UNIVERSIDAD EMPRESARIAL
SIGLO 21

TRABAJO FINAL DE GRADO.
MANUSCRITO CIENTIFICO

PREVENCION DEL DELITO Y LA VIOLENCIA: CIBERDELITO

LICENCIATURA EN CRIMINOLOGIA Y SEGURIDAD

AUTOR/A
LEYRIA, ANA PAULA

TUTOR DE TESIS: LIC. CASPANI, ANA CRUZ

RIO CUARTO, CORDOBA. NOVIEMBRE 2024

ÍNDICE

INTRODUCCIÓN **4**
Ciberdelitos **4**
Clasificación según la incidencia de las TIC en el comportamiento criminal 5
Ciberdelitos puros 6
Hacking 6
Malware 6
Ciberdelitos réplica 8
Ciberfraudes 9
El phishing 9
Ciberblanqueo de capitales 10
Ciberacoso 11
Ciberataques de contenido 12
Clasificación según el motivo del ciberataque 12
Ingenieria social 13
El ciberespacio **14**
Teorias criminológicas **16**
El ciberdelincuente **18**
Ciberdelincuentes especializados 20
Hackers 20
Ciberterrorista 21
Ciberdelincuente no especializado 22
El cibervándalo 22
Ciberdelincuentes insider y cibermula 24
Ciberhacktivista 26
El cribergroomer 27
La cibervíctima **29**
La mal llamada pornografia infantil 31
Marco Legal **35**
Convenio de budapest 38
Aplicación local en Córdoba 40
PLANTEAMIENTO DEL PROBLEMA **41**
OBJETIVOS **41**
Objetivo general 41
Objetivos específicos 42
PREGUNTAS DE INVESTIGACIÓN **42**
METODOLOGÍA **43**
Consideraciones Éticas 43
RESULTADOS **44**
DISCUSIÓN **48**
PREVENCIÓN CRIMINOLÓGICA **50**

REFERENCIAS **54**
ANEXOS **57**
Anexo 1. Experiencia personal **57**
Anexo 2. Encuesta n°1 58
Anexo 3. Encuesta n°2 59

RESUMEN En el siguiente trabajo final de grado fue abordado el fenómeno del ciberdelito desde una perspectiva criminológica, analizando cómo las dinámicas del ciberespacio facilitan la actividad delictiva y afectan tanto a cibervíctimas como a la seguridad digital. A través de encuestas realizadas, se identificaron los delitos más frecuentes y en crecimiento, destacando que muchos de ellos son sencillos y no requieren un gran conocimiento de informática por parte de los ciberdelincuentes. El trabajo profundiza en las características del ciberdelincuente y las estrategias preventivas aplicables, con énfasis en el marco normativo de Córdoba, Argentina. A lo largo del manuscrito, se deja en evidencia la necesidad de mejorar las políticas de prevención y sensibilización frente a este fenómeno en expansión.

Palabras claves: Ciberdelitos; ciberespacio; ciberdelincuente; cibervíctima; tecnología de la información y la comunicación

ABSTRACT In the following final degree project, the phenomenon of cybercrime was addressed from a criminological perspective, analyzing how the dynamics of cyberspace facilitate criminal activity and affect both cyber victims and digital security. Through surveys carried out, the most frequent and growing crimes were identified, highlighting that many of them are simple and do not require extensive computer knowledge on the part of cybercriminals. The work delves into the characteristics of the cybercriminal and the applicable preventive strategies, with emphasis on the regulatory framework of Córdoba, Argentina. Throughout the manuscript, the need to improve prevention and awareness policies against this expanding phenomenon is made evident.

Keywords: Cybercrimes; Cyberspace; cybercriminal; cyber victim; information and communication technology

INTRODUCCIÓN

Desde el descubrimiento del internet y el rápido avance tecnológico es indiscutible la infinita cantidad de beneficios que nos ha traído a nuestras vidas. No hay un solo aspecto de nuestra cotidianidad que no esté atravesado por las nuevas tecnologías de información y comunicación (TIC), permitiendo realizar un sinfín de actividades como son enviar correos, realizar videollamadas, búsqueda de información, acceder a todo tipo de material de entretenimiento, controlar cuentas bancarias, comprar y vender todo tipos de bienes y servicios, y todo esto al alcance de un simple clic en nuestras pantallas.

Pero, como los sistemas informáticos han transformado nuestro accionar habitual, los delitos también se han visto modificados, dado que la utilización de las TICs ha desbloqueado un nuevo lugar donde cometer infracciones por fuera del espacio físico, éste es llamado ciberespacio, término acuñado por primera vez por William Gibson en un relato de 1981.

Ciberdelitos

Es preciso expresar que "ciberdelito" es cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito. (Rayón Ballesteros y Gómez Hernández, 2014, pp3.)

En muchas ocasiones podemos referirnos como delito o crimen a un mismo hecho, pero este parafraseo sería equivocado, ya que, delito se utiliza más en un sentido general, y crimen, en uno más restrictivo, con lo cual todo crimen es un delito, pero no todo delito es un crimen. De esta manera se puede decir que ciberdelitos son todos aquellos delitos

concebidos desde una concepción general, mientras que el cibercrimen implica delitos que tienen mayor gravedad y que se cometen tanto como un medio para lograr un fin delictivo como un fin en sí mismo.

Esta modalidad delictiva es llevada adelante con la ayuda de programas maliciosos y tiene por fin suprimir, dañar, deteriorar, alterar u obtener datos informáticos y/o personales sin autorización, para poder sacar un rédito económico o simplemente causar algún daño.

El gran crecimiento de la tecnología acompañado de la dependencia que se fue generando en los individuos y empresas, permitió que diversos grupos se adapten y comiencen a llevar adelante esta modalidad delictiva. Ahora bien, partiendo de que el elemento común a todas las tipologías de conductas que situamos dentro del cibercrimen es la de que el ciberespacio es el ámbito en el cual las mismas se llevan a cabo podríamos clasificar a los ciberdelitos en dos tipos. Según la incidencia que tienen las TIC en el comportamiento criminal (puro, réplica y de contenido) o Según el motivo (económico, social, político).

Clasificación según la incidencia de las TIC en el comportamiento criminal

Dentro de la primera categoría encontramos a los ciberdelitos puros, son las acciones delictivas que solo pueden llevarse a cabo utilizando las TIC como medio de comisión ya que son acciones específicas que son únicamente posibles en el ciberespacio por no poseer una modalidad en el mundo físico. Luego tenemos los ataques réplica, su característica principal radica en el uso de las TIC como medio de comisión de delitos tradicionales ya previstos en una modalidad propia del mundo físico,por ende las acciones que se llevan a cabo en el plano virtual repercuten en el físico. Por último, los de contenido

que son los que enmarcan a la posesión y difusión de contenido audiovisual, es decir lo que condiciona a la clasificación es la ilicitud del mensaje o dato que el autor difunde a través de las TIC.

Ciberdelitos puros

En este tipo de ciberdelitos las TIC no sólo constituyen el medio comisivo de tales ataques, sino que son el único posible, en cuanto que son medio y objetivo, y no es posible producir la esencia de ilicitud de estas infracciones si no es en el ciberespacio. La problemática más propia se derivará de la total novedad de los comportamientos, con la consiguiente falta de estrategias preventivas de carácter criminológico frente a ellas, así como de la inexistencia de preceptos que permitan la incriminación de los mismos.

Hacking

Es la actividad de los hackers que consiste en la superación de cualquier barrera informática para acceder, manipular o explotar sistemas, redes y datos. Es decir, cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo, de una forma tal que tiene capacidad potencial de utilizar o acceder a cualquier tipo de información que esté en el sistema.

Malware

El malware (abreviatura de *malicious software*, o "software malicioso" en español) es un término que engloba cualquier tipo de programa o código diseñado para infiltrarse en sistemas informáticos, redes o dispositivos con fines dañinos, no autorizados o maliciosos. El objetivo de un malware puede variar desde robar información personal hasta dañar archivos y dispositivos, pasando por tomar el control de sistemas completos.

Existen muchos tipos de malware, cada uno con características y objetivos diferentes.

Virus:Un virus es un tipo de malware que se propaga al insertar su código en otros archivos o programas ejecutables. El virus se activa cuando el archivo infectado es ejecutado y puede hacer que se propague aún más, infectando otros archivos. Puede destruir o alterar archivos, robar información o ralentizar el sistema.

Troyano (Trojan Horse): El troyano es un malware que se disfraza de un programa legítimo o útil para engañar al usuario y hacer que lo instale. Una vez ejecutado, el troyano puede otorgar acceso remoto a un atacante, robar datos o incluso instalar otros tipos de malware. El objetivo es acceder al sistema y permitir a los atacantes realizar acciones sin el conocimiento del usuario.

Ransomware: El ransomware es un tipo de malware que cifra los archivos del usuario y exige un pago (generalmente en criptomonedas) para devolver el acceso a los archivos. En algunos casos, el ransomware también puede robar datos sensibles.

Spyware:El spyware es un software malicioso diseñado para espiar las actividades del usuario sin su consentimiento. El spyware puede capturar teclas presionadas, capturas de pantalla, historiales de navegación y otros datos sensibles, enviándolos a un atacante.

Rootkits:Los rootkits son un conjunto de herramientas diseñadas para ocultar la presencia de un malware o de un atacante dentro de un sistema. Permiten

que los atacantes mantengan el control sobre un sistema infectado sin ser detectados por el usuario o los sistemas de seguridad.

Keyloggers: Los keyloggers son programas maliciosos que registran las pulsaciones de teclas del usuario, lo que permite capturar contraseñas, mensajes, correos electrónicos y cualquier otro dato que se ingrese en el teclado.

DoS y DDos: Denial of Service o el ataque de denegación de servicio es un ataque de saturación para tumbar un servidor. Causa que un servicio o recurso sea inaccesible para los usuarios legítimos. Impide que un servidor preste su servicio.

Bots (y Botnets):Los bots son programas que ejecutan acciones automáticas. Un botnet es una red de computadoras infectadas que están controladas por un atacante. Los bots pueden usarse para llevar a cabo ataques DDoS (Denegación de Servicio Distribuida), enviar correos electrónicos de spam o robar datos.

El impacto de una infección por malware puede ser grave, dependiendo del tipo de malware y de los objetivos del atacante. Algunas de las consecuencias comunes son pérdida de datos, robo de identidad, desempeño reducido del sistema, interrupción de servicios y pérdida financiera.

Ciberdelitos réplica

Además de los intereses y bienes surgidos en el ciberespacio, éste alberga todos aquellos tradicionales que no requieren un traslado físico, sino una comunicación posible en Internet. Se trata, por tanto, de réplicas, llevadas a cabo en el ciberespacio, de crímenes que ya se realizaban, de otro modo, en el espacio físico. El principal problema radica en

el aumento del riesgo para los intereses sociales que surge del ciberespacio, un entorno vasto y complejo donde se cometen infracciones. Además, existe una evidente dificultad para que las normas penales actuales abarquen estas conductas, que aunque similares en su esencia ilícita, cambian constantemente en su forma de ejecución debido a la evolución tecnológica.

