UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE
Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO
Plan Estratégico para la Ciberseguridad: Implementación de herramientas y estrategias para adolescentes del Área Metropolitana de San Salvador

PRESENTADO POR
Jennifer Tatiana Arevalo Guillen

ASESOR
Leonardo José Castillo Perla

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América
Septiembre 2024

Contenido

Ilustraciones

Tablas

1. Introducción

En El Salvador, el problema de las amenazas cibernéticas, especialmente entre los adolescentes, está en aumento. La relación entre ciberseguridad y violencia sexual es evidente, lo que hace necesaria la formulación de un plan integral. Esta tesis propone el "Plan Estratégico para la Ciberseguridad en Adolescentes del Área Metropolitana de San Salvador". Este plan se basa en investigaciones recientes, como el "Estudio Multisectorial de Respuestas y Capacidades (MRC) El Salvador 2023" y "Centroamérica Cibersegura", que destacan la falta de estrategias integradas para combatir la ciberdelincuencia y mejorar la seguridad digital.

La colaboración entre el Ministerio de Educación y la UNODC, junto con el apoyo de organizaciones internacionales, subraya los esfuerzos para fortalecer la educación en ciberseguridad, centrándose en la prevención de ciberdelitos y la promoción de una cultura de seguridad en línea. Sin embargo, persisten desafíos, especialmente en la adopción de estas estrategias por instituciones privadas. Ejemplos positivos de formación en ciberseguridad, como el curso dirigido por el Information Risk & Security Institute (IRSI), que destacó a estudiantes salvadoreños, muestran la importancia de comenzar la educación en ciberseguridad desde edades tempranas (Diario El Salvador, 2023).

La violencia sexual contra menores es otro problema grave en El Salvador. Estudios como "Llegar a cero embarazos en niñas y adolescentes / Mapa El Salvador 2023" (UNFPA, 2023) y "Cuadernos de Población 1" (UNFPA, 2022) muestran una prevalencia alarmante de abuso y sus consecuencias en la población adolescente. Estas investigaciones destacan la profunda conexión entre ciberseguridad y protección contra la violencia sexual, reforzando la urgencia de abordar ambas áreas simultáneamente.

Esta tesis propone desarrollar y expandir programas educativos en ciberseguridad que no solo aborden los riesgos convencionales de internet, sino que también enseñen a los jóvenes a identificar y prevenir la violencia sexual digital. Este enfoque es necesario dado el contexto actual de ciberseguridad en El Salvador,

donde los adolescentes enfrentan riesgos como el ciberacoso, el robo de identidad y la extorsión digital.

El plan estratégico evaluará el éxito de las iniciativas educativas mediante métricas específicas, promoviendo un cambio cultural hacia la ciberseguridad y el desarrollo de habilidades digitales críticas. Al abordar amenazas cibernéticas específicas y fomentar una cultura de seguridad en línea, este enfoque pretende crear entornos digitales seguros para los jóvenes y construir comunidades informadas y resilientes.

2. Diagnóstico de la Situación Actual

La recopilación y análisis de noticias sobre problemáticas sociales como el bullying, el acoso, el grooming, el fraude, el phishing y otras formas de ingeniería social son cruciales para entender y mitigar los riesgos asociados a estas conductas. Estos comportamientos, a menudo malinterpretados como simples travesuras infantiles o ignorados por los adultos, pueden tener graves repercusiones en los adolescentes y en la comunidad en general.

Reconocer e identificar adecuadamente estas conductas es el primer paso para comprender que no son parte de la normalidad, sino manifestaciones de problemas más profundos que representan serios riesgos para la convivencia y el bienestar social. Por ello, es esencial mantenerse informado sobre las últimas noticias y desarrollos en El Salvador en relación con estas cuestiones para implementar acciones preventivas y correctivas eficaces.

2.1. Noticias sobre casos en El Salvador

2.1.1. La red de prostitución de menores que tiene en problemas al “Gordo Max” y otras personalidades en El Salvador

El caso involucra a Alejandro Maximiliano González Jiménez, conocido como "Gordo Max", una figura pública y presentador en la Telecorporación salvadoreña (TCS), quien ha sido acusado junto con otras tres personas de participar como cliente en una red de prostitución de menores que fue desmantelada en 2014.

González Jiménez fue arrestado y presentado ante los medios, insistiendo en su inocencia y negando ser un delincuente.

Este escándalo surge después de que, en 2014, una menor prostituida por la red, y ahora testigo protegida, afirmara que había sido contratada por González Jiménez y Ernesto José Regalado O'Sullivan entre 2011 y 2012. A pesar de que González Jiménez ya había sido mencionado en la investigación sobre la red de prostitución, la fiscalía general de la República (FGR) no lo había acusado anteriormente, optando en cambio por tratarlo como testigo y concentrarse en los tratantes.

La red, liderada por Daniel Armando Pérez, engañaba a jóvenes y menores con promesas de empleo como edecanes y modelos, para luego ser forzadas a tener relaciones sexuales con diversos clientes. Pérez organizaba los encuentros en centros comerciales y cobraba distintas tarifas, especialmente si las jóvenes eran vírgenes.

La actual administración de la Fiscalía está investigando las razones por las que la administración anterior no procesó a los clientes involucrados, incluido González Jiménez, a pesar de las evidencias y testimonios en su contra. Este cambio de dirección se enmarca en las críticas a la gestión anterior del fiscal general.

Los cargos presentados contra "Gordo Max" y los demás acusados son por la remuneración de actos sexuales con menores, no por estupro, debido a que se considera que las menores participaron con consentimiento, aunque esto ha generado controversia. Las reacciones ante el caso incluyen el retiro de González Jiménez de la programación y materiales de TCS, mientras que él y los otros acusados enfrentan el proceso legal correspondiente. (BBC News Mundo., 2017)

2.1.2. Caso de bullying a niño de 11 años termina en tragedia en La Paz

El caso de Luis Pineda, un niño de 11 años de San Luis Herradura, La Paz, ha resaltado la severidad del bullying en El Salvador. Luis, quien padecía de labio leporino, supuestamente sufrió de acoso escolar en el Centro Escolar Jorge Alberto

González Suvillaga, a pesar de la negación de la directora, quien afirmó que el niño no enfrentó bullying y que las interacciones entre los estudiantes eran normales.

La situación alcanzó un punto trágico cuando Luis intentó quitarse la vida un viernes por la noche y, a pesar de ser salvado inicialmente por su padre, falleció debido a las heridas mientras era trasladado al hospital. La familia del niño y la comunidad quedaron devastadas y confundidas, ya que Luis nunca había mostrado signos de angustia o indicados problemas en la escuela. (La prensa grafica, 2018)

2.1.3. "Que me paguen no me va a regresar a mi hijo": mamá de Mario Rivera, el niño de San José Guayabal que falleció por una broma

Mario Rivera, un niño de San José Guayabal que estaba por cumplir 16 años, falleció tras varios días en coma debido a una lesión cerebral causada por una "malteada", una broma realizada por otros jóvenes que consiste en lanzar a alguien al aire y atraparlo antes de tocar el suelo. Sin embargo, en esta ocasión, Mario fue dejado caer al suelo, resultando gravemente herido. Tras el incidente, fue llevado a casa por un vecino y más tarde al Hospital Rosales en San Salvador, donde falleció después de cinco días.

Su madre, María Guadalupe Rivera, está considerando presentar una denuncia, aunque se siente resignada, expresando que ninguna compensación podrá devolverle a su hijo. Ella espera que su caso sirva para evitar que se repitan tragedias similares. María Guadalupe señala que la pérdida de un hijo es un dolor insuperable y menciona que otros involucrados en la broma, incluidos algunos mayores de edad, han huido.

Mario era conocido por ser un niño educado y reservado, lo que posiblemente lo hacía blanco de burlas. El incidente ha conmocionado a la comunidad y ha motivado al grupo juvenil local "Yo ayudo" a iniciar una campaña de concientización contra juegos peligrosos para prevenir futuras tragedias. (La prensa grafica , 2018)

2.1.4. Familia de joven que sufría “bullying” y murió en una excursión escolar denuncia amenazas de personal de la escuela.

La familia de Carlos Eduardo Alférez Gómez, un joven que murió en circunstancias sospechosas durante una excursión escolar el 7 de abril, ha estado enfrentando una serie de amenazas e intimidaciones tras expresar su intención de presentar una denuncia formal para investigar la muerte. Carlos, estudiante de octavo grado y activo en su comunidad, había sido objeto de bullying continuo por parte de sus compañeros, situación que, según alega la familia, nunca fue abordada por el personal de la escuela Centro Escolar República de Japón.

Los eventos desafortunados se desarrollaron durante una salida a un balneario organizada por una maestra, donde se sospecha que Carlos fue forzado a consumir alcohol y posteriormente se ahogó. La falta de acción de los maestros y el director del colegio ha exacerbado la situación, con incidentes adicionales de acoso y hostigamiento hacia los miembros de la familia Alférez, especialmente hacia las hermanas de Carlos.

Una de las hermanas fue confrontada y agredida físicamente por el director Roberto Aguilar en un incidente público, lo que llevó a la familia a retirarla de la escuela por miedo a represalias. A pesar de su intento de cambiarla a otro establecimiento, han enfrentado obstáculos burocráticos, aumentando su sensación de impotencia y miedo.

Además, la familia ha experimentado dificultades al intentar obtener justicia y claridad sobre las circunstancias de la muerte de Carlos, enfrentándose a una falta de cooperación y pasividad por parte de las autoridades escolares y judiciales. A pesar de los desafíos, están determinados a seguir adelante con la denuncia ante la fiscalía general de la República, buscando responsabilizar a aquellos involucrados en el bullying y en la negligencia que, creen, condujo a la tragedia. (El salvador times, 2018)

2.1.5. Violencia sexual por medios digitales: otras violencias contra las mujeres que no le importan al Estado Salvadoreño

Sonia es una víctima de violencia sexual digital en El Salvador, un país donde, a pesar de la alta incidencia de delitos de este tipo, con más de 2100 casos reportados desde 2019 hasta 2021, se han registrado muy pocas condenas. La historia de Sonia comienza cuando descubre que fotos íntimas suyas fueron distribuidas sin su consentimiento, lo que marcó un antes y un después en su vida pública y privada.

Este caso ilustra un problema generalizado de filtración y difusión no autorizada de imágenes íntimas, una práctica penada por la ley salvadoreña pero que sigue siendo rampante debido a la ineficacia de las entidades encargadas de su persecución. Sonia, al igual que muchas otras, sufrió una exposición involuntaria y maliciosa que impactó severamente su bienestar emocional y su sentido de seguridad.

El relato destaca cómo Sonia se sintió acorralada y vulnerada, ya que inicialmente confió en alguien que terminó traicionando su privacidad. La situación escaló al punto de afectar su interacción en redes sociales y su participación en espacios públicos, viviendo en constante miedo y ansiedad. El trauma se profundizó con el descubrimiento de que sus fotos no solo se compartieron en redes sociales convencionales sino también en plataformas menos reguladas y en espacios físicos como bares, ampliando el círculo de su humillación y exposición.

Sonia se enfrentó al dilema de denunciar o no los hechos, retenida por el temor a las represalias y a la revictimización por un sistema de justicia que anteriormente le falló. La experiencia de Sonia evidencia la necesidad urgente de una respuesta institucional más efectiva y empática hacia las víctimas de violencia digital, así como de una mayor conciencia y solidaridad dentro de la comunidad y los movimientos feministas para combatir y prevenir estos delitos.

En su narrativa, Sonia también reflexiona sobre las similitudes entre la violencia sexual en el espacio físico y digital, destacando cómo ambas formas de violencia dejan a las víctimas sintiéndose desnudas, vulnerables y deshumanizadas.

Su historia subraya la importancia del apoyo colectivo y la resistencia feminista frente a una cultura que, demasiado a menudo, deja a las mujeres solas frente a sus agresores. (Revista la brujula, 2021)

2.1.6. “Sufrí de bullying por mi color de piel y mi cabello”: la confesión de un jugador de Firpo

Alex "Chocho" Mejía, destacado defensor del equipo de fútbol L.Á. Firpo, ha utilizado sus plataformas de redes sociales para compartir una experiencia profundamente personal: el enfrentamiento al racismo y al bullying durante su niñez y adolescencia. Este problema, enraizado en prejuicios sobre su color de piel y su cabello, marcó sus primeros años. Al hacer público su testimonio, Mejía no solo subraya la triste realidad del racismo y la discriminación en su entorno, sino que también promueve un mensaje de tolerancia y respeto por la diversidad. Su llamado a la acción es claro: educar a la próxima generación para valorar y respetar las diferencias individuales, evitando así perpetuar el ciclo de burlas y desprecio.

El caso de Mejía cobra especial importancia al considerar el entorno del fútbol, un espacio que, a pesar de sus políticas contra la discriminación, todavía enfrenta incidentes de racismo. A nivel mundial, el deporte se compromete a ser una zona libre de racismo, con sanciones establecidas para disuadir actitudes y comportamientos discriminatorios entre jugadores y aficionados. Sin embargo, la persistencia de estos comportamientos subraya la necesidad de continuar la lucha contra la intolerancia.

Al compartir su historia, Alex Mejía ilumina la persistente sombra del racismo y alienta un cambio hacia una mayor empatía y comprensión. Su estatus como deportista y figura pública amplifica su mensaje, inspirando tanto a seguidores como a compañeros a reflexionar y actuar contra la discriminación. Su historia de superación y compromiso con el cambio cultural refleja el poder del testimonio personal para educar y movilizar a la sociedad hacia la inclusión y el respeto mutuo.

En definitiva, "Chocho" Mejía se erige como un modelo de liderazgo y resiliencia, utilizando su experiencia para fomentar una sociedad más justa y compasiva. (elsalvador.com, 2022)

2.1.7. Exreinas de belleza alzan la voz y dicen NO al bullying contra Isabella García-Manzo

En un reciente movimiento de solidaridad, varias exreinas de belleza salvadoreñas han alzado la voz en apoyo a Isabella García-Manzo, coronada Miss Universo El Salvador 2023, condenando el bullying y el acoso que ha sufrido en las redes sociales tras su victoria el 30 de julio. Este apoyo llega en medio de controversias y acusaciones de fraude en el certamen, provocando una ola de mensajes negativos hacia la joven.

Exreinas como Alejandra Gavidia (Miss Universo El Salvador 2021), Rebeca Moreno (Miss Congeniality Universe 2008), Alejandra Guajardo (Miss El Salvador 2022), Nicole Álvarez (Miss World El Salvador 2022) y Alisson Abarca (Miss El Salvador 2017), han utilizado sus plataformas para difundir mensajes de empatía, amor y respeto, enfatizando la importancia de la solidaridad nacional y la representación positiva del país.

Estas figuras públicas han expresado que la responsabilidad de frenar el acoso no recae solamente en las concursantes del certamen, sino en todos los espectadores y usuarios de las redes sociales. Resaltan que el momento actual debe ser de apoyo a García-Manzo, quien enfrenta la gran responsabilidad de representar a El Salvador en el escenario internacional. A través de sus mensajes, buscan fomentar un cambio hacia una cultura de apoyo y respeto mutuo, instando a la comunidad en línea a optar por construir en lugar de destruir. Con esto, desean dejar un legado de positividad y orgullo nacional para las futuras generaciones. (elsalvador.com, 2023)

2.1.8. Envían a prisión a hombre que le hallaron pornografía infantil

Arístides Santamaría Palacios fue enviado a prisión provisional por el Juzgado Segundo de Paz de Santa Tecla tras una audiencia inicial, debido a su implicación en delitos relacionados con la pornografía infantil. Capturado el 14 de noviembre de 2023 en su residencia en la Colonia Santa Mónica, Santa Tecla, La Libertad, se encontraron pruebas que lo vinculan con actividades ilícitas específicamente enfocadas en la pornografía infantil.

El operativo de captura fue ejecutado por la División de Investigaciones en coordinación con la Unidad de Atención Especializada para la Mujer, Niñez y Adolescencia de San Salvador. Santamaría enfrenta cargos por la utilización y posesión de material pornográfico involucrando a menores de edad y personas con discapacidad, utilizando las tecnologías de la información y comunicación.

Las autoridades han confirmado la existencia de material pornográfico infantil en posesión de Santamaría, lo que representa una violación grave a la integridad y derechos de los niños y adolescentes. Además, la Fiscalía ha indicado que la investigación sigue en curso y que hay otras víctimas menores de edad aún no identificadas vinculadas a este caso. La detención y el proceso judicial de Santamaría son parte de los esfuerzos de la Fiscalía por combatir el abuso y la explotación sexual de menores en El Salvador. El caso ahora avanza al Juzgado Segundo de Instrucción de Santa Tecla para seguir con las etapas procesales correspondientes. (elsalvador.com, 2023)

2.1.9. "Gamer" enfrenta audiencia acusado de hacer compras en línea con la tarjeta del vecino

Marco A. es acusado de utilizar una tarjeta de débito sin consentimiento de su vecino para realizar compras en línea en una plataforma de videojuegos. La acusación detalla que se efectuaron más de 100 transacciones fraudulentas, sumando un total de $11,849.29.

La Fiscalía ha presentado cargos contra él por el delito de hurto por medios electrónicos en el Juzgado 10° de Paz de San Salvador, a raíz de la denuncia interpuesta por la víctima. Las investigaciones policiales culminaron con el arresto de Marco A. el martes, y durante el procedimiento se incautaron varios artículos electrónicos, incluyendo una consola de videojuegos, un celular y una Tablet. (elsalvador.com, 2023)

2.1.10. Tendencias y similitudes de noticias

Las noticias presentadas muestran una serie de tendencias y similitudes preocupantes en la sociedad salvadoreña, resaltando problemas significativos de violencia, abuso y discriminación. A continuación, se detallan algunas de las similitudes más notorias entre los casos mencionados:

Vulnerabilidad de los menores: Muchos de los casos involucran directamente a menores de edad, ya sea como víctimas de explotación sexual, bullying o abuso físico. Esto subraya una tendencia alarmante hacia la vulnerabilidad de los jóvenes y niños en diversos ámbitos, desde el escolar hasta el digital.

Impacto del acoso y la discriminación: El acoso escolar, el racismo y el bullying son problemas recurrentes que tienen un impacto devastador en las víctimas. Las noticias reflejan cómo estas formas de violencia pueden llevar a consecuencias trágicas, incluyendo la muerte y el trauma psicológico severo.

Cultura del silencio y el estigma: En varios casos se percibe una cultura del silencio o estigmatización que rodea a las víctimas, ya sea por miedo a represalias, vergüenza asociada a la denuncia de los abusos, o insensibilidad social hacia ciertos tipos de violencia, especialmente aquella que ocurre en el ámbito digital.

Uso de tecnología en la perpetración de abusos: La tecnología juega un rol dual, siendo tanto un medio para perpetrar abusos (como en el caso de violencia digital y fraude en línea) como una herramienta para amplificar el daño a las víctimas a través de la distribución de contenido íntimo sin su consentimiento o la organización de redes de explotación.

Estas similitudes indican desafíos profundos dentro de la sociedad salvadoreña en cuanto a la protección de los más vulnerables. Existe una necesidad urgente de fortalecer las respuestas institucionales y legales ante el abuso y la discriminación, y fomentar una cultura más empática y justa.

2.2. Estudios Realizados En El Salvador

La investigación en ciberseguridad es esencial para mejorar la conciencia y competencias digitales, desarrollando una cultura de seguridad informada y resiliente. La revisión de programas educativos enfocados en riesgos como bullying, acoso, grooming, fraude, phishing y otras formas de ingeniería social permite identificar prácticas efectivas y áreas de mejora en la prevención de ciberdelitos. Una evaluación cuidadosa de estos programas contribuye a la creación de estrategias educativas enfocadas en promover hábitos seguros en línea. La colaboración entre gobiernos, instituciones educativas y el sector tecnológico es vital para garantizar la seguridad digital y apoyar políticas públicas basadas en datos concretos.

El Salvador está trabajando para reforzar su ciberseguridad mediante políticas, estrategias gubernamentales y colaboraciones internacionales, enfrentando la ciberdelincuencia y mejorando la protección digital de sus ciudadanos y estructuras. Los esfuerzos incluyen desde reformas legislativas hasta iniciativas educativas, promoviendo una cultura de seguridad digital integral. Este análisis proporciona una visión clara de las acciones de El Salvador contra el cibercrimen, destacando tanto avances como desafíos.

2.2.1. Informe de actividades de Prevención de Ciberdelitos, Ministerio de Educación, Ciencia y Tecnología. El Salvador.

En el Informe de Actividades de Prevención de Ciberdelitos emitido por el Ministerio de Educación, Ciencia y Tecnología de El Salvador (UNODC, 2020), se describen las iniciativas dirigidas a la comunidad educativa para la prevención de ciberdelitos. Se resumen a continuación las medidas implementadas:

Desde 2017, este Ministerio ha cooperado estrechamente con el Ministerio de Educación (MINED) en la organización de iniciativas como "Las Caras del Cibercrimen", una obra teatral destinada a sensibilizar sobre los riesgos en línea. Esta campaña ha alcanzado 113 instituciones educativas en Cuscatlán, Santa Ana, La Libertad y San Salvador, beneficiando a 15,687 estudiantes y 3,416 docentes de varios niveles, promoviendo así un espacio digital seguro.

A partir de 2018, como parte de una estrategia integral contra ciberdelitos, se ha capacitado a 98 Coordinadores de Aula Informática y técnicos de la Gerencia de Tecnologías Educativas. Esta formación se ha complementado con la creación de materiales preventivos, como videos, folletos y carteles. Además, se han organizado exposiciones en los Centros Interactivos de Aprendizaje Científico (CIAC) para instruir sobre el tema. Como resultado, se ha capacitado a 3,416 docentes y sensibilizado a 15,687 estudiantes, mientras que 705 padres han participado en talleres específicos, destacando un enfoque holístico y comunitario en la prevención de ciberdelitos.

Además, se han distribuido 78,000 copias de material educativo y publicado un libro titulado "Teatro para niños y niñas", que incluye obras sobre ciberextorsión, phishing, ciberacoso y migración. Se han desarrollado materiales especializados en ciberseguridad, privacidad en Internet, sexting, grooming y sextorsión, ofreciendo un recurso exhaustivo para enfrentar los desafíos digitales contemporáneos.

2.2.2. Comunidad Educativa del Instituto de Aguilares es capacitada en prevención de ciberdelito, 2019

De acuerdo con la información proporcionada en el portal del Ministerio de Educación (MINED, 2019), la comunidad educativa del Instituto Nacional de Aguilares ha recibido capacitación en la prevención de ciberdelitos y en el uso responsable de Internet. Los participantes en estas sesiones incluyeron estudiantes, docentes y padres de familia.

Nelson Rolando Melgar, Coordinador de Aula Informática, lideró la iniciativa tras completar un programa de formación específico ofrecido por el Ministerio de Educación, Ciencia y Tecnología (MINEDUCYT) y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC).

Las capacitaciones abordaron temas críticos como grooming, sexting, ciberacoso, ciberbullying y sextorsión, demostrando ser de gran relevancia para la seguridad en línea de los jóvenes. Se destacó la importancia de la supervisión parental y la promoción de una relación de confianza entre padres e hijos como estrategias preventivas fundamentales. Es significativo que el 98% de los docentes recibieran esta formación crucial, beneficiando también a los padres con información importante.

Hasta la fecha, el MINEDUCYT y la UNODC han capacitado a 400 coordinadores de aulas informáticas en distintas escuelas de San Salvador, Santa Ana y San Miguel, proporcionándoles los conocimientos técnicos, materiales impresos y herramientas didácticas necesarias para enfrentar eficazmente este tema crítico en el ámbito educativo.

2.2.3. Estudio Multisectorial de Respuestas y Capacidades El Salvador 2023

El "Estudio Multisectorial de Respuestas y Capacidades (MRC, 2023)" ((MRC), 2023) en El Salvador, realizado por el International Centre for Missing and Exploited Children (ICMEC), es una iniciativa pionera centrada en abordar integralmente el abuso y la explotación sexual de menores en línea. Este estudio se distingue por su enfoque participativo, utilizando análisis de documentos, entrevistas y encuestas para actores clave, lo que facilita la identificación de deficiencias y la formulación de recomendaciones para mejorar la colaboración entre sectores y el gobierno, con el objetivo de reforzar la protección infantil.

El informe subraya la necesidad de un abordaje completo, multidisciplinario e intersectorial, centrado en la protección de los menores, señalando una respuesta actual insuficiente a pesar de existir un Sistema Nacional de Protección.

Destaca la urgencia de fortalecer las capacidades en política, legislación, justicia penal y otros campos relevantes. Reconoce avances en legislación, pero resalta la importancia de la formación continua para jueces, fiscales y policías para combatir eficazmente delitos como el grooming y la sextorsión. Se señalan también las deficiencias en la justicia penal, especialmente en capacidad técnica y formación en cibercrimen, lo que afecta la investigación y sentencias, instando a una mejora en estos aspectos y en la adquisición de tecnologías para el manejo de evidencia digital.

La educación y la prevención se destacan como claves para contrarrestar el abuso en línea, proponiendo una mayor educación sobre los riesgos de las TIC y temas de sexualidad enfocados en la explotación online. Se alienta al sector de las TIC a fortalecerse y colaborar con el gobierno para crear entornos seguros para los menores.

Por último, el documento recalca la responsabilidad compartida en la protección de los menores en línea, involucrando al gobierno, sociedad civil, academia, y sector privado, enfatizando en la necesidad de un esfuerzo conjunto y diverso, así como en la asignación adecuada de recursos para implementar programas dirigidos a las víctimas y a la prevención y tratamiento de agresores.

2.2.4. PASSWORD Estudio sobre prácticas de seguridad digital en salvadoreños de 16 a 24 años.

El estudio "Password 1234: Estudio sobre seguridad digital en salvadoreños de 16 a 24 años" (AlfabetaMedia, s.f.), liderado por Karla Patricia Ramos Amaya, directora de la Maestría en Gestión Estratégica de la Comunicación de la Universidad Centroamericana José Simeón Cañas (UCA), en colaboración con personal de la misma universidad y de la Escuela de Comunicación Monica Herrera, contó con el apoyo de DW Akademie y el Ministerio Federal de Cooperación Económica y Desarrollo de Alemania (BMZ).

Los hallazgos indican que aproximadamente el 70% de los jóvenes encuestados asegura no compartir sus contraseñas. La mayoría utiliza dispositivos como smartphones, laptops y tablets para navegar en Internet, accediendo principalmente a través de conexiones domiciliarias y tarjetas prepagadas. Sin embargo, un notable porcentaje reportó haber compartido sus contraseñas en alguna ocasión, y muchos admitieron tener menos de diez años de experiencia en el uso de Internet y redes sociales.

El informe resalta la importancia de incrementar la alfabetización mediática e informacional (AMI) entre la juventud salvadoreña, sugiriendo el desarrollo de programas educativos y recursos para mejorar la competencia digital y la seguridad de la información. Este estudio es relevante ya que ofrece una perspectiva detallada sobre las conductas de seguridad digital de los jóvenes en El Salvador, proporcionando una base sólida para el diseño de futuras intervenciones y políticas que busquen reforzar la seguridad en línea en la región.

2.2.5. Centroamérica Cibersegura, IPANDETEC, 2020

El informe "Centroamérica Cibersegura", creado por IPANDETEC Centroamérica (IPANDETEC, s.f.) , brinda una evaluación sobre la ciberseguridad y ciberdelincuencia en la región de Centroamérica. Utiliza una metodología de preguntas clave para ofrecer un análisis comparativo, revisando el estado actual de cada país en términos de ciberseguridad, legislación de protección de datos y adhesión a tratados internacionales, como el Convenio de Budapest.

Respecto a El Salvador, el estudio resalta aspectos importantes:

- Equipos de Respuesta a Incidentes Cibernéticos: El país cuenta con el CESIRT, vinculado al Ministerio de Justicia y Seguridad Pública, preparado para gestionar incidentes de seguridad informática.
- Legislación de Protección de Datos Personales: Sin una ley específica actualmente, se ha presentado una propuesta legislativa que busca proteger los datos personales, complementando así la Ley de Acceso a la Información Pública.

- Viceministerio de Ciencia y Tecnología: Opera dentro del Ministerio de Educación, mostrando una voluntad de integrar la ciberseguridad en la agenda gubernamental.
- Participación en Foros de Ciberseguridad: El Salvador participa activamente en el IGF de la ONU y otras plataformas a niveles regional y nacional.
- Legislación sobre Delitos Cibernéticos: Existe una ley especial desde 2016 que trata los delitos informáticos, aunque aún se requiere ampliar la regulación, especialmente en la protección de infraestructuras críticas.
- Grupos de Trabajo y Convenios Internacionales: Se evidencia un esfuerzo por mejorar el marco de ciberseguridad mediante la participación en grupos multisectoriales y la intención de unirse a convenios internacionales.
- Investigación de Delitos Cibernéticos: Aunque la fiscalía general y la Policía Nacional Civil cuentan con unidades especializadas, aún no existe una fiscalía dedicada exclusivamente a la ciberdelincuencia.
- Estrategia de Ciberseguridad: Falta una estrategia nacional consolidada en esta área.

Este estudio enfatiza la importancia de que El Salvador desarrolle una estrategia nacional de ciberseguridad, fortalezca su legislación de protección de datos y aumente su compromiso con acuerdos internacionales para abordar de manera efectiva los desafíos en el ámbito cibernético.

2.2.6. ESET Security Report 2023

El "ESET Security Report 2023" (ASSET, 2023) presenta un análisis detallado de las principales preocupaciones de seguridad informática para empresas en América Latina. Los hallazgos más destacados incluyen:

- Amenazas Persistentes Avanzadas (APT): Las APT se mantienen como una gran preocupación para las empresas debido a su capacidad para comprometer sistemáticamente la seguridad de los sistemas y la privacidad de los datos a través de ataques dirigidos y sofisticados.

- Ransomware: Esta forma de malware sigue siendo una amenaza considerable, con ciberdelincuentes empleando métodos cada vez más sofisticados para encriptar datos y solicitar rescates.
- Phishing y Suplantación de Identidad: Los ataques de phishing y la suplantación de identidad continúan siendo frecuentes, lo que subraya la necesidad de capacitar a los empleados para que puedan reconocer estos intentos de fraude.
- Internet de las Cosas (IoT): Con el aumento de dispositivos IoT, la superficie de ataque para las empresas se expande, haciendo que la seguridad de estos dispositivos sea crucial.
- Vulnerabilidades en Software y Sistemas Operativos: Es vital que las organizaciones se mantengan actualizadas respecto a las últimas actualizaciones de seguridad para protegerse contra vulnerabilidades conocidas.

El informe también señala que, a nivel global, los países latinoamericanos con las mayores tasas de detección de códigos maliciosos en campañas de phishing son: Ecuador, con un 8%; Costa Rica, con un 7.2%; Colombia, con un 5.7%; Guatemala, con un 5.2%; y El Salvador, con un 5.1%. Esto resalta la importancia de implementar estrategias de ciberseguridad efectivas en la región.

2.2.7. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe

El informe "Reporte de Ciberseguridad 2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe", realizado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) ((BID), 2020) proporciona un análisis detallado sobre la situación actual de la ciberseguridad en la región, destacando tanto los progresos realizados como los retos que aún persisten desde la última evaluación en 2016. Incorporando contribuciones de expertos internacionales, el informe investiga las tendencias en seguridad digital y mide la madurez cibernética de cada nación según el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM).

