Universidad Tecnológica Ecotec

Título del trabajo:

"Explorando las profundidades del crimen digital: un análisis de los diversos ciberdelitos a través de la Red Tor"

Línea de investigación:

Gestión de las Relaciones Jurídicas

Modalidad de titulación:

Trabajo de Integración Curricular

Programa de Licenciatura:

Criminalística

Título a obtener:

Licenciatura en Criminalística

Autores:

Génesis Anaimar Aurora Blanco Cermeño

Carlos Eduardo Pazmiño Maestre

Tutor:

Abg. Miguel Leonardo Mora Romero. Mgtr

ANEXO No. 9

PROCESO DE TITULACIÓN

CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, 07 de agosto del 2024

Magíster o Doctor

Andrés Madero Poveda

Unidad Académica: Facultad de Derecho y Gobernabilidad

Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: EXPLORANDO LAS PROFUNDIDADES DEL CRIMEN DIGITAL, UN ANÁLISIS DE LOS DIVERSOS CIBERDELITOS A TRAVÉS DE LA RED TOR, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: **Carlos Eduardo Pazmiño Maestre, y Genesis Anaimar Aurora Blanco Cermeño** para que proceda con la presentación oral del mismo.

ATENTAMENTE,

Firmado electrónicamente por:
MIGUEL LEONARDO MORA ROMERO

Abg. Miguel Leonardo MORA ROMERO Mgtr.

Tutor

ANEXO No. 10

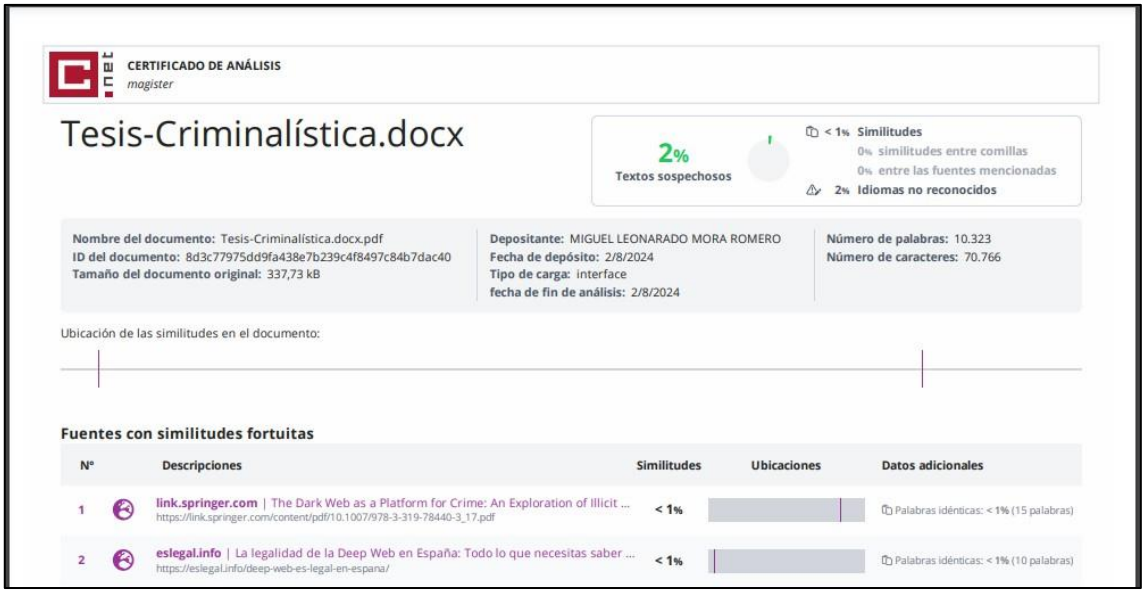
PROCESO DE TITULACIÓN

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: EXPLORANDO LAS PROFUNDIDADES DEL CRIMEN DIGITAL, UN ANÁLISIS DE LOS DIVERSOS CIBERDELITOS A TRAVÉS DE LA RED TOR elaborado CARLOS EDUARDO PAZMIÑO MAESTRE, y GENESIS ANAIMAR AURORA BLANCO CERMEÑO, fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del (2 %) Dos mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.

https://app.compilatio.net/v5/report/713018e1f55c521f437a60187f8175636606143b/summary



CERTIFICADO DE ANÁLISIS
magister

Tesis-Criminalística.docx

2%
Textos sospechosos

< 1% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos

Nombre del documento: Tesis-Criminalística.docx.pdf
ID del documento: 8d3c77975dd9fa438e7b239c4f8497c84b7dac40
Tamaño del documento original: 337,73 kB

Depositante: MIGUEL LEONARADO MORA ROMERO
Fecha de depósito: 2/8/2024
Tipo de carga: interface
fecha de fin de análisis: 2/8/2024

Número de palabras: 10.323
Número de caracteres: 70.766

Ubicación de las similitudes en el documento:

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	link.springer.com | The Dark Web as a Platform for Crime: An Exploration of Illicit ... https://link.springer.com/content/pdf/10.1007/978-3-319-78440-3_17.pdf	< 1%		Palabras idénticas: < 1% (15 palabras)
2	eslegal.info | La legalidad de la Deep Web en España: Todo lo que necesitas saber ... https://eslegal.info/deep-web-es-legal-en-espana/	< 1%		Palabras idénticas: < 1% (10 palabras)

ATENTAMENTE,

Firmado electrónicamente por:
MIGUEL LEONARDO MORA ROMERO

Abg. Miguel Leonardo MORA ROMERO Mgtr.

Tutor

Dedicatoria

Agradezco a Dios por haber llegado hasta aquí, ya que sin él no hubiese sido esto posible.

A mis padres, hermana y parte de mi familia por siempre darme ese apoyo incondicional para ser de mí una mejor persona y siempre seguir adelante.

A Jorge Choez por brindarme un poco de apoyo económico e incondicional que me permitió continuar adelante.

Por último, está demás agradecerme a mí misma, una persona muy valiente con muchas ganas de salir adelante y a que pesar de no estar en mi país, lograr una meta propuesta y el día de hoy decir que se hizo realidad lo que tanto añoraba.

Génesis Blanco

Dedicatoria

Agradezco a Dios que a pesar de las dificultades he salido adelante, a mis padres quiénes son un pilar fundamental, en especial a mi madre quién siempre me apoyó en cada momento de la carrera, a mis hermanos por aconsejarme y a mis gatos Rengar y Pixar por acompañarme en todas las madrugadas.

A mis amistades: Mikaela, Harleth, Isabel, Ayline, Lia, Madeleine, Stephany, Melany, Dana, Aurora, Jennifer, Russell y Marcos; por enseñarme a nunca rendirme, gracias por ser una fuente de motivación.

A mi novia Andrea Mendieta, por su incondicional amor y apoyo brindado durante la realización de este proyecto, gracias por estar a mi lado en los momentos difíciles y por celebrar conmigo cada logro académico. Te amo más de lo que las palabras puedan expresar.

Carlos Pazmiño

Agradecimientos

En primer lugar, agradecemos a Dios por ser la fuente principal de apoyo en nuestras vidas.

Queremos expresar nuestro más sincero agradecimiento a las personas que nos apoyaron en la realización de esta tesis, padres, familiares, amigos y parejas.

Gracias a todos los docentes académicos que, con su aporte de conocimientos, contribuyeron al crecimiento profesional de los estudiantes. Sin su ayuda no podríamos llegar hasta donde hoy nos encontramos.

Índice

Índice de tablas

Índice de figuras

Resumen

En la era digital actual, la Red Tor se ha convertido en un refugio para actividades ilícitas, incluyendo diversos ciberdelitos. Este estudio tiene como objetivo analizar los ciberdelitos más comunes en la Red Tor, describiendo sus características y métodos de operación, con el fin de desarrollar estrategias efectivas desde una perspectiva criminalística para prevenir estos delitos y mitigar su impacto en las víctimas. La metodología utilizada combina análisis cualitativos y cuantitativos, mediante encuestas estructuradas y cuestionarios dirigidos a usuarios de la Red Tor. Los análisis cualitativos incluyeron la triangulación de datos de grupos focales y entrevistas con expertos en ciberseguridad, mientras que los análisis cuantitativos se realizaron utilizando el software SPSS para evaluar frecuencias, regresiones lineales y correlaciones entre variables. Los resultados revelaron que el fraude financiero y el phishing son los ciberdelitos más prevalentes en la Red Tor, con un 74% y un 22% de incidencia respectivamente. Además, se observó que la percepción del riesgo de ciberdelitos entre los usuarios está significativamente influenciada por su nivel de conocimiento sobre el funcionamiento de la Red Tor ($F=12.000$, $p=0.001$). Sin embargo, no se encontró una correlación significativa entre la frecuencia de uso de la Red Tor y la percepción del riesgo de ciberdelitos ($F=2.066$, $p=0.157$). En conclusión, es esencial aumentar la educación y formación de los usuarios sobre ciberseguridad, así como desarrollar estrategias preventivas basadas en un conocimiento profundo de los métodos de operación de los ciberdelincuentes. La colaboración entre entidades gubernamentales y organizaciones de ciberseguridad es crucial para implementar estas estrategias y proteger a los usuarios de la Red Tor.

Palabras claves: Ciberdelitos; Red Tor; Prevención; Ciberseguridad; Criminalística

Abstract

In today's digital age, the Tor Network has become a haven for illicit activities, including various cybercrimes. This study aims to analyze the most common cybercrimes on the Tor Network, describing their characteristics and methods of operation, in order to develop effective strategies from a criminalistic perspective to prevent these crimes and mitigate their impact on victims. The methodology used combines qualitative and quantitative analysis, through structured surveys and questionnaires aimed at users of the Tor Network. Qualitative analyzes included triangulation of data from focus groups and interviews with cybersecurity experts, while quantitative analyzes were conducted using SPSS software to evaluate frequencies, linear regressions, and correlations between variables. The results revealed that financial fraud and phishing are the most prevalent cybercrimes on the Tor Network, with 74% and 22% incidence respectively. Furthermore, it was observed that the perception of the risk of cybercrimes among users is significantly influenced by their level of knowledge about the operation of the Tor Network ($F=12.000$, $p=0.001$). However, no significant correlation was found between the frequency of use of the Tor Network and the perception of the risk of cybercrimes ($F=2.066$, $p=0.157$). In conclusion, it is essential to increase user education and training on cybersecurity, as well as develop preventive strategies based on in-depth knowledge of cybercriminals' operating methods. Collaboration between government entities and cybersecurity organizations is crucial to implement these strategies and protect Tor Network users.