Ciberfraudes

Los fraudes de Internet, en los que las redes telemáticas se convierten en el instrumento mediante el cual se logra un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima. Son muchas las formas en las que se puede lograr acceder al patrimonio de terceros, utilizando las múltiples formas de relación comercial existentes en el ciberespacio, así como las propias debilidades de seguridad de los sistemas informáticos que dan directamente acceso al patrimonio o indirectamente a él, al contener las claves o datos bancarios de los usuarios. Así, algunas de las más conocidas son: los distintos fraudes de tarjetas de crédito; los fraudes de cheques; las estafas de inversión; las estafas piramidales realizadas a través de Internet; estafas de la lotería; las ventas online defraudatorias en las que no se envía el producto comprado.

El phishing

El phishing, o pesca de incautos, definido por el grupo mundial antiphishing como el mecanismo criminal que emplea ingeniería social para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias.

En la actualidad, un típico ataque de phishing incluye tres componentes claves: el mensaje, la interacción y el robo. En el primero, el mensaje, las potenciales víctimas reciben un reclamo a través de un medio electrónico. En la mayoría de las ocasiones se trata de un correo electrónico remitido por el delincuente, pero también puede ser un

SMS, mensaje en una red social e incluso en videojuegos con múltiples participantes. Este señuelo no suele ser muy sofisticado desde el punto de vista técnico, sino que a través de la ingeniería social aprovecha las debilidades de las potenciales víctimas. Poniendo en práctica diferentes estrategias de engaño, se consigue que la víctima proporcione determinada información sensible respondiendo a un correo o instale malware.

El segundo paso clave en este tipo de engaños es la interacción de la víctima. Una vez que el usuario recibe el mensaje, se le induce a visitar un sitio web falso que imita a una organización de confianza, como un banco o una tienda en línea conocida. En ese sitio, la víctima puede ser engañada para instalar malware o proporcionar información confidencial.

El tercer y último elemento es la utilización efectiva de la información robada. En algunos casos el delincuente usa directamente los datos de la víctima suplantando su identidad; no obstante, normalmente el phisher no explota por sí mismo la información obtenida, sino que la vende a terceros. De este modo, se ha generado un mercado negro de compraventa de información robada.

Ciberblanqueo de capitales

Aunque existen muy diversas técnicas para el blanqueo del dinero virtual, las más comunes hasta la fecha son el uso de mulas para el envío de dinero y el logro de divisas por medio de los juegos online. Cuando se habla de las mulas, sobre todo en el ámbito del phishing, se hace referencia a los usuarios de Internet que tienen (o abren) cuentas bancarias, y que son reclutados vía web bajo la apariencia de un contrato de trabajo realizado desde casa, y que consiste en la recepción en sus cuentas bancarias de dinero y su envío, habitualmente por medio de sistemas como Western Union, o también por transferencia bancaria, a las cuentas corrientes de los cibercriminales a cambio de una

pequeña comisión. En cuanto a las webs de juego online, éstas suponen la creación de una economía virtual en las que se intercambia el dinero real por dinero virtual para participar en los juegos. Esto es aprovechado por las organizaciones criminales para primero intercambiar el dinero real por dinero virtual y después volverlo a recuperar como real, complicando la perseguibilidad de los bienes ilícitos.

Ciberacoso

Dentro de esta categoría de infracciones tradicionales en las que lo que cambia es el medio de realización de las mismas (ahora virtual), los ataques a bienes jurídicos personalísimos caracterizados simplemente por el medio de realización del mismo, el Internet u otras TIC. Amenazas, coacciones, injurias, calumnias y otras agresiones al honor o a la integridad pueden realizarse como siempre pero a través del ciberespacio.

Aunque el ciberacoso se puede dar de muy distintas formas, las más comunes han dado lugar a categorías propias como son el ciberbullying o ciberacoso escolar o a menores (menor que atormenta, amenaza, hostiga, humilla, o molesta de alguna otra manera a otro, haciendo uso de Internet, teléfono móvil, videoconsola o alguna otra tecnología telemática de comunicación); el cyberstalking o ciberacoso continuado propiamente dicho (podría entenderse, siguiendo a Basu y Jones, como el uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien) y el ciberacoso sexual, dentro del cual estaría el cibergrooming (lo conforman todas las conductas preparatorias llevadas a cabo por el abusador sexual hasta lograr el encuentro con la víctima potencial, y consistiría generalmente en un proceso de seducción de algún menor).

Ciberataques de contenido

La categoría de ciberataques de contenido, aglutina a todos aquellos en los que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes telemáticas. Dentro de esta tipología de comportamientos, en los que la ilicitud se relaciona directamente con el contenido, habría que incluir aquellas conductas en las que no se difunde o distribuye el mismo, sino que tan sólo se posee. Generalmente la ilicitud de muchas de las conductas ilícitas relacionadas con el uso de las TIC deviene de la transmisión del contenido, pero dada la dificultad de la prueba de tal actividad no es inusual el adelantamiento de la punición a comportamientos en los que no hay comunicación del contenido pero sí posesión.

Clasificación según el motivo del ciberataque

En la segunda categoría, se dividen las motivaciones del ciberdelincuente. Encontramos las motivaciones económicas, del mismo modo que sucede fuera del mundo virtual, un ciberdelincuente puede cometer sus estafas en línea con la finalidad de robar dinero a individuos, empresas u otras organizaciones. Luego tenemos los de tipo social, son aquellos que tienen que ver con las relaciones sociales entre las personas y que no son más que la trasposición al ciberespacio de los crímenes tradicionales derivados de conflictos entre personas, en este encontramos delitos de ingeniería social, lo cual es una técnica que consiste en manipular a las personas para que revelen información confidencial, accedan a sistemas informáticos o cometan fraudes. También suelen verse hechos de acciones maliciosas, que no llegan a delitos, abusando de las vulnerabilidades humanas, como la confianza, la curiosidad, el miedo o la falta de conocimiento. Por último tenemos los de tipo político, son aquellos que tienen como objetivo perjudicar a

las instituciones gubernamentales. Normalmente, consiste en traspasar las barreras de seguridad para conseguir una ventaja competitiva o proteger la seguridad nacional propia.

Ingenieria social

Como ya fue mencionado, la ingeniería social es un tipo de cibercrimen que se basa en manipular o engañar a las personas para que realicen acciones o divulguen información confidencial que puedan ser utilizadas para fines maliciosos. Aprovecha la naturaleza humana, en lugar de vulnerabilidades técnicas, lo que puede hacer que este tipo de cibercrimen sea extremadamente eficaz. Algunas características clave de los ataques de ingeniería social son:

Manipulación emocional: Los atacantes suelen crear un sentido de urgencia, miedo o ganancia fácil para presionar a la víctima a que actúe rápidamente sin pensar. Esto puede incluir amenazas de consecuencias negativas (como una cuenta bloqueada) o promesas de recompensas (como premios).

Explotación de la confianza: Los atacantes suelen suplantar la identidad de una persona o entidad de confianza (como un amigo, un jefe, un compañero de trabajo o una institución financiera) para que la víctima se sienta más cómoda divulgando información sensible.

Aprovechamiento de la falta de conocimiento: Muchas veces los ataques de ingeniería social se dirigen a personas que no tienen una comprensión profunda de la seguridad cibernética o que no son conscientes de los métodos empleados por los atacantes.

Personalización: Los ataques dirigidos suelen ser más efectivos, ya que los ciberdelincuentes investigan a su víctima para adaptar el mensaje de manera que

sea más convincente. Esto puede incluir la obtención de información de redes sociales, sitios web públicos o incluso conversaciones informales.

Los ataques de ingeniería social pueden tener varias consecuencias graves para las víctimas, tales como, robo de identidad, los atacantes pueden obtener información personal sensible, como números de tarjetas de crédito, números de seguridad social y contraseñas para realizar fraudes financieros o suplantación de identidad, acceso no autorizado a cuentas y sistemas, al obtener credenciales de inicio de sesión los atacantes pueden acceder a las cuentas bancarias, redes sociales, correos electrónicos y otros sistemas privados de la víctima, instalación de malware, muchos ataques de ingeniería social tienen como objetivo hacer que la víctima descargue o ejecute un archivo malicioso que infecta su dispositivo con malware, ransomware u otros tipos de software dañino, pérdidas económicas la transferencia de dinero a una cuenta fraudulenta o el robo de datos bancarios pueden llevar a pérdidas financieras significativas, daño a la reputación, si un atacante se hace pasar por una organización o individuo confiable y obtiene acceso a información confidencial, puede dañar la reputación de la víctima o de la empresa comprometida.

El ciberespacio

El ciberespacio, se ha convertido en un protagonista de suma trascendencia en un mundo cada vez más virtualizado, que no reconoce fronteras y que, sin dudas fue abriendo paso a una gama de opciones que, de cierta manera, inciden en la vida de las personas. Esta diversificación que se da en el ciberespacio puede ser entendida en tres niveles, Surface Web, Deep Web y Dark Web.

En el primer nivel se encuentra la Surface Web, también conocida como red superficial. Esta, es la parte por la que se navega a diario y que representa la gran mayoría

de internet, mediante la cual se accede a través de motores de búsqueda. En esta red, las direcciones de IP son de fácil rastreo, con lo cual los usuarios pueden ser detectados. Sin embargo, el fácil y rápido acceso permite que se produzca la mayor parte de interacciones, y como consecuencia surge una realidad no tan agradable, la formación de un terreno fértil para una gran cantidad de ciberdelitos, como estafas, acosos, difamaciones y hasta apropiación intelectual.

En el segundo nivel, se encuentra la Deep Web o red profunda. En esta parte, figura el conjunto de páginas que no están indexadas por los motores de búsqueda tradicionales, como pueden ser Google, Bing o Yahoo! y, por lo tanto, cuando se realiza una búsqueda en estas plataformas, no figura el resultado debido a que su contenido no está incluido en el índice de los buscadores. La clave principal se centra en el uso de los servidores proxy o VPN, los cuales actúan como intermediarios que colocan barreras, permitiendo enmascarar la identidad de los usuarios y así evitar la detección mediante rastreo, otorgando de esa manera, una especie de anonimato.

En el último nivel, se encuentra la Dark Web o red oscura. Esta, forma una pequeña parte de la red profunda, pero requiere software personalizado para acceder a su contenido. En esta parte de la web, los usuarios tienen la posibilidad de mantener oculta su identidad, así como también su ubicación, lo que les permite escudarse con una navegación anónima de cara a otras personas y en especial, a los agentes de la ley. Es un método utilizado por particulares, pero principalmente por grandes grupos para la comisión de delitos. A través del anonimato, las organizaciones delictivas logran su objetivo y se pueden manejar de una manera en donde no quedan expuestas y, por ende, no pueden ser desmanteladas.

Teorias criminológicas

Como la cibercriminología es un campo de estudio relativamente nuevo, a menudo se recurre a la utilización de las teorías aplicadas en la criminología del mundo no digital para tratar de explicar los fenómenos criminales en el ciberespacio. Entre las teorías que más se adecuan desde una apreciación personal son las siguientes: Teoría de la oportunidad de Clarke y Felson, y Teoría de las actividades cotidianas de Cohen y Felson adaptada por Miró hacia este nuevo tipo de delincuencia.

La Teoría de la Oportunidad (Felson y Clarke, 1998) sostiene que los delitos son resultado de oportunidades específicas que los delincuentes perciben como accesibles, con bajos riesgos y altas recompensas. En el ámbito del ciberdelito, esta teoría es especialmente relevante debido a las características únicas del ciberespacio, que reducen barreras tradicionales y amplifican las oportunidades delictivas.

