%)
2 (3.7%)
0
10
20
30
40
50
Amenazas
Los "Acosador
reportada por
datos (22.2%)


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Datos del Estudio:
Resultados de la Investigación
Los gráficos a continuación se obtuvieron mediante encuestas a 54 estudiantes de la población de cuarto ciclo del CTP Turrubares. Selecciona las imágenes para acercarlas.
Inmersión Digital
La mayoría de los estudiantes (57.4%) pasa más de 30 minutos por sesión.
¿Cuánto tiempo le dedicas a las redes sociales?
54 responses
Muy poco. En sesiones de 5 a 15 minutos.
Moderado. De 15 a 30 minutos por sesión.
Bastante. De 30 minutos a más de una hora por sesión.
57.4%
7.4%
35.2%
Intermite
Además de
*muy frecu

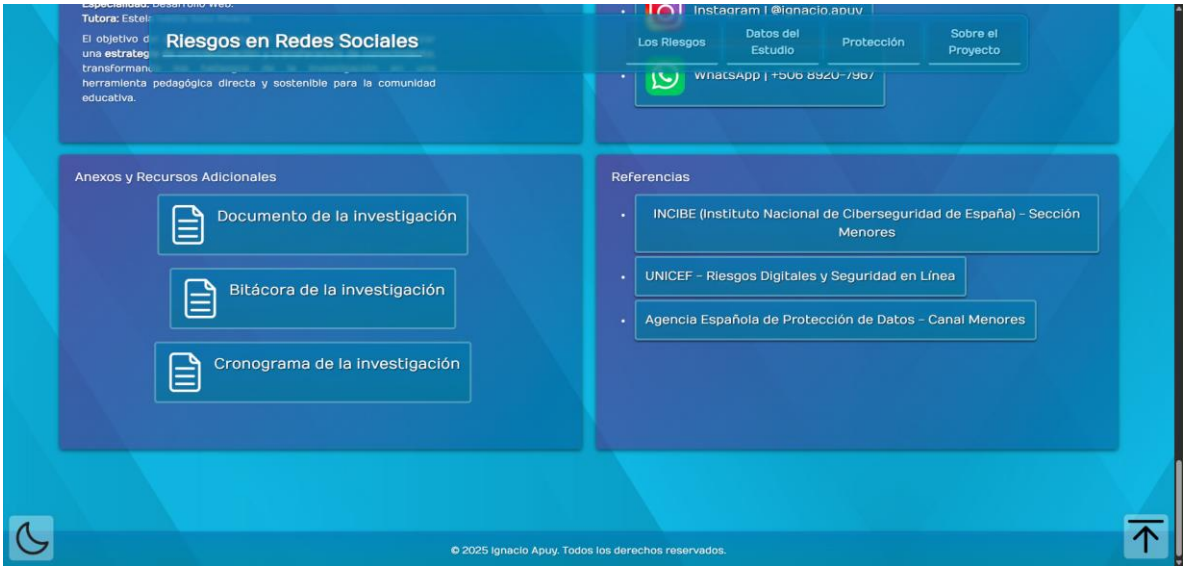

Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Datos del Estudio:
Resultados de la Investigación
Los gráficos a continuación se obtuvieron mediante encuestas a 54 estudiantes de la población de cuarto ciclo del CTP Turrubares. Selecciona las imágenes para acercarlas.
Percepción de Riesgo
Sí existe una buena percepción ante el peligro: el 50% de los estudiantes le dio la calificación más alta (5/5, Muy peligroso) a los acosadores en línea.
Personas desconocidas con intenciones de acoso u obtención de información personal (Stalkers, Groomers).
54 responses


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Métodos de Prevención:
¿Cómo Me Protejo?
La protección es una mezcla de herramientas técnicas y pensamiento crítico. Estas son algunas de las medidas más importantes en cuanto a seguridad digital.
Haz click en los cuadros para verlos.
1. Protocolos Fundamentales
2. Autenticación Multifactor (2FA)
3. Alfabetización Digital
Estos son los pilares básicos de la seguridad digital y constituyen el primer nivel de defensa de sus cuentas. Su correcta aplicación es obligatoria para la mitigación de riesgos.
Estas son algunas de las recomendaciones más comunes en cuanto a lo básico en seguridad:
Gestión de contraseñas: Establezca claves que combinen mayúsculas, minúsculas, números y símbolos. Evite el uso de la misma clave en múltiples plataformas. También se recomienda evitar utilizar información personal como nombres, apellidos, fechas, etc.
Configuración de privacidad: Revise y configure sus perfiles personales como privados por defecto. Limite el acceso a sus publicaciones y contenido únicamente a contactos conocidos.
Recuperación de cuenta: Asegure que todas sus cuentas estén vinculadas a un correo electrónico y/o número de teléfono de respaldo actualizado y seguro. Este paso es fundamental para la recuperación de su cuenta si ocurre algo.
Estas medidas establecen una base robusta, pero se debe entender que son insuficientes por sí solas contra ataques avanzados como el Phishing.
Para prevenir ataques mayores, se requieren de métodos adicionales que son altamente importantes ya que complementan la base de la seguridad.
Password
Password
Password
Sigue las recomendaciones a la hora de crear una contraseña.