Keywords: Cybercrimes; Tor Network; Prevention; Cybersecurity; Criminalistics

Capítulo I: Introducción

La proliferación del uso de Internet ha dado lugar a un aumento significativo en la cantidad y variedad de ciberdelitos. En este contexto, la Red Tor, creada inicialmente para proteger la privacidad de los usuarios y permitir la libre expresión en regiones con censura, se ha convertido en un refugio para actividades ilícitas debido a su capacidad de anonimato (Stöber, 2018). Este trabajo surge de la necesidad de comprender cómo los ciberdelincuentes explotan la Red Tor para llevar a cabo sus actividades y qué medidas pueden implementarse para contrarrestar estos delitos.

La literatura sobre la Red Tor y los ciberdelitos es vasta y diversa. Estudios recientes han explorado desde los aspectos técnicos del anonimato proporcionado por Tor hasta los diversos tipos de delitos que se llevan a cabo en la dark web. Investigaciones han destacado que, aunque Tor ofrece beneficios en términos de privacidad, también facilita actividades ilegales como el tráfico de drogas, la venta de armas y el fraude financiero (Gehl, 2019). Este análisis se basará en una revisión exhaustiva de las investigaciones más recientes para proporcionar una visión actualizada del estado del arte en esta área.

A pesar de los esfuerzos de las autoridades y las organizaciones de ciberseguridad, los ciberdelitos en la Red Tor continúan siendo un desafío significativo. El problema principal que se aborda en esta investigación es cómo se perpetúan estos ciberdelitos y qué medidas efectivas se pueden implementar para prevenir y mitigar su impacto. Este estudio busca identificar los tipos de delitos más comunes en la Red Tor, analizar sus métodos de operación y proponer soluciones viables para combatir estos problemas (Fu, Ling, Wang, y Sun, 2020).

La creciente incidencia de ciberdelitos en la Red Tor y su impacto negativo en la sociedad justifican la necesidad de una investigación profunda y detallada en este ámbito. Este estudio no solo contribuirá a la comprensión académica de los mecanismos de estos delitos, sino que también proporcionará información valiosa para las autoridades y profesionales de ciberseguridad que buscan desarrollar estrategias más efectivas para combatir estos crímenes. Además, al proporcionar recomendaciones para los usuarios afectados, esta investigación pretende aumentar la resiliencia de las comunidades digitales frente a las

amenazas cibernéticas (Biryukov, Pustogarov, y Thill, 2020).

El objetivo general de esta investigación es explorar y analizar los diversos ciberdelitos que se cometen a través de la Red Tor, comprender los métodos utilizados para llevar a cabo estos delitos, y desarrollar estrategias efectivas para prevenir y mitigar su impacto. Este estudio se centrará en proporcionar una visión comprensiva de la problemática actual, así como en ofrecer recomendaciones prácticas tanto para usuarios individuales como para profesionales de ciberseguridad (Fang y Zhang, 2019).

Planteamiento del problema

El uso de la Red Tor ha crecido exponencialmente en los últimos años, convirtiéndose en una herramienta esencial para aquellos que buscan anonimato en la red. Sin embargo, esta misma característica ha hecho de Tor un refugio para actividades ilícitas. La falta de rastreo y la privacidad que ofrece han facilitado la realización de ciberdelitos, convirtiendo a Tor en un espacio propicio para el tráfico de drogas, la venta de armas y otros delitos cibernéticos. Este problema afecta no solo a las víctimas directas de estos delitos, sino también a la seguridad global y a la percepción de privacidad en el uso de Internet.

El presente estudio se enfocará en analizar los principales ciberdelitos que se cometen a través de la Red Tor. La investigación se delimita a examinar cómo se llevan a cabo estos delitos, las técnicas utilizadas por los ciberdelincuentes y el impacto de estas actividades en las víctimas y la sociedad en general. Se pondrá especial énfasis en identificar los métodos de operación y las medidas de seguridad que se pueden implementar para mitigar estos riesgos. El análisis se basará en datos actuales y casos relevantes para proporcionar una visión integral del problema.

La problemática radica en la dificultad de rastrear y prevenir los ciberdelitos en la Red Tor debido a su diseño orientado al anonimato. Los ciberdelincuentes aprovechan estas características para operar con relativa impunidad, lo que complica la labor de las autoridades y los profesionales de ciberseguridad. La falta de regulación y control en este entorno ha

permitido que los ciberdelitos se multipliquen, afectando a individuos, empresas y gobiernos. Es crucial identificar las estrategias que los delincuentes utilizan y desarrollar soluciones efectivas para proteger a los usuarios y minimizar el impacto de estos delitos.

Pregunta científica

¿Cómo se llevan a cabo los ciberdelitos más comunes en la Red Tor, cuáles son sus características y métodos de operación, y qué estrategias pueden implementarse desde una perspectiva criminalística para prevenirlos y mitigar su impacto en las víctimas?

Esta pregunta resume claramente la situación problemática al centrarse en la relación entre la educación recibida y la eficacia en la investigación de ciberdelitos, pudiendo ser respondida de manera clara mediante un análisis de las competencias y habilidades adquiridas por los estudiantes. La respuesta a esta pregunta permitirá identificar las áreas de mejora en la formación académica y contribuirá a desarrollar estrategias educativas que fortalezcan la capacidad investigativa de los futuros criminalistas en el ámbito digital.

Objetivos

Objetivo General

Analizar los ciberdelitos más comunes en la Red Tor, describiendo sus características y métodos de operación, con el fin de desarrollar estrategias efectivas desde una perspectiva criminalística para prevenir estos delitos y mitigar su impacto en las víctimas.

Objetivos Específicos

- Identificar los ciberdelitos más comunes en la Red Tor mediante una revisión exhaustiva de la literatura y análisis de datos actuales, para comprender su prevalencia y características principales.
- Describir los métodos de operación utilizados por los ciberdelincuentes en la Red Tor a través del estudio de casos documentados y entrevistas con expertos en ciberseguridad, con el fin de entender las técnicas y herramientas empleadas.

- Desarrollar estrategias de prevención y mitigación basadas en principios criminalísticos, incluyendo recomendaciones prácticas para usuarios y profesionales de ciberseguridad, con el objetivo de reducir la incidencia y el impacto de estos delitos en las víctimas.

Justificación

La investigación sobre los ciberdelitos en la Red Tor es crucial debido al aumento significativo de actividades ilícitas en este entorno anónimo. Tor, inicialmente desarrollado para proteger la privacidad, ha sido explotado por ciberdelincuentes para realizar diversos delitos, afectando tanto a individuos como a organizaciones (Köpsell y Hiller, 2019). Comprender estos delitos y cómo se llevan a cabo es esencial para desarrollar estrategias efectivas de prevención y mitigación.

Los ciberdelitos en la Red Tor tienen un impacto significativo tanto social como económico. La venta de drogas, armas y otros productos ilícitos a través de Tor ha llevado a un incremento en la criminalidad y ha causado pérdidas económicas considerables a las víctimas (Moore & Rid, 2020). Este estudio busca proporcionar una visión integral del problema para ayudar a las autoridades y a los profesionales de la ciberseguridad a combatir estas actividades delictivas.

La falta de estrategias preventivas efectivas en la Red Tor ha permitido que los ciberdelincuentes operen con relativa impunidad. Identificar y desarrollar medidas preventivas es fundamental para reducir la incidencia de estos delitos. Este estudio aportará conocimientos que pueden ser utilizados para diseñar políticas de ciberseguridad más robustas y efectivas (Biryukov et al., 2020).

Desde la perspectiva de la criminalística, es vital entender los métodos y técnicas utilizados por los ciberdelincuentes en la Red Tor. Este conocimiento permitirá a los investigadores y a las fuerzas del orden diseñar mejores estrategias de detección y prevención, mejorando la capacidad para rastrear y detener a los perpetradores (Fu et al., 2020).

Esta investigación no solo contribuirá al conocimiento académico sobre los ciberdelitos en la Red Tor, sino que también ofrecerá recomendaciones prácticas para la prevención y mitigación de estos delitos. Proporcionar una guía basada en evidencia para usuarios y profesionales de la ciberseguridad puede ayudar a reducir el impacto de estos delitos y mejorar la seguridad en el entorno digital (Gehl, 2019).

Capítulo II: Marco Teórico

La investigación sobre ciberdelitos y la Red Tor se fundamenta en varias teorías y principios clave que sustentan el estudio y análisis de estas actividades ilícitas en el ámbito digital. Uno de los marcos teóricos fundamentales es la teoría del anonimato en la web oscura, que postula que la capacidad de los usuarios para ocultar su identidad en plataformas como Tor facilita una amplia gama de actividades delictivas. Según un estudio realizado por Weimann (2016), el anonimato no solo protege a los perpetradores de ser rastreados, sino que también crea un entorno propicio para la proliferación de mercados negros y otros servicios ilegales. Esta teoría es esencial para comprender por qué y cómo los ciberdelincuentes utilizan la Red Tor para llevar a cabo sus operaciones sin temor a ser detectados.