En el ciberdelito, los delincuentes identifican sistemas informáticos, datos personales o financieros como objetivos valiosos y relativamente accesibles. El ciberespacio facilita estas acciones al permitir que los delincuentes operen desde cualquier lugar del mundo, disminuyendo el riesgo de ser rastreados o capturados. La percepción de seguridad se ve reforzada por el anonimato que ofrecen tecnologías como las redes privadas virtuales (VPN) y la dark web.

Además, los ciberdelitos tienden a ofrecer recompensas significativas en un período breve, como ocurre con delitos como el ransomware o el fraude financiero. Estas actividades requieren un esfuerzo relativamente bajo en comparación con los delitos tradicionales, ya que pueden ejecutarse mediante herramientas automatizadas y sin necesidad de contacto físico.

El ciberespacio actúa como un catalizador que amplifica las oportunidades delictivas debido a varios factores:

-Globalización del delito: Permite que los ciberdelincuentes operen a nivel internacional, incrementando el alcance y las víctimas potenciales.

- Falta de guardianes eficaces: Muchas víctimas carecen de medidas básicas de ciberseguridad, lo que las deja vulnerables.

- Dinamismo tecnológico: Las constantes innovaciones tecnológicas generan nuevas oportunidades delictivas antes de que se implementen medidas preventivas adecuadas.

Miró (2012) plantea una versión adaptada de la Teoría de las Actividades Cotidianas para comprender la ciberdelincuencia. Este autor considera que más que la actuación de guardianes y de gestores del lugar, lo relevante es la propia actuación de la víctima en su propia protección («autoprotección»), ya que un objetivo será más adecuado cuanto menos protegido esté. Mientras, Felson (1998) entendía que para que un objetivo fuese considerado adecuado debía tener valor desde la perspectiva del delincuente, inercia, visibilidad física y accesibilidad (VIVA), Miró (2012) considera que en el ciberespacio, la adecuación de un bien u objeto dependerá de que haya sido introducido en internet (lo cual en ocasiones será determinado por las propias acciones de la potencial víctima), de que esté más o menos protegido, y de la interacción del usuario que lo haga accesible y visible a los potenciales agresores motivados. De esta forma, pasamos del acrónimo VIVA al acrónimo ISI: introduction, selfprotection, interaction (introducción, autoprotección e interacción).

El ciberdelincuente

El estudio del ciberdelincuente puede ser relevante para comprender su naturaleza y el modus operandi que requieren los diferentes delitos informáticos, además de ayudar a la identificación de los autores cuando aún son desconocidos para los medios de control social.

Los ciberdelincuentes no tienen un perfil de objetivo diseñado, sino que pueden atacar a personas, entidades públicas o privadas y gobiernos. Todo dependerá del objetivo del ataque. Arroyo Cámara (2020), define al ciberdelincuente como una persona que comete delitos en el ciberespacio aprovechando las herramientas tecnológicas para llevar a cabo actividades ilegales. Según su perspectiva, el ciberdelincuente se caracteriza por su capacidad para operar de manera anónima, eludiendo las fronteras geográficas y jurisdiccionales que suelen existir en los delitos tradicionales.

Además, Arroyo Cámara (2020) destaca que los ciberdelincuentes operan en una dimensión digital donde las leyes tradicionales muchas veces no se aplican con la misma eficacia, lo que requiere una actualización constante de las normativas y una mayor cooperación internacional para combatir estos delitos.

Florentino García (2022) señala que estos Cibercriminales cuentan con un factor a su favor, el anonimato, lo que permite que el desarrollo de sus actividades sea difícil de rastrear y reconocer, más no imposible; sin embargo, esto permite que los índices de Cibercriminalidad sean mayores que en el espacio físico; para estos casos, la cibercriminalidad se limitará a todas aquellas conductas desviadas o delictivas ocurridas en el ciberespacio, sin importar que posteriormente puedan emigrar al espacio físico, por

ello, no pierde su categoría de cibercrimen, pues este se originó dentro o a través de la red pública de internet.

Es relevante comprender que el delito por dentro del ciberespacio es completamente diverso y se mantiene en constante innovación, por ende, es probable que no logremos estandarizar un perfil para los ciberdelincuentes. Podríamos pensar que para la perpetración de un ciberdelito es requisito poseer conocimientos cualificados en materia informática, pero el avance en la disponibilidad de las TICs hace posible que la realización de actos delictivos a través de medios tecnologicos se encuentre, cada vez más frecuente, al alcance de cualquier persona que sepa manejar, aun cuando sea de manera rudimentaria, un dispositivo. En ocasiones las técnicas avanzadas en materia de informática adquiridas por algunos sujetos sirven de puerta de entrada a otros con conocimientos mucho menores, que utilizan el trabajo ya realizado por los primeros para cometer hechos delictivos, provocando así que surja una cadena criminógena, en la que unos individuos especialmente competentes generan oportunidades delictivas para otros menos capacitados. Presentando de este modo una importante problemática en el ámbito del perfilado criminal, ya que el perfil del delincuente informático puede ser muy variado en cuanto a sus competencias en el medio informático.

Existen numerosas dificultades tales como la singularidad del cibercriminal o su pertenencia a organizaciones criminales, el favorecimiento del anonimato en el ciberespacio, la clase social y profesión a la que pertenece, el género más frecuente en los ciberdelincuentes o la edad de los perpetradores, que hacen del delincuente informático un reto para los postulados clásicos de la criminología.

Para enfrentar todas estas dificultades, se realizaron diferentes estudios en los cuales coinciden que este tipo de delitos poseen una tasa de criminalidad joven, eminentemente masculina y con cierto grado de conocimientos. No es ninguna sorpresa

que este tipo de criminalidad se asocie a la juventud, las nuevas generaciones de usuarios han nacido en un entorno en el que el uso de las nuevas tecnologías se encuentra completamente normalizado.

Siguiendo a Cámara Arroyo (2020) a los ciberdelincuentes se los puede agrupar en dos tipos, los especializados y los no especializados en el manejo de las TIC.

Ciberdelincuentes especializados

Son delincuentes que poseen un alto nivel de conocimiento técnico en tecnologías de la información y comunicación, lo que les permite llevar a cabo delitos complejos en el ciberespacio. Estos individuos o grupos se destacan por su capacidad de planificación y por la sofisticación de sus ataques, que incluyen actividades como el uso de ransomware, el espionaje corporativo y las intrusiones en sistemas críticos.

Para lograr sus objetivos, emplean herramientas avanzadas, como malware, redes de bots y técnicas de ingeniería social altamente elaboradas. Además, suelen operar en redes organizadas, en las que cada miembro desempeña un rol específico, como la creación de software malicioso, la extracción de información confidencial o el lavado de activos digitales.

En términos de motivación, los cibercriminales especializados buscan principalmente beneficios económicos, acceso a información sensible o ventajas estratégicas, como afectar a una empresa o gobierno.

Hackers

Los hackers son los pioneros de las primeras formas de cibercriminalidad. Este nombre se le adjudica a un sujeto o un grupo de expertos en informática y redes, buscan

superar barreras por el mero hecho de su existencia, sin entrar en el campo de lo delictivo, incluso en ocasiones usan sus conocimientos para la mejora de la seguridad en los sistemas. No siempre que estemos ante un hacker podemos etiquetarlo como ciberdelincuente, ya que pueden dedicar sus conocimientos a realizar alteraciones técnicas en sistemas informáticos tanto de forma positiva como negativa. Dentro de esta categoría podemos encontrar tres tipos de hackers: hacker de sombrero blanco, es el encargado de la seguridad de los sistemas informáticos, dedicados a fortalecer los errores (bugs) en los mismos. Hacker de sombrero gris, se dedica a traspasar los niveles de sistemas de seguridad y ofrecen sus servicios como administradores de seguridad. Su finalidad no es delictiva, aunque se encuentra encaminada a conseguir rédito profesional. Finalmente, el hacker de sombrero negro, encaja perfectamente con el concepto de cibercriminal, puesto que se dedica a vulnerar ilegalmente la seguridad de sistemas privados con la finalidad delictiva de descubrir, revelar, apoderarse o dañar datos. De este último, se desprenden distintos perfiles, a los cuales se les adjudica un nombre dependiendo del tipo de ciberdelito que desarrollan. (Cámara Arroyo, 2020)

Ciberterrorista

El ciberterrorista es un individuo o grupo que utiliza el ciberespacio con fines terroristas, generando temor y desestabilización tanto en el ámbito digital como físico. Este tipo de ciberdelincuente tiene como objetivo principal causar un daño significativo mediante el uso de tecnologías digitales, a menudo motivado por ideologías políticas, religiosas o sociales. Las acciones del ciberterrorista incluyen, entre otras, ataques a infraestructuras críticas, el robo y difusión de información sensible, el uso de plataformas digitales para propaganda y reclutamiento, y el sabotaje de sistemas de comunicación o energía.

Este perfil de delincuente no solo tiene conocimientos avanzados en programación y ciberseguridad, sino que es capaz de llevar a cabo ataques sofisticados que requieren una planificación detallada y una ejecución precisa. El ciberterrorista experto tiene la capacidad de desarrollar herramientas personalizadas, como malware específico, y utilizar técnicas complejas para interrumpir sistemas críticos, como redes eléctricas, sistemas de transporte o plataformas de comunicación.

A pesar de que existen también colaboradores menos calificados, los ciberterroristas expertos son los que lideran la planificación y ejecución de estos ataques, organizando y dirigiendo a aquellos con menos experiencia. Este tipo de cibercriminal tiene un conocimiento profundo de las vulnerabilidades de los sistemas y puede manipular estas debilidades para cumplir con sus objetivos terroristas, generando pánico y afectando a grandes sectores de la sociedad.

Ciberdelincuente no especializado

Estos sujetos utilizan a la tecnología como un medio para cometer sus delitos, no poseen los conocimientos justos para cumplir sus objetivos, suelen ser más pragmáticos y sus motivaciones son variadas, como la venganza personal, la posibilidad de obtener un beneficio económico y la excitación sexual.

El cibervándalo

Habitualmente se suele hablar de menores víctimas de los delitos cometidos a través de las nuevas tecnologías de la comunicación. Sin embargo, en los últimos años se ha evidenciado la tendencia de algunos menores siendo autores de esta clase de delitos.

Los cibervándalos son individuos o grupos que realizan actos de vandalismo en el ciberespacio, con el fin de dañar, alterar, destruir o corromper sistemas, plataformas, redes

o contenidos digitales. Aunque sus motivaciones no siempre son económicas, buscan causar daño, generar caos o simplemente expresar una ideología de manera destructiva a través de medios digitales. Este tipo de actividad es similar al vandalismo físico, pero se lleva a cabo en el ámbito virtual, afectando tanto a individuos como a instituciones.

Una característica común entre los cibervándalos es que, en muchos casos, son menores de edad, con una alta presencia de varones. Estos jóvenes, a menudo con conocimientos limitados sobre informática, suelen ser autodidactas, adquiriendo sus habilidades a través de tutoriales en línea, foros y comunidades virtuales. Aunque su nivel de conocimiento puede ser básico o intermedio, su capacidad para realizar actos de cibervandalismo no se debe subestimar, ya que las herramientas necesarias para estos ataques están fácilmente disponibles y accesibles en la web.

