Cuadernos de RES PUBLICA en derecho y criminología
Nº 01/2023 ISSN: 2990-0697 DOI:*10.46661/respublica.8072*

Estudio criminológico del ciberdelincuente y sus víctimas

Criminological study of the cybercriminal and his victims

Víctor Rodríguez González
Universidad Internacional Isabel I, Burgos (España)
victor.rodriguez.gonzalez@ui1.es
ORCID. 0000-0002-5348-9730

Claudio Augusto Payá Santos
Universidad Internacional de Cataluña. Barcelona. (España)
claudiop@uic.es
ORCID. 0000-0002-1908-9960

Bernardo Peña Herrera
Universidad Estatal de Milagro, Milagro (Ecuador)
bpenah@unemi.edu.ec
ORCID. 0009-0000-3667-0522

Resumen

Redes sociales, páginas web de compra, foros de debate o el acceso cualquier tipo de información y contenidos, son un espacio donde cada persona puede adoptar un rol diferente. Al mismo tiempo que esta evolución para el empleo correcto de la red, se desarrolló un complejo entramado delictivo, que logra sortear cualquier medida de seguridad que se haya intentado implementar. En este trabajo se analizarán los principales datos delincuenciales a través de la red entre 2015 y 2019, buscando la causa de estos y las posibles justificaciones a la falta de esclarecimiento de los hechos delictivos, ya bien afecten de forma unipersonal o colectiva en base a los datos facilitados por el ministerio del interior. Este trabajo, pretende dar una aproximación de la figura de la ciber víctima, las características propias de las dos figuras que comprende: el delincuente y la víctima.

Palabras clave: Ciber víctima, Ciber delito, Ciber delincuente.

Abstract

Social networks, shopping websites, discussion forums or access to any type of information and content are a space where each person can adopt a different role. At the same time as this evolution for the correct use of the network, a complex criminal network has developed, which manages to circumvent any security measures that have been tried to be implemented. This paper will analyse the main criminal data through the network between 2015 and 2019, looking for the cause of these and the possible justifications for the lack of clarification of criminal acts, whether they affect individuals or groups, based on the data provided by the Ministry of the Interior. This work aims to provide an approximation of the figure of the cyber victim, the characteristics of the two figures it comprises: the offender and the victim.

Key words: Cyber victim, Cyber crime, Cyber offender.

Cómo citar este trabajo: Rodríguez González, Víctor, Payá Santos, Claudio Augusto, y Peña Herrera, Bernardo. (2023). Estudio criminológico del ciberdelincuente y sus víctimas*. Cuadernos de RES PUBLICA en derecho y criminología, (2), 95–107. https://doi.org/10.46661/respublica.8072*

Recepción: 16.02.2023 **Aceptación:** 12.04.2023 **Publicación:** 05.05.2023

1 Introducción

Desde la irrupción de Internet y el mundo ciber en nuestra era, la sociedad ha experimentado un cambio radical en su forma de ser, actuar e interactuar con el entorno. Las redes sociales, páginas web de compra, foros de debate y el acceso a la información son algunos de los ámbitos en los que se ha notado un mayor cambio, dado que la red se ha convertido en un espacio donde cada persona puede adoptar diferentes roles. Estos cambios han tenido un efecto positivo en el uso correcto de la red, sin embargo, también han generado un complejo entramado delictivo (Chou, 2015).

El crecimiento desproporcionado de las redes informáticas ha permitido el desarrollo técnico y metodológico muy avanzado de los delincuentes que logran sortear cualquier medida de seguridad que se haya intentado implementar. Este fenómeno ha llevado a la aparición de la figura de la ciber víctima, que es objeto de diferentes tipos de delitos, como el acoso cibernético, el robo de identidad, el fraude en línea, entre otros. (Payá y Delgado, 2016).

En este contexto, es fundamental analizar las características propias de las dos figuras que comprenden este fenómeno: el delincuente y la víctima. En este sentido, la investigación pretende ofrecer una aproximación multifocal a la figura de la ciber víctima y a las características propias de cada uno de estos actores en el ciberespacio. Esto permitirá comprender mejor los riesgos asociados al uso de Internet y desarrollar medidas para prevenir y abordar el ciberdelito (Luque y Liz, 2021; Liz, 2018).