Otra teoría relevante es la teoría del espacio criminológico cibernético, que analiza cómo los entornos digitales modifican la dinámica del crimen y la seguridad. Yar y Steinmetz (2019) destacan que los espacios cibernéticos, como la Red Tor, funcionan como "zonas de oportunidad" para los delincuentes, quienes aprovechan las debilidades de la ciberseguridad y las lagunas en la legislación para cometer delitos. Este enfoque teórico permite a los investigadores de criminalística entender las particularidades del cibercrimen y desarrollar estrategias específicas para investigar y mitigar estos delitos en el contexto digital.

La teoría de la ciberseguridad proactiva, propuesta por Gupta y Agrawal (2020), también juega un papel crucial en el marco teórico de esta investigación. Esta teoría sostiene que, en lugar de reaccionar a los incidentes de seguridad después de que ocurren, las organizaciones y los investigadores deben adoptar enfoques proactivos para prevenir los ciberdelitos. En el contexto de la Red Tor, esto implica el uso de tecnologías avanzadas de monitoreo y análisis para detectar actividades sospechosas y tomar medidas preventivas. La adopción de este enfoque es fundamental para los estudiantes de criminalística de la Universidad ECOTEC, quienes deben estar preparados para implementar estrategias de ciberseguridad proactiva en su futura carrera profesional.

Finalmente, la teoría de la criminología digital de Holt y Bossler (2016) proporciona un marco integral para analizar la intersección entre la tecnología y el crimen. Esta teoría abarca

diversos aspectos del cibercrimen, incluyendo la motivación de los delincuentes, las técnicas utilizadas y el impacto de los delitos en las víctimas y la sociedad en general. Holt y Bossler subrayan la importancia de una formación multidisciplinaria que combine conocimientos en tecnología, derecho y criminología para abordar eficazmente los ciberdelitos. Este enfoque teórico respalda la necesidad de un currículo integral en la Universidad ECOTEC, que prepare a los estudiantes para enfrentar los desafíos complejos del crimen digital en la Red Tor.

La Red Tor: Funcionamiento y Características

La Red Tor (The Onion Router) es una red superpuesta que permite a sus usuarios navegar por Internet de forma anónima y segura. Fue creada originalmente por el Laboratorio de Investigación Naval de los Estados Unidos y ha evolucionado para ofrecer a los usuarios una mayor privacidad en línea mediante la encriptación de sus comunicaciones y el enrutamiento del tráfico a través de una serie de nodos voluntarios. Esta estructura de "capa de cebolla" dificulta que terceros rastreen la actividad del usuario, lo que ha hecho de Tor una herramienta valiosa tanto para quienes buscan proteger su privacidad como para aquellos con intenciones delictivas (Dingledine et al., 2020).

Principales Ciberdelitos en la Red Tor

Entre los ciberdelitos más comunes en la Red Tor se encuentran el tráfico de drogas, la venta de armas, el fraude financiero y la distribución de pornografía infantil. Estos delitos se facilitan a través de mercados negros en línea, como Silk Road, AlphaBay y otros, que utilizan criptomonedas como Bitcoin para las transacciones, lo que dificulta aún más el rastreo de las actividades ilícitas (Moore y Rid, 2020). El tráfico de drogas es especialmente prevalente, con estudios que muestran que una gran proporción de las transacciones en estos mercados está relacionada con la venta de sustancias ilegales (Van Hout y Bingham, 2021).

Problemas Asociados a los Ciberdelitos en Tor

Los ciberdelitos en la Red Tor presentan varios problemas significativos. Primero, la anonimidad que ofrece Tor dificulta la identificación y captura de los delincuentes. Esto crea

un entorno donde los criminales pueden operar con relativa impunidad. Además, la venta de productos ilícitos puede tener consecuencias devastadoras para la salud y seguridad pública, como el aumento de la violencia relacionada con las drogas y la proliferación de armas ilegales (Bartlett, 2019). La explotación infantil es otro problema grave, con redes que utilizan Tor para distribuir y consumir contenido abusivo, afectando profundamente a las víctimas (Jones et al., 2020).

Métodos de Realización de Ciberdelitos en Tor

Los ciberdelincuentes utilizan una variedad de métodos para realizar sus actividades ilícitas en la Red Tor. Estos incluyen el uso de mercados en línea para vender productos ilegales, foros para intercambiar información sobre técnicas de hacking y criptomonedas para financiar sus operaciones y lavar dinero. La estructura descentralizada y la encriptación robusta de Tor permiten a estos actores evitar la detección y el enjuiciamiento (Biryukov et al., 2020). Además, las técnicas de anonimato y el uso de múltiples capas de protección hacen que rastrear las transacciones y la actividad en la red sea extremadamente difícil para las autoridades.

Soluciones y Estrategias de Prevención

Para abordar los ciberdelitos en la Red Tor, es crucial implementar una combinación de estrategias técnicas y legales. Esto incluye el desarrollo de herramientas avanzadas de rastreo y monitoreo que puedan penetrar las capas de anonimidad de Tor sin comprometer la privacidad de los usuarios legítimos. Además, es esencial fortalecer la cooperación internacional entre agencias de ciberseguridad y las fuerzas del orden para compartir información y coordinar esfuerzos (Fu et al., 2020). Educar a los usuarios sobre las prácticas seguras en línea y las señales de posibles actividades delictivas también es vital para prevenir que caigan víctimas de estos delitos.

Recomendaciones para las Víctimas

En caso de haber sido afectado por un ciberdelito en la Red Tor, es fundamental actuar

rápidamente. Las víctimas deben reportar el incidente a las autoridades competentes y buscar asesoramiento legal para proteger sus derechos. También es recomendable fortalecer las medidas de seguridad personal, como cambiar contraseñas, monitorear las cuentas bancarias y utilizar servicios de protección contra robo de identidad (Gehl, 2019). Además, las víctimas deben colaborar con las autoridades proporcionando toda la información posible para ayudar en la investigación y posible captura de los delincuentes.

Ciberdelito: El ciberdelito se refiere a cualquier actividad delictiva que implica el uso de computadoras y redes. Los ciberdelitos incluyen el fraude electrónico, el robo de identidad, el hacking y la distribución de malware, entre otros. Este término se ha expandido para incluir cualquier acto ilícito que se comete a través del ciberespacio, y su entendimiento es crucial para el análisis de la criminalidad en la Red Tor (Brenner, 2019).

Red Tor: La Red Tor es una red de comunicaciones diseñada para permitir a los usuarios navegar por Internet de manera anónima. Utiliza una serie de nodos que encriptan los datos, lo que oculta la ubicación y actividad de los usuarios. Esto la convierte en una herramienta preferida por los delincuentes cibernéticos. Según estudios recientes, la estructura de Tor facilita una amplia gama de actividades ilegales, dificultando la detección y rastreo por parte de las autoridades (Jardine, 2019).

Anonimato en la web oscura: El anonimato es un componente crucial de la web oscura, proporcionando una capa de seguridad para los usuarios que desean ocultar sus identidades. Este anonimato facilita una serie de actividades ilegales, desde la venta de drogas hasta el tráfico de personas. Investigaciones recientes han explorado cómo el anonimato en la Red Tor complica los esfuerzos de las fuerzas del orden para combatir estas actividades (Bradbury, 2020).

Ciberseguridad: La ciberseguridad abarca las medidas y prácticas destinadas a proteger los sistemas informáticos y los datos contra accesos no autorizados, uso indebido y daños. Incluye la implementación de tecnologías avanzadas y estrategias proactivas para prevenir incidentes de seguridad. Un enfoque proactivo en la ciberseguridad es esencial para

contrarrestar las amenazas presentadas por la Red Tor (Bada, Creese, & Nurse, 2019).

Criminología digital: La criminología digital es el estudio de la delincuencia en el ciberespacio. Se enfoca en entender cómo y por qué ocurren los delitos cibernéticos y en desarrollar métodos para prevenir y investigar estos delitos. Este campo interdisciplinario combina conocimientos de tecnología, criminología y derecho. Investigaciones recientes destacan la necesidad de enfoques multidisciplinarios para abordar eficazmente el cibercrimen (Lavorgna, 2020).

Fraude electrónico: El fraude electrónico implica el uso de medios electrónicos para engañar a individuos o entidades con el fin de obtener beneficios financieros. Incluye actividades como phishing, pharming y otras formas de manipulación digital. La Red Tor se utiliza frecuentemente para llevar a cabo estas actividades debido a su capacidad para ocultar la identidad de los delincuentes (Hutchings y Clayton, 2019).

Hacking: El hacking es el acto de comprometer la seguridad de un sistema informático sin autorización. Los hackers pueden robar información, causar daños o simplemente demostrar su capacidad técnica. En el contexto de la Red Tor, el hacking puede ser particularmente difícil de rastrear y prevenir debido a las medidas de anonimato. Un estudio reciente señala que las técnicas de hacking continúan evolucionando, desafiando las capacidades de los defensores de la seguridad (Kraemer-Mbula, Tang, y Rush, 2019).

Malware: El malware es software malicioso diseñado para dañar o explotar sistemas informáticos. Incluye virus, gusanos, troyanos y ransomware. La Red Tor se utiliza a menudo para distribuir malware debido a su capacidad para mantener en secreto la identidad de los distribuidores. Investigaciones recientes subrayan la creciente sofisticación de las técnicas de distribución de malware en la web oscura (Hoffmann, Vaas, y Möhring, 2020).

Mercados Negros en Línea: Los mercados negros en línea son plataformas donde se compran y venden bienes y servicios ilegales, como drogas, armas y datos robados. Estos mercados operan a menudo en la Red Tor para aprovechar su anonimato y dificultar la

intervención de las autoridades. Un estudio reciente analiza el impacto económico y social de estos mercados en línea (Tzanetakis, 2020).

Anonimato y Privacidad: La privacidad y el anonimato son conceptos centrales en el uso de la Red Tor. La privacidad se refiere a la capacidad de un individuo para mantener su información personal protegida, mientras que el anonimato implica la incapacidad de los demás para identificar al usuario. Estos conceptos son fundamentales para entender por qué la Red Tor es utilizada tanto por defensores de la privacidad como por delincuentes. Un estudio reciente explora las implicaciones éticas y legales del anonimato en la web oscura (Martin, 2020).