La motivación de estos jóvenes muchas veces está vinculada a una imagen romanizada del hacker, que es un concepto muy presente en la cultura digital. Los cibervándalos suelen sentirse atraídos por la figura del "hacker rebelde", a quien se le ha atribuido fama y reconocimiento en ciertos círculos, a menudo debido a su habilidad para burlar sistemas de seguridad o desafiar instituciones. Este fenómeno se ve amplificado por la influencia de películas, series y medios de comunicación, que representan a los hackers como figuras heroicas o con un gran poder, lo que a veces puede ser un factor de atracción para los menores que buscan identidad o pertenencia a un grupo.

Otro factor que contribuye a la actividad de los cibervándalos es su adicción o dependencia de los medios de comunicación virtual. La constante interacción con las redes sociales, videojuegos en línea, foros y comunidades digitales puede fomentar una mentalidad de desafío y exploración de los límites de lo permitido, lo que puede llevar a

algunos jóvenes a participar en actos de vandalismo digital, sin considerar las repercusiones o consecuencias legales de sus acciones.

A diferencia de los ciberdelincuentes que buscan obtener beneficios económicos a través de fraudes, robos de identidad o extorsiones, los cibervándalos no siempre tienen una motivación financiera. En su lugar, buscan causar daño, caos o simplemente demostrar su habilidad tecnológica. Su actividad, aunque menos orientada al lucro, puede tener consecuencias graves, tanto en términos de daño a la reputación de las víctimas como en la interrupción de servicios digitales. Además, los cibervándalos, al ser mayormente menores de edad, pueden enfrentarse a una falta de conciencia sobre las implicaciones legales de sus actos, lo que puede complicar la respuesta de las autoridades y de las organizaciones afectadas.

El hecho de que muchos cibervándalos sean jóvenes también plantea un desafío para la educación en ciberseguridad. La falta de madurez y comprensión sobre las implicaciones legales y éticas de sus acciones requiere que se refuercen los programas educativos en escuelas y comunidades, con el fin de promover un uso más responsable y ético de las tecnologías.

Ciberdelincuentes insider y cibermula

Los ciberdelincuentes insider y las cibermulas desempeñan roles distintos pero fundamentales en las organizaciones de ciberdelincuencia. Los insiders son personas que pertenecen o trabajan para la institución o empresa víctima de la infracción. Este perfil incluye empleados, contratistas, proveedores e incluso exempleados que aún poseen credenciales activas.

Las motivaciones de los insiders pueden variar: algunos buscan un beneficio financiero a cambio de información o acceso, otros actúan por venganza debido a conflictos internos o descontento laboral, mientras que algunos lo hacen por razones ideológicas o son coaccionados por terceros bajo amenazas. Aunque no siempre tienen conocimientos avanzados en tecnología, su familiaridad con los sistemas internos los convierte en facilitadores clave dentro de las redes de ciberdelincuentes. Su rol suele centrarse en proporcionar información sensible, credenciales de acceso, mapas de red o identificar fallas de seguridad. También pueden sabotear sistemas desde dentro o extraer datos valiosos para ser vendidos o utilizados ilícitamente.

Por otro lado, las cibermulas actúan como intermediarias para mover dinero o bienes obtenidos de manera ilegal, dificultando el rastreo de los líderes de la organización. En muchos casos, estas personas son reclutadas bajo engaños, presentándoles el rol como si fuera un trabajo legítimo, como asistente financiero. Otras veces, son coaccionadas mediante chantajes o amenazas, o aceptan participar debido a su vulnerabilidad económica, sin comprender completamente las implicaciones legales de sus acciones. En realidad, algún autor ha sostenido que "no son, desde una perspectiva criminológica, cibercriminales, puesto que no son autores del delito en el ciberespacio sino colaboradores o recolectores de los beneficios en Internet que luego envían por medios seguros de transmisión el dinero a los autores del delito (las ciberbandas) o a los responsables de los grupos organizados tradicionales que operan en Internet" (Miró Llinares, 2012),si bien lo cierto es que son esenciales en el desarrollo de muchos fenómenos delictivos que tienen su origen en el ciberespacio.

Las cibermulas generalmente no poseen conocimientos técnicos avanzados, pero su participación es crucial en las operaciones de lavado de dinero. Su rol incluye transferir dinero entre cuentas, convertir fondos en criptomonedas o recibir y reenviar productos

comprados con tarjetas robadas. Estas actividades permiten encubrir las operaciones de los líderes criminales, ya que las cibermulas son el último eslabón en la cadena y suelen asumir el mayor riesgo legal. Generalmente estas cibermulas son las únicas detenidas por estos delitos y pueden ser hechas responsables de los mismos como cooperadores necesarios o cómplices.

En las organizaciones de ciberdelincuencia, los insiders y las cibermulas cumplen funciones complementarias. Mientras los insiders son esenciales para facilitar el acceso inicial a los sistemas y datos, aportando valor estratégico a las operaciones, las cibermulas se encargan de la logística y el encubrimiento, permitiendo que las redes criminales operen con un menor riesgo de ser detectadas. Ambos perfiles son piezas clave en la compleja estructura de estas redes ilícitas.

Ciberhacktivista

El ciberhacktivista es una persona o grupo que utiliza sus conocimientos tecnológicos para realizar acciones en el ciberespacio con fines políticos, ideológicos o sociales. Su objetivo principal es generar impacto, visibilizar problemáticas, promover cambios o expresar oposición a determinadas políticas, gobiernos u organizaciones. Las actividades de los ciberhacktivistas suelen incluir ataques como DDoS (denegación de servicio distribuido), alteraciones de páginas web, publicación de información sensible (filtraciones) y hackeo de sistemas, siempre con un propósito reivindicativo o simbólico.

Aunque se consideran activistas digitales, sus acciones suelen cruzar la línea de lo legal, lo que los posiciona como cibercriminales en muchos contextos. Un ejemplo emblemático es el grupo Anonymous, que ha ejecutado ataques en defensa de la libertad de expresión y contra la censura, pero también ha enfrentado consecuencias legales debido a la naturaleza ilícita de algunas de sus tácticas.

El nivel de expertise de un ciberhacktivista varía según su rol y habilidades específicas dentro de la actividad. Si bien algunos actúan como líderes expertos, otros son simplemente seguidores o ejecutores que se adhieren al movimiento por afinidad ideológica.

El cribergroomer

El grooming es una modalidad de abuso en línea en la que un adulto se comunica de manera intencionada y prolongada con un menor, a través de plataformas digitales (redes sociales, chats, foros, juegos en línea, etc.), con el objetivo de manipular, coaccionar o engañar al niño o adolescente para que se involucre en actividades sexuales, ya sea de forma física o a través de la web. Los estudios criminológicos y psicológicos sugieren que el ciberespacio facilita que potenciales abusadores sociales se conviertan en agresores, al ofrecerles un medio para superar su aislamiento y acceder a un mayor número de víctimas.

El perfil del cibergroomer en términos generales, se trata de adultos, en su mayoría hombres aunque también existen mujeres, que tienen conocimientos básicos de las redes sociales. Estos agresores pueden tener edades que van desde los jóvenes adultos hasta personas de edad avanzada.

Una de las principales motivaciones está vinculada a la necesidad de poder y control. Este deseo de gratificación personal puede estar alimentado por factores emocionales, como la soledad, el aislamiento social, la baja autoestima o la dificultad para mantener relaciones personales en el mundo físico. Estos factores psicológicos lo llevan a buscar satisfacción en las interacciones virtuales, donde puede controlar el ambiente y las víctimas, al tiempo que satisface sus propios deseos emocionales.

A diferencia de los depredadores sexuales tradicionales, el cibergroomer suele ser más consciente de los actos que comete. Aunque su empatía hacia las víctimas es generalmente baja, lo que hace que no considere el sufrimiento que causa, sí tiene una mayor comprensión de los efectos de sus acciones. Su principal objetivo es satisfacer sus necesidades emocionales sin tener en cuenta el daño que inflige a la víctima. Es estratégico y manipulador. Se vale de diversas herramientas psicológicas, como la manipulación emocional, los halagos falsos y la creación de una falsa identidad, para ganarse la confianza de la víctima. Tiene un alto nivel de control sobre las conversaciones, lo que le permite llevar a la víctima a intercambiar contenido sexual explícito sin que esta se dé cuenta inmediatamente de las intenciones maliciosas del agresor.

Aunque el cibergroomer puede tener deseos sexuales compulsivos o distorsionados, sus actos suelen ser menos impulsivos que los de otros tipos de agresores sexuales. Esto se debe a que, en el entorno virtual, tiene más tiempo y espacio para manipular a la víctima, planificar sus acciones y obtener resultados progresivos, lo que reduce la impulsividad y le permite actuar con mayor cautela.

Finalmente, el cibergroomer tiende a evitar el contacto físico directo con la víctima. En lugar de buscar relaciones sexuales físicas, se concentra en la explotación sexual en línea. El entorno virtual le proporciona un mayor control, anonimato y menos riesgos de ser descubierto, lo que lo convierte en un espacio más atractivo para este tipo de agresores.

La cibervíctima

Cualquier usuario de Internet, cualquier persona que tenga un sistema informático conectado a una red puede ser víctima de cibercrímenes de muy distinto tipo, dependiendo

de la motivación del sujeto que realiza el ataque pero, también, del tipo de actividad que el propio usuario realice. Por tanto, escapa a lo posible la configuración de un perfil único de víctima potencial del cibercrimen, puesto que por lo menos habrá tantos perfiles como ámbitos de oportunidad criminal en el ciberespacio, pero entendiendo el ámbito de oportunidad como también definido por el actuar de la víctima. Esto significa, que no es únicamente la motivación criminal la que define el ámbito de oportunidad criminal en el ciberespacio, sino que la propia víctima con su conducta también construye los ámbitos de riesgo.

Por otro lado, la cibervictimización es el proceso de victimizar a usuarios mediante el uso de tecnologías de la información y comunicación. Esto incluye la perpetración de actos negativos, abusivos o dañinos hacia individuos, organizaciones o instituciones utilizando medios electrónicos, como el ciberacoso, la difamación en línea, el robo de identidad, la suplantación de identidad, el acoso cibernético y otros comportamientos delictivos o perjudiciales en el entorno digital.

La cibervictimización puede tener consecuencias psicológicas, emocionales, sociales y legales para las personas afectadas. Para Kimberly J. Mitchell y Michele L. Ybarra (2014), la cibervictimización es el acto de ser objeto de agresiones o acosos en línea, incluyendo insultos, amenazas, difamación y exclusión social a través de plataformas digitales.

El ciberespacio constituye un reconocido espacio victimogénico cuya arquitectura digital modifica las dinámicas de victimización y desvictimización, facilitando la acción del ciberagresor motivado, incrementando la vulnerabilidad victimal de aquellos que ingresan material sensible en la red sin las medidas de autoprotección necesarias y dificultando su proceso de desvictimización o reajuste cognitivo y emocional.

La clasificación criminológica más aceptada es la propuesta por Miró (2012), según la cual, en función del móvil o motivación criminal y los bienes atacados, se pueden distinguir tres tipos básicos de cibercrimen: económico, político y social. Estos dan lugar a tres categorías diferenciadas de cibervicictimización.

Cibervictimización económica: es la experiencia que deriva del ataque contra bienes jurídicos patrimoniales, pero siempre con el objetivo de obtener un beneficio económico.