En cuanto a El Salvador, el reporte señala que, si bien aún no se ha desarrollado una estrategia nacional de seguridad cibernética, el país tiene el objetivo de establecer una Política Nacional de Ciberseguridad como parte de su Estrategia de Gobierno Digital 2018-2022. Este esfuerzo es fruto de un extenso proceso de consulta que ha involucrado a expertos internacionales, el ámbito académico, entidades gubernamentales, el sector privado y organizaciones civiles.

El Salvador dispone de SalCERT, un equipo nacional de respuesta a incidentes cibernéticos que coordina con otros equipos similares. Ha fomentado además la colaboración internacional en protección de infraestructuras críticas y seguridad cibernética con países como Ecuador, España, Israel y la República de Corea. En el sector privado, ha habido una notable actividad en servicios de seguridad digital, desde análisis hasta formación. Asimismo, se ha constatado un aumento en la oferta educativa en ciberseguridad, aunque aún se identifican carencias en este ámbito en el nivel de educación superior.

Uno de los principales logros de El Salvador en esta materia es la aprobación de la Ley Especial contra los Delitos Informáticos y Conexos en 2016, diseñada para salvaguardar los derechos legales frente a actividades delictivas realizadas mediante tecnologías de la información y comunicación (TIC), y prevenir crímenes relacionados con datos almacenados, procesados o transmitidos. No obstante, el país todavía carece de una legislación exhaustiva sobre protección de datos y privacidad.

Finalmente, El Salvador ha avanzado en la implementación de gobierno electrónico, destacando la inauguración del Sistema Integrado de Gestión Administrativa y la Política Nacional de Datos Abiertos, así como el establecimiento de la Dirección de Gobierno Electrónico para coordinar esfuerzos entre las instituciones públicas. Desde principios de 2017, se ha puesto en marcha una plataforma que facilita el intercambio de información gubernamental, promoviendo la adhesión a estándares de seguridad pertinentes.

2.2.8. Resumen de Estudios Realizados En El Salvador

En El Salvador, la investigación y desarrollo de programas de ciberseguridad se han convertido en elementos cruciales para mejorar la conciencia y habilidades digitales de la población, desarrollando una cultura de seguridad digital informada y resiliente. Se han llevado a cabo importantes iniciativas educativas centradas en la prevención de riesgos en línea como el bullying, el acoso, el grooming, el fraude y el phishing. Estas iniciativas, documentadas en informes como el del Ministerio de Educación, Ciencia y Tecnología, han logrado un alcance significativo, beneficiando a miles de estudiantes y docentes a través de programas como "Las Caras del Cibercrimen" y la capacitación de coordinadores de aulas informáticas.

Además, en el Instituto Nacional de Aguilares, la comunidad educativa ha recibido formación especializada en la prevención de ciberdelitos, lo que subraya la importancia de la supervisión parental y de fomentar un diálogo abierto entre padres e hijos sobre la seguridad en línea. Estas medidas reflejan un enfoque proactivo en la educación y prevención de amenazas digitales, integrando a estudiantes, docentes y familias en un esfuerzo común.

Por otro lado, el "Estudio Multisectorial de Respuestas y Capacidades" y otros análisis realizados por organizaciones internacionales como el ICMEC han resaltado la necesidad de fortalecer la protección infantil en línea en El Salvador. Estos estudios recomiendan una mayor colaboración entre diferentes sectores y el gobierno, enfocándose en mejorar las políticas, la legislación y las capacidades de respuesta frente a la ciberdelincuencia.

En términos de la juventud y la seguridad digital, investigaciones como el "Password 1234" han revelado aspectos críticos de las prácticas de seguridad digital entre los jóvenes salvadoreños, sugiriendo una necesidad urgente de mejorar la alfabetización digital a través de programas educativos dirigidos. Esta investigación proporciona una base sólida para futuras intervenciones y políticas que busquen reforzar la seguridad en línea en la región.

El informe "Centroamérica Cibersegura" y el "ESET Security Report 2023" ofrecen una perspectiva más amplia sobre los desafíos de la ciberseguridad a nivel regional, incluyendo El Salvador. Destacan la importancia de enfrentar amenazas como el ransomware y el phishing y la necesidad de estrategias de ciberseguridad efectivas.

Finalmente, el "Reporte de Ciberseguridad 2020" del BID y la OEA indica tanto progresos como desafíos en la materia para El Salvador y la región. A pesar de los esfuerzos como la implementación de la Ley Especial contra los Delitos Informáticos, El Salvador todavía enfrenta la tarea de desarrollar una estrategia nacional consolidada de ciberseguridad. Sin embargo, los avances hacia el gobierno electrónico y la cooperación internacional son pasos positivos hacia la creación de un entorno digital más seguro.

En conjunto, estas acciones y estudios reflejan un compromiso en aumento con la ciberseguridad en El Salvador, destacando la importancia de la prevención, la educación y la cooperación intersectorial en la lucha contra las amenazas digitales.

2.3. Leyes para la ciberseguridad en El Salvador

En El Salvador, se han tomado varias iniciativas para mejorar la ciberseguridad y asegurar la protección de ciudadanos e instituciones frente a las amenazas digitales en aumento. Las siguientes son algunas de las medidas legislativas y políticas más relevantes implementadas en este ámbito:

- Política de Ciberseguridad: Bajo la administración del presidente Nayib Bukele, se estableció la "Política de ciberseguridad de El Salvador", oficializada el 7 de marzo de 2022 en el Diario Oficial, (2022, s.f.). Esta estrategia tiene como objetivo sincronizar los esfuerzos de ciberseguridad entre sectores públicos y privados, organizaciones no gubernamentales y la sociedad civil. En julio de 2020, se formó el "Comité de Ciberseguridad", que reanudó sus actividades en febrero de 2021, reflejando un enfoque coordinado y multidisciplinario.

La política incluye iniciativas de educación en ciberseguridad, revisión del marco jurídico actual y propone la creación de una comisión especializada en delitos informáticos, así como el desarrollo de Centros de Operaciones de Seguridad (SOC) en sectores críticos. (SV, 2022)

- Reformas a las Leyes Penales: La Asamblea Legislativa ha introducido reformas significativas al Código Procesal Penal y a la Ley Especial contra los Delitos Informáticos y Conexos para fortalecer la detección, investigación y castigo de ciberdelitos. Esta legislación, efectiva desde 2016, define y penaliza un rango extenso de actividades ilícitas en línea, salvaguardando la identidad, propiedad, intimidad e imagen de personas y entidades. La Ley de Firma Electrónica, por su parte, asegura la seguridad de las transacciones en línea validando la autenticidad e integridad de las comunicaciones y operaciones digitales. (Justicia, s.f.)
- Entes Coordinadores y Certificación: Se ha estipulado que cada entidad estatal debe nombrar un coordinador institucional para la implementación del plan de ciberseguridad, mejorando así la organización y gestión de la ciberseguridad institucional. Se ha sugerido la creación de un ente coordinador de ciberseguridad a nivel nacional y Comités de Seguridad de la Información (CSI) en cada institución, facilitando una gestión más integrada y eficiente de la seguridad de la información. Además, se contempla la certificación de procesos de ciberseguridad según normativas nacionales e internacionales, destacando el compromiso de El Salvador con la ciberseguridad global, en conformidad con la Carta de las Naciones Unidas y otros tratados internacionales.

2.3.1. Resumen de Leyes para la ciberseguridad en El Salvador

En El Salvador, se han implementado diversas iniciativas para mejorar la ciberseguridad y proteger tanto a ciudadanos como a instituciones de crecientes amenazas digitales. Destacan la "Política de ciberseguridad de El Salvador", establecida bajo la administración del presidente Nayib Bukele, que busca sincronizar esfuerzos de seguridad entre diversos sectores. Esta política incluye la educación en ciberseguridad, revisión legal y la formación de una comisión especializada en delitos informáticos.

Además, se han realizado reformas importantes en la legislación penal, específicamente en el Código Procesal Penal y la Ley Especial contra los Delitos Informáticos, para fortalecer la respuesta legal ante ciberdelitos. La Ley de Firma Electrónica también juega un papel crucial en asegurar transacciones en línea.

El Salvador ha promovido la organización institucional en ciberseguridad, exigiendo que cada entidad estatal nombre un coordinador de ciberseguridad y sugiriendo la formación de Comités de Seguridad de la Información en cada institución. Además, se fomenta la certificación de procesos de ciberseguridad conforme a estándares nacionales e internacionales, demostrando el compromiso del país con la seguridad digital global.

2.4. Leyes de El Salvador

2.4.1. Código Penal:

El Código Penal salvadoreño fue inicialmente promulgado mediante el Decreto Legislativo N° 270 el 13 de febrero de 1973. Este texto ha experimentado varias modificaciones a lo largo de los años para adaptarse a los cambios en la sociedad y las necesidades de justicia. La versión actual del Código Penal fue instaurada por el Decreto Legislativo N° 1030, aprobado el 26 de abril de 1997 y puesto en vigencia el 20 de abril de 1998.

Esta legislación moderna y actualizada está diseñada para ser una herramienta eficaz en la lucha contra la delincuencia, incluyendo disposiciones específicas sobre delitos, penas y medidas de seguridad. Además, se sustenta en principios fundamentales como el principio de legalidad, la dignidad humana y la lesividad del bien jurídico, asegurando un marco legal justo y equitativo. (Asamblea General de la Republica - Decreto 270, s.f.) (Asamblea General de la Republica - Decreto 482, s.f.)

2.4.2. Ley Especial Integral para una Vida Libre de Violencia para las Mujeres (LEIV):

Promulgada en 2012, la LEIV busca garantizar el derecho de todas las mujeres a una vida libre de violencia en El Salvador. Esta ley establece políticas públicas comprensivas para la detección, prevención, atención, protección, reparación y sanción de cualquier forma de violencia contra las mujeres. A través de esta legislación, se protegen derechos fundamentales como la vida, la integridad física y moral, la no discriminación y la dignidad. La LEIV aborda la violencia contra las mujeres desde una perspectiva integral, reconociendo y actuando contra las desigualdades de poder y las relaciones de género asimétricas. (Decreto 520, LEIV, s.f.)

2.4.3. Ley de Protección Integral de la Niñez y Adolescencia (LEPINA):

Entrada en vigor el 16 de abril de 2010, la LEPINA es fundamental para la protección de los derechos de niñas, niños y adolescentes en El Salvador. Esta ley crea un Sistema Nacional de Protección Integral de la Niñez y Adolescencia, alineándose con la Constitución del país y diversos tratados internacionales sobre derechos humanos, especialmente la Convención sobre los Derechos del Niño. La LEPINA está diseñada para salvaguardar la salud física, mental y moral de los menores, garantizando así su derecho a la educación y a recibir asistencia adecuada. (Ley Lepina, s.f.)

2.5. Estadísticas sobre ingeniería social en adolescentes

2.5.1. Análisis de sentencias sobre abusos sexuales en Internet a niños y niñas en España

Save the Children ha elaborado el "Análisis de Sentencias sobre Abusos Sexuales en Internet a Niños y Niñas en España" (Children, 2023) centrado en el fenómeno del "grooming" o ciberacoso sexual, una problemática en aumento debido a la expansión de internet y las plataformas digitales.

Este fenómeno se caracteriza por la manipulación de un adulto hacia un menor mediante canales digitales, con el objetivo de obtener favores sexuales. El análisis destaca las diversas técnicas empleadas por los perpetradores para realizar el grooming, incluyendo la manipulación emocional, la creación de falsa empatía, promesas de regalos y chantaje. Estas estrategias tienen como fin aislar a la víctima, mermar su capacidad de juicio y aumentar su susceptibilidad al abuso.

El informe resalta la imperiosa necesidad de fomentar la educación digital entre niños, padres y educadores, enfatizando en el desarrollo de un entendimiento crítico acerca de los riesgos en línea. Se busca promover una comunicación abierta y establecer directrices de seguridad para salvaguardar la privacidad y la integridad de los menores.

Desde un punto de vista legislativo y organizacional, se recomienda la instauración de políticas de prevención, legislación reforzada y sistemas de alerta temprana para proteger a los menores frente al grooming y otros peligros digitales. Se subraya la importancia de una cooperación intersectorial que abarque los sectores educativo, tecnológico y jurídico, para crear un ambiente digital más seguro.

La llamada a la acción se dirige a todos los estratos de la sociedad, resaltando la educación, legislación y colaboración como ejes centrales en la batalla contra el ciberacoso sexual. Además, el estudio ofrece un perfil detallado de víctimas y agresores, basado en la revisión de casos. Las víctimas, de una edad promedio de 13 años, presentan una distribución equitativa entre géneros, aunque con una ligera predominancia femenina. Un porcentaje importante de estas tiene discapacidades, incrementando potencialmente su vulnerabilidad. En relación a los agresores, se observa que la mayoría no poseía antecedentes penales y que, en casi la mitad de los incidentes, no había un conocimiento previo entre víctima y victimario, revelando diversos grados de relación previa, desde conocidos hasta figuras de autoridad como educadores o entrenadores.

2.5.2. Llegar a cero embarazos en niñas y adolescentes, Mapa El Salvador 2023

El informe " Llegar a cero embarazos en niñas y adolescentes, Mapa El Salvador 2023 " de UNFPA El Salvador (UNFPA, 2023) proporciona un análisis extenso sobre las tendencias de embarazos en adolescentes en El Salvador desde 2015 hasta 2022, destacando la importancia de abordar este problema a través de estrategias multifacéticas. Aquí hay hallazgos y recomendaciones más detallados del informe:

Hallazgos Clave:

- El informe sirve como una herramienta crucial para comprender la problemática del embarazo adolescente, orientando políticas públicas y programas para reducir las tasas de embarazo adolescente y promoviendo la coordinación interinstitucional nacional y municipal.
- Ha habido una disminución significativa en las inscripciones prenatales entre niñas de 10 a 14 años en un 65.5% y entre adolescentes de 15 a 19 años en un 58.1% entre 2015 y 2022. Sin embargo, el ritmo de reducción se ha ralentizado desde 2019, particularmente entre el grupo de menor edad.
- El documento enfatiza la necesidad de esfuerzos acelerados en municipios que han mostrado el menor progreso y las tasas de embarazo más altas. Sugiere centrarse en seis municipios con condiciones particularmente desfavorables: Ahuachapán Centro, Ahuachapán Sur, Sonsonate Centro, Sonsonate Norte, Sonsonate Oeste y Morazán Sur.
- Se recomienda un cambio hacia un enfoque más diferenciado entre lo urbano y lo rural debido a problemas persistentes en ambos entornos, aunque históricamente más asociados con áreas rurales.

Recomendaciones para la Política Pública:

- El informe pide estrategias que aseguren una cobertura educativa universal y acceso a servicios de salud integrales con enfoque en anticonceptivos modernos para prevenir embarazos a edad temprana.

- Enfatiza la erradicación de las uniones conyugales tempranas, que contribuyen significativamente a los embarazos adolescentes, especialmente en sectores vulnerables. Las políticas deberían apuntar a empoderar a las niñas y adolescentes para ejercer plenamente sus derechos sexuales y reproductivos y reducir su vulnerabilidad al embarazo temprano.
- La promoción de una cultura contra la impunidad sexual, particularmente crímenes contra menores, es vital. Fortalecer el papel de la familia y las autoridades en proporcionar apoyo integral a las víctimas e integrar esfuerzos judiciales para restaurar los derechos de las niñas jóvenes a través de procesos legales eficientes es crucial.
- Se aconseja un cambio de enfoque hacia enfoques territoriales adaptados a las nuevas divisiones administrativas y diferentes necesidades locales. El informe sugiere planes de acción municipales y distritales que consideren las particularidades locales para lograr el objetivo de cero embarazos entre niñas y adolescentes.
- Mejorar la lucha contra todas las formas de violencia contra niñas y adolescentes, incluyendo la violencia sexual, se considera esencial para reducir los embarazos tempranos. Esto incluye un mayor empoderamiento de derechos para las mujeres jóvenes y entornos familiares y comunitarios de apoyo.

El informe subraya la naturaleza multidimensional de los embarazos a temprana edad vinculados a reveses socioeconómicos estructurales y dinámicas culturales arraigadas. Destaca la importancia de abordar estos problemas a través de estrategias integrales e integradas que se adapten a las diferentes necesidades y realidades en los territorios de El Salvador.

2.5.3. Resumen de Análisis y Estudios sobre Problemáticas Sociales en España y El Salvador:

Análisis de Abusos Sexuales en Internet en España: El informe de Save the Children se centra en el "grooming" o ciberacoso sexual en España, resaltando las técnicas de manipulación utilizadas por los agresores para explotar sexualmente a menores

en línea. Se destaca la necesidad de mejorar la educación digital y establecer medidas de prevención y protección para los menores. Además, sugiere la importancia de la cooperación intersectorial para crear un entorno digital seguro, basándose en el perfil de las víctimas y los agresores detallado en el estudio.

Informe sobre Embarazos en Adolescentes en El Salvador: El informe de UNFPA aborda la disminución de los embarazos en adolescentes desde 2015, señalando una ralentización en la reducción de las tasas. Se recomienda una mayor atención en municipios con altas tasas de embarazo y un enfoque diferenciado entre lo urbano y lo rural. El estudio llama a políticas públicas que promuevan la educación, el acceso a servicios de salud reproductiva y la lucha contra las uniones tempranas y la violencia sexual, apuntando hacia una mayor individualización de estrategias a nivel local para prevenir embarazos en adolescentes y niñas.

Ambos informes resaltan problemas sociales significativos en sus respectivos países y enfatizan la importancia de acciones educativas, legislativas y de apoyo intersectorial para abordar estas problemáticas, orientadas tanto a la prevención como a la respuesta efectiva a estas situaciones.

3. Marco Teórico

3.1. Digitalización en El salvador

La transición hacia la digitalización en América Latina, impulsada por la Cuarta Revolución Industrial, ha tenido un impacto significativo en las interacciones sociales y el desarrollo personal, especialmente entre los adolescentes. Klaus Schwab, en su libro "La Cuarta Revolución Industrial" (2016), describe este fenómeno como un cambio de paradigma derivado de la convergencia de tecnologías en los ámbitos digital, físico y biológico. Este proceso plantea tanto oportunidades como desafíos para la humanidad, transformando radicalmente nuestra forma de vivir, trabajar y relacionarnos (Schwab, 2016).

En El Salvador, el creciente uso de tecnologías digitales por parte de los adolescentes ha generado un entorno donde las oportunidades y desafíos en el ciberespacio se entrelazan significativamente. La digitalización ha transformado profundamente la interacción social, el ámbito laboral y la vida cotidiana de esta población. Estudios evidencian cómo las fronteras entre los mundos físico y digital se difuminan cada vez más con la presencia omnipresente de dispositivos conectados y plataformas en línea (NU. CEPAL-Comisión Europea, 2013-03).

Desde 2005, El Salvador ha implementado iniciativas como las Cyberolimpiadas para abordar la brecha digital y fomentar la capacitación en tecnologías de información y comunicación (JOAO, Octubre-diciembre de 2005), Sin embargo, este panorama también expone a los adolescentes a diversos riesgos en el ciberespacio. Amenazas como la ingeniería social, el phishing y el grooming representan peligros concretos que pueden comprometer su seguridad y bienestar. Es esencial adoptar un enfoque holístico para abordar estos riesgos, integrando educación en ciberseguridad y políticas públicas efectivas que promuevan un uso seguro y responsable de la tecnología. (Universidad Luterana Salvadoreña, 2021)

El Salvador está implementando tecnología en la educación a través de diversas iniciativas y políticas. Algunas de las acciones destacadas incluyen:

- El Plan Social Educativo 2009-2014 "Vamos a la escuela" propuso la transformación del sistema educativo para fomentar una cultura científica y tecnológica, la formación docente en tecnologías de la información y la integración de la ciencia, tecnología e innovación en la educación.

- El Plan Cuscatlán de Educación (2019) apoya el fortalecimiento institucional en tecnología, recursos humanos y materiales, con programas como "Mi Nueva Escuela" que promueven Internet para todos.

- El Programa Acceso Universal a las Tecnologías Educativas "Enlaces con la educación" busca universalizar el acceso a recursos tecnológicos e incluir conectividad a Internet para estudiantes, docentes y centros educativos.

- Se han desarrollado recursos educativos como libros de lectura para Primera Infancia, libros de texto para estudiantes en diferentes áreas curriculares y guías metodológicas para docentes.

- El nuevo currículo de El Salvador se enfoca en el estudiante como actor propositivo de su propio aprendizaje, promoviendo una formación básica en ciencias, tecnología y artes.

- La Malla Curricular de Profesorado en Educación Básica incluye la asignatura "Tecnología y Educación" para desarrollar competencias en docentes en el diseño e implementación de recursos didácticos utilizando tecnologías.

Estos esfuerzos reflejan un enfoque integral hacia la integración de la tecnología en la educación salvadoreña, con el objetivo de mejorar la calidad académica, fomentar el pensamiento científico y computacional, y preparar a estudiantes y docentes para un mundo digitalizado (Unesco, 2023).

3.2. Definición de Ciberseguridad

La ciberseguridad, fundamental en la era digital, se define como la práctica enfocada en la protección de sistemas, redes y programas frente a ataques digitales. Estos ataques persiguen objetivos como acceder, alterar o destruir información confidencial; extorsionar a usuarios; o interrumpir operaciones empresariales. Su importancia es crítica en un mundo donde la dependencia tecnológica es cada vez mayor, abarcando desde la vida cotidiana hasta los ámbitos empresariales y gubernamentales. (AWS, s.f.)

Esta relevancia se intensifica en el contexto de los adolescentes, quienes, inmersos en entornos digitales para socializar, aprender y entretenerse, se exponen significativamente a riesgos online como el robo de identidad, el ciberacoso o el acceso a contenido inapropiado. Las amenazas cibernéticas son variadas y sofisticadas, incluyendo malware (virus, troyanos, spyware, ransomware, adware), ataques de ingeniería social (phishing) y ataques técnicos (inyecciones SQL, ataques de denegación de servicio), entre otros. Frente a este panorama, la

ciberseguridad adopta un enfoque multifacético que no solo incorpora el uso de software de seguridad actualizado, sino también la educación sobre prácticas seguras en línea y la promoción de hábitos digitales prudentes. (AWS, s.f.)

La protección ofrecida por la ciberseguridad es esencial para todos, desde individuos hasta grandes organizaciones y gobiernos, dado que los impactos de un ataque cibernético pueden ser devastadores, incluyendo pérdidas financieras y afectaciones a la infraestructura crítica y la seguridad nacional. Así, la ciberseguridad engloba un conjunto amplio de herramientas, prácticas y conceptos destinados a salvaguardar contra los ataques digitales y sus consecuencias, subrayando la necesidad de estrategias de seguridad integrales que atiendan especialmente a los usuarios jóvenes, dada su vulnerabilidad particular frente a ciertos ataques debido a su uso intensivo de redes sociales y plataformas en línea (AWS, s.f.)

3.3. Riesgos y Amenazas en el Ciberespacio

La ingeniería social se define como una metodología avanzada de manipulación que explota las vulnerabilidades humanas para acceder a información confidencial, sistemas asegurados o activos de valor. Esta forma de "hacking humano" es una táctica prominente dentro de la ciberdelincuencia, induciendo a individuos a revelar datos sensibles, instalar software malicioso, acceder a sitios web comprometidos, realizar pagos a impostores o incurrir en errores que comprometan su seguridad personal o empresarial. (Kaspersky, s.f.)

El éxito de estos ataques se basa en un conocimiento profundo de la psicología y el comportamiento humano, con el sabotaje y el robo como principales objetivos. El primero busca dañar o destruir información, mientras que el segundo apunta a la adquisición de activos valiosos como datos sensibles o acceso a sistemas críticos. Las estrategias empleadas, incluyendo phishing, pretexting y baiting, manipulan las emociones y los instintos de las víctimas para actuar en contra de sus intereses. Los efectos de la ingeniería social son particularmente dañinos para los

adolescentes, aumentando su exposición a amenazas y afectando negativamente su desarrollo cognitivo y rendimiento académico.

Los ataques telefónicos constituyen una modalidad prevalente de ingeniería social, caracterizada por su ingenio en la ejecución. Mediante la simple adquisición de un número telefónico, los atacantes pueden contactar a sus víctimas haciéndose pasar por terceros confiables, como técnicos, colegas o representantes de entidades reconocidas. El propósito de estas interacciones es la extracción de información crítica que pueda ser utilizada para obtener beneficios ilícitos.

En el ámbito digital, los ataques mediante Internet se erigen como una de las tácticas más tradicionales de ingeniería social. Ejemplos comunes incluyen correos electrónicos que notifican premios de concursos no participados o loterías, así como advertencias que incitan a visitar sitios web bajo amenazas de perder acceso a servicios digitales. Estas estrategias, que abarcan desde el envío de correos fraudulentos hasta la participación en foros o chats, representan una amenaza significativa para la seguridad y privacidad de la información personal. Por otro lado, la ingeniería social a través de mensajes de texto aprovecha la comunicación móvil para perpetrar ataques. Estos suelen presentarse bajo la forma de ofertas promocionales o servicios donde responder puede derivar en la divulgación de datos personales importantes o, en casos más graves, en la implicación en Estafass de mayor envergadura. (Vico, 2021).

Un ataque digital se refiere a cualquier comportamiento o acción maliciosa que utilice tecnologías de la información y comunicación, como teléfonos, sitios web, redes sociales y correos electrónicos, con el objetivo de provocar, incitar o exacerbar daños. (SocialTIC, s.f.)

Tipos de ataques digitales:

Vulneraciones técnicas: Estos ataques explotan las debilidades técnicas del diseño tecnológico para alterar o dañar su funcionamiento con fines malintencionados.

Conductas humanas: Consisten en manipular o aprovechar las relaciones humanas y sociales para causar daño.

Ejemplos de ataques de vulneraciones técnicas:

3.3.1. Fraude o Estafas

El fraude o estafa consiste en prácticas engañosas o ilegales destinadas a lograr beneficios financieros de manera deshonesta. Esto puede abarcar el mal uso de información personal, manipulación de transacciones financieras o la falsificación de documentos. En el ámbito digital, se manifiesta a través de estafas en línea, robo de identidad, falsificación de tarjetas de crédito y transferencias de fondos fraudulentas. Los delincuentes emplean una variedad de técnicas para perpetrar fraudes o estafas, incluyendo el phishing, malware e ingeniería social. (Superintendencia Del Sistema Financiero, s.f.)

3.3.2. Phishing

3.3.3. El phishing es un tipo específico de Fraude o Estafas

ejecutado mediante correos electrónicos, mensajes de texto o sitios web fraudulentos, que busca que las personas divulguen información confidencial, como contraseñas, datos de tarjetas de crédito o información bancaria. Los atacantes se hacen pasar por entidades fiables, como bancos, compañías o instituciones gubernamentales, para solicitar datos personales a sus víctimas.

Los correos electrónicos de phishing a menudo contienen enlaces maliciosos o archivos adjuntos que, al ser abiertos, pueden instalar software dañino en el dispositivo de la víctima o redirigirla a páginas web impostoras. En El Salvador, el debate sobre la legislación de delitos informáticos ha llevado a la aprobación de reformas significativas al Código Procesal Penal, autorizando operaciones encubiertas digitales para investigar delitos informáticos sin necesidad de una orden judicial previa. Sin embargo, estas medidas han generado preocupaciones en torno a la privacidad y la libertad de expresión. (Human Rights Watch, 2022)

En meses recientes, se ha visto un incremento en los casos de phishing dirigidos a usuarios de la banca privada en El Salvador. Las autoridades han estado investigando estos incidentes, que han llevado a la extracción no autorizada de fondos de cuentas bancarias. Human Rights Watch reportó estos sucesos en 2022. Según el ESET Security Report 2023, El Salvador se posiciona entre los países de América Latina con una alta tasa de detección de códigos maliciosos empleados en campañas de phishing. Este informe destaca el estado actual de la ciberseguridad y los desafíos en la región, evidenciando la necesidad de fortalecer las medidas de protección contra estas amenazas. (ASSET, 2023)

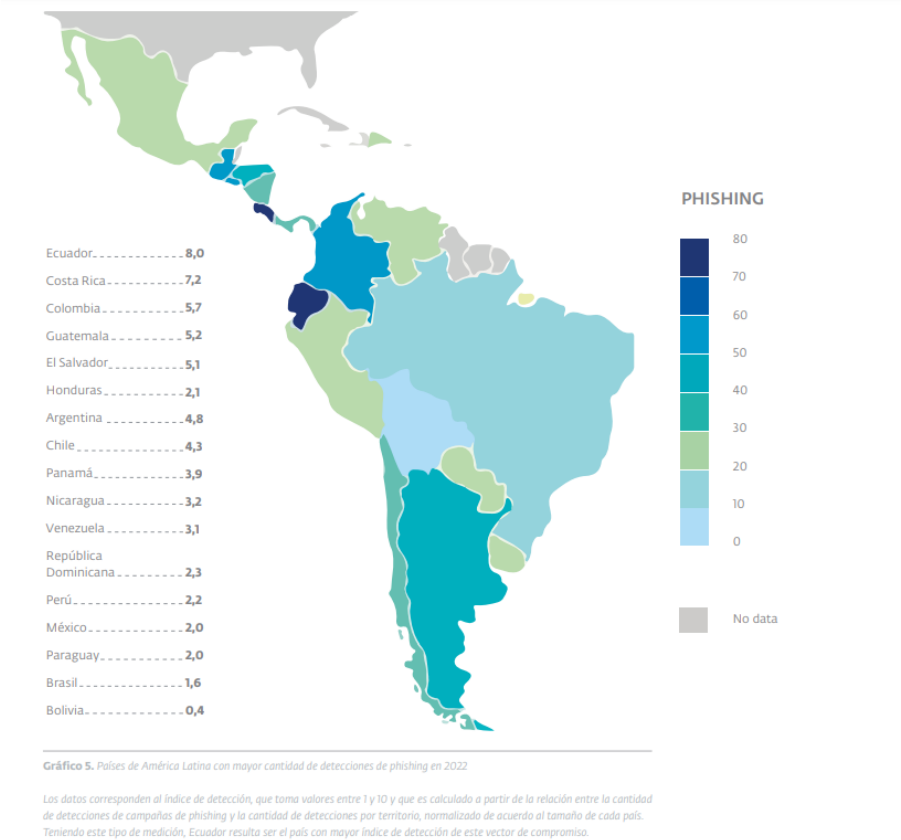


Ilustración 1. Tasa de detección de códigos maliciosos empleados en campañas de phishing, imagen tomada de (ASSET, 2023)

3.3.4. Spyware

El spyware constituye una forma avanzada de malware diseñado con el propósito específico de operar de manera subrepticia. Su principal función es la captura y monitorización exhaustiva de información personal y actividades online del usuario sin dejar rastro de su presencia. Este tipo de software malicioso es capaz de infiltrarse tanto en ordenadores como en dispositivos móviles, registrando detalladamente cada acción realizada por el usuario, incluyendo las pulsaciones de teclado y el manejo de archivos (subidas, descargas y almacenamiento).

Lo distintivo del spyware es su instalación no autorizada en una diversidad de plataformas, tales como sistemas operativos de computadoras, navegadores web y aplicaciones móviles, con el objetivo de recolectar y enviar información personal del usuario a entidades externas sin su consentimiento. A diferencia de otras variantes de malware, el spyware se enfoca en la recolección de datos de forma oculta, sin pretender causar daños directos al sistema operativo del dispositivo infectado.

Sus capacidades incluyen, pero no se limitan a, la captura de pulsaciones del teclado a través de keyloggers, el monitoreo de la actividad online, el robo de información confidencial como contraseñas y detalles financieros, así como el seguimiento de las interacciones del usuario en redes sociales y correo electrónico. El modus operandi del spyware es particularmente sigiloso, transmitiendo la información obtenida a los atacantes de manera imperceptible para el usuario.