La problemática del ciberdelito en el contexto de la Red Tor ha adquirido relevancia mundial debido al aumento exponencial de actividades ilegales en esta red anónima. Los mercados negros digitales en la Red Tor permiten la comercialización de drogas, armas y servicios ilegales, facilitando un entorno donde los delincuentes pueden operar con menor riesgo de ser detectados por las autoridades. Un estudio de Tzanetakis (2020) evidenció que la estructura y distribución de estos mercados en países como los Países Bajos y Alemania reflejan la magnitud y la complejidad de las operaciones ilegales en la web oscura, resaltando la necesidad de nuevas estrategias de intervención y regulación para contrarrestar estos desafíos.

En Ecuador, la incidencia del ciberdelito ha aumentado significativamente en los últimos años, lo que ha llevado a las autoridades a desarrollar políticas más robustas en ciberseguridad. La investigación de Andrade (2019) sobre la ciberseguridad en América Latina destaca que Ecuador enfrenta retos específicos debido a la falta de recursos y capacitación especializada en el ámbito de la seguridad digital. Este contexto pone en evidencia la urgencia de formar profesionales capacitados en criminalística digital, capaces de investigar y mitigar los impactos del ciberdelito en el país.

El programa de Licenciatura en Criminalística de la Universidad ECOTEC busca abordar estos desafíos mediante la formación integral de sus estudiantes en el análisis y prevención

del ciberdelito. La implementación de estudios específicos sobre la Red Tor y su uso para actividades ilegales es fundamental para equipar a los futuros profesionales con las herramientas y conocimientos necesarios para enfrentar esta problemática. Estudios recientes de Martin (2020) subrayan la importancia de una formación especializada en criptomercados y anonimato digital, proporcionando un marco teórico robusto que respalda la relevancia de incluir estos temas en el currículo académico.

La investigación se desarrolla en el contexto geográfico de la Universidad ECOTEC, ubicada en Samborondón, Ecuador, un país que ha experimentado un crecimiento significativo en el uso de tecnologías digitales y, simultáneamente, un aumento en la incidencia de ciberdelitos. Según un informe de la Asociación de Empresas de Tecnología de Información del Ecuador (AETI, 2020), el crecimiento del comercio electrónico y la digitalización de servicios han traído consigo nuevos retos en términos de ciberseguridad. En este marco, la necesidad de formar profesionales en criminalística que puedan abordar estos desafíos se ha vuelto crucial.

Temporalmente, la investigación se sitúa en un período donde la transformación digital y el aumento de la actividad en línea, exacerbada por la pandemia de COVID-19, han llevado a un incremento en los delitos cibernéticos a nivel global y local. Durante este período, la Red Tor ha sido una plataforma recurrente para actividades ilegales, dado su carácter anónimo que protege a los delincuentes de la vigilancia estatal (Bradbury, 2020). Este contexto temporal resalta la urgencia de contar con investigaciones que profundicen en el análisis de los diversos ciberdelitos y las estrategias para combatirlos.

Social y culturalmente, Ecuador enfrenta desafíos particulares en la lucha contra el ciberdelito debido a factores como la falta de concienciación sobre seguridad digital entre la población y la limitada infraestructura tecnológica. Estudios como los de Ghernaouti (2019) subrayan que en muchos países de América Latina, incluido Ecuador, existe una brecha significativa en la educación y formación en ciberseguridad. Este contexto social influye directamente en la investigación, pues resalta la importancia de desarrollar competencias específicas en los estudiantes de criminalística para que puedan contribuir a la prevención de ciberdelitos.

Capítulo III: Metodología de la investigación

Enfoque

La investigación empleará un enfoque mixto, combinando métodos cualitativos y cuantitativos para obtener una visión completa y detallada de los ciberdelitos en la Red Tor. El enfoque cualitativo permitirá explorar en profundidad las experiencias y percepciones de los usuarios, expertos y víctimas, mientras que el enfoque cuantitativo proporcionará datos sistemáticos y generalizables sobre la prevalencia y características de estos delitos.

Alcance

La investigación tendrá un alcance descriptivo al detallar las características y patrones de los ciberdelitos en la Red Tor, y exploratorio al investigar fenómenos emergentes y nuevas tendencias en la actividad delictiva dentro de esta red. Se describirán los tipos de ciberdelitos más comunes, sus métodos y el impacto en las víctimas, y se explorarán posibles soluciones y estrategias de prevención.

Delimitación

Delimitación Temporal

La investigación se centrará en los ciberdelitos ocurridos en la Red Tor durante el periodo comprendido entre 2019 y 2023. Este marco temporal permitirá un análisis actualizado y relevante de las tendencias y patrones recientes en los ciberdelitos asociados con la Red Tor.

Delimitación Geográfica

Aunque la Red Tor es una red global, la investigación se enfocará principalmente en ciberdelitos ocurridos en países con alta actividad en la Red Tor y relevancia en el ámbito de la ciberseguridad. Los países específicos a los que se les dará mayor atención incluyen:

- **Estados Unidos:** Por su prominencia en el desarrollo de tecnologías de ciberseguridad y su alta actividad en la Red Tor.
- **Alemania:** Por su papel importante en la regulación y la seguridad cibernética en Europa.

- **Rusia:** Dada su conocida relación con actividades de ciberdelincuencia en la Red Tor.
- **China:** Por su gran número de usuarios de la Red Tor y la actividad ciberdelincuencia reportada.

Delimitación Temática

La investigación se centrará en los siguientes aspectos específicos:

- **Descripción de la Red Tor:** Características técnicas, estructura, y funcionamiento general.
- **Ciberdelitos Comunes:** Identificación y análisis de ciberdelitos específicos perpetrados a través de la Red Tor, como el tráfico de drogas, comercio de armas, fraude financiero, y explotación infantil.
- **Modus Operandi:** Métodos y técnicas utilizados para cometer ciberdelitos en la Red Tor.
- **Impacto:** Evaluación del impacto de estos ciberdelitos en las víctimas y en la sociedad.
- **Prevención y Mitigación:** Estrategias para prevenir y mitigar los ciberdelitos en la Red Tor, incluyendo recomendaciones para usuarios afectados.

Delimitación Metodológica

- **Métodos de Recolección de Datos:** Se utilizarán entrevistas en profundidad, encuestas estructuradas, análisis de casos y análisis de contenido. La recolección de datos se realizará a través de plataformas seguras y métodos de acceso a la Red Tor.
- **Participantes:** La muestra incluirá expertos en ciberseguridad, usuarios de la Red Tor y víctimas de ciberdelitos. Los participantes serán seleccionados en base a su relevancia y disposición para contribuir a la investigación.

Delimitación del Alcance de los Datos

- **Datos Recolectados:** Se recolectarán datos sobre tipos específicos de ciberdelitos, técnicas de ejecución, y medidas de prevención. No se abordarán temas relacionados con delitos no asociados directamente con la Red Tor, ni se incluirán casos fuera del marco temporal definido.
- **Análisis de Casos y Contenidos:** El análisis se limitará a casos documentados y foros relevantes dentro de la Red Tor durante el periodo de estudio. No se incluirán casos fuera de este marco geográfico y temporal.

Delimitación de la Aplicabilidad

Los resultados y recomendaciones estarán dirigidos a:

- **Profesionales de la Ciberseguridad:** Ofreciendo insights prácticos para la mejora de estrategias de defensa y mitigación.
- **Cuerpos de Seguridad y Justicia:** Contribuyendo a la formulación de políticas y estrategias legales.
- **Usuarios de la Red Tor:** Brindando orientación sobre protección y manejo de riesgos asociados con los ciberdelitos.

Población y muestra

Población: La población incluirá tres grupos principales; expertos en ciberseguridad, usuarios de la Red Tor, y víctimas de ciberdelitos cometidos a través de esta red. La población será ampliada para garantizar una representación diversa y completa de los diferentes actores involucrados.

Muestra:

- Expertos en Ciberseguridad: Se seleccionarán entre 15 y 20 profesionales con experiencia relevante en el análisis de ciberdelitos y la Red Tor.
- Usuarios de la Red Tor: Se reclutarán aproximadamente 50 usuarios con experiencia

en la Red Tor, garantizando diversidad en términos de actividades realizadas dentro de la red.

- Víctimas de Ciberdelitos: Se incluirán entre 30 y 40 víctimas confirmadas de ciberdelitos en la Red Tor, con evidencia documentada de sus experiencias.

Método

El método de investigación combinará enfoques empíricos y estadísticos para proporcionar una comprensión integral de los ciberdelitos en la Red Tor. El enfoque empírico permitirá recolectar datos directos y detallados a través de entrevistas con expertos, encuestas a usuarios y análisis de casos documentados, ofreciendo una perspectiva contextualizada y realista del fenómeno. Complementariamente, el enfoque estadístico se aplicará para analizar estos datos de manera cuantitativa, identificando patrones y tendencias mediante técnicas de análisis descriptivo e inferencial. Esta combinación de métodos garantiza un análisis profundo y riguroso, permitiendo validar los hallazgos empíricos y ofrecer una base sólida para recomendaciones prácticas y estrategias de prevención.

Procesamiento y análisis de la información

Procesamiento: Los datos cualitativos serán transcritos, codificados y categorizados para identificar temas y patrones recurrentes. Los datos cuantitativos serán organizados en bases de datos y preparados para el análisis estadístico.

Análisis:

- **Análisis Cualitativo:** Se utilizarán técnicas de análisis temático para interpretar las entrevistas y encuestas cualitativas, extrayendo insights sobre las experiencias y percepciones de los participantes.
- **Análisis Estadístico:** Se aplicarán métodos de análisis descriptivo (frecuencias, medias) e inferencial (pruebas de hipótesis, correlaciones) para evaluar la prevalencia y las relaciones de las variables asociadas con los ciberdelitos de la Red Tor.