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Métodos de Prevención:
¿Cómo Me Protejo?
La protección es una mezcla de herramientas técnicas y pensamiento crítico. Estas son algunas de las medidas más importantes en cuanto a seguridad digital.
Haz click en los cuadros para verlos.
1. Protocolos Fundamentales
2. Autenticación Multifactor (2FA)
3. Alfabetización Digital
La Verificación en Dos Pasos (2FA) representa la capa de seguridad más importante en el ecosistema digital actual.
Su función es requerir una segunda forma de verificación (un código temporal, token o dato biométrico) después de introducir la contraseña. La implementación de la 2FA es un requisito de seguridad de primer orden en todas las plataformas.
El 2FA requiere de un solo paso extra, pero es de gran importancia.
¿Por qué es importante la 2FA?
Este protocolo está diseñado para anular la eficacia de los ataques. Si un atacante obtiene su contraseña a través de algún medio, no podrá finalizar el inicio de sesión sin el código temporal generado en su dispositivo de confianza.
¿Cómo puedo activar la 2FA en mis redes sociales?
Estos son algunos enlaces a foros oficiales de las redes sociales más utilizadas donde puedes activar la 2FA:
Tutorial para activar 2FA en WhatsApp
Tutorial para activar 2FA en Instagram
Tutorial para activar 2FA en TikTok


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Métodos de Prevención:
¿Cómo Me Protejo?
La protección es una mezcla de herramientas técnicas y pensamiento crítico. Estas son algunas de las medidas más importantes en cuanto a seguridad digital.
Haz click en los cuadros para verlos.
1. Protocolos Fundamentales
2. Autenticación Multifactor (2FA)
3. Alfabetización Digital
La mejor herramienta es tu propio criterio. La alfabetización digital, también conocida como "El saber ver", es la capacidad de analizar y evaluar críticamente lo que ves.
No siempre se puede estar seguro en un espacio tan abierto como Internet. Tampoco podemos estar totalmente exentos de cualquier ataque o mala intención. Aún así, podemos aplicar distintas reglas generales, por más sencillas que parezcan, para poder prevenir la mayor parte de situaciones con las que nos podamos enfrentar.
Debemos ser totalmente preventivos en Internet.
Desconfía de la urgencia: Los mensajes de Phishing siempre te apuran. Tómate una pausa y analiza.
Revisa el remitente: Fíjate bien en el correo o número. Usualmente tienen errores sutiles (ej. @Instagrarn.com).
Si es demasiado bueno...: ...es falso. Nadie regala IPhones o dinero fácil.
Gestiona el acoso: La regla de oro es no interactuar. No alimentes al acosador, sólo reporta y aléjate.
Documenta: Toma capturas de pantalla.
Bloquea: Elimina su capacidad de contactarte.
Reporta: Usa las herramientas de la plataforma.
Habla: Coméntalo con un adulto de confianza.
Privacidad ante desconocidos: Nunca envíes fotos íntimas. Desconfía de desconocidos que son "demasiado" amigables.


Riesgos en Redes Sociales
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Sobre el Proyecto y Contacto
Este blog informativo es el producto final del Proyecto de Graduación titulado: "Riesgos del uso de redes sociales en los estudiantes de cuarto ciclo del Colegio Técnico Profesional de Turrubares, durante el primer periodo del año 2025".
Autor: Ignacio José Apuy Anchía
Especialidad: Desarrollo Web.
Tutora: Estela Ivette Soto Rivera
El objetivo del proyecto no es solo presentar datos, sino realizar una estrategia de concientización y transferencia de conocimiento, transformando los hallazgos de la investigación en una herramienta pedagógica directa y sostenible para la comunidad educativa.
Redes sociales
Facebook | Ignacio Apuy Anchía
Instagram | @ignacio.apuy
WhatsApp | +506 8920-7967
Anexos y Recursos Adicionales
Documento de la investigación
Bitácora de la investigación
Referencias
INCIBE (Instituto Nacional de Ciberseguridad de España) – Sección Menores
UNICEF – Riesgos Digitales y Seguridad en Línea
Agencia Española de Protección de Datos – Canal Menores


Riesgos en Redes Sociales
Tutora: Estel
El objetivo d
una estrateg
transforman
herramienta pedagógica directa y sostenible para la comunidad educativa.
Los Riesgos
Datos del Estudio
Protección
Sobre el Proyecto
Instagram | @ignacio.apuy
WhatsApp | +506 8920-7967
Anexos y Recursos Adicionales
Documento de la investigación
Bitácora de la investigación
Cronograma de la investigación
Referencias
INCIBE (Instituto Nacional de Ciberseguridad de España) - Sección Menores
UNICEF - Riesgos Digitales y Seguridad en Línea
Agencia Española de Protección de Datos - Canal Menores
© 2025 Ignacio Apuy. Todos los derechos reservados.