La propagación del spyware suele efectuarse mediante descargas inadvertidas provocadas al visitar páginas web comprometidas o interactuar con anuncios maliciosos, lo cual facilita la instalación automática del spyware. Este también se promueve mediante técnicas de publicidad engañosa, ofreciéndose como herramientas supuestamente benéficas (ejemplo: aceleradores de internet o programas de limpieza de disco duro) que, una vez instaladas, liberan el spyware en el sistema. Otra estrategia frecuente es su inclusión en el software gratuito, induciendo al usuario a instalar aplicaciones dañinas sin su conocimiento. Estos métodos subrayan la complejidad y el riesgo asociados al spyware, resaltando su

posición como una amenaza significativa en el ámbito de la ciberseguridad contemporánea.

De acuerdo con el ESET Security Report 2023, El Salvador se ha ubicado entre los países de América Latina con una notable tasa de detección de este tipo de ataques. Aunque actualmente no es extremadamente prevalente, existe una tendencia creciente que sugiere que los porcentajes de incidencia podrían aumentar en un plazo breve. (ASSET, 2023)

Ilustración 2. Tasa de detección de este tipo de ataques de Spyware, imagen tomada de (ASSET, 2023)

3.3.5. Vishing:

Vishing es una técnica que implica la obtención de información a través de llamadas telefónicas. Los ciberdelincuentes se hacen pasar por familiares, personal de empresas reconocidas o de soporte técnico para engañar a las víctimas y obtener datos sensibles. Este tipo de ataque se aprovecha de la confianza y la falta de conocimiento de la víctima para obtener información personal o financiera. (Argentino, 2023)

3.3.6. Spear phishing:

El spear phishing es un ataque de phishing dirigido a individuos específicos, generalmente personas que ocupan cargos importantes en una organización o que manejan información sensible. Los atacantes realizan investigaciones previas sobre sus objetivos para personalizar los correos electrónicos fraudulentos y aumentar sus posibilidades de éxito. Esta forma de ataque es especialmente peligrosa debido a su enfoque personalizado y detallado, que puede engañar incluso a usuarios bien informados. (Argentino, 2023)

3.3.7. Concursos falsos:

Mediante esta estrategia, los delincuentes informan a las personas que han ganado un premio inexistente con el objetivo de obtener información personal bajo el pretexto de entregar el supuesto premio. Este tipo de engaño juega con la expectativa y emoción de la víctima, haciéndola más propensa a compartir información confidencial sin cuestionar la veracidad del concurso. (Argentino, 2023)

3.3.8. Doxing

El doxing es la práctica de recopilar y publicar información personal o privada de una persona en línea sin su consentimiento, con la intención de causar daño, intimidación o acoso. Esta información puede incluir nombres completos, direcciones, números de teléfono, datos de empleo, y otra información sensible. El doxing puede tener graves consecuencias para las víctimas, incluyendo amenazas físicas, acoso y daños a su reputación personal y profesional.

El doxing se considera una forma de violencia digital y una violación a la privacidad, ya que expone a las víctimas a riesgos significativos y vulnerabilidades. Las personas que realizan doxing a menudo utilizan múltiples fuentes de información en línea, como redes sociales, registros públicos y bases de datos, para compilar un perfil detallado de la víctima. La motivación detrás del doxing puede variar desde venganza personal hasta campañas de acoso coordinadas por grupos en línea. (kaspersky, s.f.)

Algunos ejemplos de Ataques de Conductas Humanas son:

3.3.9. Ciberacoso u ciberbullying

El ciberacoso u ciberbullying, una modalidad de acoso ejecutada en el entorno digital, ha visto un incremento alarmante con el auge de las redes sociales, las plataformas de comunicación en línea, y los juegos interactivos, particularmente entre los adolescentes. Este tipo de acoso abarca acciones como enviar mensajes de texto hostiles, difundir rumores en línea, publicar fotos o videos embarazosos sin consentimiento, y crear perfiles falsos para molestar a una persona. (El tiempo latino, 2018)

En El Salvador, la prevalencia del ciberacoso en niños, adolescentes y jóvenes es motivo de creciente preocupación. Este fenómeno se agrava por el acceso generalizado a teléfonos móviles y redes sociales, a pesar de que un considerable porcentaje de escuelas en el país no dispone de acceso a Internet. Plataformas como Snapchat, conocidas por la circulación de contenidos inapropiados, son particularmente problemáticas. Los estudios indican que los jóvenes salvadoreños tienen un alto nivel de acceso a dispositivos móviles, lo cual se refleja en el significativo gasto mensual en telefonía celular. Las consecuencias del ciberacoso pueden ser graves, incluyendo problemas de concentración, aislamiento, delirios de persecución y tendencias suicidas. (El tiempo latino, 2018)

Rocío de Cáceres, psicóloga, subraya la importancia de atender tanto al acosador como a la víctima. El ciberacoso frecuentemente se origina en inseguridades personales, aprovechando la facilidad de ataque que ofrece el mundo digital. Los acosadores a menudo replican patrones de comportamiento aprendidos o buscan satisfacer necesidades emocionales a través de la intimidación. El impacto psicológico del ciberacoso es considerable, dada su capacidad de ocurrir en cualquier lugar y momento. (Salvador, 2021)

3.3.10. Sextorsión

La sextorsión es una forma de extorsión en la que los ciberdelincuentes obtienen imágenes, videos o información sexualmente explícita de una víctima y luego la amenazan con publicar dicho material si no cumplen con sus demandas. Estas demandas pueden incluir dinero, más imágenes explícitas o favores sexuales.

La sextorsión puede tener efectos devastadores en las víctimas, llevándolas a experimentar miedo, vergüenza y angustia emocional. Los adolescentes son particularmente vulnerables a este tipo de amenaza debido a su uso frecuente de redes sociales y plataformas de mensajería. Aunque no hay datos específicos sobre la sextorsión en El Salvador, se sabe que las mujeres son víctimas frecuentes de extorsión y violencia en general. La falta de denuncias específicas sobre sextorsión no significa que no sea un problema en el país. (National Center for Missing & Exploited Children, s.f.)

3.3.11. Grooming

El grooming representa una modalidad de abuso digital caracterizada por la manipulación y explotación sexual de menores de edad por parte de adultos. Esta práctica delictiva se lleva a cabo principalmente a través de plataformas digitales, donde el agresor establece una comunicación con el objetivo de construir una relación de confianza con niños, niñas o adolescentes. La estrategia subyacente en el grooming incluye el uso de engaños, sobornos o coacción, aprovechando la comunicación electrónica como un medio eficaz para lograr sus propósitos nefastos y orientar gradualmente al menor hacia la participación en actividades sexuales. (Children, 2023)

La dinámica del grooming se inicia con el agresor intentando presentarse como un par del menor, a menudo falseando su edad y mostrando una falsa empatía hacia los problemas personales del joven. Este enfoque tiene como fin último ganarse la confianza del menor, facilitando así el proceso de manipulación. Los agresores suelen emplear regalos o promesas para fortalecer este vínculo de confianza,

creando una dependencia emocional que puede ser explotada para fines de chantaje.

Una vez establecida esta relación de confianza, el agresor trabaja para aislar al menor de su entorno natural de apoyo, incluyendo familiares y amigos, aumentando la vulnerabilidad del joven a la manipulación. Esta estrategia de aislamiento es crítica, ya que reduce la probabilidad de que el menor busque ayuda o asesoramiento exterior.

A medida que avanza la relación, el agresor introduce gradualmente temas de índole sexual dentro de las conversaciones, normalizando este tipo de contenido para el menor. El paso final en el proceso de grooming es la explotación sexual del menor, donde el agresor busca obtener material sexual explícito, a menudo bajo amenazas, manipulación o chantaje, llegando incluso a presionar por encuentros sexuales físicos. (Children, 2023)

Aunque en El Salvador el grooming no se define específicamente como delito, la denuncia de estos casos ante las autoridades es de vital importancia. Información proporcionada por el Ministerio del Interior señala que, durante el año 2022, se registraron 954 denuncias por delitos sexuales cibernéticos, siendo el 64.6% de las víctimas chicas.

3.3.12. Farming:

El farming implica una serie de comunicaciones con la víctima con el fin de ganarse su confianza y recolectar progresivamente la mayor cantidad posible de información personal. Este método se basa en la construcción de una relación de confianza con la víctima, lo que facilita la obtención de datos sensibles de manera gradual. (Argentino, 2023)

3.3.13. Creación de perfiles falsos:

La creación de perfiles falsos implica la elaboración de identidades ficticias que se emplean con diversos propósitos, algunos de ellos malintencionados. Los

atacantes, por ejemplo, utilizan estos perfiles falsos para suplantar a micro-influencers en redes sociales, con el objetivo de engañar a seguidores y obtener información o recursos valiosos de manera fraudulenta. (Casillas, 2023)

Ilustración 3. Ataques de ingeniería social, imagen tomada de (Institute, s.f.)

3.4. Vulnerabilidades de los Adolescentes

La vulnerabilidad de los adolescentes en el ciberespacio constituye una preocupación creciente dentro del ámbito académico y social, principalmente debido a la convergencia de varios factores críticos como la falta de experiencia, la sobreexposición en redes sociales y una curiosidad innata por explorar lo desconocido. Este documento explora en profundidad estos aspectos, apoyándose en estadísticas y estudios relevantes para comprender mejor la magnitud y las implicaciones de esta problemática. (conversation, 2018)

Uno de los desafíos más significativos que enfrentan los adolescentes al navegar por el ciberespacio es su limitada experiencia. Esta falta de madurez digital no solo afecta su capacidad para identificar riesgos potenciales, sino que también limita su entendimiento respecto a las consecuencias a largo plazo de sus acciones en línea. La interacción con individuos malintencionados o la divulgación inadvertida de información personal son ejemplos claros de cómo la falta de experiencia puede comprometer su seguridad en la red.

Las redes sociales representan un doble filo para los adolescentes. Por un lado, ofrecen un espacio para la expresión personal y la conexión social; por otro, pueden convertirse en plataformas de riesgo donde la sobreexposición de información personal es moneda corriente. Esta práctica incrementa la vulnerabilidad de los jóvenes frente a amenazas como el ciberacoso y la explotación digital, fenómenos cada vez más prevalentes en nuestra sociedad hiperconectada.

La innata curiosidad de los adolescentes puede impulsarlos hacia la exploración de áreas riesgosas del ciberespacio, desde la interacción con desconocidos hasta la navegación por sitios web de dudosa seguridad. Esta tendencia no solo expone a los jóvenes a contenido inapropiado, sino que también incrementa el riesgo de descargar aplicaciones o contenido malicioso, poniendo en peligro su integridad digital y física.

Un estudio focalizado en El Salvador reveló que el 60% de los jóvenes reconoce el valor de sus datos personales y su uso por empresas para la venta de productos y servicios. Sin embargo, un 13% reporta haber sido víctima de ciberataques, lo que subraya la necesidad de una mayor conciencia y protección digital (elsalvador.com, 2021). En el contexto de Centroamérica, se ha registrado un incremento en crímenes cibernéticos como el phishing y el robo de datos, destacando la prevalencia y la diversificación de estas amenazas en la región.

Además, la Asociación de Internet MX indica que, en Latinoamérica, el 65% de los niños y adolescentes posee acceso a un teléfono inteligente, y uno de cada tres dispone de al menos tres dispositivos conectados a internet (MX, 2023). Esta conectividad, si bien facilita el acceso a información y oportunidades educativas, también amplía el espectro de riesgos a los que están expuestos los jóvenes.

4. Metodología

En el contexto del progreso científico y tecnológico, particularmente en áreas como la ciberseguridad y la informática, los métodos de investigación son herramientas cruciales para abordar la complejidad creciente de los sistemas digitales. Según se

expone en la obra "Metodología de la Investigación" de Roberto Hernández Sampieri y sus coautores (2014, McGraw-Hill) (Sampieri) , estos métodos implican una combinación de estrategias y técnicas diseñadas para la recolección y el análisis de datos. Esta mezcla, que abarca tanto enfoques cuantitativos como cualitativos, es esencial para alinearse con los diversos fines de la investigación en el ámbito tecnológico.

Los métodos de investigación destacados en este libro son clave para una comprensión profunda y sistemática de los fenómenos tecnológicos. Permiten no solo la generación de nuevo conocimiento sino también la verificación y refinamiento de teorías preexistentes. Estos métodos son especialmente valiosos en el desarrollo de tecnologías avanzadas, donde proporcionan un marco para la experimentación, el análisis de datos y la deducción de conclusiones confiables, impulsando así el avance de la ciencia y la tecnología.

La relevancia de estos métodos de investigación trasciende la adquisición de conocimientos, extendiéndose a la formación académica y profesional. A través de ellos, estudiantes y profesionales adquieren la habilidad para realizar investigaciones de manera ética y rigurosa, una competencia fundamental para abordar los desafíos actuales y contribuir al bienestar y desarrollo sostenible de la sociedad.

4.1. Importancia y Aplicaciones de los Métodos de Investigación en Ciberseguridad

La importancia y las aplicaciones de los métodos de investigación en ciberseguridad son amplias y diversas, reflejando la complejidad y la naturaleza dinámica de la seguridad en el ámbito digital. Estos métodos no solo permiten el desarrollo de soluciones y políticas basadas en evidencias, incrementando la eficacia en la protección contra amenazas digitales, sino que también son cruciales para comprender las amenazas emergentes. Mediante el uso de técnicas cuantitativas y cualitativas, es posible identificar tendencias y patrones en ataques cibernéticos, así

como obtener una comprensión profunda de las tácticas y procedimientos de los ciberdelincuentes. (Picado, 2023)

Además, los métodos de investigación son fundamentales para evaluar y mejorar las estrategias de defensa actuales, permitiendo desarrollar nuevas tácticas para una eficaz prevención, detección y respuesta ante incidentes de seguridad. Esto incluye la revisión y evaluación de herramientas de seguridad existentes, la implementación de algoritmos de cifrado y la adecuación de políticas de gestión de riesgos. La formación y sensibilización también se benefician enormemente de estos métodos, ya que proporcionan insights valiosos sobre las actitudes y comportamientos de los usuarios respecto a la ciberseguridad.

En lo que respecta a las aplicaciones prácticas, los métodos de investigación en ciberseguridad abarcan desde la evaluación de herramientas y tecnologías de seguridad, hasta el análisis de riesgos y vulnerabilidades en sistemas de información. La investigación también es instrumental en el desarrollo de políticas de seguridad personalizadas y efectivas para organizaciones, así como en la creación de programas de educación y concienciación que mejoren las prácticas de seguridad entre los distintos grupos de interés.

Adicionalmente, estos métodos permiten la anticipación de futuras amenazas mediante el análisis de tendencias en ciberseguridad y la preparación adecuada frente a posibles ataques. Importante también es el estudio del comportamiento humano relacionado con la ciberseguridad, fundamental para diseñar sistemas y políticas que no solo sean técnicamente eficientes, sino también comprensibles y manejables para los usuarios finales. (Picado, 2023)

4.2. Metodología Mixt

La metodología mixta, presentada en el libro "Metodología de la Investigación" de Roberto Hernández Sampieri y sus coautores (2014, McGraw-Hill), (Sampieri), se erige como un enfoque de investigación relevante y estratégico, especialmente por su habilidad para integrar elementos cuantitativos y cualitativos dentro de un mismo

estudio. Este enfoque híbrido no solo amalgama las fortalezas de ambos métodos, sino que también abre el camino hacia una comprensión más exhaustiva y matizada de los problemas de investigación. (Sampieri),

4.2.1. Integración de Elementos Cuantitativos y Cualitativos

La metodología mixta destaca por su habilidad para armonizar la precisión cuantitativa con la riqueza cualitativa en el ámbito de la investigación. Esta síntesis permite la triangulación de datos, un proceso en el cual los hallazgos obtenidos a través de un enfoque se examinan y complementan con los de otro, mejorando notablemente la confiabilidad y validez de los resultados. Este enfoque facilita la exploración de preguntas desde diversas perspectivas, profundizando significativamente la comprensión del fenómeno investigado. (Sampieri),

Las fortalezas de la metodología mixta residen en su potencial para superar las limitaciones de los métodos cuantitativos y cualitativos cuando se utilizan de manera aislada. Al aplicar ambos en simultáneo, se maximizan las ventajas de cada uno, compensando sus debilidades respectivas., tales como:

- Comprensión Integral: Ofrece una visión holística y detallada sobre los problemas de investigación.
- Validación y Triangulación: Aumenta la confianza en los resultados a través de la validación y enriquecimiento de los hallazgos.
- Flexibilidad: Se adapta a una amplia gama de contextos y cuestionamientos investigativos, permitiendo estudios a medida de las necesidades y complejidades específicas.
- Conclusiones Informadas: Facilita interpretaciones robustas de los datos, derivando en conclusiones bien fundamentadas y con implicaciones prácticas significativas.

Seleccionar una metodología de investigación adecuada es crucial para abordar con eficacia los desafíos en áreas críticas como la ciberseguridad. Esto implica una evaluación rigurosa de los objetivos del estudio y la naturaleza de los datos

disponibles. Por ejemplo, al investigar nuevos métodos de ataques informáticos, una estrategia que combine análisis cuantitativos de patrones de ataques con indagaciones cualitativas sobre las tácticas de los atacantes puede desvelar estrategias de defensa innovadoras y más efectivas. (Sampieri),

En campos como la ciberseguridad y las tecnologías de la información, adoptar metodologías de investigación adecuadas es esencial para el avance del conocimiento y el desarrollo de soluciones novedosas. La cuidadosa selección y aplicación de métodos investigativos, apoyados por ejemplos relevantes y evidencia concreta, son vitales para superar los retos de seguridad en el entorno digital actual. La adopción de enfoques metodológicos mixtos, en particular, se revela como una estrategia especialmente eficaz. Estos enfoques permiten navegar la complejidad y el dinamismo de los desafíos informáticos actuales, ofreciendo una panorámica más rica y detallada que contribuye de manera significativa a contrarrestar las amenazas digitales emergentes.

4.3. Diseño de Investigación

En "Metodología de la Investigación" de Roberto Hernández Sampieri y sus coautores (2014, McGraw-Hill) (Sampieri), se destaca la importancia de un diseño de investigación meticulosamente planificado que se adapte a las necesidades específicas de cada estudio. Este diseño integra el uso estratégico de encuestas, entrevistas y grupos focales, facilitando tanto la recolección de datos cuantitativos como cualitativos, lo que constituye la base para una exploración exhaustiva del fenómeno de interés.

4.3.1. Recolección de Datos: Encuestas, Entrevistas y Grupos Focales

Encuestas: Utilizadas para recoger datos cuantitativos a través de cuestionarios estructurados, estas herramientas permiten obtener información de una muestra representativa, facilitando el análisis estadístico y la generalización de los resultados. (Sampieri)

Entrevistas: Ofrecen una profundidad única para recolectar datos narrativos. Mediante el diálogo directo y preguntas abiertas, se capturan las percepciones, experiencias y opiniones de los participantes, aportando una rica comprensión cualitativa del estudio. (Sampieri)

Grupos Focales: Reúnen a varios individuos para discutir un tema específico, profundizando en las percepciones y experiencias compartidas, lo que aporta valiosos insights cualitativos. (Sampieri)

La elección y aplicación rigurosa de estas herramientas son cruciales para garantizar la fiabilidad y validez de los datos recopilados, ajustándose a las exigencias particulares de la investigación.

4.3.2. Integración y Análisis de Datos

Una vez que los datos han sido recolectados, se procede a su análisis de acuerdo con sus características inherentes:

Análisis Cuantitativo: Utiliza técnicas estadísticas para procesar los datos numéricos recopilados. Este análisis busca identificar tendencias, examinar relaciones entre variables y verificar hipótesis. (Sampieri)

Análisis Cualitativo: Se centra en la interpretación de los datos narrativos obtenidos de entrevistas y grupos focales, proporcionando una comprensión detallada de las percepciones y experiencias de los participantes. (Sampieri)

4.3.3. Interpretación Holística

La interpretación de los datos recolectados se realiza de manera holística, integrando tanto los hallazgos cuantitativos como cualitativos para obtener una visión comprensiva del fenómeno estudiado. Este enfoque permite una interpretación integrada que combina lo mejor de ambos enfoques metodológicos, proporcionando una visión completa del problema de investigación. (Sampieri)

4.3.4. Categorización y triangulación

En el ensayo de Francisco Cisterna Cabrera, "Categorización y triangulación como procesos de validación del conocimiento en investigación cualitativa" (Theoria, Vol. 14, 2005), (Cisterna Cabrera, 2005) se destacan la categorización y la triangulación como elementos clave en la validación del conocimiento en investigaciones cualitativas. Estos procesos son esenciales para construir y validar hallazgos de forma confiable y profunda.

La categorización implica organizar los datos recogidos en grupos o categorías significativas, lo que facilita su posterior análisis e interpretación. Cabrera identifica dos tipos de categorías: apriorísticas, definidas antes de la recolección de los datos, y emergentes, que se desarrollan a partir de los datos obtenidos.

Este enfoque es vital para estructurar datos complejos y revelar patrones no inmediatamente evidentes, especialmente en estudios sobre fenómenos humanos y sociales. Por otro lado, la triangulación se presenta como una estrategia metodológica crucial para reforzar la validez y confiabilidad de los resultados investigativos. Consiste en el empleo de diversas metodologías, fuentes de datos, teorías o investigadores para examinar un fenómeno desde múltiples ángulos. Esta pluralidad metodológica supera las limitaciones de los enfoques unilaterales, proporcionando una visión más rica y detallada del objeto de estudio. Cabrera introduce el concepto de "triangulación hermenéutica", que se refiere a la integración de toda la información relevante, mejorando así la solidez de los resultados mediante la validación cruzada. (Cisterna Cabrera, 2005)

4.3.5. Integración de Categorización y Triangulación

La integración de la categorización y la triangulación en la investigación cualitativa permite a los investigadores no solo organizar los datos de manera efectiva sino también validar sus interpretaciones a través de una variedad de lentes y perspectivas. Este enfoque metodológico refuerza la rigurosidad y profundidad del análisis, contribuyendo significativamente a la construcción del conocimiento.

La aplicación de estas estrategias metodológicas asegura que los hallazgos de la investigación sean robustos, confiables y bien fundamentados, reflejando la complejidad del fenómeno estudiado y proporcionando insights valiosos para la teoría y la práctica en el campo de estudio.

En resumen, la categorización y la triangulación son procesos complementarios que, cuando se aplican de manera conjunta, enriquecen la investigación cualitativa, facilitando una interpretación más rica y una validación más fuerte de los resultados obtenidos. (Cisterna Cabrera, 2005)

4.3.6. Matriz de Congruencia

En "Metodología de la Investigación" de Roberto Hernández Sampieri y sus coautores (2014, McGraw-Hill) (Sampieri), la matriz de congruencia, por otro lado, es una herramienta utilizada para comparar y contrastar hallazgos obtenidos mediante diferentes métodos o fuentes de datos dentro de la misma investigación. Funciona alineando los resultados cuantitativos y cualitativos lado a lado para identificar patrones, contradicciones o nuevas preguntas. Esta técnica es particularmente útil para:

- Validar hallazgos: La correspondencia entre resultados cuantitativos y cualitativos puede aumentar la confianza en la precisión de los hallazgos.
- Identificar discrepancias: Las diferencias entre los datos pueden señalar áreas que necesitan más investigación o una reflexión más profunda sobre el diseño del estudio.
- Generar una comprensión holística: Permite una interpretación integrada que combina lo mejor de ambos enfoques metodológicos, proporcionando una visión comprensiva del fenómeno estudiado.

La matriz de congruencia es una representación visual o tabular que facilita este proceso de comparación, ayudando a los investigadores a sintetizar los resultados y a tejer una narrativa coherente que refleje la complejidad del fenómeno investigado. (Sampieri)

4.3.7. Adaptación a las Necesidades de la Investigación

La flexibilidad de estas herramientas permite su adaptación a las necesidades particulares de cada investigación, ofreciendo un espectro amplio de datos que abarca desde visiones generales hasta análisis en profundidad. Mientras que las encuestas proporcionan una panorámica cuantitativa y generalizable del fenómeno estudiado, las entrevistas y los grupos focales permiten una exploración detallada de los aspectos cualitativos, arrojando luz sobre los contextos, matices y complejidades que los datos numéricos por sí solos no pueden revelar.

Esta sinergia metodológica no solo enriquece el proceso investigativo, sino que también asegura una comprensión más completa y contextualizada del tema en estudio, fortaleciendo así la validez y relevancia de los hallazgos. La implementación consciente de estas herramientas dentro del diseño de investigación refleja un compromiso con la obtención de resultados que son a la vez rigurosos y profundamente informativos, abriendo caminos hacia conclusiones más sólidas y aplicaciones prácticas efectivas. (Sampieri)

4.4. Aplicación de Metodologías en el Plan Estratégico para la Ciberseguridad.

4.4.1. Técnicas a Utilizar: entrevistas y focus group

a) Entrevista

La investigación por encuesta es considerada una rama de la investigación social científica orientada a la valoración de poblaciones enteras mediante el análisis de muestras representativas (Kerlinger, 1983). Según Garza (1988), la investigación por encuesta se caracteriza por la recopilación de testimonios, orales o escritos, provocados y dirigidos con el propósito de averiguar hechos, opiniones y actitudes. Para Baker (1997), la investigación por encuesta es un método de recolección de datos en el cual se definen grupos específicos de individuos que responden a un conjunto de preguntas específicas. (Baray, 2016)

En resumen, las definiciones anteriores indican que la encuesta se utiliza para estudiar poblaciones mediante el análisis de muestras representativas con el fin de explicar las variables de estudio y su frecuencia.

La instrumentación consiste en el diseño de un cuestionario o una entrevista elaborados para medir opiniones sobre eventos o hechos específicos. Estos instrumentos se basan en una serie de preguntas. En el cuestionario, las preguntas se administran por escrito a numerosas unidades de análisis. En una entrevista, las respuestas pueden registrarse en la entrevista o llevarse a cabo en una interacción cara a cara.

Cuestionario y Entrevista

Cuando la muestra a encuestar es numerosa, se recomienda utilizar el cuestionario en lugar de la entrevista. Ambos requieren una preparación cuidadosa y exhaustiva de un programa similar en estructura. Una entrevista puede transformarse en un cuestionario y viceversa. Los tipos de ítems utilizados en un programa son de alternativa fija (estructurados) y abiertos (no estructurados):

Ítems Estructurados:

Son preguntas de alternativa fija que ofrecen al respondiente la elección entre dos o más respuestas. Se debe evitar obtener respuestas simples de "sí" o "no", ya que no aportan información relevante. Ventajas: uniformidad de medición y facilidad de codificación. Desventajas: superficialidad y falta de profundidad. (Baray, 2016)

Ítems No Estructurados:

Son preguntas abiertas que permiten al respondiente profundizar en sus respuestas libremente. Son útiles para obtener un marco referencial sobre las respuestas y realizar estimaciones precisas de las opiniones de los respondientes. (Baray, 2016)

b) Focus Group o Grupos focales

El Focus Group es una técnica de investigación cualitativa que reúne a un grupo de participantes con el objetivo de expresar sus opiniones, debatir y responder preguntas sobre un tema específico. Esta técnica se utiliza para obtener información valiosa y extraer insights que permitan diseñar soluciones adecuadas para los usuarios objetivo. Los Focus Groups pueden aplicarse tanto en la fase de investigación exploratoria como en la fase de validación. (Design Thinking España, s.f.)

Características clave de los Focus Groups:

- Duración: Por lo general, la duración de un Focus Group oscila entre una hora y media y dos horas.
- Participantes: El número ideal de participantes es entre 4 y 6, otros dicen que 4 y 10. A estos se les denomina informantes.
- Selección de Informantes: La selección adecuada de los informantes es crucial, ya que representa el 50% del éxito de un Focus Group.
- Moderador: La sesión es moderada por un especialista, quien guía la discusión y da la palabra a los participantes.

Rol del Moderador:

- Asegurar que se alcancen los objetivos planteados para el Focus Group.
- Estar atento a lo que dicen y hacen los participantes.
- Detectar y explorar temas emergentes relevantes para la investigación.
- Mantener el ritmo de la sesión y dinamizarla adecuadamente.
- Garantizar la participación equitativa de todos los informantes, evitando que unos pocos monopolicen la atención o influyan excesivamente sobre el resto.

4.4.2. Matriz de Congruencia

La Matriz de Congruencia, aplicada al Plan Estratégico de Ciberseguridad para Adolescentes en el Área Metropolitana de San Salvador, actúa como un marco

estructurado para relacionar directamente el problema de investigación con los objetivos, hipótesis, unidades de análisis, variables, indicadores, y los métodos de recolección y análisis de datos. Este enfoque asegura una comprensión clara del problema principal —la carencia de conocimiento y conciencia sobre ciberseguridad entre adolescentes— y articula cómo cada elemento del plan, especialmente los objetivos específicos, avanza hacia el cumplimiento del objetivo global. Se destacan las hipótesis que orientan el estudio hacia expectativas de cambio y mejoras mediante las intervenciones propuestas, estableciendo una guía clara para la implementación y evaluación del programa educativo diseñado.

Tabla 4-1.

Matriz de Congruencia

Elemento	Descripción
Tema	Plan Estratégico para la Ciberseguridad: Implementación de herramientas y estrategias para adolescentes del Área Metropolitana de San Salvador.
Enunciado del Problema	¿Cómo puede desarrollarse un Plan Estratégico de Ciberseguridad para fortalecer la conciencia y protección de los adolescentes en el Área Metropolitana de San Salvador frente a riesgos cibernéticos?
Objetivo General	Desarrollar un Plan Estratégico de Ciberseguridad para Adolescentes en el Área Metropolitana de San Salvador, con el propósito de fortalecer su conciencia y protección en entornos digitales.
Hipótesis General	La implementación de un programa educativo interactivo sobre ciberseguridad aumentará significativamente el nivel de conciencia y conocimiento de los adolescentes sobre la ciberseguridad, disminuyendo así los riesgos asociados a amenazas cibernéticas.

Tabla 4-2.

Tabla de referencia de objetivos específicos

Objetivo Específico	*Matriz de congruencia*	*Matriz de categorización y triangulación*
Evaluar el nivel de conciencia y conocimiento sobre ciberseguridad	Ver Tabla 4.3	Ver Tabla 4.6
Desarrollar un programa educativo interactivo sobre ciberseguridad	Ver Tabla 4.4	Ver Tabla 4.7
Implementar un sistema de seguimiento y evaluación	Ver Tabla 4.5	Ver Tabla 4.8

Tabla 4-3.

Matriz de Congruencia - Evaluación de Conciencia sobre Ciberseguridad

Objetivos Específicos	**Evaluar el nivel de conciencia y conocimiento sobre ciberseguridad.**
Hipótesis Específicas	Los adolescentes en el Área Metropolitana de San Salvador tienen un nivel de conciencia y conocimiento sobre ciberseguridad por debajo del ideal.
Unidades de Análisis	Adolescentes en el Área Metropolitana de San Salvador
Variables	Conciencia y conocimiento sobre ciberseguridad
Operacionalización de Variables	Encuestas y entrevistas estructuradas pre y post intervención
Indicadores	Porcentaje de respuestas correctas; Número de conceptos conocidos
Técnicas a Utilizar	Encuestas estructuradas; Entrevistas estructuradas
Tipos de Instrumentos a Utilizar	Cuestionarios; Guías de entrevista

Tabla 4-4.