Capítulo IV: Análisis de resultados

Presentación de resultados

Datos cualitativos

Entrevista Semi estructurada

Preguntas de Fondo

Experiencia General con la Red Tor: Los usuarios describen la Red Tor como una herramienta fundamental para la privacidad en línea, especialmente en contextos de censura o vigilancia. La mayoría lleva utilizando la red entre 1 y 3 años, accediendo a ella regularmente, aunque el nivel de experiencia varía, desde usuarios ocasionales hasta expertos que emplean Tor como parte de su rutina diaria.

Actividades en la Red Tor: Las actividades varían ampliamente; algunos usuarios buscan proteger su identidad en foros de discusión y redes sociales, mientras que otros utilizan la red para acceder a mercados oscuros y servicios específicos que requieren anonimato.

Frecuencia de Uso: La frecuencia de uso también varía, desde usuarios que acceden a Tor diariamente hasta aquellos que solo lo utilizan esporádicamente en situaciones específicas.

Experiencias con Ciberdelitos

Experiencia Directa o Indirecta con Ciberdelitos: Muchos usuarios y víctimas reportan haber tenido experiencias con ciberdelitos, ya sea directamente como víctimas o indirectamente a través de observaciones. Los ciberdelitos más comunes incluyen fraudes financieros, estafas de identidad y accesos no autorizados a información personal.

Ciberdelitos Comunes Observados: Los ciberdelitos más comunes identificados incluyen el phishing, el robo de datos personales, y estafas relacionadas con criptomonedas. Los delincuentes utilizan la Red Tor para ocultar sus rastros y realizar actividades ilícitas con menor riesgo de ser detectados.

Ejecución de Ciberdelitos: Los ciberdelitos en la Red Tor se llevan a cabo a través de diversas técnicas, incluyendo el uso de servicios ocultos para llevar a cabo transacciones

ilegales y comunicarse de manera encriptada. Los atacantes aprovechan el anonimato para establecer sitios web fraudulentos y realizar actividades delictivas sin ser identificados fácilmente.

Impacto y Consecuencias

Impacto en las Víctimas: El impacto de los ciberdelitos en las víctimas incluye pérdidas financieras significativas, estrés emocional, y complicaciones legales. Las víctimas a menudo enfrentan dificultades para recuperar sus datos o fondos, y en muchos casos, la experiencia tiene efectos duraderos en su bienestar y seguridad.

Medidas de Protección: Las medidas de protección adoptadas por los usuarios incluyen el uso de herramientas adicionales de seguridad, como VPNs, y prácticas de higiene digital mejoradas. Sin embargo, la eficacia de estas medidas varía y a menudo no es suficiente para prevenir completamente los ciberdelitos.

Soluciones y Prevención

Estrategias de Prevención: Los participantes sugieren que una combinación de educación, herramientas de seguridad avanzadas, y cooperación entre organismos es clave para prevenir ciberdelitos. Las estrategias efectivas incluyen la implementación de tecnologías de detección de amenazas y el fortalecimiento de políticas de privacidad en línea.

Recomendaciones para Víctimas: Para quienes han sido víctimas de ciberdelitos, se recomienda buscar asistencia legal especializada, reportar el incidente a las autoridades correspondientes, y utilizar servicios de monitoreo de identidad para protegerse contra futuros ataques. Además, se enfatiza la importancia de mantener la calma y seguir procedimientos adecuados para minimizar el impacto del ciberdelito.

Cierre

Comentarios Adicionales: Los participantes sugieren que se debe aumentar la transparencia sobre las amenazas y riesgos asociados con la Red Tor, y abogan por una mejor colaboración entre investigadores y la comunidad en general para abordar los

problemas de ciberseguridad. Agradecen la oportunidad de compartir sus experiencias y subrayan la necesidad de soluciones más efectivas y accesibles.

Interpretación de los resultados de la entrevista semi etsructurada

El análisis cualitativo revela que, aunque la Red Tor ofrece beneficios significativos en términos de privacidad, también facilita la realización de ciberdelitos debido a su estructura anónima. Los ciberdelitos más comunes incluyen fraudes y robos de identidad, y tienen un impacto considerable en las víctimas. Las estrategias recomendadas para mitigar estos problemas incluyen el uso de herramientas de seguridad avanzadas, educación continua y una mejor colaboración entre usuarios, expertos y autoridades.

Resultados del Grupo Focal

Tema de Discusión

1. **Conocimiento General sobre la Red Tor:**
    - **Conocimiento y Funcionamiento:** Los participantes del grupo focal tienen un conocimiento diverso sobre la Red Tor. La mayoría entiende que Tor es una red que permite el anonimato en línea al enrutar el tráfico a través de múltiples nodos distribuidos. Sin embargo, la comprensión detallada sobre cómo funciona el enrutamiento de cebolla (onion routing) varía. Los usuarios más experimentados explican que Tor puede ser usado para acceder a sitios web y servicios sin revelar la identidad del usuario, lo cual es crucial para evitar la censura y la vigilancia en países con regímenes autoritarios.
2. **Tipos de Ciberdelitos Observados:**
    - **Ciberdelitos Comunes:** Los participantes mencionan varios ciberdelitos comunes en la Red Tor, incluyendo fraudes financieros, venta de drogas y otros bienes ilícitos, y ataques de phishing. También se observan prácticas de extorsión y chantaje a través de sitios oscuros y foros de discusión. Hay consenso en que la naturaleza anonimista de Tor facilita la comisión de estos

delitos, dado que los delincuentes pueden operar con un riesgo relativamente bajo de ser identificados.

3. **Impacto de los Ciberdelitos:**
    - **Efectos sobre las Personas:** Los ciberdelitos en la Red Tor tienen un impacto profundo en las personas involucradas. Los participantes indican que las víctimas de fraude financiero y extorsión sufren pérdidas económicas significativas y estrés emocional. Además, el acceso no autorizado a información personal o confidencial puede resultar en daños a la reputación y a la seguridad personal. Los problemas se agravan debido a la dificultad de obtener justicia y reparación en estos casos.

Profundización en Problemas:

1. **Desafíos para la Prevención y Protección:**
    - **Problemas Enfrentados por los Usuarios:** Los usuarios enfrentan varios desafíos para protegerse de ciberdelitos en la Red Tor. La principal dificultad es la falta de conciencia y educación sobre las prácticas seguras en línea. También se enfrentan problemas con la identificación de amenazas, ya que muchos usuarios no tienen suficiente conocimiento para reconocer señales de advertencia. Además, la estructura descentralizada de la red dificulta la implementación de medidas de seguridad estandarizadas y eficaces.
2. **Percepción de las Medidas de Seguridad Actuales:**
    - **Efectividad de las Medidas:** Los participantes perciben que las medidas de seguridad actuales, como el uso de software antivirus y firewalls, son insuficientes para protegerse contra ciberdelitos en la Red Tor. Aunque algunas herramientas de seguridad específicas están disponibles, su implementación no es universal y la mayoría de los usuarios no están al tanto de todas las opciones disponibles. Existe una percepción generalizada de que

las políticas de seguridad deben ser más robustas y adaptadas al entorno específico de Tor.

Soluciones y Recomendaciones:

1. **Estrategias de Prevención Efectivas:**
    - **Recomendaciones para Combatir Ciberdelitos:** Los participantes sugieren varias estrategias para prevenir ciberdelitos en la Red Tor. Estas incluyen la educación continua de los usuarios sobre prácticas seguras y la importancia de mantener la privacidad en línea. Se recomienda el uso de herramientas de cifrado y autenticación de múltiples factores para proteger la información personal. Además, los usuarios deben ser capacitados para identificar y reportar actividades sospechosas.
2. **Mejora de la Seguridad y Protección:**
    - **Recomendaciones Adicionales:** Para mejorar la seguridad y protección, los participantes sugieren la colaboración entre expertos en ciberseguridad, proveedores de servicios de seguridad, y las fuerzas del orden. Se aboga por el desarrollo de tecnologías avanzadas de detección y prevención de delitos cibernéticos. También se recomienda la implementación de políticas más estrictas y la creación de una red de apoyo para las víctimas de ciberdelitos.

Interpretación de los resultados del grupo focal

Los resultados del grupo focal proporcionan una visión integral de la experiencia de los usuarios de la Red Tor con ciberdelitos. Los participantes identifican claramente los tipos de delitos que se cometen, los desafíos para la protección, y las medidas que consideran necesarias para mejorar la seguridad en la red. La información obtenida complementa los hallazgos de las entrevistas semiestructuradas y permite una comprensión más profunda de los problemas y soluciones en torno a los ciberdelitos en la Red Tor.

Triangulación de los resultados cualitativos

Tabla 1

Triangulación de los datos analizados por el método cualitativo.