Cibervictimización política: deriva de los cibercrímenes que tienen un objetivo ideológico o institucional e incluyen los delitos de odio, la ciberguerra, el ciberterrorismo y el hacktivismo o ciberactivismo político y mediante ataques de denegación de servicios contra páginas web.

Cibervictimización social: deriva de los cibercrímenes sociales que afectan a bienes jurídicos personalísimos, como la libertad, el honor, la indemnidad o la integridad sexual.

La mal llamada pornografia infantil

En el marco de la cibervictimización social es relevante considerar que, en el ámbito de la protección infantil y la lucha contra la explotación sexual, es fundamental reconocer que el lenguaje tiene un impacto significativo en la forma en que entendemos y abordamos los problemas sociales. Tradicionalmente, el término "pornografía infantil" ha sido utilizado para referirse al material que explota sexualmente a menores. Sin embargo, en la actualidad se recomienda un cambio cultural en el uso de esta terminología, promoviendo el uso del término MASI, que hace referencia a Material Abusivo Sexual Infantil. Este cambio no solo es un ajuste técnico en el vocabulario, sino

que también tiene implicaciones profundas en la percepción pública del fenómeno y en las estrategias de prevención y sanción

El término "pornografía infantil" es ampliamente reconocido, pero su uso tiene serias implicaciones que pueden diluir la gravedad del delito que representa. Al referirse a estos contenidos como "pornografía", se está equiparando, implícitamente, el abuso sexual infantil con una categoría de material que puede ser considerado, de manera errónea, como un "género" o "tipo de contenido". La palabra "pornografía" suele estar asociada con la idea de un acto consentido entre adultos, lo que puede llevar a la trivialización del abuso y la explotación de los menores. Además, este término no refleja adecuadamente el carácter violento y abusivo de los actos perpetrados contra los niños, niñas y adolescentes.

Al usar la palabra "pornografía", el foco se desvía del abuso que se está cometiendo, y se centra en el contenido como un producto a consumir, lo cual deshumaniza a las víctimas. Este enfoque puede generar una percepción distorsionada de la magnitud del problema, desinformando a la sociedad y dificultando una respuesta legal y social adecuada.

El término MASI (Material Abusivo Sexual Infantil) tiene una carga más precisa y ética, ya que pone el énfasis en el abuso que sufren los menores y en el carácter criminal de la producción, distribución y consumo de este material. Usar "MASI" subraya que estos actos son crímenes de abuso sexual y no una forma de entretenimiento o material con valor estético, como podría implicar el término "pornografía". Esta terminología orienta mejor las intervenciones legales y sociales, ya que enfatiza el hecho de que lo que se está tratando no es solo un "producto" o "contenido", sino un delito que violenta los derechos fundamentales de los niños.

Además, la adopción del término MASI es parte de un esfuerzo por humanizar y proteger a las víctimas, que son niños y niñas que sufren abuso físico, psicológico y sexual. Al emplear este término, se envía un mensaje claro de que no hay nada consentido ni aceptable en el abuso sexual infantil, y que la sociedad y el sistema de justicia deben tratar el tema con la gravedad que corresponde.

El cambio de terminología no es un simple ajuste lingüístico; es un cambio cultural fundamental que busca modificar la percepción social del abuso infantil. Adoptar el término MASI implica reconocer la necesidad de transformar la manera en que tratamos y abordamos este problema, tanto a nivel legislativo como educativo y mediático. El uso de un término más preciso y cargado de responsabilidad permite generar una mayor conciencia pública sobre la naturaleza criminal del abuso infantil y las consecuencias devastadoras para las víctimas.

Además, este cambio de lenguaje también refuerza el mensaje de que los menores no son sujetos pasivos ni objetos de consumo. Son víctimas de actos horrendos y deben ser vistos como tal, con el respeto y la dignidad que les corresponde. Al emplear términos más adecuados como MASI, se contribuye a una mayor sensibilización social y se fomenta una actitud de rechazo hacia la explotación infantil, cambiando, poco a poco, la mentalidad y las respuestas institucionales hacia este delito.

El uso del término MASI también tiene implicaciones clave en la legislación y la prevención. La legislación internacional, incluida la Convención sobre los Derechos del Niño, y leyes nacionales de muchos países, ya han comenzado a incorporar la idea de que la producción, distribución y posesión de material abusivo sexual infantil son crímenes graves. El uso adecuado de la terminología en estos marcos jurídicos ayuda a garantizar que las penas por estos delitos sean proporcionales a la gravedad del crimen y contribuye

a la implementación de políticas públicas que se enfoquen en la protección integral de los menores y la erradicación de la explotación.

Asimismo, las campañas de prevención y sensibilización pueden ser más efectivas si se utiliza un lenguaje que responsabilice a los perpetradores del abuso y que resalte el impacto destructivo sobre las víctimas. Esto no solo mejora el entendimiento público, sino que también ayuda a que la sociedad se sienta más comprometida con la protección de la infancia y la denuncia de estos crímenes.

Antecedentes históricos

El vínculo malicioso con los hackeos se documentó por primera vez en los años 70, cuando los primeros teléfonos informatizados se convirtieron en un objetivo. Los expertos en tecnología conocidos como “phreakers” encontraron una forma de evitar el pago de las llamadas de larga distancia mediante una serie de códigos. Fueron los primeros hackers.

En la década del 80, empezaron los primeros desarrollos y propagación de virus. Pero, especialmente, entre 1996 y 2000, con una mayor proliferación de virus informáticos destinados a ocasionar daños en general, ya sea a empresas o a individuos. Entre ellos, encontramos al virus I love you, que fue creado en Filipinas, pero se propagó por todo el mundo rápidamente afectando grandes instituciones como El Pentágono, la CIA y el Parlamento Británico.

La primera persona en ser declarada culpable de un delito cibernético fue Ian Murphy, también conocido como Capitán Zap, y eso sucedió en 1981. Había pirateado la compañía telefónica estadounidense para manipular su reloj interno, de modo que los usuarios aún pudieran realizar llamadas gratis en horas pico.

Otro caso, que fue registrado en nuestro país fue el que, en octubre del 2022, la UFECI reportó una modalidad de estafa a través de correos electrónicos que aparentaban provenir del Correo Argentino. En tal correo se indicaba que debían depositar unas sumas de dinero para liberar un paquete retenido en el depósito de la sucursal de Retiro de la empresa oficial. Los pagos solicitados se concretaban mediante transferencias en billeteras virtuales y las víctimas eran personas que efectivamente esperaban un envió a través de esa empresa. Como paso previo a proporcionar la cuenta para depositar el dinero, los autores de la maniobra exigían fotos del documento de identidad (frente y dorso) y dos selfies (una con cara neutra y otra haciendo un gesto), fotos con las cuales les permite a los ciberdelincuentes pasar por los procesos de validación de identidad que requieren las empresas Fintech para la creación de una cuenta. De esta forma se les posibilita hacer una suplantación de identidad y cometer otras maniobras delictivas.

Que los sistemas informáticos se encuentren conectados en un ámbito de comunicación transnacional-universal (ciberespacio), es decir, desde cualquier espacio físico ubicado en cualquier lugar del mundo, da a lugar a la posibilidad de que se cometan ilícitos que puedan afectar, en lugares distintos y simultáneamente, a bienes jurídicos tan diversos como el patrimonio, la intimidad, la libertad e integridad sexual, el honor, la dignidad personal, la seguridad del estado, entre otros. Esto representa una compleja y creciente problemática, y por consecuencia las oportunidades de ser una potencial víctima de algún tipo de ciberdelito se torna inevitable.

Marco Legal

El ciberdelito, entendido como la actividad delictiva cometida mediante o contra sistemas informáticos, ha crecido exponencialmente en Argentina, incluyendo en la provincia de Córdoba. En Argentina, los ciberdelitos están regulados principalmente por

el Código Penal y diversas leyes nacionales que buscan prevenir, sancionar y mitigar los delitos informáticos. En la provincia de Córdoba, la aplicación de estas normativas se adapta a las dinámicas locales a través de instituciones especializadas y mecanismos de colaboración con organismos nacionales e internacionales.

Normativa nacional aplicable:

Ley 26.388 (2008): Modificación del Código Penal, esta ley introdujo nuevos tipos penales que tipifican:

- Acceso indebido a sistemas informáticos (Artículo 153 bis):

"Será reprimido con prisión de quince días a seis meses el que, mediante cualquier medio, accediere ilegítimamente a un sistema o dato informático de acceso restringido."

Este artículo sanciona el acceso no autorizado a sistemas informáticos, especialmente cuando se compromete la privacidad de las personas o entidades.

- Intercepción de comunicaciones electrónicas (Artículo 153):

"Será reprimido con prisión de un mes a dos años el que, indebidamente, accediera, interrumpiera o interceptara comunicaciones electrónicas de carácter privado, salvo que cuente con el consentimiento del emisor o del destinatario."

- Aplica a casos de espionaje o vigilancia no autorizada en el ciberespacio.

- Daño informático (Artículo 183):

"Será reprimido con prisión de quince días a un año el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble, total o parcialmente ajena."

- Este artículo cubre el daño a sistemas informáticos o bases de datos.

Artículo 184:

"Las penas se agravarán si el daño recae sobre sistemas destinados al servicio público, comunicaciones o transporte de datos esenciales."

- Defraudación informática (Artículo 173, inciso 16):

"Será reprimido con prisión de un mes a seis años el que, mediante manipulación informática o engaño, lograre que alguien realice una disposición patrimonial en perjuicio propio o de un tercero."

- Esta disposición abarca fraudes electrónicos como phishing o manipulación de software financiero.

- Suplantación de identidad digital (Artículo 292):

"Será reprimido con prisión de tres a seis años el que falsificare un documento público o privado, físico o digital, con el fin de inducir a error a otra persona o entidad."

- Aplica a casos de perfiles falsos y robo de identidad en plataformas digitales.

Ley 25.326 (2000): Protección de Datos Personales

Regula la recopilación, almacenamiento y uso de datos personales. Este marco es fundamental para combatir el robo de identidad y la divulgación indebida de información sensible.

Artículo 128 del Código Penal: Material de abuso sexual infantil

"Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comercializare, publicare, facilitare, distribuyere o poseyere material pornográfico que tuviera como representación la imagen de menores de 18 años."

- Incluye sanciones por posesión para uso personal y agravantes para la producción o el uso de menores con fines de explotación.

Ley 27.411 (2017): Aprueba el convenio de Budapest sobre ciberdelincuencia, que armoniza normativas internacionales, promueve la cooperacion entre paises y establece herramientas comunes para la persecución penal del delito informatico.

Convenio de budapest

El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 por el Consejo de Europa, representa el primer tratado internacional que aborda de manera integral los delitos cometidos en el ciberespacio. Su principal objetivo es armonizar las legislaciones nacionales, fomentar la cooperación internacional y desarrollar herramientas efectivas para combatir este tipo de delitos. Aunque surgió como una iniciativa europea, su relevancia global ha llevado a que países de otros continentes, como Argentina, lo adopten para reforzar sus sistemas legales y de justicia en el ámbito digital.