Matriz de Congruencia - Desarrollar un Programa Educativo Interactivo sobre Ciberseguridad

Objetivos Específicos	**Desarrollar un programa educativo interactivo sobre ciberseguridad.**
Hipótesis Específicas	La participación en el programa educativo interactivo incrementará el conocimiento y la conciencia sobre ciberseguridad entre los adolescentes.
Unidades de Análisis	Programa educativo interactivo
Variables	Eficacia del programa educativo
Operacionalización de Variables	Creación y evaluación de material educativo; Sesiones piloto
Indicadores	Número de sesiones realizadas; Participación y evaluaciones de satisfacción
Técnicas a Utilizar	Observación directa; Encuestas de satisfacción
Tipos de Instrumentos a Utilizar	Materiales educativos; Formularios de feedback

Tabla 4-5.

Matriz de Congruencia - Implementar un Sistema de Seguimiento y Evaluación del Impacto del Programa Educativo

Objetivos Específicos	**Implementar un sistema de seguimiento y evaluación del impacto del programa educativo.**
Hipótesis Específicas	El seguimiento y evaluación del programa educativo demostrará una mejora en la aplicación de prácticas seguras en entornos digitales.
Unidades de Análisis	Sistema de seguimiento y evaluación
Variables	Impacto del programa educativo en prácticas seguras
Operacionalización de Variables	Recolección y análisis de datos post-programa; Encuestas de seguimiento
Indicadores	Cambios en el conocimiento y comportamiento sobre ciberseguridad
Técnicas a Utilizar	Análisis de datos; Encuestas de seguimiento

Tipos de Instrumentos a Utilizar	Plataformas de análisis de datos; Cuestionarios de seguimiento

4.4.1. Matriz de categorización y triangulación

La matriz de categorización y triangulación es una herramienta esencial en la investigación y el análisis de datos. Se utiliza especialmente al desarrollar e implementar un Plan Estratégico de Ciberseguridad para Adolescentes en el Área Metropolitana de San Salvador.

Este enfoque metodológico permite identificar y clasificar sistemáticamente las dimensiones y variables que influyen en el conocimiento, actitudes y comportamientos de los adolescentes respecto a la ciberseguridad. Además, facilita la comparación y el contraste de información recopilada de diferentes fuentes y métodos, como encuestas y entrevistas.

Tabla 4-6.

Matriz de Categorización y Triangulación - Evaluación de Conciencia sobre Ciberseguridad

Objetivo específico: Evaluar el nivel de conciencia y conocimiento sobre ciberseguridad.	
Conocimiento General	
Subcategoría	Uso de Internet, Fuentes de Conocimiento, Actividades en Línea
Fuente	Encuestas
Técnica	Cuantitativa
Indicadores	Porcentaje de conocimiento correcto
Ítems	¿Con qué frecuencia utilizas internet? ¿Qué actividades realizas principalmente en línea? ¿Has recibido alguna formación específica sobre ciberseguridad? ¿Cómo evaluarías tu conocimiento general sobre ciberseguridad? ¿Cómo adquiriste tu conocimiento sobre ciberseguridad?
Experiencias y Percepciones	
Subcategoría	Formación en Ciberseguridad, Problemas de Seguridad
Fuente	Entrevistas

Técnica	Cualitativa
Indicadores	Incidencia de problemas de seguridad
Ítems	Describe una situación donde te sentiste inseguro(a) en línea y cómo respondiste. ¿Cuáles crees que son los mayores riesgos de seguridad en línea para los adolescentes hoy? ¿Has cambiado tus hábitos en línea debido a preocupaciones de seguridad? Si es así, explica qué te motivó.

Tabla 4-7.

Matriz de Categorización y Triangulación - Desarrollar un Programa Educativo Interactivo sobre Ciberseguridad

Objetivos Específicos: Desarrollar un programa educativo interactivo sobre ciberseguridad.	
Contenido Educativo	
Subcategorías	Formación en Ciberseguridad
Fuente	Encuestas
Técnica	Cuantitativa
Indicadores	Eficacia del contenido educativo
Ítems	¿Qué medidas de seguridad utilizas habitualmente cuando estás en línea? ¿Qué te motivaría a modificar tu uso de las redes sociales? ¿Alguna vez has aceptado a desconocidos en redes sociales o videojuegos y compartida información personal? ¿Con qué frecuencia revisas las configuraciones de privacidad en tus cuentas en línea? ¿Cuántas veces has cambiado tus contraseñas en el último año?
Experiencias y Percepciones	
Subcategorías	Medidas de Seguridad Implementadas
Fuente	Entrevistas
Técnica	Cualitativa
Indicadores	Nivel de participación
Ítems	¿Cuáles crees que son los mayores riesgos de seguridad en línea para los adolescentes hoy? ¿Has cambiado tus hábitos en línea debido a preocupaciones de seguridad? Si es así, explica qué te motivó. ¿Qué método consideras más efectivo para enseñar ciberseguridad a los adolescentes? ¿Reconoces los signos de acoso en línea?

Tabla 4-8.

Matriz de Congruencia y Triangulación - Implementar un Sistema de Seguimiento y Evaluación

Objetivos Específicos: Implementar un sistema de seguimiento y evaluación del impacto del programa educativo.	
Impacto del Programa	
Subcategorías	Aplicación de Prácticas Seguras, Cambios en Hábitos Digitales
Fuente	Encuestas
Técnica	Cuantitativa
Indicadores	Cambios en conocimiento y comportamiento, Adopción de medidas de seguridad
Ítems	¿Cómo te sientes ahora en términos de tu capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético? ¿Con qué frecuencia planeas actualizar tus contraseñas después de lo aprendido en la sesión? Después de la sesión, ¿considerarías importante discutir temas de ciberseguridad con amigos y familiares? ¿Qué prácticas de ciberseguridad te parecen más relevantes para aplicar en tu vida diaria? ¿Cómo calificarías el contenido de la sesión de ciberseguridad?
Experiencias y Percepciones	
Subcategorías	Medidas de Seguridad Implementadas
Fuente	Entrevistas
Técnica	Cualitativa
Indicadores	Mejora en prácticas de seguridad, Reducción de incidentes de seguridad
Ítems	Cuéntame sobre una ocasión en que aplicaste lo aprendido en el programa sobre ciberseguridad. ¿Cómo influyó el programa en tu percepción de los riesgos en línea? ¿Hubo algo en la sesión de ciberseguridad que te haya llevado a reconsiderar cómo interactúas en línea? ¿Cómo describirías la importancia de la ciberseguridad para alguien que no asistió a la sesión?

4.4.2. Instrumentos

a) Encuesta de apertura

Encuesta de Ciberseguridad para Adolescentes

Instrucciones: Responde las siguientes preguntas según tu experiencia y conocimientos. Esta encuesta es confidencial.

1. **¿Con qué frecuencia utilizas internet?**

Varias veces al día

Una vez al día

Varias veces a la semana

Raramente

2. **¿Qué actividades realizas principalmente en línea?** (Selecciona todas las opciones que aplican)

Navegar en redes sociales

Jugar videojuegos en línea

Realizar tareas o estudiar

Comprar o realizar transacciones

Ver contenido en streaming (películas, series, videos)

Otras actividades

3. **¿Has recibido alguna formación específica sobre ciberseguridad?**

Sí (Si tu respuesta fue SI responde la pregunta 4, 5 y 6, antes de continuar la encuesta)

No (Si tu respuesta fue NO responde de la pregunta 7 en adelante)

4. **¿Cómo adquiriste tu conocimiento sobre ciberseguridad?** (Selecciona todas las opciones que aplican)

Escuela o educación formal

Padres o tutores

Amigos o compañeros

Internet y redes sociales

Cursos en línea o tutoriales

5. **¿Has modificado tu comportamiento en línea tras recibir formación sobre ciberseguridad?**

Sí, significativamente

Sí, en algunos aspectos

No, no he hecho cambios

6. **¿Cómo evaluarías tu conocimiento general sobre ciberseguridad?**

Excelente

Bueno

Regular

Pobre

7. **¿Has experimentado alguna forma de acoso en línea, como bullying, hostigamiento o cualquier otro tipo de acoso cibernético?**

Sí

No

8. **¿Qué medidas de seguridad utilizas habitualmente cuando estás en línea?** (Selecciona todas las opciones que aplican)

Contraseñas fuertes y únicas

Autenticación de dos factores

Software de seguridad (antivirus, firewall)

Revisión de configuraciones de privacidad

Cautela al compartir información personal

No uso medidas de seguridad específicas

9. **¿Qué te motivaría a modificar tu uso de las redes sociales?**

Preocupaciones sobre privacidad

Experiencias negativas en línea (acoso, bullying)

Consejos de seguridad en línea

Observar malas experiencias de otros

Nada me motivaría a cambiar

10. **¿Alguna vez has aceptado a desconocidos en redes sociales o videojuegos y compartida información personal?**

Sí

No

11. **¿Con qué frecuencia revisas las configuraciones de privacidad en tus cuentas en línea?**

Regularmente (al menos una vez al mes)

Ocasionalmente (varias veces al año)

Raramente (una vez al año o menos)

Nunca

12. **¿Cuántas veces has cambiado tus contraseñas en el último año?**

Más de 5 veces

Entre 3 y 5 veces

1 o 2 veces

No he cambiado mis contraseñas

Instrucciones de cierre: Gracias por completar esta encuesta. Tu participación nos ayuda a entender mejor cómo apoyar a los adolescentes en mantenerse seguros en línea.

b) Encuesta de Seguimiento

Evaluación de la Sesión de Ciberseguridad para Adolescentes

Instrucciones: Ahora que has completado la sesión de ciberseguridad, por favor, toma un momento para responder las siguientes preguntas. Esta encuesta nos ayudará a entender cómo podemos mejorar futuras sesiones.

1. ¿Cómo te sientes ahora en términos de tu capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético?

Mucho más seguro

Algo más seguro

Igual que antes

Menos seguro

2. ¿Con qué frecuencia planeas actualizar tus contraseñas después de lo aprendido en la sesión?

Después de cada 3 meses

Después de cada 6 meses

Una vez al año

No planeo cambiar mis contraseñas con más frecuencia

3. Después de la sesión, ¿considerarías importante discutir temas de ciberseguridad con amigos y familiares?

Sí, definitivamente

Probablemente sí

No estoy seguro(a)

Probablemente no

No

4. ¿Qué prácticas de ciberseguridad te parecen más relevantes para aplicar en tu vida diaria? (Selecciona todas las opciones que aplican)

Crear y utilizar contraseñas fuertes y únicas

Activar la autenticación de dos factores donde sea posible

Revisar y ajustar regularmente las configuraciones de privacidad en mis cuentas

Ser más cuidadoso(a) al compartir información personal en línea

Utilizar software de seguridad, como antivirus o antimalware

5. ¿Cómo calificarías el contenido de la sesión de ciberseguridad en términos de claridad y comprensión?

Muy claro y fácil de entender

Bastante claro

Algo claro

No muy claro

Confuso

Instrucciones de cierre: Agradecemos sinceramente tu tiempo y tus respuestas. La información que has proporcionado es invaluable para nosotros y nos ayudará a mejorar la eficacia de nuestras sesiones educativas sobre ciberseguridad. ¡Gracias por contribuir a un internet más seguro para todos!

c) Entrevista inicial

Entrevista Inicial sobre Ciberseguridad para Adolescentes

Introducción: Gracias por participar en esta entrevista. Tu perspectiva es muy valiosa para nosotros, ya que buscamos comprender mejor las preocupaciones y experiencias de los adolescentes respecto a la ciberseguridad. Las siguientes preguntas están diseñadas para explorar tus experiencias, percepciones y necesidades en relación con la seguridad en línea. Por favor, siéntete libre de compartir tus pensamientos de manera abierta y honesta.

Preguntas:

- **Describe una situación donde te sentiste inseguro(a) en línea. ¿Cómo respondiste a esa situación?**

- **¿Reconoces los signos de acoso en línea, como la publicación no consentida de fotos, insultos o rumores? ¿Has experimentado o visto esto?**
- **¿Cuáles crees que son los mayores riesgos de seguridad en línea para los adolescentes hoy?**
- **¿Has cambiado tus hábitos en línea debido a preocupaciones de seguridad? Si es así, explica qué te motivó a hacer esos cambios.**
- **¿Hay algún tema específico de ciberseguridad sobre el que te gustaría aprender más? ¿Por qué ese interés?**
- **¿Qué método consideras más efectivo para enseñar ciberseguridad a los adolescentes?**
- **Si pudieras diseñar un programa educativo sobre ciberseguridad, ¿qué elementos incluirías para asegurar que sea interesante y efectivo para adolescentes como tú?**

Cierre: Agradecemos sinceramente tu tiempo y tu disposición para compartir tus experiencias y opiniones. La información que nos has proporcionado es invaluable para el desarrollo de programas educativos más efectivos y pertinentes sobre ciberseguridad para adolescentes. ¡Gracias por contribuir a un entorno en línea más seguro para todos!

d) Entrevista de cierre

Entrevista de Seguimiento sobre Ciberseguridad para Adolescentes

Introducción: Gracias por dedicar tu tiempo a esta entrevista de seguimiento. Tu participación en el programa de ciberseguridad ha sido invaluable, y ahora estamos interesados en escuchar cómo esta experiencia ha impactado tus acciones y percepciones sobre la seguridad en línea. Tus respuestas nos ayudarán a entender el efecto real del programa y a identificar áreas para futuras mejoras. Por favor, comparte tus experiencias y opiniones con total sinceridad.

Preguntas:

- **Cuéntame sobre una ocasión en que aplicaste lo aprendido en el programa sobre ciberseguridad.**
- **¿Cómo influyó el programa en tu percepción de los riesgos en línea?**
- **¿Hubo algo en la sesión de ciberseguridad que te haya llevado a reconsiderar cómo interactúas en línea? Por favor, explica.**
- **¿Cómo describirías la importancia de la ciberseguridad para alguien que no asistió a la sesión?**

Cierre: Agradecemos profundamente tu tiempo y tus aportes en esta entrevista de seguimiento. La información que has compartido es crucial para nosotros, ya que nos permite medir el impacto de nuestro programa y seguir mejorando en nuestro esfuerzo por educar a los adolescentes sobre la seguridad en línea. Tu voz es esencial en este proceso, y te agradecemos por ayudarnos a hacer del internet un lugar más seguro para todos.

5. Desarrollo del Plan Estratégico de Ciberseguridad

5.1. Definición de Adolescencia

Según la Organización Mundial de la Salud, (OMS, s.f.) la adolescencia constituye la fase de transición entre la niñez y la adultez, abarcando desde los 10 hasta los 19 años. Esta etapa se distingue por ser un período clave en el desarrollo humano, donde se establecen las bases fundamentales para una buena salud futura.

Durante la adolescencia, los jóvenes atraviesan un crecimiento acelerado en los ámbitos físico, cognitivo y psicosocial, lo que repercute en su manera de sentir, pensar, tomar decisiones e interactuar con el mundo que los rodea.

Basándonos en el análisis de las etapas de la adolescencia realizado por Brittany Allen, MD, FAAP, y Helen Waterman, DO, (Brittany Allen, s.f.) distinguimos tres fases principales: temprana, media y tardía, cada una definida por evoluciones particulares en el desarrollo físico, emocional y cognitivo.

Adolescencia Temprana (10-13 años): Esta fase se caracteriza por un notable crecimiento físico y el comienzo de la pubertad. Los adolescentes notan cambios significativos en su cuerpo, tales como el desarrollo de vello corporal y características sexuales secundarias. Este periodo despierta curiosidad y, en ocasiones, ansiedad, debido a estos cambios. La reflexión sobre la identidad de género puede ser especialmente desafiante para algunos, incluyendo a jóvenes transgénero. A medida que se incrementa la autoconsciencia, surgen pensamientos extremos, una necesidad elevada de privacidad y un deseo de independencia familiar. (Brittany Allen, s.f.)

Adolescencia Media (14-17 años): En esta etapa continúan los cambios físicos, siendo común un crecimiento acelerado. Aumenta el interés por las relaciones románticas y sexuales, así como la exploración de la identidad sexual. Se genera mayor conflicto con los padres a medida que los adolescentes buscan más autonomía. El aspecto físico y la influencia de los pares alcanzan un pico de importancia. El desarrollo cerebral aún está en proceso, influenciando la toma de decisiones y el control de impulsos, aunque ya se empieza a pensar de manera más abstracta. (Brittany Allen, s.f.)

Adolescencia Tardía (18-21 años): Esta fase marca la culminación del desarrollo físico y mejora en el control de impulsos y evaluación de riesgos y beneficios. Los jóvenes desarrollan una identidad más firme, se proyectan hacia el futuro y sus decisiones se basan en sus aspiraciones e ideales. Las relaciones se vuelven más estables y la separación de la familia se intensifica, aunque frecuentemente se establecen nuevas relaciones "adultas" con los padres. (Brittany Allen, s.f.)

5.2. Sistema educativo según edades

Según la REDEM, Red educativa Mundial (redem, s.f.). el sistema educativo de El Salvador está estructurado en diversos niveles que abarcan desde la etapa inicial de aprendizaje hasta la educación superior, cada uno con el objetivo de fomentar el desarrollo integral de los estudiantes a lo largo de sus diferentes fases vitales.

Educación Inicial (0 a 6 años): Este nivel se centra en el desarrollo integral de los niños en sus primeros años de vida, dividido en dos etapas esenciales: maternal y preescolar. (redem, s.f.)

Educación Básica (7 a 15 años): Con una duración de nueve años, este nivel educativo está estructurado en tres ciclos formativos: de primer grado a tercer grado, de cuarto grado a sexto grado, y de séptimo grado a noveno grado. (redem, s.f.)

Educación Media (16 a 18 años): Este nivel, que dura tres años, se ofrece en dos modalidades: bachillerato general y bachillerato técnico. (redem, s.f.)

Cada uno de estos niveles del sistema educativo salvadoreño está cuidadosamente diseñado para responder a las necesidades formativas de los estudiantes, asegurando su desarrollo integral y preparándolos para los retos futuros, tanto académicos como profesionales.

5.3. Determinación del Tamaño de Muestra para un Estudio en el Departamento de San Salvador, con Estadísticas de Matrícula 2023

En el contexto de la investigación, la selección adecuada de una muestra es fundamental para obtener resultados válidos y generalizables. En el artículo “Técnicas de Muestreo sobre una Población a Estudio”, los autores Tamara Otzen y Carlos Manterola (Otzen, 2017) exploran las diferentes técnicas de muestreo que permiten obtener muestras representativas.

La representatividad de una muestra es esencial para extrapolar los resultados observados en ella hacia la población accesible y, a partir de ahí, a la población objetivo. Una muestra se considera representativa si fue seleccionada al azar y si el número de sujetos seleccionados refleja numéricamente la población original en términos de la variable estudiada. (Otzen, 2017)

Las **técnicas de muestreo** incluyen:

1. **Muestreo Aleatorio**: En este enfoque, los sujetos se seleccionan al azar de la población. Es la técnica más utilizada y permite inferencias precisas.

2. **Muestreo Sistemático**: Se selecciona un elemento de la población cada cierto intervalo (por ejemplo, cada décimo individuo). Es útil cuando no es posible realizar un muestreo completamente aleatorio.

3. **Muestreo Estratificado**: La población se divide en estratos (subgrupos) según características específicas (como edad o género). Luego, se toma una muestra aleatoria de cada estrato.

4. **Muestreo por Conglomerados**: La población se divide en grupos o conglomerados (como escuelas o comunidades). Se seleccionan aleatoriamente algunos conglomerados y luego se toma una muestra de los individuos dentro de esos conglomerados.

Estas técnicas permiten realizar inferencias con un alto grado de certeza, siempre que se puedan reproducir las distribuciones y valores de las diversas variables con márgenes de error calculables. (Otzen, 2017)

5.3.1. Cálculo de muestra para encuesta de apertura

El cálculo adecuado del tamaño de muestra constituye una fase esencial para garantizar que los resultados obtenidos en una investigación reflejen fielmente la realidad de la población estudiada. Ante la ausencia de estadísticas de matrícula para el año 2024, se ha optado por utilizar como base los datos correspondientes al año 2023, los cuales fueron obtenidos del portal del Ministerio de Educación, Ciencia y Tecnología de El Salvador, específicamente de su sección de estadísticas educativas (Educativas, 2023)

Paso 1: Definición de la Población Objetivo

El estudio se centrará en estudiantes matriculados desde 7mo grado hasta 3er año de Bachillerato Técnico en el departamento de San Salvador, exclusivamente en la zona urbana y abarcando tanto el sector público como el privado.

Paso 2: Criterios de Filtrado de Datos

Los datos fueron filtrados para incluir solo aquellos pertinentes a la población objetivo, basándose en los siguientes criterios:

- **Sector:** Público y Privado
- **Zona:** Urbana
- **Departamento:** San Salvador
- **Grados Escolares:** Desde 7mo grado hasta 3er año de Bachillerato Técnico, abarcando niveles de educación básica y media. Esta etapa educativa está dirigida a adolescentes de entre 14 y 19 años de edad

Paso 3: Cálculo del Tamaño de Muestra

El tamaño de muestra se estableció utilizando la fórmula para poblaciones finitas, tomando como punto de partida un universo conocido de estudiantes que cumplen con los criterios establecidos. La fórmula implementada es la siguiente:

$$n = (Z^2 * p * q + x * N) / (E^2 + (Z^2 * N - 1))$$

Donde:

El universo conocido de los estudiantes según el ministerio de educación es:

Tabla 5-1.

Distribución de estudiantes según el ministerio de educación

Grado	Hombre	Mujer	Total
7mo grado	48788	46656	95444
8vo grado	44911	44922	89833
9no grado	40200	41368	81568
1er año de bachillerato general	26778	29421	56199
2do año de bachillerato general	24448	27890	52338
1er año de bachillerato técnico	14320	13267	27587
2do año de bachillerato técnico	10717	10688	21405
3er año de bachillerato técnico	8621	9493	18114

Por lo que:

n representa el tamaño de la muestra, Z el Z-score correspondiente al nivel de confianza del 95% (Z=1.96), p la proporción estimada de la característica de interés (0.5 para maximizar el tamaño de la muestra), E el margen de error del 5% y N el tamaño total de la población (442488). Insertando los valores se obtuvo una muestra de aproximadamente **384 estudiantes,** que ofrece un 95% de nivel de confianza con un margen de error del 5%.

5.3.2. Cálculo de muestro estratificado para encuesta de apertura

El muestreo estratificado es un método de recolección de datos que clasifica la población en grupos uniformes, o estratos, según características clave pertinentes al estudio. La selección aleatoria dentro de estos estratos asegura una muestra comprensiva y representativa de la diversidad poblacional. Esta técnica mejora notablemente la exactitud y la fiabilidad de los resultados del estudio al incluir proporcionalmente a todos los segmentos relevantes de la población.

En la preparación del estudio para el Departamento de San Salvador, basado en las estadísticas de matrícula de 2023, es esencial definir los estratos significativos, que

en este caso corresponden a los niveles educativos, desde 7mo grado hasta 3er año de Bachillerato Técnico, así como el género de los estudiantes.

La distribución de la población estudiantil será la siguiente:

Tabla 5-2.

Distribución de muestra estratificada para encuesta de apertura

Grados Escolares	% de la Población	% por Sexo	Estudiantes Necesarios (n=384)	Estudiantes Necesarios por Sexo
7mo Grado	17.68%	Hombres: 50.59%, Mujeres: 49.41%	68	Hombres: 34, Mujeres: 34
8vo Grado	17.36%	Hombres: 49.60%, Mujeres: 50.40%	67	Hombres: 33, Mujeres: 34
9no Grado	16.85%	Hombres: 49.61%, Mujeres: 50.39%	65	Hombres: 32, Mujeres: 33
1er Año Bachillerato General	14.73%	Hombres: 46.95%, Mujeres: 53.05%	57	Hombres: 27, Mujeres: 30
2do Año Bachillerato General	14.48%	Hombres: 46.17%, Mujeres: 53.83%	56	Hombres: 26, Mujeres: 30
1er Año Bachillerato Técnico	7.87%	Hombres: 54.73%, Mujeres: 45.27%	30	Hombres: 16, Mujeres: 14
2do Año Bachillerato Técnico	5.93%	Hombres: 53.24%, Mujeres: 46.76%	23	Hombres: 12, Mujeres: 11
3er Año Bachillerato Técnico	5.09%	Hombres: 49.79%, Mujeres: 50.21%	20	Hombres: 10, Mujeres: 10

5.3.3. Cálculo de muestra para encuesta de seguimiento

Para evaluar el impacto de la capacitación realizada, se seleccionará una muestra de los 384 estudiantes inicialmente encuestados para llevar a cabo la encuesta final de seguimiento.

Cálculo del Tamaño de Muestra

El tamaño de la muestra se determinó utilizando la fórmula para poblaciones finitas, basada en un universo conocido de estudiantes que cumplen con los criterios establecidos. La fórmula utilizada es la siguiente:

n = (Z^2 * p * q + x * N) / (E^2 + (Z^2 * N - 1))

Donde:

n representa el tamaño de la muestra, Z el Z-score correspondiente al nivel de confianza del 95% (Z=1.96), p la proporción estimada de la característica de interés (0.5 para maximizar el tamaño de la muestra), E el margen de error del 5% y N es el tamaño total de la población (384), Por lo tanto, se necesitará una muestra de aproximadamente 192 estudiantes para la encuesta de seguimiento. Esta muestra permitirá realizar un análisis estadísticamente significativo del impacto de la capacitación en ciberseguridad, asegurando que los resultados sean representativos de la población estudiada.

5.3.4. Cálculo de muestro estratificado para encuesta de seguimiento

La distribución de la población estudiantil será la siguiente:

Tabla 5-3.

Distribución de muestra estratificada para encuesta de seguimiento

Grados Escolares	% de la Población	% por Sexo	Estudiantes Necesarios (n=192)	Estudiantes Necesarios por Sexo
7mo Grado	17.68%	Hombres: 50.59%, Mujeres: 49.41%	34	Hombres: 17, Mujeres: 17
8vo Grado	17.36%	Hombres: 49.60%, Mujeres: 50.40%	33	Hombres: 16, Mujeres: 17
9no Grado	16.85%	Hombres: 49.61%, Mujeres: 50.39%	32	Hombres: 16, Mujeres: 16
1er Año Bachillerato General	14.73%	Hombres: 46.95%, Mujeres: 53.05%	28	Hombres: 13, Mujeres: 15
2do Año Bachillerato General	14.48%	Hombres: 46.17%, Mujeres: 53.83%	28	Hombres: 13, Mujeres: 15
1er Año Bachillerato Técnico	7.87%	Hombres: 54.73%, Mujeres: 45.27%	15	Hombres: 8, Mujeres: 7
2do Año Bachillerato Técnico	5.93%	Hombres: 53.24%, Mujeres: 46.76%	11	Hombres: 6, Mujeres: 5
3er Año Bachillerato Técnico	5.09%	Hombres: 49.79%, Mujeres: 50.21%	10	Hombres: 5, Mujeres: 5

5.3.5. Cálculo de muestro Sistemático para entrevista de apertura

El muestreo sistemático es un tipo de muestreo probabilístico en el que se selecciona aleatoriamente el primer elemento de la muestra y, a partir de ahí, se eligen los elementos posteriores utilizando intervalos fijos o sistemáticos hasta alcanzar el tamaño de la muestra deseado. Este método es eficiente, sencillo y

económico, y asegura que la muestra sea representativa de la población en general. (Question Pro, s.f.)

Ventajas del Muestreo Sistemático

Es fácil de aplicar y no requiere una enumeración completa de la población. Además, garantiza que la muestra cubra toda la población de manera uniforme, evitando sesgos que podrían surgir de un muestreo aleatorio simple.

Procedimiento para Seleccionar la Submuestra para el Focus Group

Para seleccionar una submuestra de la muestra total de 384 estudiantes (ver Tabla 5.1. Distribución de muestra estratificada para encuesta de apertura), se emplea un muestreo sistemático con el objetivo de formar un focus group de 10 estudiantes.

El cálculo del intervalo de muestreo se realiza utilizando la siguiente fórmula: **Intervalo de muestreo = Número total de estudiantes / Tamaño de la submuestra.**

En este caso, con un número total de 384 estudiantes y un tamaño de submuestra de 10, el cálculo es el siguiente: Intervalo de muestreo = 384 / 10 = 38.4

El intervalo se redondea a 38, lo que significa que se seleccionará un estudiante cada 38 estudiantes. Para seleccionar el punto de inicio aleatorio, se escoge un número entre 1 y 38. En este caso, el número aleatorio seleccionado es 5.

A partir del estudiante número 5, se selecciona cada 38° estudiante:

Tabla 5-4.

Distribución de muestra Sistemático para encuesta de apertura

Estudiante	Número de Estudiante	Estudiante	Número de Estudiante
Primer estudiante	5	**Segundo estudiante**	43
Tercer estudiante	81	**Cuarto estudiante**	119
Quinto estudiante	157	**Sexto estudiante**	195
Séptimo estudiante	233	**Octavo estudiante**	271
Noveno estudiante	309	**Décimo estudiante**	347

5.3.6. Cálculo de muestro Sistemático para entrevista de seguimiento

Para seleccionar una submuestra de la muestra total de 192 estudiantes (ver Tabla 5.2. Distribución de muestra estratificada para encuesta de seguimiento), se emplea un muestreo sistemático con el objetivo de formar un focus group de 10 estudiantes.

El cálculo del intervalo de muestreo se realiza utilizando la siguiente fórmula: Intervalo de muestreo = Número total de estudiantes / Tamaño de la submuestra.

En este caso, con un número total de 192 estudiantes y un tamaño de submuestra de 10, el cálculo es el siguiente: Intervalo de muestreo = 192 / 10 = 19.2

El intervalo se redondea a 19, lo que significa que se seleccionará un estudiante cada 19 estudiantes. Para seleccionar el punto de inicio aleatorio, se escoge un número entre 1 y 19. En este caso, el número aleatorio seleccionado es 5.

A partir del estudiante número 5, se selecciona cada 19° estudiante hasta completar la muestra deseada de 10 estudiantes. Esta metodología asegura que todos los estudiantes tengan la misma probabilidad de ser seleccionados, preservando la equidad y la integridad del proceso de muestreo. La implementación de este muestreo sistemático es crucial para la efectividad de la investigación, permitiendo

una evaluación rigurosa y sistemática del impacto de la intervención a lo largo del tiempo, y facilitando la gestión logística del estudio.

Tabla 5-5.

Distribución de muestra Sistemático para encuesta de seguimiento

Estudiante	Número de Estudiante	Estudiante	Número de Estudiante
Primer estudiante	5	**Segundo estudiante**	24
Tercer estudiante	43	**Cuarto estudiante**	62
Quinto estudiante	81	**Sexto estudiante**	100
Séptimo estudiante	119	**Octavo estudiante**	138
Noveno estudiante	157	**Décimo estudiante**	176

6. Resultado de Encuestas y Entrevistas

6.1. Encuestas

Los datos recogidos a través de la encuesta inicial, descrita en la sección 4.4.2 del documento bajo el título "Instrumentos", específicamente en el inciso a) "Encuesta de Apertura" y b) “Encuesta de Seguimiento” que proporcionaron una base sólida para nuestro análisis de ciberseguridad entre adolescentes.

Para llevar a cabo los análisis y visualizaciones de los datos, se utilizó el lenguaje de programación R. La elección de R se fundamenta en varias ventajas clave que lo hacen especialmente adecuado para este tipo de trabajos:

- Capacidades Estadísticas Avanzadas: R es reconocido por sus robustas capacidades estadísticas y su amplia gama de paquetes especializados en análisis

de datos. Esto permite realizar análisis complejos y detallados de los datos recogidos.