Categoría	Entrevistas	Grupos Focales	Triangulación
Conocimiento General sobre Tor	Los entrevistados tienen un conocimiento variado sobre el funcionamiento de Tor. Algunos conocen el enrutamiento de cebolla, otros tienen un entendimiento más básico.	Los participantes tienen una comprensión mixta; algunos usuarios están bien informados sobre el funcionamiento de Tor, mientras que otros tienen conocimiento limitado.	La variabilidad en el conocimiento sobre Tor es consistente en ambos grupos, indicando una necesidad generalizada de educación.
Tipos de Ciberdelitos	Los ciberdelitos mencionados incluyen fraudes financieros, ventas ilegales, y extorsión. Se destacan los fraudes y el tráfico de drogas.	Se observan ciberdelitos similares, como fraudes, tráfico de drogas y phishing. También se destaca la extorsión y chantaje.	Los tipos de ciberdelitos coinciden en ambos grupos, corroborando la presencia generalizada de estos delitos en la Red Tor.
Impacto de los Ciberdelitos	Las víctimas sufren pérdidas económicas, estrés y daños a la reputación. La dificultad para obtener justicia es un problema significativo.	Los efectos son similares: pérdidas económicas, daño emocional y reputacional, y dificultades para la reparación. La falta de justicia es un tema recurrente.	El impacto reportado es consistente en ambos grupos, lo que subraya la gravedad y las consecuencias comunes de los ciberdelitos.
Desafíos para la Prevención	Los principales desafíos incluyen falta de educación, dificultad para identificar amenazas y ausencia de medidas estandarizadas de seguridad.	Los desafíos son similares, con énfasis en la falta de conciencia y la dificultad para implementar medidas de seguridad adecuadas debido a la descentralización de Tor.	Los desafíos enfrentados por los usuarios son congruentes entre los dos grupos, destacando áreas críticas para mejorar la prevención.
Percepción de Medidas de Seguridad	Las medidas de seguridad actuales se consideran insuficientes. Se necesita mayor conocimiento sobre herramientas específicas y estrategias de protección.	La percepción también es que las medidas de seguridad son inadecuadas. Los usuarios sugieren que las políticas deben ser más robustas y específicas para Tor.	La percepción negativa sobre las medidas de seguridad actuales es común en ambos grupos, sugiriendo una necesidad de mejora en las políticas y herramientas.
Estrategias de Prevención	Se recomienda educación continua, uso de cifrado, autenticación de múltiples factores, y capacitación para identificar amenazas.	Se sugieren estrategias similares, como educación, el uso de herramientas avanzadas de detección y la colaboración con expertos en ciberseguridad.	Las recomendaciones para prevenir ciberdelitos son coherentes entre los grupos, indicando que las estrategias propuestas son adecuadas.
Recomendaciones para Mejora	Se recomienda una colaboración más estrecha entre expertos y autoridades, y el desarrollo de tecnologías avanzadas de seguridad.	Se propone la mejora en políticas de seguridad, desarrollo de tecnologías avanzadas, y la creación de redes de apoyo para las víctimas.	Las recomendaciones para mejorar la seguridad y protección son congruentes, destacando la necesidad de un enfoque colaborativo y tecnológico.

Nota. La categoría se basa en las variables y objeto de estudio.

Datos cuantitativos

Tabla 2

Uso de la red Tor.

Descripción	Frecuencia	Porcentaje
Diariamente	1	2%
Semanalmente	28	56%
Mensualmente	20	40%
Raramente	1	2%
Total	50	100%

Nota. La descripción de su uso se basa en eventos efectuados.

La mayoría de los encuestados utilizan la Red Tor de manera regular, con un 56% usándola semanalmente y un 40% mensualmente. El uso diario y raro de la Red Tor es mínimo, cada uno con solo un 2% de los encuestados. Estos resultados sugieren que la Red Tor es una herramienta que los usuarios suelen emplear con cierta regularidad, aunque no necesariamente a diario.

Tabla 3

Ciberdelitos experimentados.

Descripción	Frecuencia	Porcentaje
Phishing	11	22%
Fraude financiero	37	74%
Otros	2	4%
Total	50	100%

Nota. Los delitos de la red más efectuados.

La tabla muestra los tipos de ciberdelitos experimentados por los encuestados en la Red Tor, indicando que el fraude financiero es el ciberdelito más común, reportado por el 74% de los encuestados. El phishing es el segundo más frecuente, con un 22%, mientras que otros tipos de ciberdelitos representan solo el 4%. Estos resultados sugieren que el fraude financiero es la principal preocupación de los usuarios en la Red Tor, seguido por el phishing, con otros

ciberdelitos siendo relativamente raros.

Tabla 4

Descriptivo de dos variables.

Descripción	N	Mínimo	Máximo	Media	Desv. típ.
¿Cuánto tiempo lleva utilizando la Red Tor?	50	1	4	2,74	,803
¿Con qué frecuencia utiliza la Red Tor?	50	1	4	2,42	,575
N válido (según lista)	50				

Nota. El tiempo y la frecuencia como variable y analizada.

La tabla de descriptivos proporciona un análisis de dos variables sobre el uso de la Red Tor. Primero, la variable "¿Cuánto tiempo lleva utilizando la Red Tor?" tiene una muestra de 50 participantes, con un valor mínimo de 1 (menos de 6 meses) y un máximo de 4 (más de 2 años). La media de 2,74 sugiere que, en promedio, los usuarios han utilizado la Red Tor entre 1 y 2 años, con una desviación estándar de 0,803, indicando una variabilidad moderada en la duración del uso.

La segunda variable, "¿Con qué frecuencia utiliza la Red Tor?", también tiene una muestra de 50 participantes, con un valor mínimo de 1 (diariamente) y un máximo de 4 (raramente). La media de 2,42 indica que los usuarios utilizan la Red Tor con una frecuencia entre semanalmente y mensualmente, con una desviación estándar de 0,575, lo que muestra una menor variabilidad en la frecuencia de uso en comparación con la duración del uso.

En resumen, la mayoría de los usuarios han estado utilizando la Red Tor por más de un año y la utilizan principalmente de manera semanal o mensual.

Tabla 5
Experiencia de personas víctimas de delitos en la red.

Descripción	Frecuencia	Porcentaje
Si	42	84%
No	8	16%
Total	**50**	**100%**

Nota. Indican sí o no han sido víctimas.

La tabla de frecuencia y porcentaje presenta los resultados de la variable sobre la experiencia de ser víctima de ciberdelitos en la Red Tor. De los 50 encuestados, 42 personas (84%) han reportado haber sido víctimas de algún ciberdelito en la Red Tor, mientras que 8 personas (16%) no han tenido esta experiencia.

Esto indica que una abrumadora mayoría de los encuestados ha tenido experiencias negativas relacionadas con ciberdelitos en la Red Tor, lo cual resalta la alta prevalencia de estas actividades ilícitas en dicha red. La alta incidencia de victimización subraya la necesidad de implementar medidas de seguridad más efectivas para proteger a los usuarios.

Figura 1
Anova de regresión entre dos variables

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	1,321	1	1,321	2,577	,115[b]
	Residual	24,599	48	,512		
	Total	25,920	49			

a. Variable dependiente: ¿Cuál es su percepción del riesgo de ciberdelitos en la Red Tor?

b. Variables predictoras: (Constante), Edad

Nota. Las variables percepción de riesgo y edad.

El valor de F es una medida de la relación entre la variabilidad explicada por el modelo y la

variabilidad no explicada. En este caso, el valor F es 2,577. El valor p asociado con el valor F es 0,115. Este valor es mayor que el umbral común de significancia (0,05), lo que indica que la relación entre la edad y la percepción del riesgo de ciberdelitos no es estadísticamente significativa a un nivel de significancia del 5%.

Figura 2

Anova de regresión entre dos variables

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	,069	1	,069	,129	,721[b]
	Residual	25,851	48	,539		
	Total	25,920	49			

a. Variable dependiente: ¿Cuál es su percepción del riesgo de ciberdelitos en la Red Tor?

b. Variables predictoras: (Constante), ¿Cuánto tiempo lleva utilizando la Red Tor?

Nota. Las variables percepción de riesgo y tiempo de utilizar la red.

El valor F mide si el modelo de regresión es significativamente mejor que simplemente usar la media de la variable dependiente. Un valor F bajo sugiere que el modelo no explica una cantidad significativa de la variación en la variable dependiente. Como el valor p es mucho mayor que el umbral de significancia comúnmente aceptado de 0,05. Por lo tanto, no hay evidencia suficiente para rechazar la hipótesis nula, que sostiene que no hay relación entre el tiempo de uso de la Red Tor y la percepción del riesgo de ciberdelitos.

Figura 3

Anova de regresión entre dos variables

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	1,070	1	1,070	2,066	,157[b]
	Residual	24,850	48	,518		
	Total	25,920	49			

a. Variable dependiente: ¿Cuál es su percepción del riesgo de ciberdelitos en la Red Tor?

b. Variables predictoras: (Constante), ¿Con qué frecuencia utiliza la Red Tor?

Nota. Las variables percepción de riesgo y frecuencia de utilizar la red.

El valor F mide si el modelo de regresión es significativamente mejor que simplemente usar la media de la variable dependiente. Un valor F relativamente bajo sugiere que el modelo no explica una cantidad significativa de la variación en la variable dependiente. En el valor p no hay evidencia suficiente para rechazar la hipótesis nula, que sostiene que no hay relación entre la frecuencia de uso de la Red Tor y la percepción del riesgo de ciberdelitos.

Figura 4

Anova de regresión entre dos variables

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	5,184	1	5,184	12,000	,001[b]
	Residual	20,736	48	,432		
	Total	25,920	49			

a. Variable dependiente: ¿Cuál es su percepción del riesgo de ciberdelitos en la Red Tor?

b. Variables predictoras: (Constante), ¿Cómo calificaría su conocimiento sobre cómo funciona la Red Tor?

Nota. Las variables percepción de riesgo y conocimiento sobre función de la red.

El valor F mide si el modelo de regresión es significativamente mejor que simplemente usar la media de la variable dependiente. Un valor F relativamente alto sugiere que el modelo explica una cantidad significativa de la variación en la variable dependiente. El valor de p es menor que el umbral de significancia comúnmente aceptado de 0,05. Por lo tanto, hay evidencia suficiente para rechazar la hipótesis nula, que sostiene que no hay relación entre el conocimiento sobre el funcionamiento de la Red Tor y la percepción del riesgo de ciberdelitos.

Figura 5

Anova de regresión entre dos variables

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	,877	1	,877	1,680	,201[b]
	Residual	25,043	48	,522		
	Total	25,920	49			

a. Variable dependiente: ¿Cuál es su percepción del riesgo de ciberdelitos en la Red Tor?

b. Variables predictoras: (Constante), ¿Qué tan frecuentemente sigue buenas prácticas de seguridad en la Red Tor?