2 Aparición del espacio virtual: nicho para el delincuente encubierto

Datamos el nacimiento de internet en 1969. Se conoce como internet un conjunto descentralizado de centros de comunicación que tiene múltiples usos y gran parte de la población que recurre a ellos, lo hace con este afán, pero hay otro pequeño porcentaje que lo hace con unos fines no lícitos.

El fenómeno web fue tan revolucionario que en poco tiempo provoca un enorme aumento del número de usuarios pasando de los 14 millones de 1993, hasta los 4383 millones de usuarios en el 2019, siendo aproximadamente un 57% de la población mundial (Statista, 2021). En la actualidad, la mayoría de la población muestra cierto grado de dependencia diaria a la red, para cualquier tipo de uso social, económico o personal. Además, desde la aparición del virus SaRs-Cov-2, los confinamientos y las restricciones de movilidad y aforos, el mundo cibernético se ha visto potenciado por una necesidad imperiosa, por parte de la sociedad, para intentar mantener ciertas actividades sociales de una forma cuasi normal.

Según Curtis (2011), podríamos definir el ciberespacio como el dominio artificial construido de forma diferenciada de los cuatro dominios: tierra, aire, mar y espacio. Sin embargo, se ha confirmado que este espacio generado artificialmente, sí que puede afectar a los otros dominios. Además, el ciberespacio no está aislado, sino que está vinculado a una serie de medios físicos, por lo que también se puede ver influido por el dominio terrenal.

De forma simultánea a este desarrollo tecnológico, y como contraparte, se ha originado un polo negativo en el que encontramos términos como pueden ser los ciberdelincuentes y ciberdelitos, que engloban aspectos ilícitos acaecidos en el ciberespacio, amparando cuatro características, “se cometen fácilmente, necesitan pocos recursos para llevarse a cabo, pueden cometerse a nivel internacional y se aprovechan de las carencias de la punibilidad que existen en ciertos estados” (Zunzunegui, 2008, pp. 171).

Según Ponce (2012) la llegada de la web como la conocemos hoy en día ha revolucionado el concepto de red, en donde se comparte todo tipo de información en constante actualización. Esta web, denominada 2.0, se

ha llegado a llamar como web social o de los medios sociales, dado el auge que estos han tenido con el desarrollo de la red y con un aumento aún mayor en el año 2020, debido al COVID-19.

"El ataque se puede producir desde cualquier ubicación del mundo" (Centeno, 2015). Este hecho ofrece al delincuente unas capacidades casi ilimitadas a la hora de llevar a cabo sus planteamientos ilícitos. Principalmente, se debe a que el ciberdelincuente se siente seguro desde su ubicación por la lejanía de sus víctimas; una sensación de impunidad dadas las lagunas legislativas existentes y por la difícil intervención de las fuerzas y cuerpos de seguridad frente a un delito que pueda cometerse en tiempo y lugar determinados. Aprovechando la distancia y el anonimato que ofrece la red, cualquier persona usuaria de un equipo informático con conexión a internet, puede ser un objetivo potencial. Además, los conocimientos técnicos que han de poseer y la inversión económica que les permita llevar a cabo el delito son mínimos.

Cualquier ciberataque se lleva a cabo aprovechando una vulnerabilidad del sistema informático, por una falta de protección individual o, en ocasiones, por descuido. Todos los ciberataques, llevan asociados un alto impacto social y su difusión a través de medios de comunicación, bien sea por la entidad atacada o por el bien lesionado. El desarrollo tecnológico ha dado lugar a la aparición de un polo negativo, donde se encuentran términos como ciberdelincuentes y ciberdelitos, que incluyen actividades ilícitas en el ciberespacio. Estos delitos se caracterizan por ser fáciles de cometer, necesitar pocos recursos, poder llevarse a cabo a nivel internacional y aprovechar las carencias de la punibilidad en algunos estados.

Los delitos más típicos son los de fraude, chantaje, robo y falsificación. Pero, a través de las modificaciones legislativas de los últimos años, se han incorporado nuevos delitos como pueden ser el acoso a través de la red, revelación de secretos, delitos contra la propiedad industrial o todos los relacionados con abusos y fines sexuales. En el siguiente gráfico se pueden observar los datos de los delitos cometidos a través de la red de los últimos 5 años (Sistema estadístico de criminalidad).