- Flexibilidad y Potencia en la Manipulación de Datos: R proporciona herramientas poderosas para la manipulación de datos, lo que facilita la limpieza, transformación y preparación de los datos para el análisis.

- Visualización de Datos: R tiene paquetes como ggplot2 que son excepcionales para la creación de gráficos de alta calidad y visualmente atractivos. Estas visualizaciones ayudan a comunicar los hallazgos de manera clara y efectiva.

- Comunidad Activa y Recursos Abundantes: La comunidad de R es muy activa y hay una abundancia de recursos, como tutoriales, foros y documentación, que facilitan la resolución de problemas y el aprendizaje continuo.

- Reproducibilidad y Transparencia: R facilita la creación de scripts reproducibles, lo que garantiza que los análisis puedan ser replicados y verificados por otros investigadores, aumentando la transparencia del estudio.

En este estudio, se aplicaron diversas técnicas y herramientas del software estadístico R para analizar los datos de encuestas sobre ciberseguridad en adolescentes, proporcionando insights clave acerca de sus prácticas de seguridad en línea, nivel de conocimiento y las incidencias de problemas de seguridad que enfrentan. Los resultados, detallados en las secciones siguientes del documento, destacan tanto los métodos de análisis utilizados como los hallazgos obtenidos. Gracias al uso de R, se logró un análisis profundo y riguroso, acompañado de visualizaciones claras y precisas que facilitan la interpretación y comunicación de los resultados, haciendo los datos más accesibles y comprensibles para los lectores.

6.1.1. Análisis de la Encuesta de Apertura.

La ciberseguridad es un tema crucial para los adolescentes en la era digital. La alta dependencia de internet y la falta de conocimiento adecuado sobre cómo protegerse en línea los hace vulnerables a diversos riesgos. Esta encuesta busca entender el estado actual del conocimiento y las prácticas de ciberseguridad entre los adolescentes y propone acciones para mejorar su protección.

1. Conocimiento sobre Ciberseguridad y Fuentes de Información

Más de la mitad de los adolescentes (62.6%) han recibido formación en ciberseguridad, principalmente a través de la escuela (35.4%). Sin embargo, un preocupante 37.4% aún no tiene conocimientos fundamentales para protegerse en línea. Este dato indica la necesidad de ampliar los programas educativos para cubrir a todos los estudiantes y garantizar que todos tengan acceso a esta información esencial.

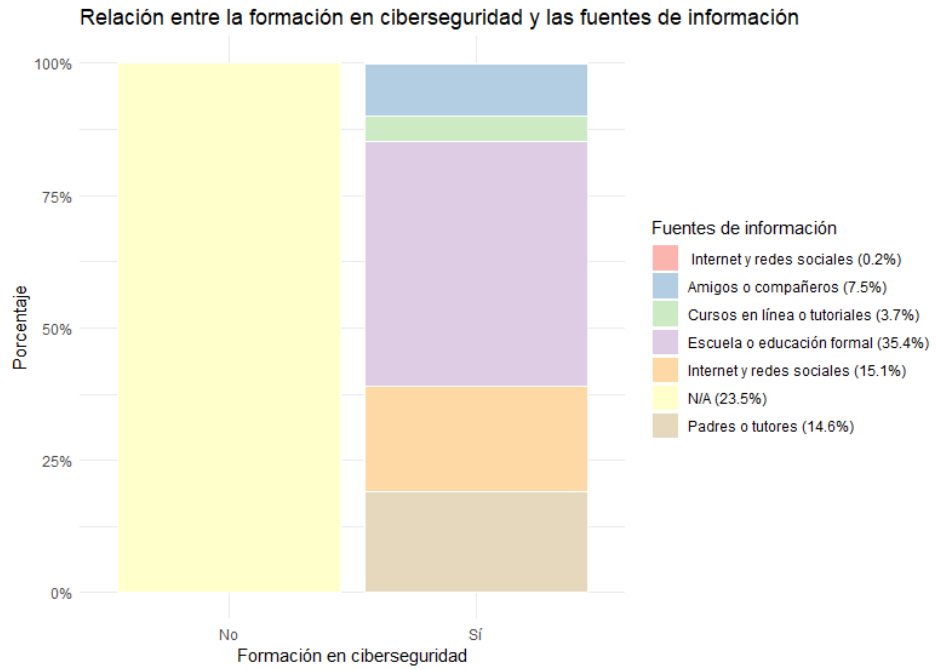


Ilustración 4. Conocimiento sobre Ciberseguridad y Fuentes de Información

2. Relación entre la Frecuencia de Uso de Internet y Experiencia de Acoso en Línea

Una mayor frecuencia de uso de Internet está generalmente asociada con una mayor probabilidad de experimentar acoso en línea entre los adolescentes. Los adolescentes que usan Internet "Varias veces al día" tienen un 28.8% de probabilidad de experimentar acoso en línea, mientras que aquellos que lo usan "Varias veces a la semana" tienen un 32.8%. Por otro lado, los que usan Internet "Una vez al día" tienen una incidencia equilibrada del 50%, y los que lo usan "Raramente" tienen la menor probabilidad, con solo un 20% experimentando acoso. Estos datos subrayan la necesidad de abordar y prevenir el acoso en línea, especialmente entre los adolescentes que pasan más tiempo conectados.

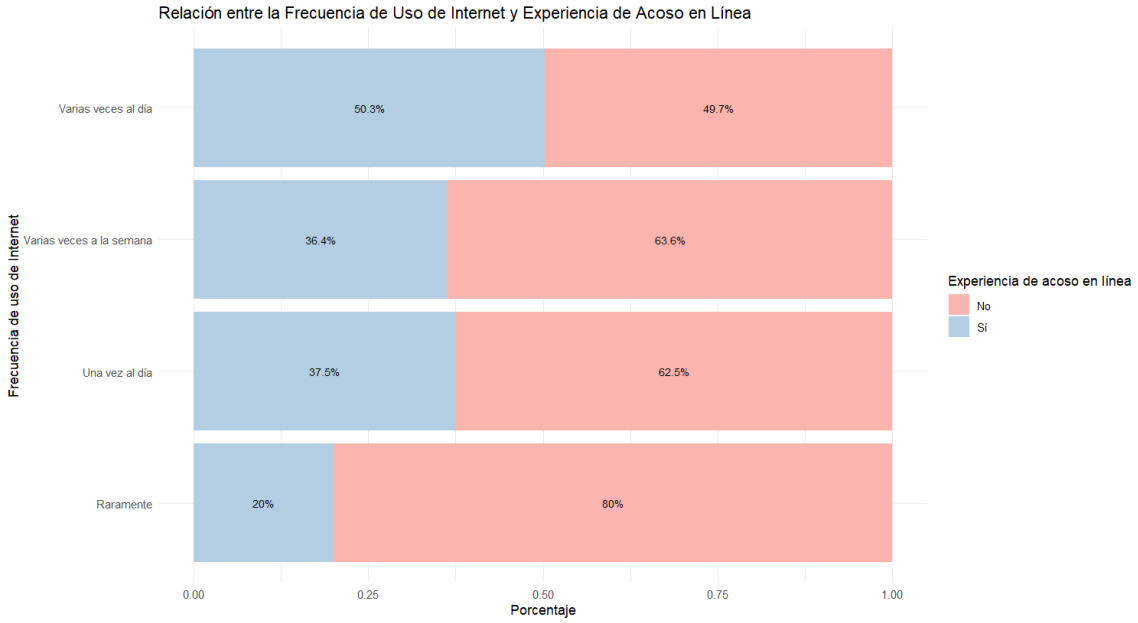


Ilustración 5. Incidencia de Problemas de Seguridad y Frecuencia de Uso de Internet

3. Actividades Principales en Línea y Edad

Los adolescentes usan internet principalmente para estudiar (29.8%) y para redes sociales (28.7%). Las actividades en línea varían con la edad: el uso de redes sociales es común en todas las edades, pero ver contenido en streaming aumenta con la edad.

Las pruebas estadísticas confirman estas diferencias, indicando que los programas educativos deben ser adaptados según las diferentes necesidades y comportamientos de cada grupo de edad.

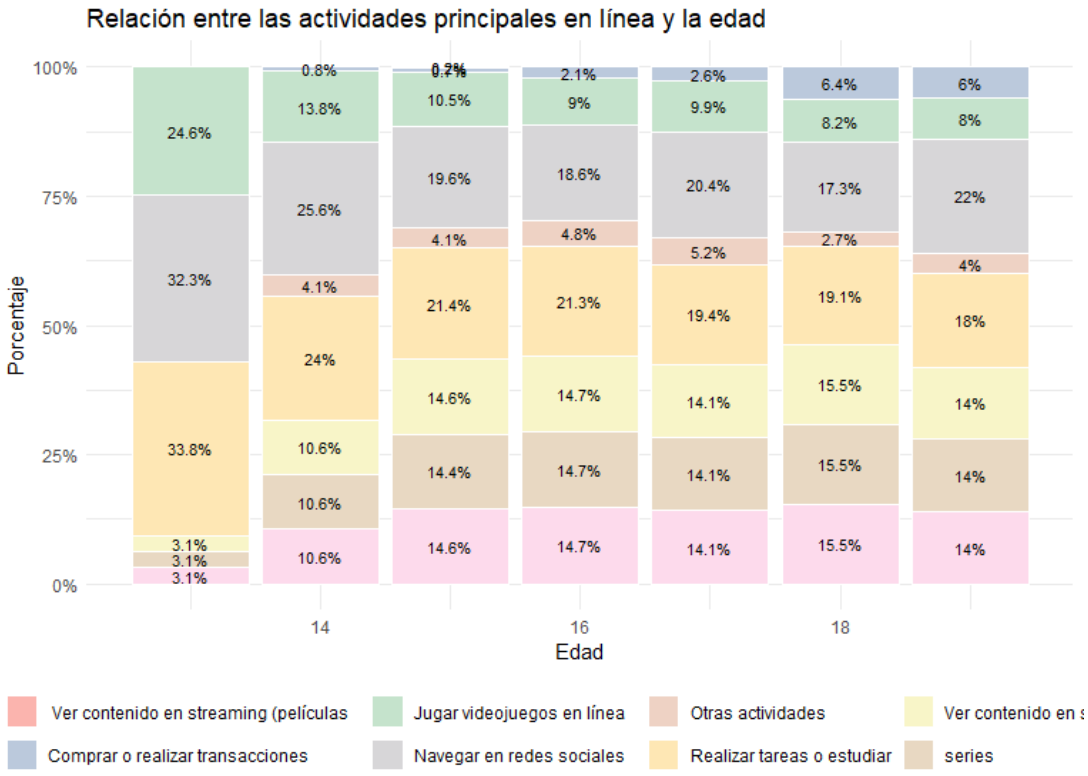


Ilustración 6. Actividades Principales en Línea y Edad

4. Motivaciones para Modificar Uso de Redes Sociales y Formación en Ciberseguridad

Las preocupaciones sobre privacidad son la principal razón (32.7%) por la que los adolescentes cambian cómo usan las redes sociales, seguidas por las experiencias negativas en línea (acoso y bullying) con un 27.4%. Aquellos adolescentes que han recibido formación en ciberseguridad son más propensos a modificar su comportamiento en línea tras observar malas experiencias de otros (20.4%) y seguir consejos de seguridad en línea (20.7%). En contraste, un 10% de los adolescentes sin formación indican que nada los motivaría a cambiar. Esto demuestra la efectividad de la educación en ciberseguridad para cambiar actitudes y comportamientos, subrayando la importancia de estos programas.

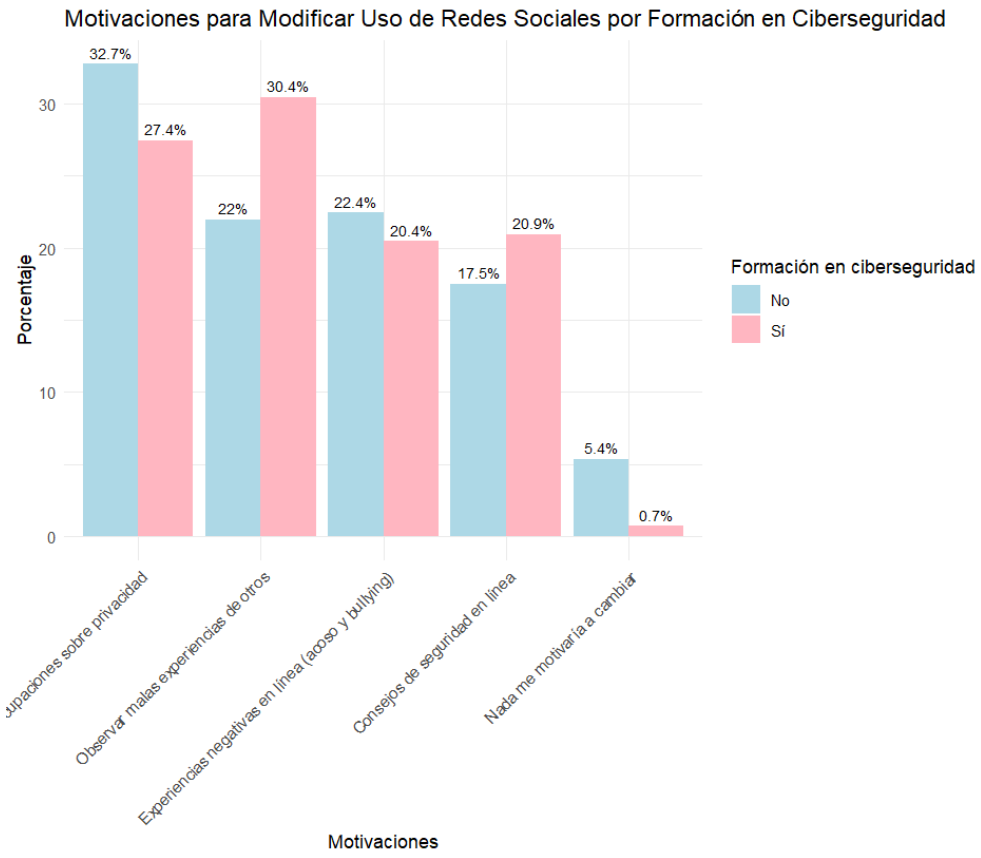


Ilustración 7. Motivaciones para Modificar Uso de Redes Sociales y Formación en Ciberseguridad

5. Frecuencia de Uso de Internet y Género

Tanto el género femenino como masculino usan internet con la misma frecuencia. Las pruebas estadísticas (chi-cuadrado y Fisher) confirman que no hay diferencias significativas entre ellos. Sin embargo, existen variaciones en las medidas de seguridad que adoptan según su género. Por ejemplo, las chicas tienden a usar más configuraciones de privacidad en redes sociales, mientras que los chicos son más propensos a utilizar software de seguridad. Esto sugiere que las estrategias educativas deben ser igualmente accesibles y relevantes para ambos géneros, pero también adaptadas a las diferencias en comportamientos de seguridad.

```
R 4.2.1 · ~/
> # Crear tabla de contingencia (usando backticks porque hay caracteres especiales en los nombres de las columnas)
> contingency_table <- table(data$Sexo, data$`¿Con qué frecuencia utilizas internet?`)
> print(contingency_table)

           Raramente Una vez al día Varias veces a la semana Varias veces al día
  Femenino         3              3                       12                 167
  Masculino        2              5                       10                 167
> # Prueba de chi-cuadrado
> chi_square_test <- chisq.test(contingency_table)
Warning message:
In chisq.test(contingency_table) :
  Chi-squared approximation may be incorrect
> print(chi_square_test)

        Pearson's Chi-squared test

data:  contingency_table
X-squared = 0.87911, df = 3, p-value = 0.8305

>
> # Si la aproximación chi-cuadrado no es adecuada, usar la prueba exacta de Fisher
> if(any(chi_square_test$expected < 5)) {
+     fisher_test <- fisher.test(contingency_table)
+     print(fisher_test)
+ }

        Fisher's Exact Test for Count Data

data:  contingency_table
p-value = 0.8669
alternative hypothesis: two.sided
```

Ilustración 8. Cálculos para frecuencia de Uso de Internet por género

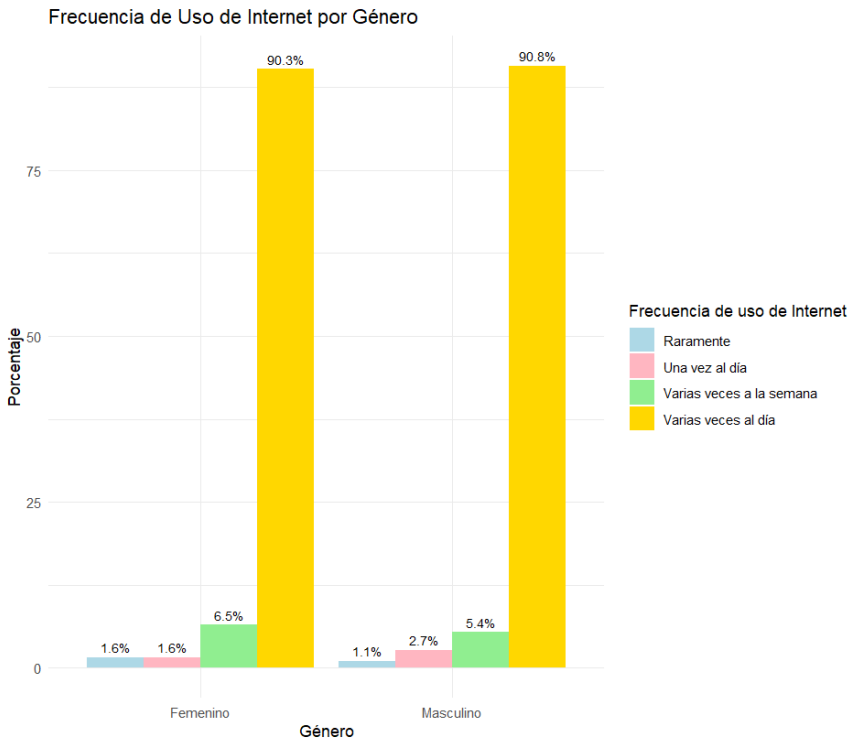
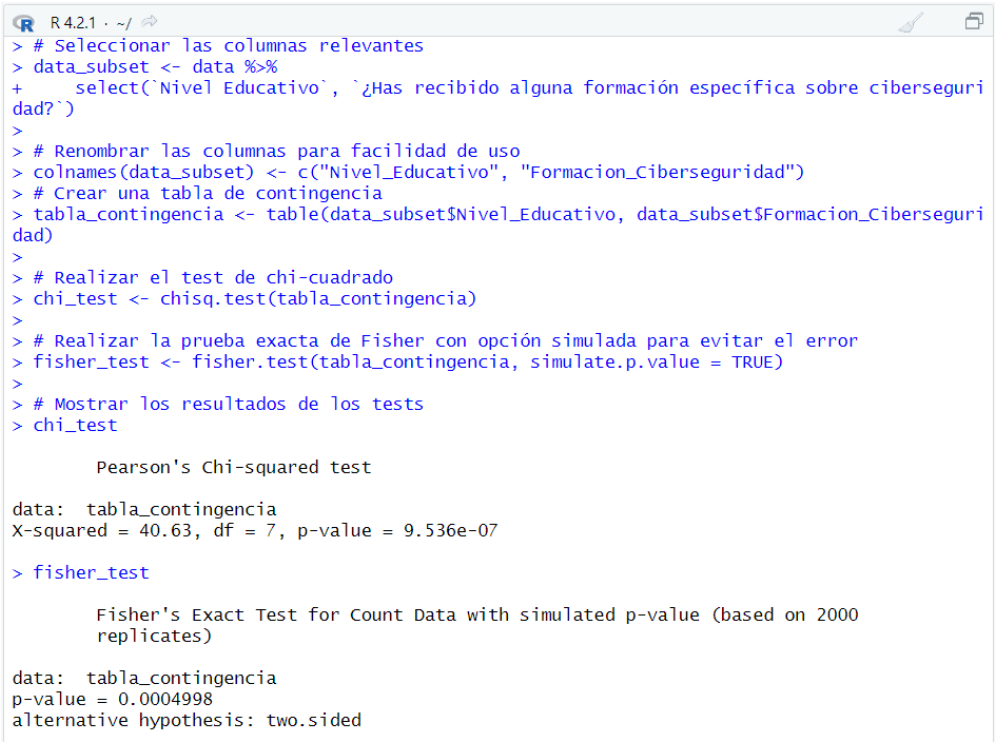


Ilustración 9. Frecuencia de Uso de Internet por género

6. Nivel Educativo y Recepción de Formación en Ciberseguridad

La formación en ciberseguridad varía según el nivel educativo. Los niveles educativos más bajos están mejorando en este aspecto, indicando un esfuerzo por enseñar ciberseguridad desde etapas tempranas. Sin embargo, es crucial seguir ampliando estos programas para asegurar que todos los estudiantes reciban la formación necesaria.



```
R 4.2.1 · ~/
> # Seleccionar las columnas relevantes
> data_subset <- data %>%
+     select(`Nivel Educativo`, `¿Has recibido alguna formación específica sobre ciberseguri
dad?`)
>
> # Renombrar las columnas para facilidad de uso
> colnames(data_subset) <- c("Nivel_Educativo", "Formacion_Ciberseguridad")
> # Crear una tabla de contingencia
> tabla_contingencia <- table(data_subset$Nivel_Educativo, data_subset$Formacion_Ciberseguri
dad)
>
> # Realizar el test de chi-cuadrado
> chi_test <- chisq.test(tabla_contingencia)
>
> # Realizar la prueba exacta de Fisher con opción simulada para evitar el error
> fisher_test <- fisher.test(tabla_contingencia, simulate.p.value = TRUE)
>
> # Mostrar los resultados de los tests
> chi_test

        Pearson's Chi-squared test

data:  tabla_contingencia
X-squared = 40.63, df = 7, p-value = 9.536e-07

> fisher_test

        Fisher's Exact Test for Count Data with simulated p-value (based on 2000
        replicates)

data:  tabla_contingencia
p-value = 0.0004998
alternative hypothesis: two.sided
```

Ilustración 10. Cálculos para Nivel Educativo y Recepción de Formación en Ciberseguridad

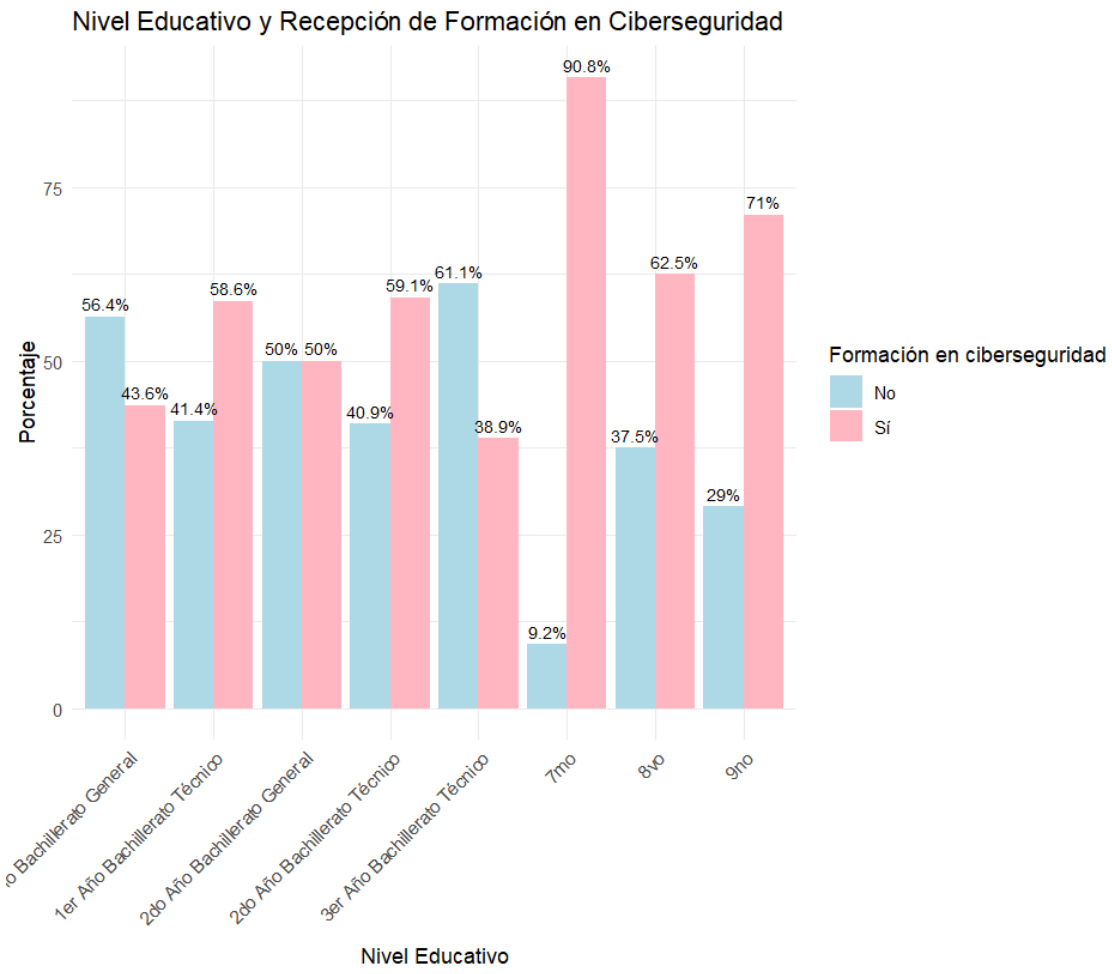


Ilustración 11. Nivel Educativo y Recepción de Formación en Ciberseguridad

7. Relación entre Aceptación de Desconocidos y Experiencia de Acoso en Línea

Un 67.2% de los adolescentes que han aceptado solicitudes de amistad de desconocidos en redes sociales han experimentado acoso en línea, mientras que solo un 32.8% de los adolescentes que han aceptado solicitudes de amistad de desconocidos no han experimentado acoso en línea. Por otro lado, un 71.2% de los adolescentes que no han aceptado solicitudes de amistad de desconocidos no han experimentado acoso en línea, comparado con un 28.8% de los adolescentes que no han aceptado solicitudes de amistad de desconocidos y sí han experimentado acoso en línea.

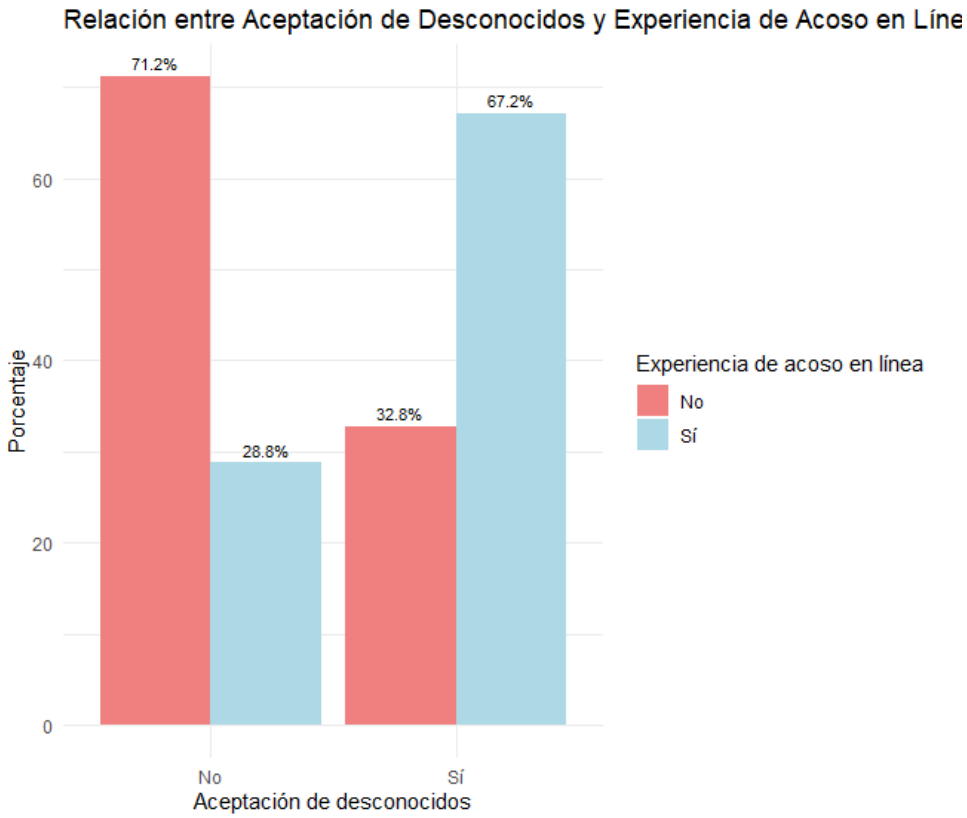


Ilustración 12. Relación entre Aceptación de Desconocidos y Experiencia de Acoso en Línea

8. Relación entre Edad y Aceptación de Desconocidos

Adolescentes de menor edad (14-16 años) tienden a aceptar solicitudes de amistad de desconocidos en mayor porcentaje, posiblemente debido a una menor conciencia sobre los riesgos asociados con aceptar desconocidos en línea o a una mayor influencia de la presión social y la curiosidad. En contraste, adolescentes de mayor edad (17-19 años) muestran una tendencia a ser más selectivos y cautelosos, con un menor porcentaje aceptando solicitudes de desconocidos, reflejando una mayor madurez, experiencia y comprensión de los riesgos de seguridad en línea.

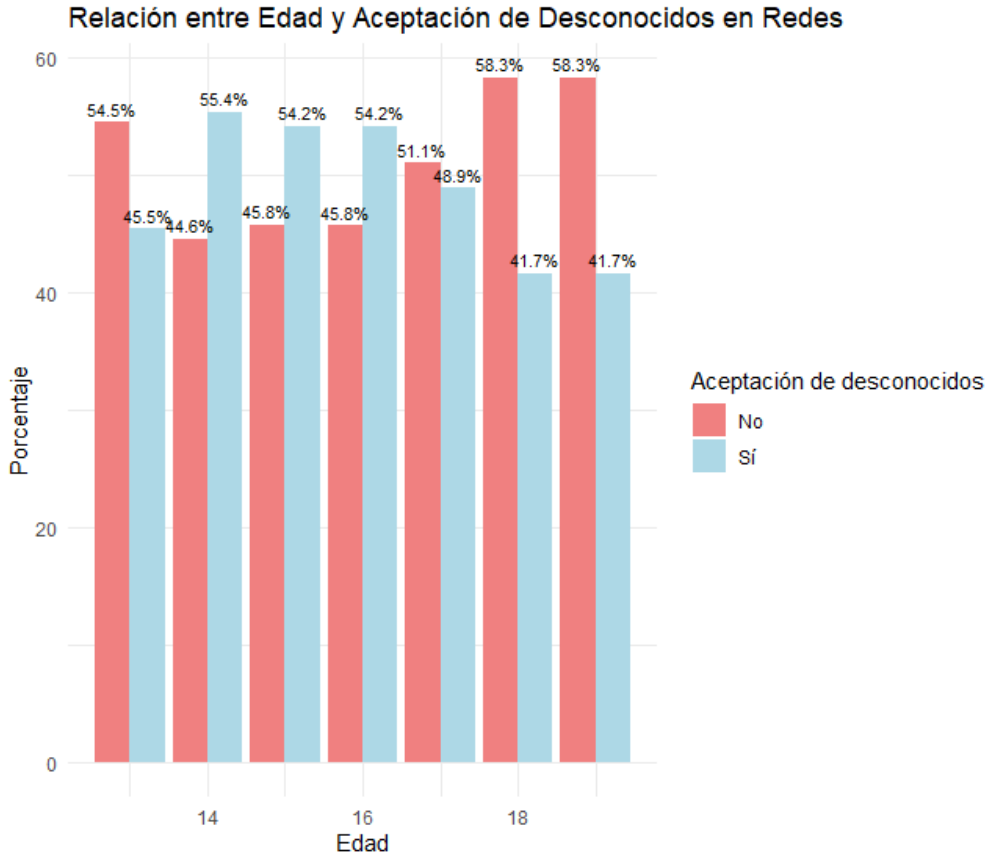


Ilustración 13. Relación entre Edad y Aceptación de Desconocidos

9. Formación en Ciberseguridad y Evaluación de Conocimiento en Ciberseguridad

El análisis muestra que los adolescentes que han recibido formación en ciberseguridad tienden a autoevaluarse con un nivel de conocimiento más alto que aquellos que no han sido capacitados. Entre los que han sido entrenados, el 40% se considera con un nivel 'Bueno', el 35% con un nivel 'Regular' y el 25% con un nivel 'Excelente'. Por otro lado, entre los adolescentes sin formación en ciberseguridad, el 50% se autoevalúa con un nivel 'Regular', el 30% con un nivel 'Bueno' y el 20% con un nivel 'Pobre'. Esto resalta la importancia de la educación en ciberseguridad para mejorar la percepción de los adolescentes sobre sus habilidades y conocimientos en este ámbito.