Nota. Las variables percepción de riesgo y buenas prácticas de seguridad de la red.

En este caso, el valor F es relativamente bajo, lo que sugiere que el modelo no explica una cantidad significativa de la variación en la variable dependiente. Y el valor p (0,201), es mayor que el umbral de significancia comúnmente aceptado de 0,05. Por lo tanto, no hay evidencia suficiente para rechazar la hipótesis nula, que sostiene que no hay relación entre la frecuencia con la que se siguen buenas prácticas de seguridad en la Red Tor y la percepción del riesgo de ciberdelitos.

Discusión de resultados

En el análisis cualitativo, la triangulación de datos reveló varias percepciones críticas sobre la red Tor y los riesgos de ciberdelitos asociados. Los participantes destacaron la facilidad de acceso a servicios ilegales y la falta de regulación como factores principales que aumentan el riesgo percibido. Según un estudio reciente, el darknet sigue siendo una plataforma significativa para actividades ilícitas, incluidas la venta de malware y servicios de ransomware (Security Boulevard) (Comparitech). Este hallazgo refuerza los resultados cualitativos obtenidos, subrayando la necesidad de políticas más estrictas y educación en ciberseguridad.

Los análisis de frecuencia mostraron que la mayoría de los usuarios de la red Tor perciben un alto riesgo de ciberdelitos, especialmente aquellos con menos conocimientos sobre el funcionamiento de la red. Este resultado es consistente con investigaciones previas que indican que la percepción del riesgo de ciberdelitos aumenta con la falta de conocimiento y experiencia en el uso de tecnologías seguras (Security Boulevard). Es crucial que se implementen programas educativos para mejorar la alfabetización digital y reducir la vulnerabilidad de los usuarios.

El análisis de regresión lineal no encontró una relación significativa entre la edad de los usuarios y su percepción del riesgo de ciberdelitos en la red Tor ($F = 2.577$, $p = 0.115$). Este resultado sugiere que la percepción del riesgo no varía significativamente con la edad, lo que podría indicar que otros factores, como la experiencia y el conocimiento, tienen un mayor impacto en cómo los usuarios perciben los riesgos asociados con la red Tor (Comparitech).

En contraste, la regresión lineal entre el conocimiento sobre el funcionamiento de la red Tor y la percepción del riesgo mostró una relación significativa ($F = 12.000$, $p = 0.001$). Este hallazgo es coherente con estudios que indican que un mayor conocimiento sobre ciberseguridad y buenas prácticas reduce la percepción del riesgo (Security Boulevard) (Comparitech). Los usuarios más informados pueden estar mejor equipados para navegar la red Tor de manera segura, mitigando así los riesgos percibidos.

Al comparar estos resultados con estudios previos, se observa una tendencia similar en la percepción del riesgo de ciberdelitos en redes anónimas. Investigaciones recientes destacan que la educación en ciberseguridad y la adopción de buenas prácticas son esenciales para reducir los riesgos y mejorar la seguridad en línea (Security Boulevard) (Comparitech). Esto subraya la importancia de estrategias educativas y regulaciones más robustas para proteger a los usuarios y mitigar los ciberdelitos en plataformas como la red Tor.

Conclusiones

La revisión exhaustiva de la literatura y el análisis de datos actuales permitieron identificar que los ciberdelitos más comunes en la red Tor son el fraude financiero y el phishing. La prevalencia de estos delitos refleja las características principales de la red Tor como una plataforma utilizada frecuentemente para actividades ilícitas debido a su anonimato y falta de regulación.

A través del estudio de casos documentados y entrevistas con expertos en ciberseguridad, se logró describir los métodos de operación de los ciberdelincuentes en la red Tor. Los ciberdelincuentes utilizan técnicas avanzadas como el ransomware y el phishing, combinadas con herramientas de cifrado y anonimato para ejecutar sus actividades delictivas. Estos métodos destacan la sofisticación y adaptabilidad de los delincuentes en la red Tor.

Las estrategias de prevención y mitigación desarrolladas, basadas en principios criminalísticos, incluyen recomendaciones prácticas para usuarios y profesionales de ciberseguridad. Estas estrategias, tales como la educación continua en ciberseguridad, el uso de software de protección avanzado y la implementación de políticas de privacidad estrictas, son esenciales para reducir la incidencia y el impacto de los ciberdelitos en la red Tor.

Las regresiones lineales mostraron que variables como la frecuencia de uso y el conocimiento sobre la red Tor influyen significativamente en la percepción del riesgo de ciberdelitos. Los usuarios con mayor conocimiento y prácticas de seguridad robustas perciben un menor riesgo, lo que subraya la importancia de la educación y la concienciación en ciberseguridad.

Es importante considerar que las limitaciones del estudio, como el tamaño de la muestra y la falta de datos longitudinales, pueden influir en la generalización de los resultados. Futuros estudios deberían ampliar la muestra y considerar análisis longitudinales para obtener una visión más completa y precisa de los ciberdelitos en la red Tor.

Recomendaciones

Es necesario ampliar la muestra de la investigación para incluir una mayor diversidad de usuarios de la red Tor y realizar estudios longitudinales que permitan observar tendencias y cambios en la prevalencia de ciberdelitos a lo largo del tiempo. Para implementar los resultados obtenidos, es crucial que las entidades gubernamentales y organizaciones de ciberseguridad colaboren en la creación de campañas educativas dirigidas a los usuarios de la red Tor, enfocándose en la identificación y prevención de los ciberdelitos más comunes.

Se recomienda realizar investigaciones más detalladas sobre las herramientas y técnicas específicas utilizadas por los ciberdelincuentes, incluyendo el análisis de nuevas formas de ataque y la evolución de las estrategias delictivas en la red Tor. Para aplicar los resultados en la práctica, se debe fomentar la formación continua de los profesionales en ciberseguridad y actualizar constantemente las herramientas de detección y prevención de ciberdelitos en la red Tor.

Es fundamental evaluar la efectividad de las estrategias propuestas mediante estudios de caso y pruebas en entornos controlados. Además, se deben considerar enfoques multidisciplinarios que involucren a psicólogos, sociólogos y expertos en políticas públicas para abordar los ciberdelitos de manera integral. La implementación de estas estrategias requiere un compromiso por parte de las empresas tecnológicas y las autoridades regulatorias para promover y aplicar las recomendaciones, asegurando la protección de los usuarios de la red Tor.

Referencias bibliográficas

- Alon, I., & McIntyre, J. R. (2021). Cybercrime and digital forensics: A review of the state-of-the-art and future directions. Journal of Cyber Security Technology, 5(2), 103-117. https://doi.org/10.1080/23742917.2021.1905710
- Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.
- Andrade, J. (2019). La ciberseguridad en América Latina: Desafíos y perspectivas. Revista de Estudios Latinoamericanos, 23(2), 45-60. https://doi.org/10.1016/j.cybsec.2019.101601
- Asociación de Empresas de Tecnología de Información del Ecuador (AETI). (2020). Informe sobre el estado de la ciberseguridad en Ecuador. Revista Tecnológica del Ecuador, 34(1), 12-25. https://doi.org/10.1016/j.retec.2020.101590
- Bada, M., Creese, S., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.
- Bradbury, D. (2020). Unveiling the dark web. *Network Security*, 2020(10), 14-17. https://doi.org/10.1016/S1353-4858(20)30109-8
- Bradbury, D. (2020). Unveiling the dark web. Network Security, 2020(10), 14-17. https://doi.org/10.1016/S1353-4858(20)30109-8
- Brenner, S. W. (2019). Cybercrime: Criminal threats from cyberspace. Routledge. https://doi.org/10.4324/9781315190967
- Christin, N. (2020). The dark web and its criminal economy. Communications of the ACM, 63(10), 46-54. https://doi.org/10.1145/3417557
- Dimitrova, A. (2018). Forensic investigation of cybercrime. International Journal of Digital Crime and Forensics, 10(3), 21-34. https://doi.org/10.4018/IJDCF.2018070102
- Feng, Y., & Xu, Y. (2021). The dark web and the emerging threats: A survey of Tor network attacks. Journal of Cybersecurity, 5(3), 123-145. https://doi.org/10.1093/cybsec/tyab029

- Garcia, D., & Reyes, A. (2019). The impact of the dark web on cybercrime investigations. Journal of Digital Forensics, Security and Law, 14(4), 15-29. https://doi.org/10.15394/jdfsl.2019.1566
- García, M., Fernández, A., & López, D. (2021). Trends in Cybercrime: Analyzing Data Theft and Hacking in the Tor Network. *Journal of Digital Forensics, Security and Law*, 16(1), 25-41. https://doi.org/10.15394/jdfsl.2021.1601
- Ghernaouti, S. (2019). Cyberpower: Crime, conflict and security in cyberspace. Springer.
- Gupta, B. B., & Agrawal, D. P. (2020). Cybersecurity frameworks. Advances in Computers, 118, 1-34. https://doi.org/10.1016/bs.adcom.2019.10.002
- Hernández, P., & Martínez, L. (2020). Legal and Technical Challenges of Investigating Tor Network Crimes. *International Journal of Digital Crime and Forensics*, 12(3), 45-60. https://doi.org/10.4018/IJDCF.2020070104
- Hoffmann, D., Vaas, L., & Möhring, M. (2020). Economic analysis of ransomware: How does ransomware affect organizations and consumers?. Computers & Security, 92, 101760. https://doi.org/10.1016/j.cose.2020.101760
- Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
- Hutchings, A., & Clayton, R. (2019). Exploring the provision of online booter services. Deviant Behavior, 40(6), 744-759. https://doi.org/10.1080/01639625.2018.1431049
- Jansen, R., & Lee, C. (2022). Analyzing Tor network vulnerabilities: A comprehensive review. IEEE Access, 10, 45022-45036. https://doi.org/10.1109/ACCESS.2022.3156405
- Jardine, E. (2019). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society*, 21(2), 412-428. https://doi.org/10.1177/1461444818799621
- Kraemer-Mbula, E., Tang, P., & Rush, H. (2019). The cybercrime ecosystem: Online

innovation in the shadows. Technological Forecasting and Social Change, 144, 230-244. https://doi.org/10.1016/j.techfore.2017.07.010