Este convenio abarca dos tipos de delitos: los específicos del ciberespacio, como el acceso no autorizado a sistemas informáticos, el daño o alteración de datos y la creación o distribución de herramientas diseñadas para cometer ciberdelitos, y los delitos tradicionales que utilizan tecnologías digitales como medio, tales como el fraude informático, la pornografía infantil y las violaciones de derechos de autor. Uno de los aspectos destacados del convenio es la obligación de los países signatarios de crear leyes nacionales que tipifiquen estos delitos y establecer mecanismos de cooperación internacional para facilitar la lucha contra ellos.

En el ámbito de la criminología, el convenio ofrece un marco para analizar y entender los fenómenos delictivos en el ciberespacio. Este enfoque permite estudiar tanto el perfil de los ciberdelincuentes como las motivaciones que los llevan a actuar, a la vez que proporciona una base para desarrollar estrategias preventivas y políticas públicas. Además, resalta la importancia de capacitar a los operadores del sistema de justicia en materia de ciberseguridad y recolección de pruebas electrónicas.

Uno de los pilares del Convenio de Budapest son los mecanismos de investigación que establece, diseñados para abordar los desafíos únicos que presenta la ciberdelincuencia. Entre ellos, se encuentra la capacidad de preservar datos electrónicos de manera inmediata, una medida clave para evitar la pérdida de información crucial debido a la volatilidad de los sistemas digitales. Además, el convenio permite la recolección expedita de pruebas electrónicas, estableciendo procedimientos claros para garantizar que estas sean admisibles en los tribunales.

Otro mecanismo importante es la interceptación de datos en tiempo real, que incluye la monitorización de tráfico de datos y comunicaciones cuando hay sospechas razonables de actividades delictivas. Esto se complementa con el establecimiento de redes de cooperación internacional rápida, las cuales permiten a los países signatarios compartir información y coordinar acciones de investigación de manera eficiente, especialmente en casos de ciberdelitos transnacionales.

En cuanto a la situación en Argentina, el país se adhirió al Convenio de Budapest en el año 2017, marcando un hito como el primer país de América Latina en integrarse a este esfuerzo global. Esta adhesión refuerza el compromiso de Argentina con la lucha contra los ciberdelitos, especialmente a través de la cooperación internacional y la modernización de su marco legal.

En síntesis, el Convenio de Budapest es un instrumento esencial para enfrentar los desafíos de la ciberdelincuencia, integrando elementos legales, tecnológicos y criminológicos. Al ofrecer herramientas efectivas para la investigación, la cooperación internacional y la creación de políticas públicas, se ha convertido en un referente global en la protección del ciberespacio.

Aplicación local en Córdoba

En Córdoba, estas normativas nacionales se implementan a través de organismos especializados:

- Unidad Fiscal Especializada en Ciberdelitos (UFEIC): Encargada de investigar delitos como fraudes informáticos, acoso digital, sextorsión y distribución de material de abuso sexual infantil.
- Policía Judicial de Córdoba: Realiza pericias informáticas y análisis de evidencia digital, siendo un actor clave en la recolección de pruebas en casos complejos.

Córdoba enfrenta retos significativos en la aplicación de este marco legal, entre los que se destacan la dificultad para definir la jurisdicción adecuada, ya que no siempre es claro si los casos deben ser tratados a nivel provincial o federal. Además, existe una escasez de recursos, tanto de personal técnico capacitado como de herramientas tecnológicas avanzadas, lo que limita la eficacia en la implementación de las normativas. Finalmente, la evolución tecnológica presenta otro desafío, ya que las leyes actuales no siempre son lo suficientemente flexibles para abarcar las nuevas modalidades delictivas que surgen con el avance tecnológico.

El marco legal vigente ofrece herramientas para abordar el ciberdelito en Córdoba, pero su aplicación requiere un enfoque multidisciplinario que combine recursos tecnológicos, formación especializada y cooperación interinstitucional. La constante actualización de las normativas y la sensibilización de la ciudadanía son fundamentales para enfrentar los desafíos que plantea el ciberespacio en el ámbito local.

PLANTEAMIENTO DEL PROBLEMA

Si bien es indudable que algunos ciberdelitos no requieren de un alto grado de conocimientos técnicos por parte del ciberdelincuente, existen algunos que sí requieren

de esos conocimientos pero son los que se encuentran en menor medida. En cambio, los de baja complejidad, los que están más relacionados a un engaño a través de un medio digital cotidiano para obtener algo de la víctima, son los más frecuente y los que actualmente están en mayor crecimiento. Por más que los ciudadanos busquen herramientas y estrategias para aumentar su seguridad en línea, existe una falta de información sistemática sobre la prevalencia de estas experiencias delictivas entre la población general. Este vacío de información también limita la capacidad de las autoridades y organizaciones para implementar medidas efectivas de prevención y concientización.

OBJETIVOS

Objetivo general

- Contribuir al entendimiento de la magnitud del problema, identificar la mecánica del ciberdelito, el perfil del ciberdelincuente y las circunstancias que convierten a los individuos en cibervictimas para alcanzar una mejor visión de las tendencias de victimización, de los factores que contribuyen al aumento de estos delitos y de las mejores formas de prevención.

Objetivos específicos

- Examinar el ciberespacio como ámbito propicio para la comisión de delitos.
- Caracterizar al ciberdelincuente, analizando sus motivaciones, modus operandi y perfiles comunes en el entorno digital.
- Entender el impacto de los ciberdelitos en las víctimas.
- Llevar a cabo encuestas que permitan identificar cuántas personas han sido víctimas de delitos cibernéticos.
- Comprender las circunstancias y características de los delitos cibernéticos.

- Analizar el marco normativo sobre ciberdelitos en la provincia de Córdoba.
- Proponer estrategias de prevención.

PREGUNTAS DE INVESTIGACIÓN

Para complementar esta investigación se proponen dos tipos de encuestas, la primera, dirigida a los ciudadanos que suelen ser los que están más desprotegidos y propensos a convertirse en cibervictimas, y la segunda encuesta, dirigida a profesionales del sistema jurídico, ya que estos actores son los que reciben las denuncias y manejan casos relacionados a ciberdelitos.

La primera encuesta responde a las siguientes preguntas de la investigación:

- ¿Las personas tienen presente la existencia de los ciberdelitos?
- ¿Cuántas personas han sido víctimas de ciberdelitos?
- ¿De qué edades han sido más frecuentes las víctimas?
- ¿Qué tipos de ciberdelitos son los más frecuentes?

La segunda encuesta responden a la siguientes preguntas de la investigación:

- ¿Los ciberdelitos se suelen denunciar?
- ¿Qué sector es el más afectado?
- ¿Es un delito en aumento?

METODOLOGÍA

Para abordar el estudio de los ciberdelitos, se emplea el método cualitativo-cuantitativo. Esta metodología mixta permite una comprensión más completa y profunda del fenómeno, integrando tanto el desarrollo teórico como la recolección y análisis de datos empíricos.

El desarrollo teórico se basa en una revisión exhaustiva de la literatura existente sobre ciberdelincuencia. Se analiza estudios previos, teorías criminológicas relevantes y casos documentados para construir un marco teórico sólido que sustente la investigación.

Se diseña y administran dos tipos de encuestas estructuradas. Por un lado, a una muestra representativa de la población, y por el otro a profesionales del sistema judicial. La encuesta incluye preguntas cerradas y escalas Likert para medir la percepción y experiencia de las víctimas y las percepciones de los profesionales encargados de gestionar estos delitos.

Consideraciones Éticas

Se garantiza la confidencialidad y el anonimato de todos los participantes. Además, se obtiene el consentimiento informado de cada uno de ellos antes de la recolección de datos. La investigación cumple con todas las normativas éticas vigentes en el ámbito académico y profesional.

RESULTADOS

Resultados de la primer encuesta:

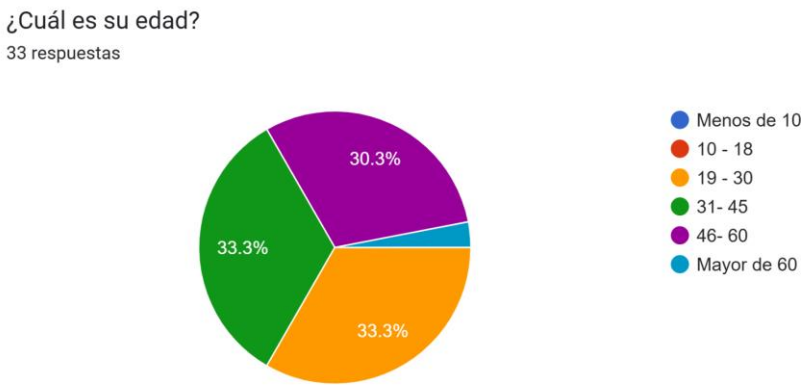

Gráfico n°1. Encuesta de ciberdelitos muestra representativa de población.

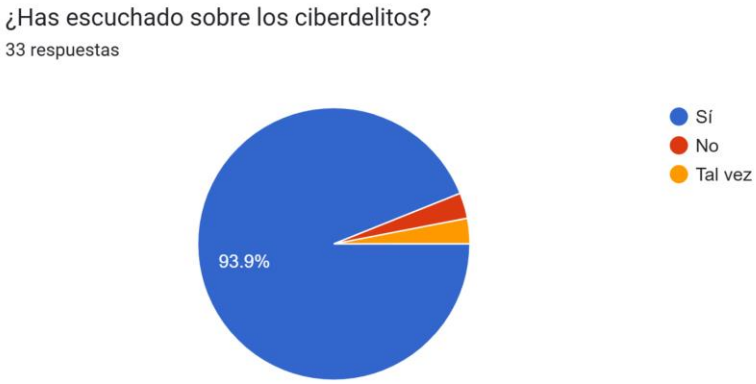

Gráfico n°2. Encuesta de ciberdelitos muestra representativa de población.

Gráfico n°3. Encuesta de ciberdelitos muestra representativa de población.

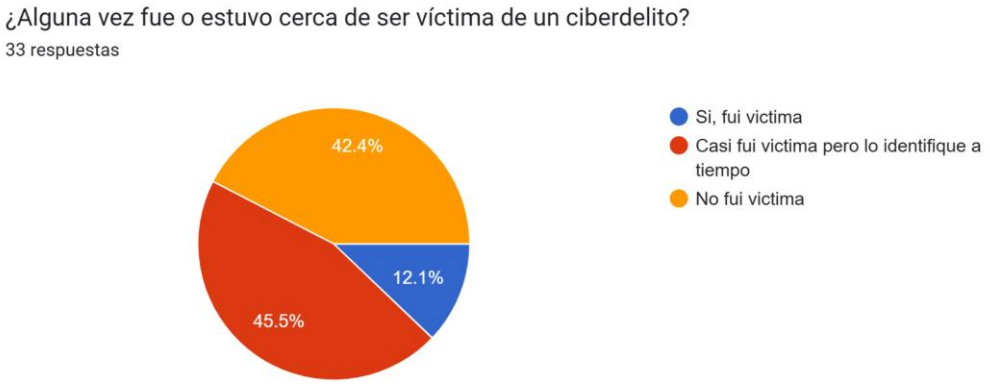

Gráfico n°4. Encuesta de ciberdelitos muestra representativa de población.