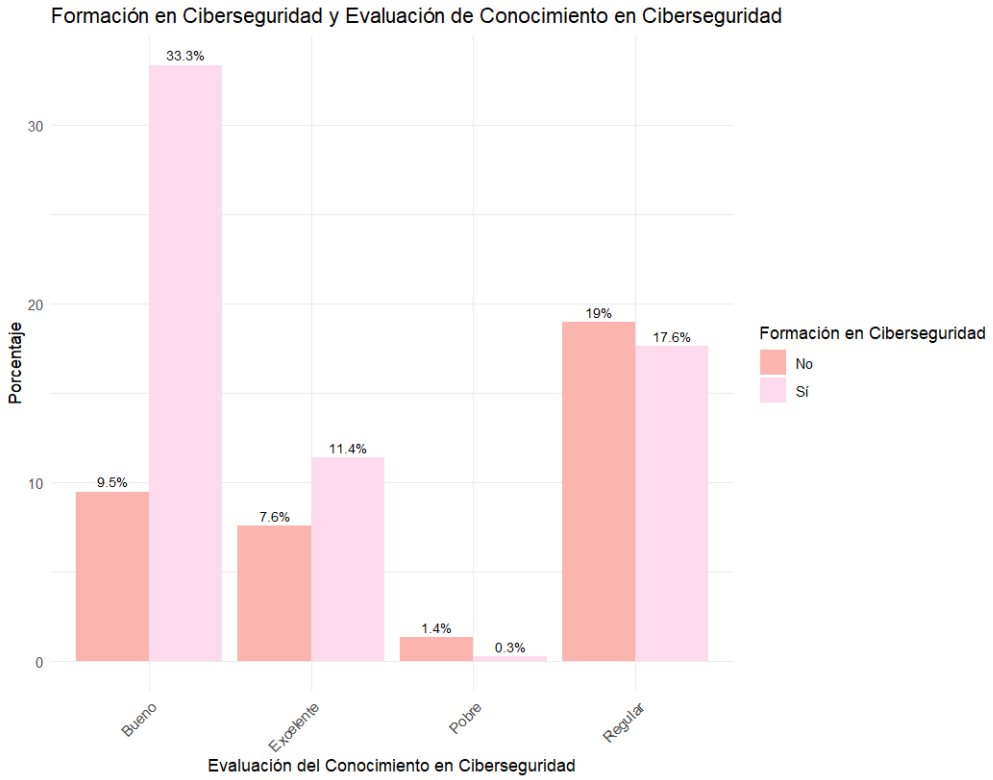


Ilustración 14. Formación en Ciberseguridad y Evaluación de Conocimiento en Ciberseguridad

6.1.2. Análisis de la Encuesta de Seguimiento.

El programa 'Navegando Seguros' ha sido meticulosamente diseñado para dotar a los adolescentes con las herramientas fundamentales necesarias para navegar con seguridad los desafíos del mundo digital. En este esfuerzo, la Encuesta de Seguimiento emerge como un componente crítico, facilitando la evaluación precisa del conocimiento y las prácticas de ciberseguridad de los participantes. El análisis meticuloso de las respuestas permite identificar áreas clave que demandan atención y mejora, y así formular estrategias robustas que incrementen la protección en línea de los jóvenes.

1. Capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético y frecuencia de actualización de contraseñas

El 70% de los participantes que se sienten "Algo más seguro" y el 80% de los que se sienten "Mucho más seguro" planean actualizar sus contraseñas cada 3 meses, mientras que el 30% y el 20% respectivamente optan por una actualización anual. Esto sugiere que una mayor confianza en la capacidad de identificar amenazas de seguridad se asocia con prácticas de seguridad más proactivas.

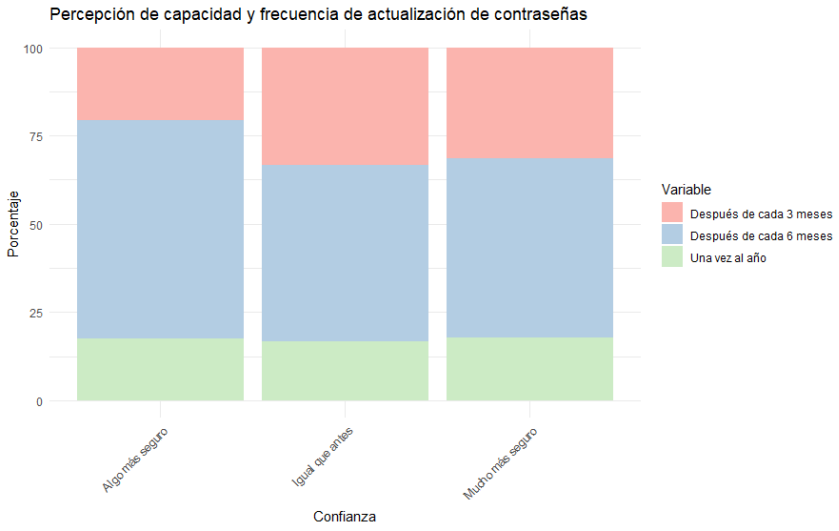


Ilustración 15. Capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético y frecuencia de actualización de contraseñas

2. Capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético y la importancia de discutir temas de ciberseguridad

El 70% de los participantes que se sienten "Mucho más seguros" consideran "definitivamente" importante discutir temas de ciberseguridad, lo que sugiere una mayor concienciación.

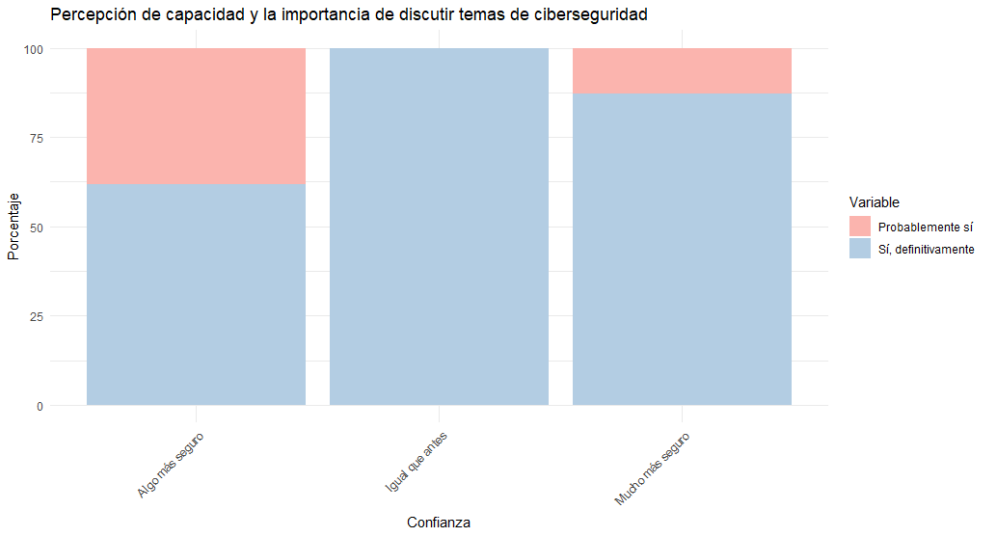


Ilustración 16. Capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético y la importancia de discutir temas de ciberseguridad

3. Capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético y la adopción de prácticas de ciberseguridad

Los participantes "Mucho más seguros" adoptan más prácticas de crear contraseñas fuertes (28.1%) y utilizar software de seguridad (22.3%), mientras que los "Algo más seguros" también revisan las configuraciones de privacidad (19.2%).

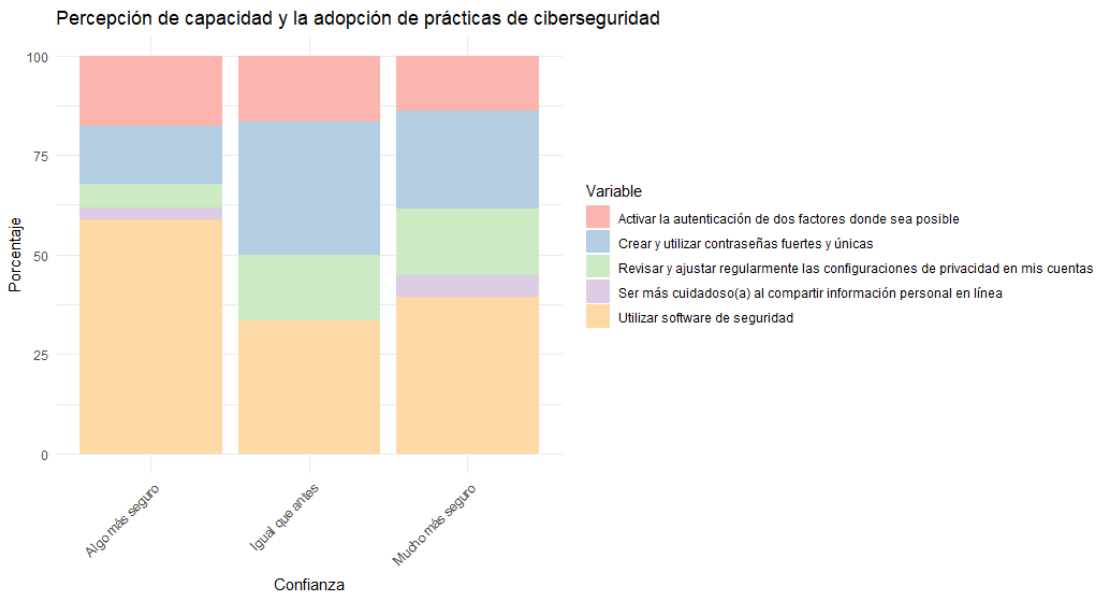


Ilustración 17. Capacidad para identificar intentos de bullying, hostigamiento o cualquier otro tipo de acoso cibernético y la adopción de prácticas de ciberseguridad

4. Claridad de la sesión y la adopción de prácticas de ciberseguridad

Los participantes que encontraron la sesión "Muy clara y fácil de entender" adoptan más la práctica de crear contraseñas fuertes (28.1%) y utilizar software de seguridad (22.3%), sugiriendo que la claridad en la presentación influye positivamente en la adopción de medidas de seguridad.

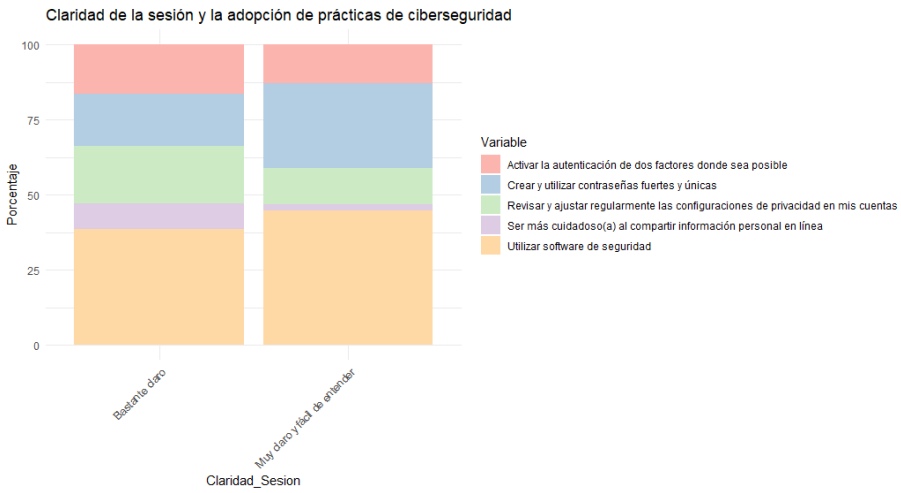


Ilustración 18. Claridad de la sesión y la adopción de prácticas de ciberseguridad

6.2. Entrevistas

6.2.1. Análisis de la Entrevista diagnostico

a) Comentarios

Situaciones de Inseguridad en Línea

1. **Interacciones no solicitadas**: Varios entrevistados expresaron preocupaciones sobre recibir mensajes de desconocidos, incluyendo intentos de hackeo y acoso.

2. **Acceso no autorizado y Estafas**: Algunos enfrentaron intentos de acceso no autorizado a cuentas personales y Estafas con tarjetas de débito.

3. **Exposición de información privada**: Se mencionó la preocupación por la exposición no deseada de información privada, como ubicaciones y datos personales.

Reconocimiento y Experiencia de Acoso en Línea

Varios participantes reconocen los signos de acoso en línea, incluyendo publicaciones no consentidas y mensajes inapropiados. Algunos han experimentado directamente estos incidentes o han sido testigos de ellos en sus círculos sociales.

Principales Riesgos para Adolescentes

1. **Suplantación de identidad y cyberbullying:** Se identificaron como los mayores riesgos, junto con la ingenuidad que es explotada por malintencionados.

2. **Exposición en redes sociales:** El riesgo de compartir demasiado en redes sociales fue un tema común, con ejemplos de cómo la información personal puede ser usada en contra de los adolescentes.

Cambios en Hábitos en Línea

- Muchos entrevistados han modificado sus comportamientos en línea por razones de seguridad, como cambiar contraseñas frecuentemente, limitar la información personal compartida, y ajustar la configuración de privacidad de sus perfiles.

Intereses en Temas Específicos de Ciberseguridad

- Hay un interés notable en aprender más sobre la seguridad de las contraseñas, las cookies, y las implicaciones de la IA en la ciberseguridad.

Métodos Efectivos para Enseñar Ciberseguridad

- Los entrevistados favorecen métodos interactivos y prácticos, como juegos, videos educativos cortos y conferencias. Sugieren que las lecciones sean dinámicas y directamente relevantes a sus experiencias diarias.

-

Diseño de un Programa Educativo sobre Ciberseguridad

- Un programa ideal incluiría casos reales, definiciones claras de conceptos de ciberseguridad, y estrategias prácticas. Los adolescentes valoran los formatos interactivos que incluyan historias, ejemplos visuales y actividades prácticas.

b) Insights Importantes de entrevista

1. **Precaución en la Interacción Social**: Hay una clara necesidad de educar sobre los riesgos de interactuar con desconocidos en línea y cómo gestionar la privacidad.

2. **Conciencia de Seguridad**: Los adolescentes están conscientes de los peligros en línea, pero a menudo necesitan herramientas y conocimientos para manejarlos adecuadamente.

3. **Educación Práctica e Interactiva**: Resalta la importancia de enfoques educativos que sean atractivos y prácticos, que realmente resuenen con los jóvenes.

4. **Impacto de las Experiencias Personales en la Percepción de Riesgo**: Las experiencias personales negativas aumentan la conciencia y la precaución en los jóvenes, indicando que compartir estas historias podría ser efectivo para la educación.

5. **Interés en la Tecnología Emergente**: La curiosidad sobre la IA y sus implicaciones en la ciberseguridad muestra un área potencial para futuras investigaciones y educación.

6.2.2. Análisis de la Entrevista de seguimiento

a) Comentarios

Aplicación de lo Aprendido en Ciberseguridad

1. **Mejora de prácticas de seguridad:** Los entrevistados han aplicado el conocimiento adquirido para mejorar la seguridad de sus correos electrónicos, actualizando contraseñas y configurando mejor sus cuentas y dispositivos personales.

2. **Instalación de medidas de protección:** Varios mencionaron haber instalado programas antivirus y ajustado la configuración de privacidad en redes sociales para limitar quién puede ver su información.

Influencia del Programa en la Percepción de Riesgos

Los participantes reportaron un aumento en su conciencia sobre la importancia de proteger su información personal y ser cuidadosos con lo que comparten en línea.

Cambios en la Interacción en Línea

Algunos entrevistados mencionaron haber reconsiderado y modificado la información que comparten en línea, incluyendo números de teléfono y detalles personales, como resultado directo de lo aprendido en el programa.

Descripción de la Importancia de la Ciberseguridad

Los participantes destacaron la ciberseguridad como esencial para protegerse contra ataques y amenazas en línea. Resaltaron la importancia de ser proactivos en la protección de información personal, especialmente para los adolescentes que pasan mucho tiempo en el mundo digital.

b) Insights Importantes

1. **Conciencia y Educación Continua:** La educación en ciberseguridad influye significativamente en el comportamiento en línea de los adolescentes, haciéndolos más cautelosos y conscientes de los riesgos.

2. **Prácticas de Seguridad Activas:** Hay un claro beneficio en enseñar prácticas de seguridad activas, como la actualización de contraseñas y el uso de software antivirus.

3. **Importancia de la Configuración de Privacidad:** Ajustar la configuración de privacidad para controlar quién ve la información personal es una práctica comúnmente adoptada tras la capacitación.

4. **Impacto en la Percepción del Riesgo:** La formación en ciberseguridad mejora la percepción del riesgo y motiva a los jóvenes a tomar iniciativas de protección personal en línea.

5. **Enseñanza de la Consecuencia de las Acciones en Línea:** Resaltar las posibles consecuencias de acciones inseguras en línea (como compartir información personal) es un método efectivo para enseñar ciberseguridad.

6.3. Análisis por etapa

6.3.1. Conclusión General de la Etapa Diagnóstica:

La etapa diagnóstica ha revelado una intersección crítica entre la alta dependencia de los adolescentes en internet y su nivel de conocimiento y prácticas de ciberseguridad. A pesar de algunos esfuerzos educativos, sigue habiendo un segmento significativo de la población juvenil que es vulnerable a diversos riesgos en línea, lo que subraya la necesidad urgente de estrategias educativas más inclusivas y efectivas.

Insuficiente Cobertura Educativa:

Aunque una mayoría ha recibido alguna forma de educación sobre ciberseguridad, más de un tercio de los adolescentes carecen del conocimiento fundamental necesario para protegerse en línea. Esto indica una brecha crítica en la cobertura y efectividad de los programas de ciberseguridad actuales.

Correlación entre Uso de Internet y Riesgos:

La frecuencia de uso de internet está directamente relacionada con la exposición a riesgos, como el acoso en línea. Los usuarios más frecuentes enfrentan mayores riesgos, lo que requiere un enfoque preventivo en los programas de educación.

Diversidad en las Actividades en Línea según la Edad:

Las diferencias en las actividades en línea basadas en la edad sugieren la necesidad de personalizar los programas de ciberseguridad para abordar los intereses y riesgos específicos asociados con cada grupo de edad.

Motivación y Educación en Ciberseguridad:

Las experiencias negativas y las preocupaciones sobre la privacidad son los principales motivadores para cambiar las prácticas en las redes sociales. La educación en ciberseguridad aumenta la probabilidad de que los adolescentes adopten comportamientos más seguros en línea.

Impacto del Género en las Prácticas de Seguridad:

Aunque no hay diferencias significativas en la frecuencia de uso de internet entre géneros, sí existen variaciones en las prácticas de seguridad adoptadas. Esto destaca la necesidad de abordar estas diferencias en la educación sobre ciberseguridad.

Variación según Nivel Educativo:

La recepción de formación en ciberseguridad varía considerablemente con el nivel educativo, con mejoras notables en los niveles más bajos. Continuar la expansión de estos programas es crucial para garantizar una cobertura completa.

Riesgos Asociados con la Aceptación de Desconocidos:

Aceptar solicitudes de amistad de desconocidos está fuertemente correlacionado con experiencias de acoso en línea. Es esencial educar a los adolescentes sobre los riesgos de interacciones no seguras en las redes sociales.

Diferencias de Edad en la Aceptación de Desconocidos:

Los adolescentes más jóvenes son más susceptibles a aceptar desconocidos en línea, lo que refleja la necesidad de enfocar los esfuerzos educativos en aumentar la conciencia de los riesgos entre este grupo de edad más vulnerable.

Autoevaluación del Conocimiento en Ciberseguridad:

La formación en ciberseguridad tiene un impacto positivo en cómo los adolescentes evalúan su propio conocimiento, con aquellos capacitados calificándose más alto en comparación con los no capacitados.

6.3.2. Conclusión General de la Etapa de Seguimiento

La etapa de seguimiento del programa 'Navegando Seguros' ha demostrado un impacto positivo significativo en las prácticas y percepciones de ciberseguridad de los adolescentes. Los datos obtenidos de las encuestas y entrevistas indican una mejora considerable en la capacidad de los participantes para identificar y gestionar amenazas en línea, así como una adopción más proactiva de medidas de seguridad. La formación recibida ha elevado la conciencia sobre la importancia de proteger la información personal y ha motivado cambios positivos en los comportamientos en línea. Estos resultados subrayan la necesidad de mantener y expandir estos esfuerzos educativos para asegurar que los adolescentes estén bien equipados para navegar de manera segura en el entorno digital.

Mejora en la Capacidad para Identificar Acoso Cibernético y Prácticas de Seguridad:

Los adolescentes que se sienten más seguros en su capacidad para identificar intentos de bullying, hostigamiento o acoso cibernético tienden a adoptar prácticas de seguridad más proactivas, como actualizar sus contraseñas con mayor frecuencia. Esto sugiere que la formación que incrementa la confianza en la identificación de amenazas también motiva comportamientos de seguridad más fuertes.

Importancia de Discutir Temas de Ciberseguridad:

Un alto porcentaje de los participantes que se sienten "Mucho más seguros" consideran definitivamente importante discutir temas de ciberseguridad. Esto indica una mayor concienciación y disposición a compartir y promover prácticas seguras en su entorno.

Adopción de Prácticas de Ciberseguridad:

Los adolescentes que se sienten mucho más seguros son más propensos a adoptar prácticas de seguridad como la creación de contraseñas fuertes y el uso de software de seguridad. Aquellos que se sienten algo más seguros también muestran un compromiso con la revisión de configuraciones de privacidad, lo que sugiere una adopción de múltiples capas de seguridad.

Influencia de la Claridad de la Sesión en la Adopción de Medidas de Seguridad:

La claridad en la presentación de las sesiones de ciberseguridad tiene un impacto positivo en la adopción de medidas de seguridad. Los participantes que encontraron la sesión muy clara y fácil de entender son más propensos a adoptar prácticas de seguridad esenciales, como crear contraseñas fuertes y utilizar software de seguridad.

Aplicación de lo Aprendido en Prácticas de Seguridad:

Los adolescentes han implementado activamente lo aprendido, mejorando la seguridad de sus correos electrónicos y actualizando contraseñas regularmente. También han configurado mejor sus cuentas y dispositivos personales, demostrando la efectividad de la formación recibida.

Instalación de Medidas de Protección:

Muchos participantes han instalado programas antivirus y ajustado la configuración de privacidad en redes sociales, lo que refleja una mayor conciencia sobre la importancia de proteger su información personal en línea.

Aumento en la Conciencia sobre los Riesgos:

Los participantes informaron un aumento en su percepción de los riesgos asociados con compartir información personal en línea. Este cambio en la percepción es un indicador positivo del impacto del programa en la concienciación sobre ciberseguridad.

Cambios en la Interacción en Línea:

Como resultado directo del programa, algunos adolescentes han reconsiderado y modificado la información que comparten en línea, limitando detalles personales como números de teléfono y otros datos sensibles.

Importancia de la Ciberseguridad:

Los adolescentes reconocen la ciberseguridad como esencial para protegerse contra ataques y amenazas en línea. Han destacado la importancia de ser proactivos en la protección de su información personal, especialmente dado el tiempo significativo que pasan en el mundo digital.

7. Conclusiones

7.1. Conclusiones de la Investigación

Hallazgos Iniciales sobre Ciberseguridad y Adolescentes: Desde el inicio de la investigación, se identificó que los adolescentes en el Área Metropolitana de San Salvador enfrentan una variedad de amenazas cibernéticas, incluyendo el ciberacoso, el grooming y el phishing. La revisión de la literatura y los estudios previos subrayaron la necesidad de un enfoque educativo que aumentara la conciencia y el conocimiento de los adolescentes sobre estos riesgos.

Necesidad de un Plan Estratégico: Los estudios realizados en El Salvador revelaron una falta de programas educativos integrales en ciberseguridad dirigidos a adolescentes. Esto destacó la necesidad de desarrollar un Plan Estratégico de Ciberseguridad que abordara específicamente las vulnerabilidades y necesidades de este grupo etario.

Desarrollo del Programa 'Navegando Seguros': A partir de los hallazgos iniciales, se diseñó e implementó el programa 'Navegando Seguros'. Este programa educativo interactivo se enfocó en proporcionar a los adolescentes las herramientas y conocimientos necesarios para navegar de manera segura en el entorno digital.

Impacto del Programa 'Navegando Seguros': La etapa de seguimiento del programa demostró un impacto positivo significativo en las prácticas y percepciones de ciberseguridad de los adolescentes. Los datos obtenidos de las encuestas y entrevistas indicaron una mejora considerable en la capacidad de los participantes para identificar y gestionar amenazas en línea, así como una adopción más proactiva de medidas de seguridad. La formación recibida elevó la conciencia sobre la importancia de proteger la información personal y motivó cambios positivos en los comportamientos en línea.

Mejora en la Capacidad para Identificar y Adoptar Prácticas de Seguridad: Los adolescentes que se sienten más seguros en su capacidad para identificar intentos

de bullying, hostigamiento o acoso cibernético tienden a adoptar prácticas de seguridad más proactivas, como actualizar sus contraseñas con mayor frecuencia. Además, estos adolescentes son más propensos a implementar lo aprendido, mejorando la seguridad de sus correos electrónicos, instalando programas antivirus y ajustando la configuración de privacidad en redes sociales, reflejando una mayor conciencia sobre la importancia de proteger su información personal en línea.

Importancia de Discutir Temas de Ciberseguridad y Claridad en las Sesiones: Un alto porcentaje de los participantes que se sienten "mucho más seguros" consideran definitivamente importante discutir temas de ciberseguridad, indicando una mayor concienciación y disposición a compartir y promover prácticas seguras en su entorno. Además, la claridad en la presentación de las sesiones de ciberseguridad tiene un impacto positivo en la adopción de medidas de seguridad. Los participantes que encontraron la sesión muy clara y fácil de entender son más propensos a adoptar prácticas de seguridad esenciales como crear contraseñas fuertes y utilizar software de seguridad.

7.2. Conclusiones de la Implementación del Programa 'Navegando Seguros'

Efectividad del Programa: La implementación del programa 'Navegando Seguros' ha sido efectiva en aumentar el nivel de conciencia y conocimiento sobre ciberseguridad entre los adolescentes del Área Metropolitana de San Salvador. Los participantes demostraron una mejora significativa en su capacidad para identificar y gestionar amenazas cibernéticas.

Participación Activa de los Adolescentes: Los adolescentes mostraron un alto nivel de participación y compromiso con las actividades del programa. Esto sugiere que el enfoque interactivo y práctico del programa es atractivo y relevante para ellos.

Desarrollo de Habilidades Prácticas: El programa ha logrado desarrollar habilidades prácticas en los adolescentes, como la creación de contraseñas

seguras, la configuración de privacidad en redes sociales y la instalación de software de seguridad. Estas habilidades son cruciales para la protección en línea.

Mejora en la Comunicación sobre Ciberseguridad: Los adolescentes han comenzado a discutir temas de ciberseguridad con sus familias y amigos, promoviendo una cultura de seguridad en su entorno inmediato. Esto indica un cambio positivo en la percepción y comportamiento respecto a la ciberseguridad.

Necesidad de Seguimiento Continuo: Para mantener y mejorar los resultados positivos del programa, es crucial establecer un sistema de seguimiento y evaluación continuo. Esto permitirá ajustar y mejorar las estrategias educativas en función de las necesidades cambiantes de los adolescentes.

8. Recomendaciones

8.1. Recomendaciones Basadas en la Investigación

Expansión y Continuidad del Programa 'Navegando Seguros': Dado el éxito demostrado, se recomienda la expansión del programa 'Navegando Seguros' a más instituciones educativas en el Área Metropolitana de San Salvador. Mantener la continuidad del programa asegurará que más adolescentes reciban la formación necesaria para protegerse en línea.

Fortalecimiento de la Educación en Ciberseguridad: Es esencial que los programas educativos incorporen módulos de ciberseguridad que sean interactivos y relevantes para los adolescentes. La educación debe ser continua, adaptándose a las nuevas amenazas y tecnologías emergentes.

Involucrar a las Familias y la Comunidad: Involucrar a las familias y la comunidad en la educación en ciberseguridad puede fortalecer el entorno de apoyo para los adolescentes. Organizar talleres y sesiones informativas para padres y tutores puede mejorar la comprensión y la importancia de la ciberseguridad en el hogar.

Evaluación y Mejora Continua: Implementar un sistema de seguimiento y evaluación para medir la efectividad de los programas de ciberseguridad. Utilizar los resultados de estas evaluaciones para mejorar y adaptar continuamente los programas a las necesidades de los adolescentes.

Colaboración con Expertos en Ciberseguridad: Colaborar con expertos y organizaciones especializadas en ciberseguridad puede proporcionar recursos adicionales y conocimiento especializado para fortalecer los programas educativos.

8.2. Recomendaciones para la Implementación del Programa 'Navegando Seguros'

Desarrollo de Contenidos Actualizados: Actualizar regularmente los contenidos del programa para incluir las últimas amenazas y mejores prácticas en ciberseguridad. Esto asegurará que los adolescentes estén siempre informados sobre los riesgos más recientes y cómo mitigarlos.

Integración de Nuevas Tecnologías: Incorporar tecnologías emergentes como la realidad virtual y la inteligencia artificial en el programa para crear experiencias de aprendizaje más inmersivas y atractivas.

Feedback y Retroalimentación Continua: Establecer canales de feedback continuo con los participantes para obtener retroalimentación sobre el programa y realizar ajustes según sea necesario para mejorar su efectividad.

Fomento de una Cultura de Seguridad Digital: Promover la importancia de la ciberseguridad no solo entre los adolescentes, sino también entre sus familias y comunidades, mediante campañas de concienciación pública y actividades comunitarias.

Capacitación de Docentes y Facilitadores: Asegurar que los docentes y facilitadores del programa reciban capacitación continua en ciberseguridad para que puedan impartir el contenido de manera efectiva y actualizada.