Tabla 1. Principales tipos de cibercriminalidad entre 2015 y 2019.

	2019	2018	2017	2016	2015
Acceso e interceptación ilícita	4004	3384	3150	3243	2893
Amenazas y coacciones	12782	12800	11812	12036	10607
Contra el honor	1422	1448	1561	1546	2205
Contra la propiedad industrial	197	232	121	129	172
Delitos sexuales	1774	1581	1392	1231	1306
Falsificación informática	4275	3436	3280	3017	2644
Fraude informático	192375	136656	94792	70178	62038
Interferencia en los datos y sistemas	1.473	1192	1291	1336	1193
Total	218302	160729	117399	92716	83058

Fuente: elaboración propia según datos del Ministerio del interior (2021)

Como se puede comprobar, los casos se han multiplicado por casi por 6 en un periodo de tan solo 8 años, incluso han aparecido nuevas tipologías delictivas.

En el gráfico podemos observar la distribución de las infracciones penales relacionadas con la cibercriminalidad acaecidas en el año 2019, suponiendo el fraude informático un 60.67% de todos ellos, seguido por las amenazas y coacciones, con un 25.59%.

Según el último informe de ENISA (Agencia europea para la seguridad de las redes y la información) y, con base en Centeno (2015, 4-

5), se puede hacer referencia a las amenazas más relevantes, que son:

- Malware
- Botnets
- Phishing
- Denegación de servicio
- Correo basura
- Ransomware
- Robo o pérdida de información
- Robo de identidad
- Filtraciones de información

En el ámbito de la informática, se conoce como malware a todos aquellos programas maliciosos que afectan directamente a los contenidos de los sistemas informáticos a los que acceden. Estos softwares tienen como objetivo dañar, alterar o robar información del sistema en cuestión. Por lo general, el malware actúa a través de dos vías principales.

En primer lugar, podemos encontrar los ataques producidos en las webs utilizadas por el navegador, los cuales son muy comunes en la actualidad. En estos casos, el malware se instala en la computadora del usuario al visitar una página web infectada. Una vez que el software malicioso ha sido descargado, comienza a realizar diversas acciones que pueden poner en riesgo la seguridad de la información almacenada en el equipo.

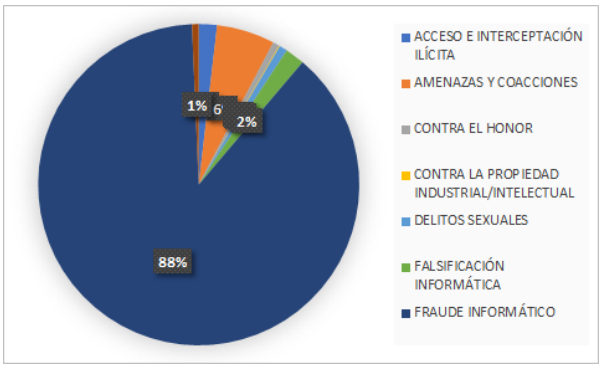
La otra vía utilizada por el malware es a través de aplicaciones web que dejan expuestas las vulnerabilidades del sistema. En estos casos, el software malicioso aprovecha las debilidades del sistema para infiltrarse y realizar sus acciones maliciosas.

Entre los tipos de malware más conocidos, podemos encontrar los ataques de denegación de servicio (DDoS), que buscan hacer imposible el acceso a los recursos de una entidad, y en algunos casos, piden una cuantía económica para detener el ataque. También están los bots, que son programas que toman el control de otros equipos de forma remota y se utilizan normalmente para la comisión de otros delitos.

Otro tipo de malware es el phishing, el cual se produce cuando alguien suple la identidad de otra persona o empresa para obtener información confidencial de la víctima. Este tipo de ataque es muy peligroso, ya que puede poner en riesgo la seguridad de datos sensibles, como contraseñas o información bancaria.