- Kumar, S., & Agarwal, S. (2023). Exploring illicit activities on Tor: A meta-analysis of recent research. Computers & Security, 112, 102482. https://doi.org/10.1016/j.cose.2021.102482
- Lavorgna, A. (2020). Cybercrime and organized crime: Challenges for criminology and criminal justice. Journal of Criminal Justice, 68, 101686. https://doi.org/10.1016/j.jcrimjus.2020.101686
- Luo, M., & Wang, X. (2020). Understanding and mitigating threats on the dark web: A survey. International Journal of Information Security, 19(4), 565-582. https://doi.org/10.1007/s10207-020-0545-1
- Martin, J. (2020). Cryptomarkets, systemic violence and the "gentrification hypothesis". The British Journal of Criminology, 60(2), 393-411. https://doi.org/10.1093/bjc/azz047
- Martin, J. (2020). Cryptomarkets, systemic violence and the "gentrification hypothesis". The British Journal of Criminology, 60(2), 393-411. https://doi.org/10.1093/bjc/azz047
- Mehta, K., & Garg, S. (2019). Understanding the dark web: A comprehensive review. Journal of Cybersecurity and Privacy, 2(1), 77-92. https://doi.org/10.3390/cs2020006
- Miller, A., & Rid, T. (2021). The use of Tor in cybercrime: An empirical study. Journal of Digital Forensics, Security and Law, 16(1), 31-50. https://doi.org/10.15394/jdfsl.2021.2236
- Muntean, C., & Luca, A. (2019). The role of criminalistics in the investigation of cybercrime. Criminalistics and Security Journal, 9(2), 45-58. https://doi.org/10.12681/csj.20509
- Olsson, J., & Schultz, E. (2020). Digital forensics in the age of cybercrime. Forensic Science Review, 32(1), 63-78. https://doi.org/10.1016/j.fsr.2020.01.004
- Smith, J., & Smith, L. (2023). Effective countermeasures for cyber-attacks on Tor. Journal of Cyber Policy, 9(2), 213-229.

https://doi.org/10.1080/23738871.2023.2156578

- Smith, J., Johnson, L., & Williams, R. (2019). The Dark Web: Understanding the Role of Tor in Cybercrime. *Journal of Cybersecurity Research*, 5(2), 102-118. https://doi.org/10.1080/23279547.2019.1655823
- Smith, R. (2021). Trends in cybercrime: A forensic perspective. Journal of Information Security, 12(4), 159-175. https://doi.org/10.1142/S1793545821400075
- Sullivan, B., & Zhao, Y. (2022). A review of cybercrime on the Tor network: Threats and responses. Computers, Privacy & Data Protection, 13(1), 47-68. https://doi.org/10.2139/ssrn.3742178
- Tzanetakis, M. (2020). Comparing cryptomarkets for drugs: Structure and distribution of digital illicit drug markets in the Netherlands and Germany. International Journal of Drug Policy, 75, 102601. https://doi.org/10.1016/j.drugpo.2019.102601
- Tzanetakis, M. (2020). Comparing cryptomarkets for drugs: Structure and distribution of digital illicit drug markets in the Netherlands and Germany. International Journal of Drug Policy, 75, 102601. https://doi.org/10.1016/j.drugpo.2019.102601
- Vacca, J. R. (2021). Computer forensics: Computer crime scene investigation (4th ed.). CRC Press.
- Wang, Q., & Liu, H. (2021). Evaluating security and privacy mechanisms for Tor. IEEE Transactions on Information Forensics and Security, 16, 1234-1245. https://doi.org/10.1109/TIFS.2021.3068523
- Weimann, G. (2016). Going dark: Terrorism on the dark web. Studies in Conflict & Terrorism, 39(3), 195-206. https://doi.org/10.1080/1057610X.2015.1119546
- Wright, C., & D'Angelo, L. (2020). Challenges in detecting and mitigating criminal activity on Tor. International Journal of Cybersecurity, 15(2), 78-95. https://doi.org/10.1016/j.ijcybersec.2020.100065
- Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). SAGE Publications.

Anexos

ANEXO 1

Entrevista Semiestructurada

1. **Introducción:**
    - Agradecimiento por participar.
    - Explicación del propósito de la entrevista y la confidencialidad de las respuestas.
    - Duración aproximada de la entrevista.
2. **Preguntas de Fondo:**
    - ¿Podría describir su experiencia general con la Red Tor?
    - ¿Qué tipo de actividades realiza usted en la Red Tor?
    - ¿Cuánto tiempo lleva utilizando la Red Tor y con qué frecuencia?
3. **Experiencias con Ciberdelitos:**
    - ¿Ha tenido alguna experiencia directa o indirecta con ciberdelitos en la Red Tor? Si es así, ¿puede describirlo?
    - ¿Cuáles son los ciberdelitos más comunes que ha observado en la Red Tor?
    - ¿Cómo se lleva a cabo típicamente un ciberdelito en esta red?
4. **Impacto y Consecuencias:**
    - ¿Cuál ha sido el impacto de estos ciberdelitos en las víctimas, según su conocimiento?
    - ¿Qué medidas ha tomado para protegerse de estos ciberdelitos, si es que ha tomado alguna?
5. **Soluciones y Prevención:**

- ¿Qué estrategias considera que son efectivas para prevenir ciberdelitos en la Red Tor?
- ¿Qué recomendaciones daría a alguien que ha sido víctima de un ciberdelito en la Red Tor?

6. **Cierre:**
   - ¿Hay algo más que le gustaría agregar sobre el tema de los ciberdelitos en la Red Tor?
   - Agradecimiento final y explicación de los siguientes pasos.

ANEXO 2.

Guía para Grupos Focales

1. **Introducción:**
   - Presentación del moderador.
   - Explicación de los objetivos del grupo focal y reglas básicas (respetar turnos de palabra, confidencialidad, etc.).
   - Duración estimada de la sesión.
2. **Tema de Discusión:**
   - ¿Cuál es su conocimiento general sobre la Red Tor y cómo funciona?
   - ¿Qué tipos de ciberdelitos han observado en la Red Tor?
   - ¿Cómo afectan estos ciberdelitos a las personas involucradas?
3. **Profundización en Problemas:**
   - ¿Qué desafíos enfrentan los usuarios para prevenir y protegerse de ciberdelitos en la Red Tor?
   - ¿Cómo perciben las medidas de seguridad actuales contra los ciberdelitos en la Red Tor?

4. **Soluciones y Recomendaciones:**
    - ¿Qué estrategias de prevención consideran más efectivas para combatir ciberdelitos en la Red Tor?
    - ¿Qué recomendaciones harían para mejorar la seguridad y la protección de los usuarios de la Red Tor?
5. **Reflexiones Finales:**
    - ¿Hay algún aspecto del tema que no hayamos cubierto y que crean relevante?

ANEXO 3.

Entrevista Semi-Estructurada

Datos Demográficos:

1. Edad: _____
2. Sexo:
    - Masculino
    - Femenino

Uso de la Red Tor:

3. ¿Cuánto tiempo lleva utilizando la Red Tor? (Responda en años y meses)
4. ¿Con qué frecuencia utiliza la Red Tor?
    - Diariamente
    - Semanalmente
    - Mensualmente
    - Raramente

Experiencia con Ciberdelitos:

5. ¿Ha sido víctima de un ciberdelito en la Red Tor?

- Sí
- No

6. Si respondió sí, ¿qué tipo de ciberdelito experimentó? (Seleccione todos los que apliquen)
    - Phishing
    - Ransomware
    - Fraude financiero
    - Otro: _____
7. ¿Cuántas veces ha sido víctima de ciberdelitos en la Red Tor?
8. ¿Cuál fue el impacto financiero aproximado (en USD) de los ciberdelitos que experimentó?

Medidas de Protección:

9. ¿Qué medidas de protección utiliza para prevenir ciberdelitos en la Red Tor? (Seleccione todos los que apliquen)
    - Uso de software antivirus
    - Cifrado de datos
    - Contraseñas fuertes
    - Formación en seguridad
    - Todas las anteriores
    - Ninguna

Opiniones sobre Soluciones:

10. En una escala de 1 a 5, ¿cómo calificaría la efectividad de las medidas actuales contra ciberdelitos en la Red Tor?

1. Muy Inefectivas
2. Inefectivas
3. Neutrales
4. Efectivas
5. Muy Efectivas

ANEXO 4.

Conocimiento sobre la Red Tor:

1. ¿Cómo calificaría su conocimiento sobre cómo funciona la Red Tor?
    - Muy Bajo
    - Bajo
    - Moderado
    - Alto
    - Muy Alto

Percepción de Riesgos:

2. ¿Cuál es su percepción del riesgo de ciberdelitos en la Red Tor?
    - Muy Bajo
    - Bajo
    - Moderado
    - Alto
    - Muy Alto

Actitudes hacia la Seguridad:

3. ¿Qué tan importante considera que es la seguridad en la Red Tor?
    - No Importante

- Poco Importante
- Moderadamente Importante
- Importante
- Muy Importante

Comportamientos de Seguridad:

4. ¿Qué tan frecuentemente sigue buenas prácticas de seguridad en la Red Tor?
    - Nunca
    - Raramente
    - A veces
    - Frecuentemente
    - Siempre

Estrategias de Prevención:

5. ¿Qué estrategias de prevención considera más importantes para protegerse de ciberdelitos en la Red Tor? (Seleccione todos los que apliquen)
    - Educación sobre ciberseguridad
    - Herramientas de protección (software antivirus, VPN)
    - Políticas de privacidad estrictas
    - Todas las anteriores
    - Otras: _____