9. Bibliografía

(BID), B. I. (2020). Obtenido de https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

(MRC), E. M. (2023). Obtenido de https://cdn.icmec.org/wp-content/uploads/2023/05/MRC-El-Salvador-Espanol-2023.pdf

2022, D. O. (s.f.). Obtenido de https://www.diariooficial.gob.sv/seleccion/30760

AlfabetaMedia. (s.f.). Obtenido de https://alfabetamedia.org/wp-content/uploads/2022/09/DOCUMENTO_AMI_21_SEP_2022_ALTA-copy.pdf

Argentino, M. d. (2023). Obtenido de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

Asamblea General de la Republica - Decreto 270. (s.f.). Obtenido de https://biblioteca.asamblea.gob.sv/32009_cdigo-penal-decreto-no-270?q=

Asamblea General de la Republica - Decreto 482. (s.f.). Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/37C67D16-0F45-4C75-8B2B-1A1D3C0C4BE3.pdf

ASSET. (2023). Obtenido de https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/what-is/cybersecurity/

Baray, H. L. (2016). *Introducción a la metodología de la investigación.*

BBC News Mundo. (5 de Enero de 2017). Obtenido de https://www.bbc.com/mundo/noticias-america-latina-38521423

BID . (2020). Obtenido de https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Brittany Allen, M. F. (s.f.). *healthy children*. Obtenido de https://www.healthychildren.org/Spanish/ages-stages/teen/Paginas/Stages-of-Adolescence.aspx

Casillas, L. (2023). *ClearSale Blog*. Obtenido de https://es.clear.sale/blog/perfiles-falsos-en-redes-sociales-e-ingenieria-social-como-protegerse

Children, S. T. (2023). Obtenido de https://www.savethechildren.es/sites/default/files/2023-11/OnlineGrooming_ESP.pdf

Cisterna Cabrera, F. (2005). Categorización y triangulación como procesos de validación del conocimiento en investigación cualitativa.

conversation, t. (2018). Obtenido de https://theconversation.com/lo-que-deben-saber-los-adolescentes-sobre-seguridad-cibernetica-102453

Decreto 520, LEIV. (s.f.). Obtenido de https://oig.cepal.org/sites/default/files/2011_decreto520_elsvd.pdf

Design Thinking España. (s.f.). *Design Thinking España*. Obtenido de https://xn--designthinkingespaa-d4b.com/que-es-un-focus-group-y-como-disenarlo

Diario El Salvador. (2023). Obtenido de https://diarioelsalvador.com/jovenes-salvadorenos-destacaron-en-curso-de-ciberseguridad/445431/

Educativas, E. (2023). *MINED*. Obtenido de https://www.mined.gob.sv/2023/06/12/estadisticas-educativas/

El salvador times. (2018). *El salvador times*. Obtenido de https://www.elsalvadortimes.com/articulo/sucesos/dire/20180419120439040142.html

El tiempo latino. (2018). Obtenido de https://eltiempolatino.com/2018/07/02/noticias-latinoamerica/el-ciberacoso-gana-terreno-en-el-salvador/

elsalvador.com. (2021). Obtenido de https://historico.elsalvador.com/historico/909187/estudio-revela-que-jovenes-salvadorenos-son-vulnerables-en-internet.html

elsalvador.com. (2022). *elsalvador.com*. Obtenido de https://www.elsalvador.com/deportes/futbol/bullying-racismo-piel-cabello-firpo/1005500/2022/

elsalvador.com. (2023). *elsalvador.com*. Obtenido de https://www.elsalvador.com/entretenimiento/espectaculos/instagram-exreinas-belleza-alzan-voz-condenar-bullying-contra-isabella-garcia-manzo/1080478/2023/

elsalvador.com. (19 de Nov de 2023). *elsalvador.com*. Obtenido de https://www.elsalvador.com/noticias/nacional/pornografia-infantil-abuso-sexual-santa-tecla-prision-provisional-la-libertad/1105074/2023/

elsalvador.com. (2023). *elsalvador.com*. Obtenido de https://www.elsalvador.com/noticias/nacional/jugador-videojuegos-audiencia-hurto-san-salvador/1106179/2023/

Fondo de Población de las Naciones Unidas El Salvador. (julio de 2023). *Llegar a cero embarazos en niñas y adolescentes.* Recuperado el 1 de May de 2024, de UNFPA El Salvador: https://elsalvador.unfpa.org/sites/default/files/pub-pdf/mapa_embarazos_2023_web.pdf

Human Rights Watch. (2022). Obtenido de https://www.hrw.org/es/news/2022/02/24/en-el-salvador-leyes-amplias-sobre-delitos-informaticos-amenazan-derechos

Institute, L. (s.f.). Obtenido de https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

IPANDETE. (Junio de 2023). Obtenido de https://www.ipandetec.org/wp-content/uploads/2023/06/Centroamerica-Cibersegura.pdf

IPANDETEC. (s.f.). Obtenido de https://www.ipandetec.org/wp-content/uploads/2023/06/Centroamerica-Cibersegura.pdf

JOAO, O. P. (Octubre-diciembre de 2005). *Brecha digital en el sector educativo salvadoreño.* Revista de Educación y Desarrollo.

Justicia, C. s. (s.f.). Obtenido de https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF

kaspersky. (s.f.). Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-doxing

Kaspersky. (s.f.). Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering.

La prensa grafica . (01 de MARZO de 2018). *laprensagrafica.com.* Obtenido de https://www.laprensagrafica.com/elsalvador/Que-me-paguen-no-me-va-a-regresar-a-mi-hijo-mama-de-Mario-Rivera-el-nino-de-San-Jose-Guayabal-que-fallecio-por-una-broma-20180301-0071.html

La prensa grafica. (20 de MARZO de 2018). *laprensagrafica.com*. Obtenido de https://www.laprensagrafica.com/elsalvador/Caso-de-bullying-a-nino-de-11-anos-termina-en-tragedia-en-La-Paz-20180320-0074.html

Ley Lepina. (s.f.). Obtenido de https://www.elsalvador.law.pro/Leyes/LEPINA.pdf

MINED. (2019). Obtenido de https://www.mined.gob.sv/2019/07/23/comunidad-educativa-del-instituto-de-aguilares-es-capacitada-en-prevencion-de-ciberdelito/

MX, E. (2023). Obtenido de https://expansion.mx/tecnologia/2023/01/18/ninos-son-vulnerables-en-internet-padres-no-saben-cuidarlos#google_vignette

National Center for Missing & Exploited Children. (s.f.). *National Center for Missing & Exploited Children*. Obtenido de https://www.missingkids.org/es/theissues/sextortion

NU. CEPAL-Comisión Europea. (2013-03). *La integración de las tecnologías digitales en las escuelas de América Latina y el Caribe: una mirada multidimensional.* CEPAL.

OMS. (s.f.). Obtenido de https://www.who.int/es/health-topics/adolescent-health#tab=tab_1

Otzen, T. &. (2017). Técnicas de Muestreo sobre una Población a Estudio. . *International Journal of Morphology 35(1),*, 227-232.

Picado, R. L. (17 de Mayo de 2023). Obtenido de https://www.linkedin.com/pulse/la-importancia-de-investigaci%25C3%25B3n-cient%25C3%25ADfica-en-desde-lema%25C3%25AEtre-picado/

Question Pro. (s.f.). *Question Pro*. Obtenido de https://www.questionpro.com/blog/es/muestreo-sistematico/

redem. (s.f.). Obtenido de https://www.redem.org/america-central-y-el-caribe/el-salvador/

Revista la brujula. (2021). *Revista la brujula*. Obtenido de https://revistalabrujula.com/2021/05/25/violencia-sexual-por-medios-digitales-otras-violencias-contra-las-mujeres-que-no-le-importan-al-estado-salvadoreno/

Salvador, D. E. (2021). *ciberacoso escolar un problemalatente*. Obtenido de https://diarioelsalvador.com/ciberacoso-escolar-un-problema-latente/43323/

Sampieri, R. H. (s.f.). *Metodología de la Investigación.* MC GRAW HILL education. Obtenido de https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Schwab, K. (2016). *La cuarta revolución industrial.* Editorial Debate. Obtenido de La Cuarta Revolución Industrial. Futuro Hoy,: http://ojs.ssh.org.pe/index.php/Futuro-Hoy/article/view/1/118

SocialTIC. (s.f.). *Protege.la*. Obtenido de https://protege.la/ataques/

Superintendencia Del Sistema Financiero. (s.f.). Obtenido de https://ssf.gob.sv/estafas/prevencion-2/

SV, D. E. (Mayo de 2022). Obtenido de https://diario.elmundo.sv/politica/el-salvador-aprueba-y-publica-su-politica-de-ciberseguridad

Unesco. (03 de 08 de 2023). Obtenido de https://education-profiles.org/es/america-latina-y-el-caribe/el-salvador/~tecnologia

UNFPA. (Marzo de 2022). *UNFPA*. Obtenido de https://elsalvador.unfpa.org/sites/default/files/pub-pdf/cuadernospoblacion_1_unfpa-sv.pdf

UNFPA. (2023). *UNFPA*. Obtenido de https://elsalvador.unfpa.org/sites/default/files/pub-pdf/mapa_embarazos_2023_web.pdf

Universidad Luterana Salvadoreña. (20 de 04 de 2021). *Universidad Luterana Salvadoreña*. Obtenido de http://curc.uls.edu.sv/pagina.php?id=251

UNODC . (s.f.). Obtenido de https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/EL_SALVADOR_IEG_Cybercrime.pdf

UNODC. (2020). Obtenido de https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/EL_SALVADOR_IEG_Cybercrime.pdf

Vico, A. (2021). Obtenido de https://befullness.com/ingenieria-social/

10. Anexo:

10.1. E-book Navegando Seguros: Conoce los Peligros en Línea y como enfrentarlos

Navegando Seguros: Conoce los Peligros en Línea y como enfrentarlos

Contenido

¿Por qué te debería importar la ciberseguridad?

La vida online es tu día a día: chateas, exploras, juegas y estudias en un mundo virtual lleno de posibilidades. Sin embargo, al igual que en una gran ciudad, existen zonas peligrosas.

Imagina que alguien robara tu contraseña, publicara cosas extrañas en tu Instagram, vaciara tu cuenta bancaria online, o te acosara en línea. Tal vez incluso descubras que alguien ha creado un perfil falso usando tus fotos para engañar a otros.

Suena preocupante, ¿verdad?

La ciberseguridad es como el escudo que te protege de estos riesgos, y aquí te vamos a enseñar cómo fortalecerlo.

Estadísticas que te abrirán los ojos:

En El Salvador y en otras partes del mundo, jóvenes como tú están expuestos a riesgos significativos en línea. Desde el engaño por parte de adultos malintencionados hasta el fraude; los peligros son reales y cercanos. Es esencial estar alerta y conocer las maneras de protegerte en este entorno digital.

Aquí te compartimos algunas estadísticas y hallazgos de informes recientes que muestran la magnitud del problema:

Informe de actividades de Prevención de Ciberdelitos, Ministerio de Educación, Ciencia y Tecnología, El Salvador.

¿Sabías que el teatro puede ser una herramienta poderosa contra el cibercrimen? En El Salvador, más de 15,000 estudiantes y 3,416 docentes han participado en obras como "Las Caras del Cibercrimen", aprendiendo sobre los peligros en línea de una manera creativa y memorable. Esta iniciativa ha llegado a decenas de escuelas, utilizando el arte para abrir los ojos de los jóvenes sobre cómo protegerse en el vasto mundo digital. (UNODC , s.f.)

Centroamérica Cibersegura, IPANDETEC, 2020

Este informe es como una radiografía de la ciberseguridad en Centroamérica, mostrando lo que cada país está haciendo para combatir los ciberdelitos. En El Salvador, aunque faltan algunas leyes clave, hay esfuerzos para mejorar, desde equipos especiales hasta participación en foros globales. Este estudio nos enseña que estar informados y preparados es crucial para proteger nuestra vida digital. (IPANDETE, 2023)

Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe

¿Cómo está avanzando El Salvador en el mundo de la ciberseguridad? Este informe detallado del BID y la OEA muestra tanto los logros como los desafíos desde 2016. Aunque hay avances, como la creación de equipos de respuesta a incidentes, aún hay mucho trabajo por hacer en legislación y educación, lo que nos afecta a todos, especialmente en nuestra forma de interactuar en línea. (BID , 2020)

Llegar a cero embarazos en niñas y adolescentes, Mapa El Salvador 2023

El informe de UNFPA El Salvador analiza los avances en la reducción del embarazo adolescente desde 2015. Aunque ha habido progreso, especialmente en la disminución de registros prenatales de niñas de 10 a 14 años, queda mucho por hacer. Es crucial acelerar esfuerzos en áreas con altas tasas de embarazo y adaptar estrategias a condiciones urbanas y rurales. Las recomendaciones incluyen asegurar la educación universal, el acceso a servicios de salud reproductiva, erradicar las uniones tempranas y combatir la violencia sexual. El estudio resalta la necesidad de una respuesta integral para enfrentar este problema que afecta a las jóvenes y al desarrollo de la sociedad. (Fondo de Población de las Naciones Unidas El Salvador, 2023).

Estas cifras nos muestran que los riesgos en línea son abundantes y muy reales.

¿Qué vemos en las noticias?

Cuando miras las noticias, ya sea en redes sociales o televisión, verás patrones preocupantes en nuestra sociedad:

★ Vulnerabilidad de los menores: Jóvenes como tú sufren explotación sexual, bullying y abuso físico, mostrando cuán vulnerables son tanto en la escuela como online.

★ Impacto del acoso y la discriminación: Estas prácticas causan daños emocionales y físicos significativos, y pueden conducir a tragedias evitables.

★ Cultura del silencio y el estigma: Muchos no hablan de su abuso por miedo o vergüenza, especialmente cuando ocurre en internet.

★ Uso de tecnología en la perpetración de abusos: La tecnología puede facilitar abusos, amplificar daños y crear redes para la explotación.

Estos temas son pesados, pero super importantes. Saber sobre ellos es el primer paso para protegerte a ti y a tus amigos, y para ayudar a hacer que nuestro mundo digital (y real) sea un lugar más seguro para todos.

¿Qué Riesgos Hay en Internet?

Ataques digitales mediante conductas humanas.

Ciberacoso: ¡Defiéndete en la Red!

El ciberacoso incluye comportamientos en línea que buscan intimidar, excluir, o dañar psicológica o emocionalmente a otros. Puede manifestarse de diversas maneras:

- ✓ Insultos o amenazas enviadas por texto, correo electrónico o redes sociales.
- ✓ La difusión de información falsa o humillante en redes sociales.
- ✓ Crear perfiles falsos en nombre de otra persona.
- ✓ Excluir intencionadamente a alguien de grupos en línea.
- ✓ Distribución de imágenes o videos sin consentimiento
- ✓ Presionar para obtener declaraciones o acciones que luego se utilizan de forma perjudicial.

Consecuencias legales de cometer ciberacoso

En El Salvador, el ciberacoso es tratado con seriedad por la ley, y existen varias legislaciones que protegen a las víctimas y penalizan a los agresores:

- ✓ Código Penal: Incluye delitos como violación de la intimidad personal y familiar, y amenazas, que se aplican al ciberacoso.
- ✓ Ley Especial Integral para una Vida Libre de Violencia contra las Mujeres (LEIV): Protege a las mujeres contra la violencia mediática y simbólica, que puede incluir formas de ciberacoso.
- ✓ Ley de Protección Integral de la Niñez y Adolescencia (LEPINA): Protege a niños y adolescentes de la violencia y el abuso, incluyendo el ciberacoso.
- ✓ Las sanciones pueden variar desde multas hasta penas de prisión, dependiendo de la severidad del caso.

¿Cómo protegerte del ciberacoso?

- ✓ Configura la privacidad: Ajusta la configuración de privacidad en tus cuentas.
- ✓ Sé selectivo con tus contactos: Solo conecta con personas que conoces y confías.
- ✓ No respondas a provocaciones: A menudo, ignorar a los acosadores los desmotiva.
- ✓ Guarda evidencia: Conserva capturas de pantalla y registros de todos los incidentes.
- ✓ Bloquea y denuncia: Utiliza las herramientas de bloqueo y denuncia de las plataformas.
- ✓ Busca apoyo: Habla con amigos, familiares o profesionales si el acoso te afecta emocionalmente.

¿Qué hacer si eres testigo o víctima de ciberacoso?

Si te encuentras en una situación de ciberacoso, ya sea como testigo o víctima, es crucial que tomes medidas activas para manejar la situación de manera efectiva. Primero, asegúrate de no participar ni perpetuar el acoso de ninguna manera.

Es fundamental que documentes cualquier comportamiento abusivo, guardando copias de mensajes, comentarios o cualquier otra forma de acoso. Denuncia este comportamiento ante las plataformas correspondientes y, si la gravedad del caso lo requiere, ante las autoridades.

Además, busca apoyo para manejar el impacto emocional y legal del acoso. Esto puede incluir hablar con amigos de confianza, familiares o profesionales de la salud mental, y considerar asesoría legal si fuera necesario. Tomar estas acciones no solo te ayudará a ti, sino que también puede prevenir que otros sufran situaciones similares.

Recuerda, estar informado no solo te permite protegerte, sino también evitar involucrarte en acciones que podrían tener graves consecuencias legales. Denuncia y actúa, no solo por ti, sino por el bienestar de todos en línea.

Sexting: ¡Cuidado con lo que Envías!

El sexting implica enviar, recibir o compartir fotos y mensajes de contenido sexual, tanto con consentimiento como sin él. Esta práctica puede ser vista como una forma de explorar la identidad sexual o establecer una conexión íntima.

Sin embargo, es fundamental ser consciente de los riesgos significativos involucrados, especialmente porque los mensajes o fotos que se consideran privados y temporales pueden ser guardados y utilizados sin tu permiso. Una vez que algo se comparte en línea, puede ser casi imposible eliminarlo por completo.

Consecuencias legales del sexting

Participar en el sexting, especialmente con menores, puede tener serias consecuencias legales. Puede resultar en acusaciones de producción, posesión o distribución de pornografía infantil, y la extorsión sexual ("sextorsión"), donde se amenaza con divulgar imágenes para obtener dinero o más imágenes. Además, la difusión de material sexual sin consentimiento es penalizada bajo la ley en muchos países, incluyendo acciones que puedan considerarse como acoso o amenazas en línea.

En El Salvador, específicamente, estas acciones están reguladas por el Código Penal y otras leyes como la Ley Especial Integral para una Vida Libre de Violencia para las Mujeres (LEIV) y la Ley de Protección Integral de la Niñez y Adolescencia (LEPINA), que sancionan la distribución de imágenes sin consentimiento, el acoso sexual y la violación de la intimidad. Las sanciones pueden incluir multas severas y penas de prisión, dependiendo de la gravedad del delito.

¿Cómo protegerte del sexting?

- ✓ Infórmate y educa: Conoce tus derechos y las leyes aplicables sobre el intercambio de contenido sexual.

- ✓ Habla sobre el tema: Discute con amigos y familiares sobre los peligros del sexting y cómo enfrentar situaciones relacionadas.

- ✓ Fortalece tu red de apoyo: Asegúrate de tener contactos de confianza a quienes recurrir en caso de necesitar ayuda o consejo.

- ✓ Considera las consecuencias antes de compartir: Evalúa cómo podría afectarte a largo plazo el compartir contenido íntimo, especialmente en Internet.

- ✓ Denuncia cualquier abuso: Si recibes o te ves involucrado en situaciones de sexting no consentido, no dudes en denunciarlo a las autoridades competentes.

¿Qué hacer si eres testigo o víctima de sexting?

En situaciones de sexting, ya sea como testigo o víctima, es crucial actuar con prudencia y estar consciente de las consecuencias. Reflexiona sobre las implicaciones a largo plazo antes de compartir contenido sexual y establece claramente tus límites personales, asegurándote de que se respeten. Usa tecnología de forma segura, ajustando la privacidad y eligiendo aplicaciones con protecciones como mensajes que se autodestruyen para evitar la distribución no autorizada. No reenvíes imágenes sin consentimiento, pues es ilegal e irrespetuoso.

Si enfrentas presiones o comportamientos inapropiados, bloquea a los agresores y reporta la situación a las autoridades o administradores de la plataforma. Estas medidas son esenciales para manejar la situación de manera responsable y segura.

Considera cuidadosamente las implicaciones de participar en el sexting. Aunque puede parecer una actividad privada, los riesgos y las consecuencias potenciales pueden impactar profundamente tu vida y bienestar. Es más prudente errar del lado de la precaución y priorizar tu seguridad y privacidad. Proteger tu información personal es crucial en un mundo digital donde el contenido compartido puede ser imposible de recuperar o eliminar completamente.

Grooming: No Todos los Amigos en Línea Son Reales

El grooming es cuando un adulto se conecta emocionalmente con un menor en internet para ganar su confianza con fines inapropiados o abusivos. Usan plataformas como redes sociales y videojuegos.

Cómo se presenta:

- ✓ Mensajes amistosos en redes sociales
- ✓ Ofrecen códigos para juegos, suscripciones o regalos virtuales como señal de "amistad".
- ✓ Te invitan a conversaciones privadas fuera de plataformas públicas.
- ✓ Tras ganarse tu confianza, piden fotos o información comprometedora.

Consecuencias legales del grooming

En El Salvador, el grooming está reconocido como un delito grave que viola las leyes de protección a menores. El Código Penal y la Ley de Protección Integral de la Niñez y Adolescencia (LEPINA) proporcionan un marco legal para sancionar severamente a quienes manipulen a menores con fines de explotación sexual o emocional. Las sanciones pueden incluir multas y penas de prisión, dependiendo de la gravedad del delito.

¿Cómo protegerte del Grooming?

- ✓ Conoce las señales de alerta: Presta atención a comportamientos como regalos inesperados, atención excesiva, o intentos de aislar a un niño de amigos y familiares.
- ✓ Mantén la privacidad en línea: No compartas información personal (dirección, números de teléfono, imágenes íntimas) con desconocidos y ajusta las configuraciones de privacidad de tus redes sociales.
- ✓ Comunica límites claros: Establece y comunica firmemente tus límites personales. No temas decir "no" si alguien te hace sentir incómodo.
- ✓ Habla sobre tus interacciones en línea: Comparte regularmente con un adulto de confianza detalles sobre tus interacciones en línea y las personas con las que te comunicas.
- ✓ Utiliza la tecnología de forma segura: Elige aplicaciones y plataformas con políticas de seguridad y privacidad robustas y asegúrate de entender cómo reportar comportamientos inapropiados.
- ✓ Reporta comportamientos sospechosos: Si sospechas que tú o alguien que conoces está siendo víctima de grooming, reporta la situación a las autoridades competentes o a los administradores de la plataforma.

¿Qué hacer si eres testigo o víctima de grooming?

Si eres testigo o víctima de grooming, es crucial adoptar medidas de precaución y alerta. Desconfía de los desconocidos en línea y mantén una actitud crítica hacia cualquier persona nueva que conozcas en internet. Es importante mantener privada tu información personal, evitando compartir detalles como tu ubicación o fotos con alguien que no conoces en persona.

Además, es vital hablar sobre tus interacciones en línea con tus padres, tutores o un maestro, especialmente si estas involucran a nuevas personas. Familiarízate con las señales de alerta del grooming: solicitudes para que guardes secretos, comportamientos que te hagan sentir incómodo, o peticiones de fotos o información personal son indicativos de que algo no está bien. Reconocer y responder a estas señales es fundamental para protegerte en el entorno digital.

Es crucial construir amistades y relaciones en un entorno seguro y saludable. Verifica siempre quién está al otro lado de la pantalla y nunca sientas que debes hacer algo incómodo o inseguro para mantener una amistad en línea. ¡Protege tu bienestar y asegura que tus interacciones en línea sean seguras! Reconocer los signos de grooming tempranamente y actuar de manera preventiva es esencial para evitar situaciones de abuso.

Concursos Falsos: No Todo lo que Brilla es Oro

¿Te han informado alguna vez que ganaste un premio en un concurso al que nunca te inscribiste? Aunque suene tentador, ten cuidado. Esto podría ser una estrategia para obtener tu información personal o dinero. Imagina recibir un mensaje, correo electrónico o llamada anunciando: "¡Felicidades! Has ganado un iPhone nuevo" o "Eres el afortunado ganador de un viaje todo incluido".

Pero hay una trampa: para reclamar tu premio, solicitan tus datos personales o el pago de una "pequeña" tarifa de administración.

Consecuencias legales de los concursos falsos

En El Salvador, los concursos falsos pueden ser considerados como estafas bajo las leyes de protección al consumidor. Estas prácticas engañosas están tipificadas y pueden llevar a sanciones severas, incluyendo multas y penas de cárcel para quienes las perpetren. La legislación salvadoreña protege a los consumidores de prácticas fraudulentas y busca asegurar transacciones honestas y transparentes.

¿Cómo protegerte de los concursos falsos?

- ✓ Verifica la legitimidad: Investiga el sitio web oficial del organizador y busca referencias confiables. Desconfía de concursos sin reglas claras o marcas reconocidas.

- ✓ Protege tu información: No participes en concursos que pidan datos personales sensibles como identificación, información bancaria o contraseñas.

- ✓ Cuidado con las tarifas: Si te piden pagar para reclamar un premio, es probablemente una estafa.

- ✓ Evita enlaces sospechosos: No hagas clic en enlaces de correos o mensajes de redes sociales sobre concursos, a menos que estés seguro de su origen.

- ✓ Concursos no solicitados: Si te dicen que ganaste en un concurso en el que no participaste, es un engaño.

- ✓ Consulta a un adulto: Si tienes dudas sobre la legitimidad de un concurso, habla con un adulto de confianza.

- ✓ Configura tus redes: Limita quién puede ver y compartir tu información para reducir el riesgo de ser blanco de estafadores.

¿Qué hacer si eres testigo o víctima de concursos falsos?

Si sospechas que has sido víctima de un concurso falso, es importante que no proporcionen ninguna información personal ni realices ningún pago. Reporta el incidente a las autoridades locales y alerta a tus conocidos sobre el engaño para prevenir que otros caigan en la misma trampa.

La próxima vez que te digan que has ganado algo inesperadamente, tómate un momento para evaluar la situación. Verifica la fuente y recuerda: si suena demasiado bueno para ser verdad, probablemente no lo sea.

¡Mantente alerta y protege tu información!

Farming: La Confianza que Cuesta Caro

¿Alguna vez has notado que alguien intenta ganarse tu confianza gradualmente a través de mensajes frecuentes o interacciones en línea? Esto podría ser un caso de "farming", una estrategia donde alguien se presenta como un nuevo mejor amigo con el objetivo de acceder a tu información personal. Imagina que conoces a alguien en línea que parece compartir tus intereses; empiezan a chatear regularmente, haciéndote sentir especial y comprendido. Sin embargo, su verdadero propósito es desarrollar suficiente confianza para que, cuando te pidan información personal o acceso a tus cuentas, no dudes en dársela.

Consecuencias legales del farming

El farming puede ser considerado una forma de fraude o engaño bajo las leyes de El Salvador, especialmente cuando conlleva la obtención de información personal de manera deshonesta. Esto puede estar sujeto a sanciones legales, incluyendo cargos por violación de la privacidad o delitos informáticos, dependiendo de la gravedad y las consecuencias del acto.

¿Cómo protegerte del farming?

- ✓ Sé cauteloso con la información que compartes: No reveles datos sensibles como dirección, teléfono o información financiera en línea.
- ✓ Verifica la identidad de tus contactos en línea: Revisa perfiles y busca consistencia en fotos y detalles.
- ✓ Mantén privadas tus configuraciones en redes sociales: Solo permite que amigos cercanos y familia vean tus publicaciones. Desconfía de solicitudes de desconocidos.
- ✓ Estate alerta a señales de alarma: Desconfía si alguien en línea te pide información personal o muestra un interés excesivo en tus datos.
- ✓ Usa verificación en dos pasos y contraseñas seguras: Activa la autenticación de dos factores y utiliza contraseñas fuertes para mayor seguridad.
- ✓ Desconfía de urgencias y ofertas: Si te presionan para tomar decisiones rápidas o te ofrecen oportunidades demasiado buenas para ser verdad, sé cauteloso.

¿Qué hacer si eres testigo o víctima de farming?

Si te encuentras en una situación donde sospechas que alguien está intentando "farmearte", lo primero es detener toda comunicación con la persona y no compartir ninguna información adicional. Informa a las autoridades locales sobre cualquier intento sospechoso de obtener tu información personal de manera fraudulenta. Además, considera hablar sobre el incidente con amigos o familiares para obtener consejos y apoyo.

Construir amistades genuinas es importante, pero cuando se trata de nuevos contactos en línea, es esencial proceder con cautela. La confianza se debe ganar con el tiempo y no debe ser usada como moneda de cambio para mantener una amistad.

Protege tu información con el mismo cuidado con que protegerías tu teléfono nuevo: no se lo des a cualquiera!

¿Qué Riesgos Hay en Internet?

Ataques digitales mediante vulneraciones técnicas

Phishing: ¡Alerta en tu Inbox!

El phishing es una técnica de fraude en línea utilizada para engañar a las personas y hacer que revelen información personal, como contraseñas y detalles de tarjetas de crédito, a través de correos electrónicos que aparentan ser de fuentes confiables. Estos correos suelen incitar a "verificar" tu cuenta o "actualizar" tu contraseña mediante enlaces fraudulentos que te redirigen a páginas falsas.

Consecuencias legales del phishing

En El Salvador, el phishing está tipificado como un delito informático bajo la Ley Especial contra los Delitos Informáticos y Conexos. Las personas que cometan actos de phishing pueden enfrentarse a penas de prisión y multas significativas. Esta ley protege la integridad de la información personal y financiera de los ciudadanos, y proporciona las bases legales para procesar a aquellos que realizan estas actividades fraudulentas.

¿Cómo protegerte del phishing?

- ✓ Verifica siempre el remitente: Asegúrate de que la dirección de correo electrónico del remitente sea legítima y corresponda a la entidad que dice representar.
- ✓ Cuidado con los enlaces y archivos adjuntos: Evita hacer clic en enlaces o descargar archivos de correos electrónicos no solicitados o sospechosos.
- ✓ Utiliza la autenticación de dos factores: Refuerza la seguridad de tus cuentas activando esta característica, que añade una capa adicional de protección.
- ✓ Mantén actualizados tus sistemas: Asegúrate de que tanto tu sistema operativo como tus aplicaciones tengan las últimas actualizaciones de seguridad instaladas.
- ✓ Instala software de seguridad: Utiliza un programa antivirus que incluya protección contra phishing para ayudar a bloquear sitios maliciosos.
- ✓ Desconfía de las solicitudes urgentes: Los estafadores a menudo crean una sensación de urgencia para presionarte a actuar rápidamente. Siempre verifica la información de manera independiente si te sientes presionado.

¿Qué hacer si eres testigo o víctima de phishing?

Si te enfrentas al phishing, actúa rápidamente para proteger tu información. Verifica la autenticidad del remitente y evita clics en enlaces o descargas de correos dudosos, que podrían contener malware. Usa autenticación de dos factores para reforzar la seguridad de tus cuentas y asegúrate de mantener tus sistemas y aplicaciones actualizados para defenderte de nuevas amenazas. Instala un software de seguridad con protección contra phishing para bloquear sitios maliciosos. Además, desconfía de las solicitudes urgentes sin verificación previa, ya que los estafadores suelen presionar para provocar errores. Estas acciones son esenciales para mantener tu seguridad en línea.

Estar informado y mantenerse alerta son tus mejores defensas contra el phishing. Si recibes un correo electrónico sospechoso, es mejor ignorarlo y verificar la información contactando directamente a la fuente oficial. Protege tu información personal y navega por internet con precaución. El conocimiento y la vigilancia son esenciales para evitar caer en las trampas de los ciberdelincuentes y mantener segura tu información en el vasto mundo digital.