Finalmente, el spam o correo basura es uno de los tipos de malware más conocidos. Su objetivo es perjudicar al receptor a través del envío masivo de correos electrónicos no deseados. En ocasiones, este tipo de ataque se combina con el phishing para intentar obtener información confidencial de la víctima. Es importante que los usuarios estén siempre alerta y tomen medidas para proteger sus sistemas informáticos contra el malware.

Gráfico 1. Infracciones penales conocidas durante el año 2019



Fuente: elaboración propia según datos del Ministerio del interior (2021)

El malware es un término amplio que engloba todas las formas de software malicioso que pueden afectar directamente a los sistemas informáticos. El ransomware es un ejemplo de software malicioso que puede acceder al sistema y bloquearlo, dejando al atacante en control total del equipo. Además, los atacantes suelen pedir un rescate económico a cambio de desbloquear el equipo.

Las amenazas internas son otro tipo de amenaza que surge desde el interior de la organización y pueden causar daños significativos. Por ejemplo, los empleados con

acceso a información o aplicaciones confidenciales pueden utilizar estos privilegios para robar información sensible o identidades, con el fin de obtener mayores privilegios.

Los ataques informáticos pueden ser muy efectivos y pueden causar un daño económico significativo, especialmente cuando se aprovechan las brechas de seguridad existentes en los sistemas, en las personas o en las puertas traseras que ofrece la red. Es por eso por lo que es necesario establecer alianzas internacionales para luchar contra la delincuencia cibernética, ya que muchos de estos ataques tienen un carácter transfronterizo.

El término ciberterrorismo hace referencia a toda acción ilegal informática que tiene como objetivo dañar sistemas operativos y redes de internet a gran escala. Sin embargo, algunos delitos no están correctamente legislados o aparecen nuevos tipos que dificultan su persecución legal y la imposición de una sanción coherente. La preparación y ejecución de ataques cibernéticos suelen estar respaldados por el uso de múltiples medios en red, que permiten a los atacantes conectar con otras personas que persiguen los mismos objetivos y generar un caldo de cultivo perfecto para la elaboración de grandes ataques con grandes perjuicios a personas e instituciones.

El aumento de la ciberdelincuencia requiere de medidas de seguridad más efectivas y de una cooperación internacional más sólida para combatir estas amenazas y reducir su impacto. La educación y la conciencia sobre las amenazas cibernéticas también son clave para prevenir futuros ataques.

Los ciberataques pueden tener consecuencias mucho más allá de la esfera digital, ya que pueden generar daños físicos y provocar una crisis económica y social a gran escala. Por ejemplo, un ataque que cause una sobrecarga en los servidores centrales de una entidad bancaria o un ayuntamiento podría generar un cortocircuito físico y provocar un periodo de caos y desconocimiento generalizado. En el caso de grandes entidades bancarias, como menciona el texto, esto podría llevar a que cientos o miles de personas pierdan su dinero, generando una crisis económica y social de grandes proporciones.

Por otro lado, el ciberterrorismo se fundamenta en la conexión online de diferentes grupos que buscan sembrar el terror y desestabilizar la sociedad y el Estado. Estos grupos utilizan la red para intercambiar información estratégica, fuentes de financiación y planificar ataques. En muchos casos, estos grupos tienen una motivación ideológica concreta y buscan generar pánico y alarma social.

Es importante destacar que la ciberdelincuencia y el ciberterrorismo son delitos que conllevan implicaciones más graves que los delitos comunes, debido a su potencial impacto y alcance en la sociedad. Por lo tanto, es necesario que las entidades gubernamentales establezcan alianzas estratégicas internacionales para combatir este tipo de delitos, que a menudo tienen un carácter transfronterizo y requieren una respuesta coordinada a nivel global. Además, se debe prestar especial atención a la legislación de estos delitos para poder sancionarlos de manera coherente y efectiva.

El ciberespacio es un término cada vez más presente en nuestro vocabulario diario, y es que, como bien señala el Departamento de Defensa de Estados Unidos en su definición del año 2016, este entorno digital es un lugar de suma importancia para la sociedad actual. Se trata de un espacio global de información que se configura como una red interdependiente, que aglutina diferentes redes de telecomunicación, hardware y sus correspondientes controladores. De esta manera, el ciberespacio se ha convertido en una herramienta fundamental para la realización de actividades cotidianas, pero también en un objetivo codiciado por grupos criminales que buscan aprovecharse de las oportunidades que ofrece para alcanzar sus objetivos estratégicos (Delgado, 2023).