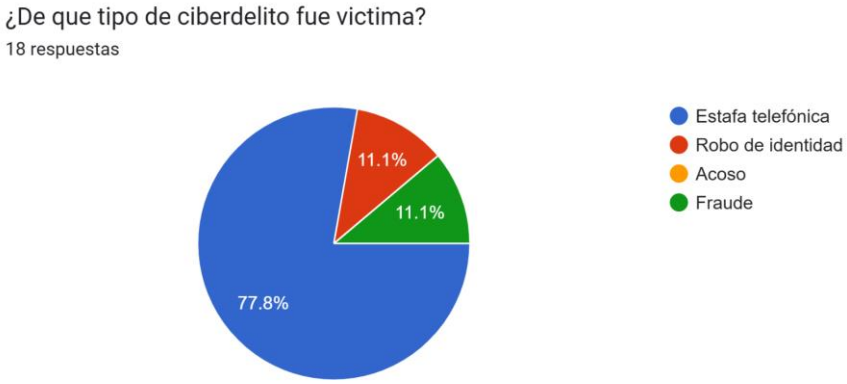

Gráfico n°5. Encuesta de ciberdelitos muestra representativa de población.

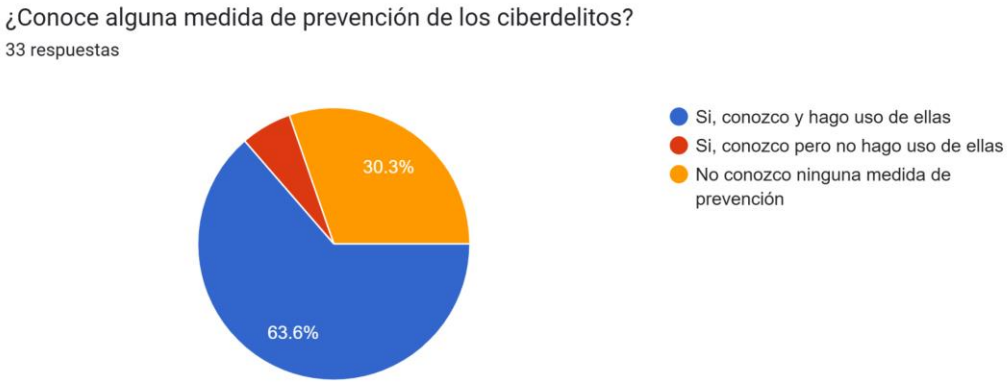

Gráfico n°6. Encuesta de ciberdelitos muestra representativa de población.

Gráfico n°7. Encuesta de ciberdelitos muestra representativa de población.

En el marco de la presente investigación, la primera encuesta fue respondida en su mayoría por personas de edades comprendidas entre los 30 y 60 años, quienes utilizan Internet diariamente. Los resultados, de acuerdo con las respuestas, muestran que los encuestados se sienten moderadamente seguros al realizar transacciones en línea, aunque la mayoría ha estado cerca de ser víctima de ciberdelitos. Sin embargo, algunos de los

encuestados lograron darse cuenta de la situación antes de verse perjudicados, siendo las estafas telefónicas el tipo de delito más frecuente que enfrentan.

En cuanto a las medidas que toman en respuesta a posibles ciberdelitos, la mayoría de los participantes opta por alertar a familiares y amigos, seguido de la denuncia formal del incidente. Un menor número de encuestados decide no tomar ninguna acción al respecto. Además, la mayoría implementa medidas de autoprotección para salvaguardar su información.

Todos los participantes consideran que los ciberdelitos son un fenómeno muy frecuente en la actualidad. Asimismo, la mayoría de ellos opina que los ciberdelitos representan una problemática más grave que otros tipos de delitos. También hay un gran porcentaje en que un ciberdelincuente puede acceder fácilmente a sus datos sin consentimiento. Todos los encuestados coinciden en que el ciberdelito es un problema que afecta significativamente a la sociedad en general.

Los resultados de la segunda encuesta fueron los siguientes:

Gráfico n°1. Encuesta a profesionales del sistema judicial.

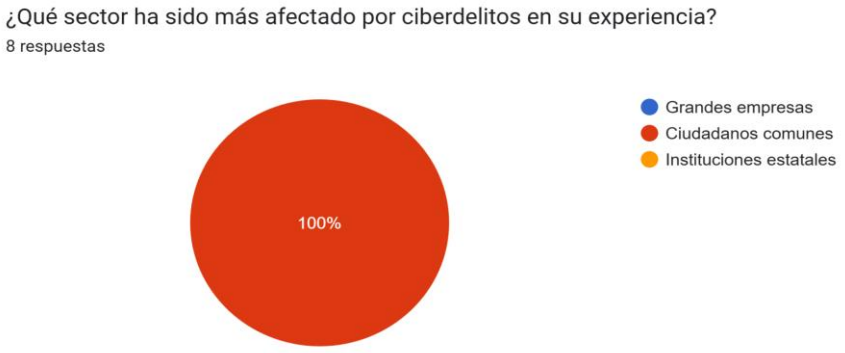

Gráfico n°2. Encuesta a profesionales del sistema judicial.

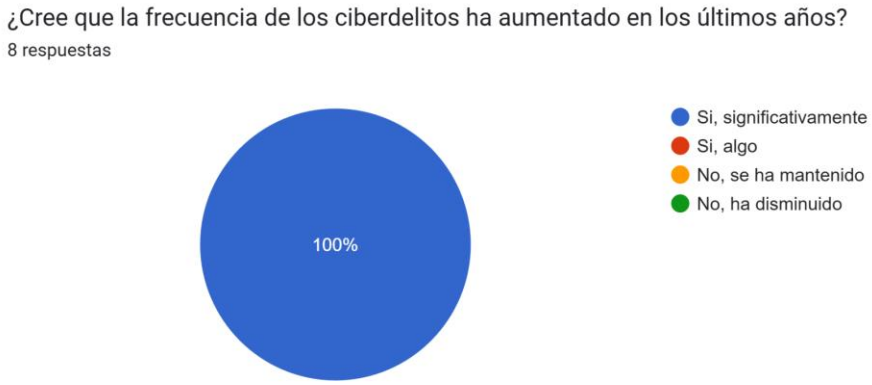

Gráfico n°3. Encuesta a profesionales del sistema judicial.

La segunda encuesta que fue realizada a profesionales del sistema jurídico revela, según las respuestas obtenidas, que casi la totalidad de los participantes ha manejado entre 10 y más 50 casos de ciberdelitos en el presente año. Todos los casos reportados han tenido como víctimas a ciudadanos comunes, lo que destaca la vulnerabilidad de la población general ante este tipo de delitos.

Los encuestados coinciden en que, en los últimos años, la frecuencia de los ciberdelitos ha aumentado considerablemente. Identifican varios factores como causantes de este incremento, entre los que se destacan la escasa información y concientización sobre el tema, la falta de educación en los usuarios, la alta cantidad de datos personales almacenados en dispositivos tecnológicos, la limitada difusión de campañas informativas y la tendencia de las personas a vivir a un ritmo acelerado, lo que las hace más propensas a caer en engaños fáciles.

En cuanto a las mejores formas de prevención, los profesionales señalan la importancia de informarse y capacitarse sobre ciberdelitos, la implementación de campañas de prevención y, lo más crucial, la necesidad de denunciar siempre cualquier incidente relacionado con este tipo de delitos. Estos resultados subrayan la urgencia de abordar el ciberdelito desde múltiples frentes para proteger a la ciudadanía.

DISCUSIÓN

En virtud de los resultados obtenidos en este trabajo de investigación se obtienen respuestas suficientes, a las preguntas de investigación, y se puede derivar en que la mayoría de los ciberdelitos cotidianos que vulneran la seguridad digital de los individuos no requieren sofisticadas habilidades informáticas de parte de los delincuentes, sino que desarrollan destrezas de ingeniería social causando un impacto profundo en las cibervíctimas. En este sentido y en función de la información del marco teórico es imperativo desarrollar estrategias de prevención y seguridad digital (con educación y conciencia pública) adaptadas a este nuevo entorno delictivo coincidiendo con lo señalado por Miró (20212) quien destaca la autoprotección ante estos hechos delictivos, ya que un objetivo será más adecuado mientras menos protegido este.

Atendiendo al hilo conductor de esta investigación se concluye que, si bien el internet y las nuevas tecnologías han transformado nuestras vidas de manera significativa y positivamente, también han generado un entorno propicio para la comisión de delitos cibernéticos. Este fenómeno demanda un enfoque renovado, tanto en la prevención como en la respuesta institucional y social.

Es importante señalar que muchos ciberdelitos no requieren altos conocimientos técnicos. En lugar de sofisticadas habilidades informáticas, los ciberdelincuentes se especializan en manipular psicológicamente a las víctimas, explotando su confianza y vulnerabilidades emocionales para lograr sus fines delictivos. Esta forma de "hackear" la mente humana, a través de engaños y persuasiones, demuestra que la complejidad de los ciberdelitos no siempre radica en la tecnología, sino en las estrategias de manipulación social empleadas por los atacantes.

Esta investigación pone de manifiesto la importancia de comprender tanto el perfil de los ciberdelincuentes como las circunstancias que llevan a los individuos a convertirse en cibervíctimas. Esto subraya la urgencia de desarrollar una educación digital más efectiva, que no solo informe sobre los riesgos tecnológicos, sino que también fomente habilidades de autoprotección frente a manipulaciones psicológicas. La prevención debe incluir no solo medidas reactivas, sino también una conciencia generalizada sobre los riesgos del ciberespacio y las formas de protegerse ante ellos.

sobre la base de los resultados de las encuestas realizadas se concluye, también que existe también una percepción generalizada de vulnerabilidad y la necesidad de información más accesible y clara sobre los ciberdelitos. Esto resalta la necesidad de una respuesta colaborativa entre la ciudadanía, las instituciones educativas y las autoridades,

con el objetivo de fortalecer la cultura de seguridad en línea y mejorar las estrategias de prevención.

PREVENCIÓN CRIMINOLÓGICA

A pesar de los esfuerzos para mejorar la protección de los sistemas informáticos, los ataques cibernéticos han dejado de tener metodologías que requieran conocimientos técnicos, sino que los ciberdelincuentes buscan el error humano. En este contexto,uno de los conceptos que han surgido para encasillar a varias estrategias direccionadas a combatir la ciberdelincuencia es la gobernanza de la ciberseguridad. Se refiere a la creación de políticas públicas que fomenten la cultura de la ciberseguridad, promoviendo principios éticos y responsables en el tratamiento de la información digital. La criminología contribuye a este enfoque al reconocer que, más allá de las medidas técnicas, la educación en seguridad cibernética y la promoción de comportamientos responsables son cruciales para reducir los riesgos de victimización (Mehan, 2014).

Para lograr la gobernanza efectiva de la ciberseguridad, es necesario un conjunto de políticas coherentes y coordinadas que permitan a los Estados anticiparse a los riesgos digitales. Estas políticas deben estar acompañadas de investigación tecnológica constante, debido a que las vulnerabilidades evolucionan con el avance de las tecnologías. Además, la cooperación internacional es esencial, dado que los ciberdelitos no respetan fronteras y a menudo son perpetrados desde lugares distantes, lo que requiere una respuesta global (Ochoa Marcillo, 2021).

Fernando Miró ha dado algunas recomendaciones para reducir los riesgos de ser víctimas de ciberdelitos. Estas indicaciones están dirigidas al ámbito preventivo en su mayoría.