Malware: ¡Cuidado con los intrusos digitales!

¿Sabías que existen programas maliciosos conocidos como malware que nadie quiere en su computadora o celular? Estos pueden robar tu información o incluso dañar tus dispositivos. Virus, troyanos y ransomware son solo algunos ejemplos de estos indeseables que pueden causar un verdadero desastre.

¿Qué tipos de malware existen?

1. Virus: Se replican e infectan tus archivos, causando estragos.
2. Troyanos: Parecen programas seguros, pero una vez instalados, facilitan problemas adicionales.
3. Ransomware: Bloquean tu dispositivo y exigen un pago para desbloquearlo, como un rescate en las películas, pero en tu vida digital.

Consecuencias legales del malware

En El Salvador, la distribución y uso de malware es un delito informático tipificado bajo la Ley Especial contra los Delitos Informáticos y Conexos. Las personas involucradas en la creación, distribución o uso de malware para infiltrar sistemas sin consentimiento pueden enfrentarse a penas de prisión y multas severas, dependiendo de la gravedad del daño causado.

¿Cómo protegerte del malware?

- ✓ Usa software antivirus y antimalware: Instala un programa de seguridad confiable en todos tus dispositivos y mantenlo actualizado para detectar y eliminar el malware.
- ✓ Mantén tus sistemas actualizados: Asegura que tanto tu sistema operativo como tus aplicaciones estén al día. Las actualizaciones frecuentes contienen parches de seguridad esenciales.
- ✓ Ten cuidado con correos electrónicos y archivos adjuntos: Evita abrir correos y archivos de remitentes desconocidos, ya que el malware a menudo se distribuye de esta manera.
- ✓ Evita sitios web no seguros: No descargues nada de sitios de dudosa reputación. Al navegar, evita sitios sospechosos o ilegítimos que pueden contener malware.
- ✓ Utiliza firewalls: Activa firewalls en tus dispositivos y redes para bloquear accesos no autorizados.
- ✓ Realiza copias de seguridad regulares: Guarda periódicamente tus archivos importantes en un lugar seguro, como un dispositivo externo o en la nube, para recuperarlos si son afectados por malware.
- ✓ Sé cauteloso con los dispositivos extraíbles: Ten cuidado al conectar dispositivos USB desconocidos a tus sistemas, ya que pueden contener malware.

¿Qué hacer si eres testigo o víctima de malware?

Si sospechas que tu dispositivo ha sido infectado por malware, es crucial actuar rápidamente para minimizar los daños. Desconecta el dispositivo de cualquier red para evitar la propagación del malware. Utiliza tu software de seguridad para escanear y eliminar el malware. Si el problema persiste, considera buscar ayuda profesional. Es importante también cambiar todas tus contraseñas después de una infección y monitorear tus cuentas para detectar cualquier actividad sospechosa.

Es mejor prevenir que lamentar. Con las precauciones adecuadas, puedes mantener alejados a estos invasores digitales y asegurarte de que tus dispositivos y tu información permanezcan seguros.

¡No dejes que el malware arruine tu día digital!

Vishing: La Estafa que te Llama

¿Has recibido alguna vez una llamada de alguien que dice ser de tu compañía de telefonía o de un popular juego en línea, pidiéndote que verifiques tus datos? Ten cuidado, podría tratarse de vishing, una estafa telefónica diseñada para que creas que estás hablando con una fuente confiable y entregues información personal. Este método es sutil y engañoso; los estafadores se hacen pasar por representantes de organizaciones conocidas y alegan que es necesario verificar tu cuenta para reactivar un servicio o confirmar tu identidad para reclamar un premio.

Consecuencias legales del vishing

En El Salvador, el vishing, como forma de fraude telefónico, es ilegal y se castiga bajo las leyes contra el fraude y el engaño. Las personas involucradas en estas estafas pueden enfrentar sanciones que incluyen multas y penas de prisión, dependiendo de la gravedad del delito y el daño causado a las víctimas.

¿Cómo protegerte del vishing?

- ✓ Desconfía de las llamadas no solicitadas: Si recibes una llamada inesperada que solicita información personal, financiera o de seguridad, sé extremadamente cauteloso. Las empresas legítimas rara vez piden este tipo de datos por teléfono de manera no solicitada.
- ✓ No proporcionar información personal: Evita compartir datos personales como tu número de seguro social, contraseñas, PINs o información bancaria por teléfono, a menos que tú hayas iniciado la llamada y estés seguro de la identidad de tu interlocutor.
- ✓ Verifica la identidad del llamante: Si alguien que dice ser de una organización conocida te llama y pide información sensible, cuelga y llama al número oficial de la empresa para confirmar que la solicitud es legítima. Utiliza números de contacto que encuentres en el sitio web oficial de la empresa o en tu correspondencia oficial, nunca los proporcionados por el llamante.
- ✓ Usa el identificador de llamadas: Estate atento a llamadas de números desconocidos o que parezcan sospechosos. Ten en cuenta que algunos estafadores pueden usar técnicas de "spoofing" para hacer que su número parezca legítimo.
- ✓ No te dejes presionar: Los estafadores a menudo crean un sentido de urgencia para presionarte a actuar rápidamente. Tómate tu tiempo para pensar y verificar antes de proporcionar cualquier información.

¿Qué hacer si eres testigo o víctima de vishing?

Si sospechas que has sido víctima de vishing, reporta inmediatamente la llamada a las autoridades competentes. Proporciona todos los detalles que puedas recordar, incluyendo el número desde el que te llamaron, la fecha y hora de la llamada, y cualquier otra información que pueda ayudar en una investigación. No respondas a solicitudes adicionales sin verificar su legitimidad.

Las llamadas pueden ser más traicioneras de lo que parecen. Antes de dar cualquier información, tómate un momento para pensar y verificar.

¡Mantén tu información segura y no dejes que una llamada te meta en problemas!

Spear Phishing: Cuidado con los Engaños Personalizados

¿Sabías que los estafadores podrían estar diseñando trampas especialmente para ti? Esto se conoce como spear phishing y está dirigido directamente a adolescentes, utilizando información recogida de tus actividades en línea. Aquí te explico algunas formas en que podrían intentar engañarte: emails aparentando ser de organizaciones legítimas que solicitan información personal o dinero para procesar tu solicitud; anuncios de trabajo que buscan obtener tus datos personales o bancarios; invitaciones a eventos exclusivos; alertas de problemas con tu cuenta, mensajes que parecen de plataformas conocidas, incitándote a hacer clic en enlaces maliciosos o a entregar tus contraseñas; y promociones de productos populares, anuncios de tecnología, ropa o contenido digital que requieren ingresar datos para ganar un premio o conseguir un descuento.

Consecuencias legales del spear phishing

El spear phishing, como forma de fraude cibernético, está penalizado bajo las leyes salvadoreñas relacionadas con delitos informáticos. Quienes cometan este tipo de fraude pueden enfrentarse a sanciones significativas, que pueden incluir multas y tiempo en prisión, dependiendo de la severidad del daño causado y la cantidad de datos personales comprometidos.

¿Cómo protegerte del spear phishing?

- ✓ Sé crítico con correos y mensajes: Aunque un mensaje parezca provenir de una fuente confiable, verifica siempre su autenticidad antes de responder. Desconfía de solicitudes de información personal detallada o pagos.
- ✓ Verifica las fuentes: Antes de proporcionar cualquier información personal, asegúrate de que la solicitud sea legítima. Visita el sitio web oficial de la organización o llama directamente para confirmar la validez del correo.
- ✓ Mantén privada tu información: Sé cauteloso con lo que compartes en línea, especialmente en redes sociales. Los estafadores pueden usar esta información para personalizar ataques de spear phishing.
- ✓ Usa configuraciones de privacidad avanzadas: Ajusta las configuraciones de privacidad en tus redes sociales para limitar quién puede ver tu información y tus publicaciones, dificultando así la tarea de los estafadores.

¿Qué hacer si eres testigo o víctima de spear phishing?

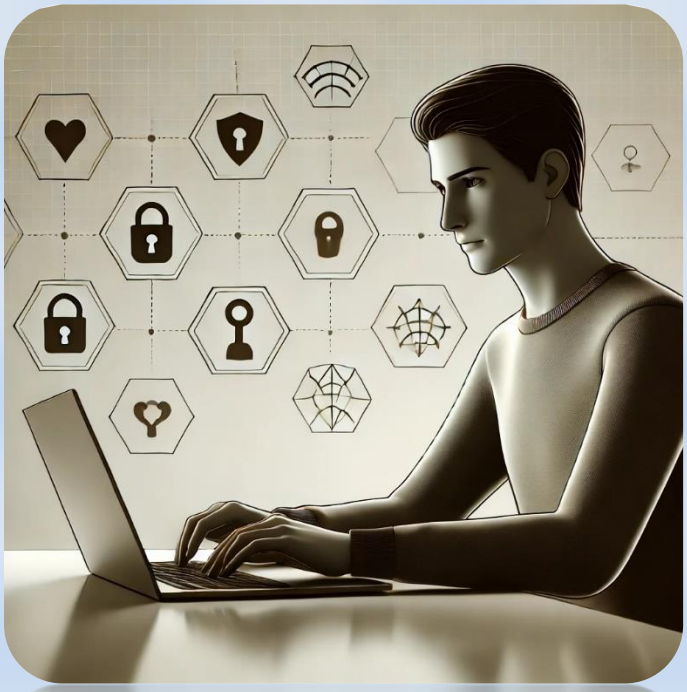
Si crees que has sido objetivo de un ataque de spear phishing, es vital que actúes rápidamente para minimizar el daño. No respondas ni interactúes con el mensaje sospechoso. Informa del intento de fraude a las autoridades pertinentes y considera cambiar tus contraseñas si has compartido alguna información. También es recomendable alertar a tu círculo cercano para prevenir ataques similares.

Estar informado y alerta es tu mejor defensa. Reconocer estas tácticas te ayudará a mantener a raya a los estafadores y proteger tu información personal.

¡No permitas que el spear phishing te engañe!

Guía de Ciberseguridad:

Cómo Mantener Segura Tu Vida Digital



Facebook:

Centro de Seguridad: facebook.com/safety

- **Normas Comunitarias:** facebook.com/communitystandards
- **Herramientas de Seguridad:** Incluyen opciones para bloquear, dejar de seguir u ocultar personas y publicaciones; además de reportar cuentas o contenidos abusivos. Puedes dejar de seguir a alguien para no ver sus publicaciones en tu News Feed sin eliminarlo como amigo, bloquear para impedir que te agreguen o vean lo que compartes, y eliminar a personas de tus amigos para restringir el contacto a través del chat de Facebook o publicaciones en tu biografía.
- **Reportes:**
  Reportar violaciones: facebook.com/help/reportviolation
  Recuperar cuenta comprometida: facebook.com/hacked
  Robo de identidad: facebook.com/help/contact/295309487309948
  Imágenes íntimas sin consentimiento: facebook.com/help/contact/567360146613371

Twitter:

- **Reglas Comunitarias:** twitter.com/rules
- **Formularios de Reporte:**
  Apelaciones y reportes de violaciones: help.twitter.com/forms
  Explotación sexual infantil: help.twitter.com/forms/cse
  Robo o suplantación de identidad: help.twitter.com/forms/impersonation
  Abuso y amenazas: help.twitter.com/forms/abusiveuser
- **Herramientas de Interacción:** Ofrece funciones para silenciar o bloquear cuentas, y la posibilidad de importar o exportar listas de cuentas bloqueadas para gestionar interacciones no deseadas.

Instagram:

- **Normas de Comunidad:** help.instagram.com/477434105621119
- Reportes:
  Suplantación de identidad: help.instagram.com/contact/636276399721841
  Contenido abusivo o spam: help.instagram.com/contact/383679321740945
  Acoso u hostigamiento: help.instagram.com/contact/584460464982589
  Reporte de correos electrónicos sospechosos: phish@instagram.com

Chats:

- **WhatsApp:** Reportar grupos o contactos en faq.whatsapp.com/21197244/#Report
- **Telegram:** Reportar contacto, grupo, canal o bots a abuse@telegram.org.
- **Signal:** Permite bloquear números de teléfono, contactos o grupos.

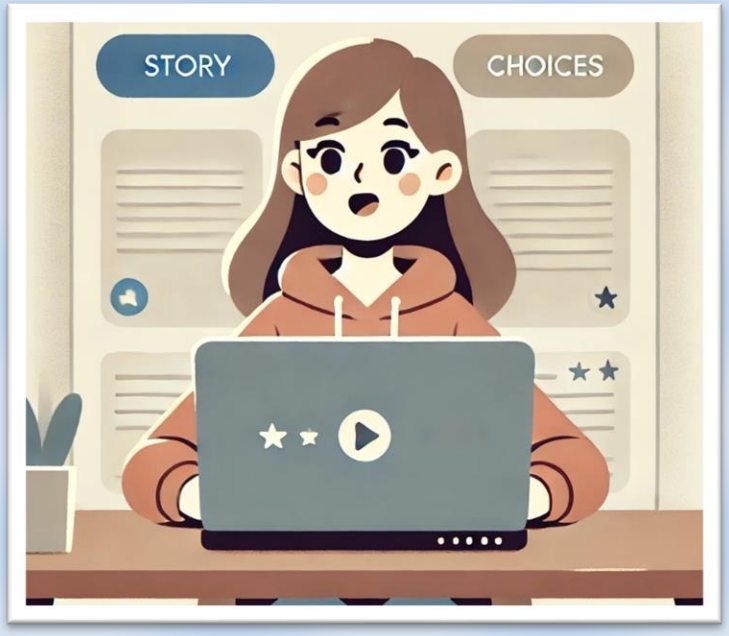
Recursos Digitales:

- **Configuración de Privacidad:** Ajusta la visibilidad de tus publicaciones en redes sociales para que solo tus amigos puedan verlas.
- **Contraseñas Fuertes:** Usa combinaciones de letras, números y símbolos para crear contraseñas robustas. Considera usar gestores como Bitwarden o 1Password.
- **Descargas Seguras:** Prefiere fuentes oficiales como Google Play o App Store y usa antivirus como Kaspersky.
- **Privacidad de Ubicación:** Desactiva la localización en apps innecesarias y sé cauteloso con la información personal compartida en línea.
- **Autenticación de Dos Factores:** Activa esta opción en tus cuentas para una seguridad adicional.
- **Firewalls y VPNs:** Utiliza estos para proteger tus conexiones, especialmente en redes Wi-Fi públicas.
- **Copias de Seguridad:** Programa copias automáticas para proteger datos importantes.
- **Seguridad en Dispositivos y Navegadores:** Asegura tus dispositivos y conexiones con herramientas como HTTPS Everywhere.

Educación y Actualización Continua:

- Mantente informado sobre las últimas amenazas y mejores prácticas en ciberseguridad a través de recursos educativos y plataformas de aprendizaje.
- Mantener a tus padres informados sobre lo que haces en línea puede ayudarte a navegar de forma segura. Pueden ser un gran apoyo en situaciones complicadas.

Pongamos en practica tus conocimientos



Aventura Narrativa

¿Tú qué harías?

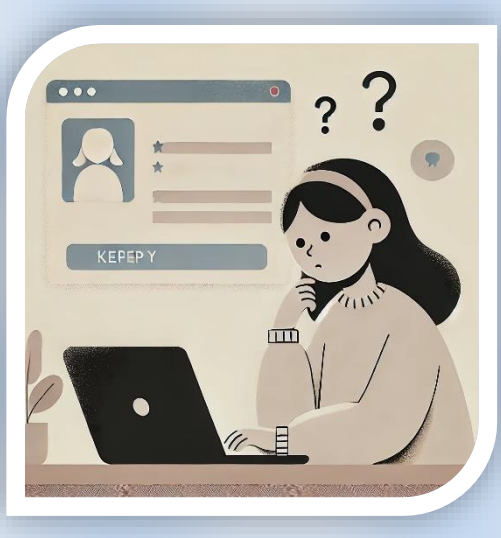
Instrucciones: Participa en una aventura narrativa donde tomarás decisiones que definirán el curso de la historia. Cada elección te llevará por un camino diferente y te enseñará lecciones importantes sobre la privacidad y seguridad en redes sociales.

Aventura Narrativa 1: El Misterio de la Invitación en Redes Sociales

Introducción: Recibes una solicitud de amistad de alguien que no conoces en una red social. La persona parece tener intereses similares a los tuyos y muchos amigos en común. Te sientes intrigado pero también un poco cauteloso. ¿Cómo responderás?

Opciones:

1. Aceptar la solicitud y empezar a chatear con la persona.
2. Ignorar la solicitud por ahora y hacer más investigaciones sobre la persona.
3. Rechazar la solicitud y configurar tus opciones de privacidad para ser más restrictivas.



Desarrollo:

- **Opción 1**: Después de aceptar la solicitud, la persona comienza a hacerte preguntas muy personales. ¿Cómo manejas esto?
- **Seguir respondiendo y compartir información personal**: Descubres que la persona usó tus respuestas para intentar robar tu identidad.
- **Dejar de responder y bloquear a la persona**: Aprendes a ser más precavido sobre a quién le das acceso en redes sociales.
- **Opción 2**: Haces una búsqueda de imagen inversa de la foto de perfil y descubres que es una imagen de stock utilizada en perfiles falsos. Reportas el perfil como sospechoso y ayudas a prevenir que otros sean engañados.
- **Opción 3**: Al rechazar la solicitud y ajustar tus configuraciones de privacidad, te aseguras de que solo las personas que realmente conoces tengan acceso a tu información personal. Además, tomas un curso en línea sobre privacidad en redes sociales para fortalecerte aún más.

Aventura Narrativa 2: La Amistad Oculta

Introducción: Estás jugando en línea cuando un nuevo jugador se une a la partida. Después de unas rondas, te envía una solicitud de amistad y comienza a chatear contigo, mostrando un gran interés en tus gustos y ofreciéndote códigos para juegos gratuitos. Aunque parece amigable, recuerdas lo que aprendiste sobre el grooming en el ebook. ¿Cómo procederás?

Opciones:

1. Aceptas los códigos y sigues interactuando.
2. Agradeces pero decides investigar más sobre esta persona antes de continuar la conversación.
3. Informas de inmediato a un adulto o usas la función de reporte del juego.

Desarrollo:

- **Opción 1**: Luego de un tiempo, la persona comienza a pedirte fotos y datos personales. Te das cuenta de que podrías estar en una situación de riesgo.
- **Compartir información personal**: Te enfrentas a consecuencias negativas al revelar datos a un desconocido.
- **Detener la comunicación y bloquear al usuario**: Aprendes la importancia de mantener límites seguros en línea.
- **Opción 2**: Tu investigación revela que varios jugadores han reportado comportamientos similares de esta persona. Decides bloquearla y alertas a otros en la comunidad.
- **Opción 3**: Al tomar acción inmediata, proteges tu información y contribuyes a un ambiente seguro en el juego. Además, reafirmas las lecciones sobre cómo manejar interacciones sospechosas en línea.

Aventura Narrativa 3: El Premio que no Esperabas

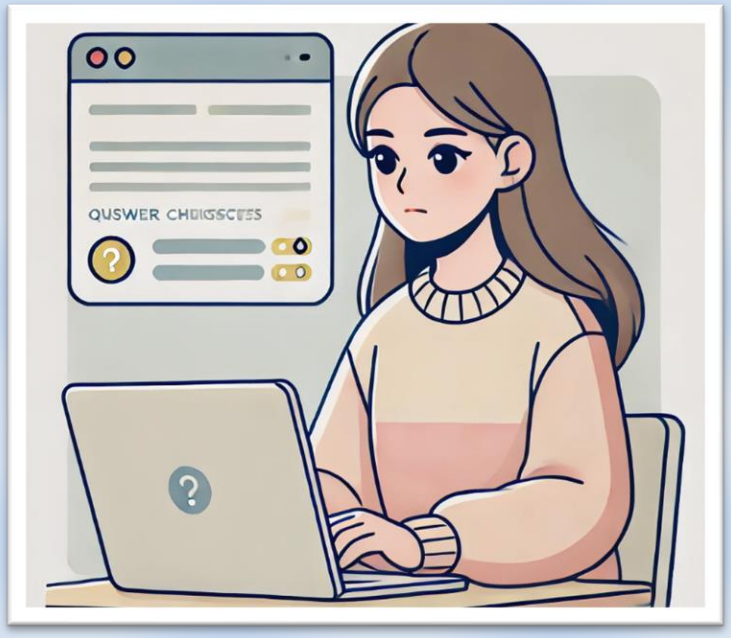
Introducción: Recibes un email anunciando que has ganado un gran premio en un sorteo en línea al que nunca te inscribiste. El mensaje te pide que pagues una pequeña tarifa de administración para reclamar tu premio. Recuerdas el capítulo sobre concursos falsos en el ebook y te preguntas cómo deberías responder.

Opciones:

1. Pagar la tarifa esperando recibir el premio anunciado.
2. Ignorar el email, pero sin tomar más acciones.
3. Investigar más sobre la organización y el concurso antes de responder.

Desarrollo:

- **Opción 1**: Después de pagar, el premio nunca llega y descubres que has sido víctima de una estafa.
- **Opción 2**: Al ignorar el correo, evitas una estafa directa, pero también pierdes la oportunidad de reportar a los estafadores.
- **Opción 3**: Tu investigación muestra que el concurso es una estafa común reportada por muchos usuarios. Decides reportar el correo como fraudulento y educas a tus amigos y familiares sobre cómo reconocer y evitar concursos falsos.



Cuestionario:

¿Es Seguro o No?

Instrucciones: Responde las siguientes preguntas eligiendo si el comportamiento descrito es seguro o no. Al final del cuestionario, encontrarás las respuestas correctas y explicaciones para entender mejor cada situación.

Pregunta 1

Recibes un email de tu banco pidiendo que hagas clic en un enlace para verificar tu cuenta debido a una supuesta actividad sospechosa.

a) Seguro
b) No seguro

Pregunta 2

Un amigo te envía un mensaje por una red social compartiendo un video sorprendente con un enlace para verlo.

a) Seguro
b) No seguro

Pregunta 3

Te llega un mensaje de texto de un número desconocido que dice que has ganado un premio y debes ingresar a un enlace para reclamarlo.

a) Seguro
b) No seguro

Pregunta 4

En un foro en línea, alguien que comparte muchos de tus intereses te pide tu email para enviarte información sobre un evento próximo.

a) Seguro
b) No seguro

Pregunta 5

Una aplicación que descargaste recientemente te pide permisos para acceder a tus contactos, aunque la aplicación es para editar fotos.

a) Seguro
b) No seguro

Pregunta 6

Al navegar por Internet, te aparece un anuncio que dice "Tu computadora está infectada. Haz clic aquí para hacer un escaneo gratuito."

a) Seguro
b) No seguro

Pregunta 7

Un nuevo juego en línea te pide que crees una cuenta usando tu perfil de una red social para guardar tus progresos y compartir logros.

a) Seguro
b) No seguro

Pregunta 8

Recibes un correo electrónico de un servicio de entrega que usas con frecuencia, solicitando que actualices tu método de pago a través de un enlace provisto en el mensaje.

a) Seguro
b) No seguro

Pregunta 9

En un chat de grupo, alguien que no conoces pero que es amigo de un amigo, te pide que le envíes una pequeña cantidad de dinero para un proyecto caritativo urgente mediante una aplicación de pago.

a) Seguro
b) No seguro

Pregunta 10

Te registras para un nuevo servicio en línea y el sitio te pide que establezcas una contraseña que incluya tanto letras como números, y que tenga al menos 12 caracteres de largo.

a) Seguro
b) No seguro

Respuestas y Explicaciones

Respuesta 1: b) No seguro

- **Explicación**: Los bancos nunca solicitarán que verifiques información sensible mediante enlaces en correos electrónicos porque estos enlaces pueden redirigirte a sitios web falsos diseñados para robar tus datos personales y financieros. Este es un claro intento de phishing.

Respuesta 2: b) No seguro

- **Explicación**: Aunque el mensaje provenga de un amigo, es posible que su cuenta haya sido comprometida o que el enlace sea parte de un malware diseñado para infectar tu dispositivo. Siempre verifica directamente con la persona por otro medio antes de hacer clic en cualquier enlace sospechoso.

Respuesta 3: b) No seguro

- **Explicación**: Los concursos que prometen premios pero requieren hacer clic en un enlace o proporcionar información personal son generalmente estafas. Los estafadores usan esta táctica para capturar información personal o financiera bajo la falsa promesa de un premio.

Respuesta 4: b) No seguro

- **Explicación**: Compartir tu dirección de correo electrónico con desconocidos en foros puede exponerte a riesgos de seguridad como spam y phishing. Es mejor mantener la comunicación dentro de las plataformas seguras y no compartir información personal con usuarios que no conoces bien.

Respuesta 5: b) No seguro

- **Explicación**: Las aplicaciones deben solicitar sólo los permisos necesarios para su funcionamiento. Una aplicación de edición de fotos que pide acceso a tus contactos podría estar intentando recopilar información para fines publicitarios o peor, para vender tus datos a terceros.

Respuesta 6: b) No seguro

- **Explicación**: Los pop-ups o anuncios que alertan sobre virus y ofrecen escaneos gratuitos suelen ser engaños para que instales software malicioso. Siempre es recomendable usar software antivirus de proveedores reconocidos y evitar hacer clic en anuncios alarmantes.

Respuesta 7: b) No seguro

- **Explicación**: Conectar aplicaciones o juegos a tus redes sociales puede darles acceso a tu información personal y la de tus contactos. Esto puede poner en riesgo tu privacidad y la de tus amigos. Es más seguro usar un correo electrónico y una contraseña única para nuevos registros.

Respuesta 8: b) No seguro

- **Explicación**: Solicitar actualizar información de pago a través de un enlace en un correo electrónico es una técnica común de phishing. Es mejor acceder a tu cuenta mediante la página oficial directamente en tu navegador para realizar cualquier actualización segura.

Respuesta 9: b) No seguro

- **Explicación**: Enviar dinero a alguien que apenas conoces, especialmente en una situación presentada como urgente, es un riesgo alto. Los estafadores suelen crear escenarios de emergencia para presionar a las víctimas a actuar rápidamente sin verificar la legitimidad de la solicitud.

Respuesta 10: a) Seguro

- **Explicación**: Establecer una contraseña robusta es una práctica de seguridad crítica. Contraseñas fuertes y únicas para cada servicio ayudan a proteger tus cuentas contra accesos no autorizados y reducen el riesgo de ser afectado en caso de una violación de datos en un servicio.

Convertirse en un Defensor de la Ciberseguridad

¡Felicidades por terminar este eBook sobre ciberseguridad!

A lo largo de estas páginas, has descubierto cómo proteger tu información personal, usar las redes sociales de manera segura y detectar amenazas como el phishing y el malware. Estos conocimientos no son solo un logro personal, sino también herramientas esenciales para tu futuro.

Ahora que conoces estas estrategias clave, es hora de pasar de la teoría a la acción. Tu papel en la comunidad digital es crucial: cada acción segura que tomes ayuda a crear un entorno más seguro para todos.

Te animo a que te conviertas en un defensor activo de la ciberseguridad, compartiendo lo que has aprendido y sirviendo como ejemplo para otros. Habla con tus familiares y amigos sobre la importancia de usar contraseñas seguras y de implementar la autenticación de dos factores. Procura que tus propias prácticas de seguridad sean ejemplares, mostrando con el ejemplo lo efectivas que pueden ser. Además, mantente al día con los últimos avances en ciberseguridad y comparte tus descubrimientos, promoviendo el aprendizaje continuo en tu entorno.

Recuerda, posees el conocimiento y la habilidad para marcar la diferencia. Si te enfrentas a dudas o desafíos, busca el apoyo de profesionales o mentores. Cada conversación, cada consejo y cada acción que tomas contribuye a crear una cultura de ciberseguridad consciente y educada.

Gracias por tu esfuerzo en aprender sobre ciberseguridad. Ahora es tu momento de liderar y hacer la diferencia. Levántate, sal y comienza a hablar sobre lo que has aprendido. Tu viaje como defensor de la ciberseguridad está solo comenzando.

Con aprecio por tu compromiso y confianza en tu liderazgo.

Recursos legales

Código Penal:

El Código Penal salvadoreño fue inicialmente promulgado mediante el Decreto Legislativo N° 270 el 13 de febrero de 1973. Este texto ha experimentado varias modificaciones a lo largo de los años para adaptarse a los cambios en la sociedad y las necesidades de justicia. La versión actual del Código Penal fue instaurada por el Decreto Legislativo N° 1030, aprobado el 26 de abril de 1997 y puesto en vigencia el 20 de abril de 1998.

Esta legislación moderna y actualizada está diseñada para ser una herramienta eficaz en la lucha contra la delincuencia, incluyendo disposiciones específicas sobre delitos, penas y medidas de seguridad. Además, se sustenta en principios fundamentales como el principio de legalidad, la dignidad humana y la lesividad del bien jurídico, asegurando un marco legal justo y equitativo.. (Asamblea General de la Republica - Decreto 270, s.f.) (Asamblea General de la Republica - Decreto 482, s.f.)

Ley Especial Integral para una Vida Libre de Violencia para las Mujeres (LEIV):

Promulgada en 2012, la LEIV busca garantizar el derecho de todas las mujeres a una vida libre de violencia en El Salvador. Esta ley establece políticas públicas comprensivas para la detección, prevención, atención, protección, reparación y sanción de cualquier forma de violencia contra las mujeres. A través de esta legislación, se protegen derechos fundamentales como la vida, la integridad física y moral, la no discriminación y la dignidad.

La LEIV aborda la violencia contra las mujeres desde una perspectiva integral, reconociendo y actuando contra las desigualdades de poder y las relaciones de género asimétricas. (Decreto 520, LEIV, s.f.)

Ley de Protección Integral de la Niñez y Adolescencia (LEPINA):

Entrada en vigor el 16 de abril de 2010, la LEPINA es fundamental para la protección de los derechos de niñas, niños y adolescentes en El Salvador. Esta ley crea un Sistema Nacional de Protección Integral de la Niñez y Adolescencia, alineándose con la Constitución del país y diversos tratados internacionales sobre derechos humanos, especialmente la Convención sobre los Derechos del Niño. La LEPINA está diseñada para salvaguardar la salud física, mental y moral de los menores, garantizando así su derecho a la educación y a recibir asistencia adecuada. (Ley Lepina, s.f.)

Trabajos citados

Asamblea General de la Republica - Decreto 270. (s.f.). Obtenido de https://biblioteca.asamblea.gob.sv/32009_cdigo-penal-decreto-no-270?q=

Asamblea General de la Republica - Decreto 482. (s.f.). Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/37C67D16-0F45-4C75-8B2B-1A1D3C0C4BE3.pdf

BID . (2020). Obtenido de https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Decreto 520, LEIV. (s.f.). Obtenido de https://oig.cepal.org/sites/default/files/2011_decreto520_elsvd.pdf

Fondo de Población de las Naciones Unidas El Salvador. (julio de 2023). *Llegar a cero embarazos en niñas y adolescentes.* Recuperado el 1 de May de 2024, de UNFPA El Salvador: https://elsalvador.unfpa.org/sites/default/files/pub-pdf/mapa_embarazos_2023_web.pdf

IPANDETE. (Junio de 2023). Obtenido de https://www.ipandetec.org/wp-content/uploads/2023/06/Centroamerica-Cibersegura.pdf

Ley Lepina. (s.f.). Obtenido de https://www.elsalvador.law.pro/Leyes/LEPINA.pdf

UNODC . (s.f.). Obtenido de https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/EL_SALVADOR_IEG_Cybercrime.pdf