En primer lugar, indica que se deben identificar zonas de riesgo. Esto se logra mediante campañas de información sobre riesgos, avisos en red de infección de spam, sistemas de listas blancas y negras de webs y spam. Señala también que se deben separar los objetivos, cuestión que puede conseguirse creando subredes de seguridad o separando la información. En el mismo sentido, también resulta efectivo ocultar los objetivos, cuestión que se puede realizar mediante encriptación, evitar el uso de datos personales en la red, o mejorar los niveles de protección de los canales de pago online (Miró, 2012).

El autor también señala que es importante descontaminar constantemente las máquinas con las que trabajamos y en las que almacenamos información, ya que, es más probable la presencia de virus mientras menos desinfección se haga; para esto se necesita también un buen sistema de detección de intrusos como herramientas antispam, antivirus, etc. En relación con lo último, se debe controlar el acceso al sistema, es decir, limitar quiénes pueden acceder a lo que se busca proteger, cuestión que se puede alcanzar, por ejemplo, mediante el uso de claves y su renovación continua (El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, 2012).

Entre las acciones que pueden permitir la prevención del cibercrimen, pero al mismo tiempo pueden servir para perseguirlo, encontramos en primer lugar que se debería aumentar el número de guardianes, esto no quiere decir que se aumente la cantidad de personas que están cuidando la información, sino que se implementen guardianes virtuales, por ejemplo: moderadores de foros, sistemas echelon, enfopol, carnivore, etc. En este mismo sentido, también se debería reforzar la vigilancia formal a través de equipos especializados de persecución del cibercrimen o grupos encargados de identificar el ciberdelito y darle seguimiento (Miró, 2012).

Por último, la mayor recomendación es el establecimiento de reglas internacionales, acompañado de canales de cooperación que permitan más celeridad y eficacia en el combate al cibercrimen. Al tratarse de un fenómeno transnacional, que puede ejecutar desde cualquier parte del mundo sin la necesidad de estar presente en el espacio físico en donde se encuentra el objetivo, la ciberdelincuencia se beneficia del trato diferenciado que da la legislación interna de cada país al problema.

Al no existir una forma concreta de combatirlo, o incluso al existir realidades en donde ni siquiera se da un tratamiento a esta criminalidad, las normas pueden convertirse en un límite y, por ende, obstáculo en la lucha contra el ciberdelito. La armonización internacional del derecho en este ámbito libera la posibilidad de unir esfuerzos para que las soluciones que se pretendan ejecutar también sean globales

Desde la criminología, opino que las siguientes propuestas pueden ser útiles para prevenir y combatir la ciberdelincuencia de manera efectiva:

- Capacitación continua en ciberseguridad: Incluir programas de formación en ciberseguridad dentro del ámbito educativo, desde la escuela hasta la universidad, para crear una cultura de seguridad digital desde edades tempranas. La prevención primaria también debe incorporar la concienciación pública sobre los ciberdelitos frente a los que se ven más vulnerables como lo es el grooming.
- Fomentar la responsabilidad ética en el uso de la tecnología: Promover la ética digital es una medida preventiva clave. Los usuarios deben ser conscientes de la importancia de proteger su privacidad y respetar la privacidad de los demás. Esto se puede lograr mediante campañas de sensibilización y el desarrollo de materiales educativos que expliquen las consecuencias legales y sociales de las actividades ilegales en línea.

- Fortalecimiento de la ciberpolicía y la cooperación internacional: Los cuerpos de seguridad deben estar bien entrenados y equipados para hacer frente a los ciberdelincuentes. Esto incluye la creación de unidades especializadas en delitos cibernéticos y la promoción de la cooperación internacional a través de organizaciones como Interpol o Europol para coordinar la lucha contra el cibercrimen en un nivel global.

REFERENCIAS

Santoyo, A. E. (2020). *Ciberdelitos: Retos y perspectivas jurídicas en el ciberespacio*. Tirant lo Blanch. https://books.google.com.ar/books?hl=es&lr=&id=iYvcDwAAQBAJ

Definición.de. (n.d.). *Ciberespacio*. Definición de ciberespacio. Recuperado el 18 de noviembre de 2024, de https://definicion.de/ciberespacio/#:~:text=En%20la%20actualidad%2C%20el%20concepto,servidores%20y%20de%20los%20usuarios

Ministerio Público Fiscal. (2023, junio 22). *Pedidos de selfies y de fotos del DNI: aumentan los fraudes vinculados con los servicios puerta a puerta del Correo Argentino*. Fiscales.gob.ar.

Martínez García, M. (2011). *El ciberespacio como nuevo ámbito de control social: Perspectivas criminológicas*. *Revista Electrónica de Ciencia Penal y Criminología*, *13*(7), 1–26. http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Gómez Vásquez, M. C., & Zambrano Alvarado, V. (2017). *La ciberdelincuencia: Análisis del ciberacoso en redes sociales desde el derecho penal ecuatoriano*. *Revista Arbitrada Interdisciplinaria de Ciencias Sociales y Educación*, *1*(2), 63–77. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992017000200063&lang=es

Cibercrim. (n.d.). *Fenomenología de la ciberdelincuencia*. Cibercrim. Recuperado el 18 de noviembre de 2024, de https://cibercrim.com/fenomenologia-de-la-ciberdelincuencia/#elementor-toc__heading-anchor-0

UOC. (2021, septiembre 23). *Ciberdelincuencia: Qué es y cómo combatirla*. Blogs UOC. https://blogs.uoc.edu/edcp/es/ciberdelincuencia-que-es-y-como-combatirla/

Leonel Benitz. (2018). *Delitos en la era digital: Cibercrimen y crimen organizado en un mundo interconectado*. Pensamiento Penal.

Irene Montiel Juan. (2020). Introducción a la civervictimizacion.

Dirección de Defensa del Niño y Adolescente de Córdoba. (2021). *Programa de protección digital*. Gobierno de la Provincia de Córdoba. https://ddna.cba.gov.ar/wp-content/uploads/2021/05/Programa-de-Proteccion-digital.pdf

Cibercriminología. (2024, noviembre 18). En *Wikipedia*. Recuperado el 18 de noviembre de 2024, de https://es.wikipedia.org/wiki/Cibercriminolog%C3%ADa

College of the Desert. (n.d.). *Module 3: Rational Choice Theory*. College of the Desert Pressbooks. Recuperado el 18 de noviembre de 2024.

Ley 26.388 (2008): Congreso de la Nación Argentina. (2008). *Ley 26.388: Modificación del Código Penal sobre delitos informáticos*. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar

Ley 25.326 (2000): Congreso de la Nación Argentina. (2000). *Ley 25.326: Ley de protección de datos personales*. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar

Ley 26.904 (2013): Congreso de la Nación Argentina. (2013). *Ley 26.904: Modificación del Código Penal sobre grooming*. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar

Consejo de Europa. (2001). *Convenio de Budapest sobre ciberdelincuencia*.

Consejo de Europa. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Ministerio de Justicia y Derechos Humanos de la Nación. (2017). *Argentina se convirtió en el primer país de América Latina en adherirse al Convenio de Budapest sobre ciberdelincuencia*. https://www.argentina.gob.ar/justicia

Consejo de Europa. (n.d.). *Explanatory Report to the Convention on Cybercrime*. Consejo de Europa. https://www.coe.int/en/web/cybercrime/explanatory-report

Organización de las Naciones Unidas. (2013). *Comprehensive Study on Cybercrime*. Oficina de las Naciones Unidas contra la Droga y el Delito. https://www.unodc.org

Ybarra, M. L., & Mitchell, K. J. (2020). *Ciberacoso y su impacto en el bienestar: Perspectivas y estrategias de intervención*. https://books.google.com.ar/books?hl=es&lr=&id=iYvcDwAAQBAJ

ANEXOS

Anexo 1. Experiencia personal

Durante el proceso de redacción de este Trabajo Final de Grado, experimenté una situación inesperada que, aunque incómoda, resultó ser una fuente valiosa de aprendizaje práctico sobre los métodos utilizados por los ciberdelincuentes en el ámbito de las estafas telefónicas. A través de WhatsApp, recibí un mensaje que, al principio, parecía ser una notificación legítima de una posible compra realizada con mi tarjeta bancaria. El mensaje solicitaba mi colaboración para "cancelar" la transacción, lo cual generó una sensación de urgencia.

Sin embargo, al percatarme de que algo no parecía correcto, decidí actuar con cautela y responder al ciberdelincuente con una actitud desconfiada. Tras unos minutos

de conversación, en los que traté de mantener la calma, decidí revelar al estafador el campo en el que estoy estudiando, mencionando que me encontraba escribiendo una tesis sobre la seguridad digital y que ya conocía las tácticas de los estafadores. De esta manera, busqué poner al descubierto sus intenciones. A mi sorpresa, esto no solo lo desarmó, sino que abrió una oportunidad para entablar una conversación más profunda.

Durante la charla, el ciberdelincuente compartió detalles sobre su modus operandi. Me explicó que su estrategia consistía en contactar, al azar, a personas mayores de edad, a quienes informaba sobre una supuesta compra fraudulenta realizada con sus tarjetas bancarias. Para "cancelar" la compra, las víctimas debían aceptar una videollamada en la que se les pedía compartir su pantalla. Este proceso, aparentemente inocente, en realidad permitía a los estafadores acceder a información confidencial, como los datos de las cuentas bancarias, con el fin de robarles el dinero.

Asimismo, pude indagar que el ciberdelincuente formaba parte de un grupo de jóvenes, en su mayoría hombres, que operaban bajo este mismo esquema. A pesar de las implicaciones negativas de su actividad, me resultó curioso observar que, según su testimonio, la mayoría de sus víctimas no eran personas mayores, sino adultos jóvenes, que por sus horarios de trabajo y la falta de tiempo para investigar, solían ser más vulnerables. La mayoría de estas personas eran profesionales ocupados que, al recibir las llamadas al mediodía, pensaban que se trataba de un problema urgente que necesitaba ser resuelto rápidamente. Esta urgencia llevó a que, sin darse cuenta, cooperaran con los estafadores, brindándoles acceso a su información personal y bancaria.

Este encuentro me permitió reflexionar profundamente sobre la vulnerabilidad de las personas ante los fraudes digitales y la importancia de la educación en ciberseguridad. La experiencia también me reafirmó en la necesidad de fomentar la conciencia sobre estos

riesgos y de promover prácticas más seguras en el uso de tecnologías, particularmente en lo que respecta a la protección de datos personales.

Anexo 2. Encuesta n°1

- ¿Cuál es su edad?
- ¿Has escuchado sobre los ciberdelitos?
- ¿Qué tan seguro te sientes realizando transacciones por internet?
- Alguna vez estuvo o estuvo cerca de ser víctima de un ciberdelito?
- ¿De qué tipo de ciberdelito fue víctima?
- ¿Conoce alguna medida de prevención de ciberdelitos?
- ¿Qué tan probable cree que es que un ciberdelincuente pueda obtener su información personal sin su consentimiento?

Anexo 3. Encuesta n°2

- En el último año, ¿Cuántos casos de ciberdelitos se le han dado a conocer?
- ¿Qué sector ha sido más afectado por ciberdelitos en su experiencia?
- ¿Cree que la frecuencia de los ciberdelitos ha aumentado en los últimos años?
- ¿Cuáles considera que son los principales factores que contribuyen al aumento de ciberdelitos?
- ¿Qué recomendaciones haría para mejorar la prevención de ciberdelitos?