Además, estas organizaciones criminales han encontrado en el ciberespacio una plataforma ideal para difundir sus campañas de radicalización y odio, adoctrinar nuevos reclutas para sus fines y conseguir más recursos económicos. Es importante destacar que, gracias a la interconexión global que caracteriza al ciberespacio, estas actividades pueden tener una gran repercusión a nivel mundial, lo que amplifica aún más su impacto (Cruz y Liz, 2019).

En este sentido, el ciberespacio se ha convertido en un escenario clave para el desarrollo de la ciberdelincuencia, siendo utilizado por grupos criminales para llevar a cabo acciones como el robo de información, el secuestro de datos o la realización de ataques informáticos que buscan obtener un beneficio económico o un beneficio político. Es por ello por lo que la seguridad en el ciberespacio se ha convertido en una prioridad para los gobiernos y organizaciones, quienes deben estar preparados para prevenir y combatir los ataques cibernéticos que puedan poner en peligro su integridad y su estabilidad.

3 Ciber víctimas. Las víctimas de la red

Cuando se trata de evaluar la probabilidad de que alguien sea víctima de un ciberataque, hay varios factores que deben tenerse en cuenta. Uno de ellos es la especialización del ciberdelincuente, que se refiere a qué tipo de delitos cibernéticos comete con qué frecuencia. Otro factor importante es la visibilidad de la víctima, es decir, su presencia en línea y la cantidad de información personal que comparte en internet. La falta de seguridad y la accesibilidad de la víctima también pueden ser factores determinantes.

Es importante destacar que algunos ciberataques están dirigidos específicamente a una persona en particular, que es el objetivo principal del delincuente. Esto puede ser motivado por la posibilidad de obtener ganancias económicas debido al poder adquisitivo de la persona objetivo, o simplemente por el deseo de causar daño y perturbar la vida normal en línea de la persona.

El tipo de ataque y las personas objetivo dependen en gran medida de estos factores, así como de los recursos disponibles para cometer el delito. Por ejemplo, es común realizar campañas de phishing a miles de cuentas de correo electrónico de manera completamente aleatoria sin conocer a los destinatarios en particular. Sin embargo, esto solo es posible si se tiene acceso a grandes bases de datos de correos electrónicos registrados por los usuarios, que pueden ser proporcionados a terceros de manera fraudulenta para llevar a cabo estafas o extorsiones.

El desafío a la autoridad y la falta de respeto a las normas legales que regulan el uso adecuado de las tecnologías de la información, incluyendo el envío de correos electrónicos a desconocidos y el incumplimiento sistemático de las leyes de protección de datos, aumenta exponencialmente las posibilidades y capacidades de los grupos delictivos que operan en la red. Estos grupos tienen un mercado vasto y en constante crecimiento, ya que actualmente más del 60% de la población mundial tiene acceso a internet, y este número ha aumentado en más de 300 millones de personas en el último año debido a la pandemia de COVID-19.

El aumento masivo de usuarios de internet y la propagación del teletrabajo durante la pandemia de COVID-19 han llevado a un importante aumento de la delincuencia cibernética, con un incremento de alrededor del 300%. El confinamiento y el miedo al contagio han alterado significativamente los hábitos sociales, llevando a muchas personas a pasar más tiempo en línea, navegando por una variedad de sitios web y redes sociales, lo que ha abierto un gran número de oportunidades para los ciberdelincuentes.

Es importante destacar que los delincuentes cibernéticos aprovechan esta situación y

utilizan diferentes técnicas y herramientas para engañar a un gran número de personas con muy pocos recursos. La mayoría de las veces, el beneficio obtenido es muy elevado en comparación con los pocos recursos que se han utilizado para cometer el delito. Algunas de las técnicas más comunes utilizadas por los ciberdelincuentes incluyen el phishing, el malware y la suplantación de identidad, entre otras.

Además, la resolución de los casos de delitos cibernéticos sigue siendo un desafío importante para las autoridades. El índice de esclarecimiento de los hechos conocidos es inferior al 20%, lo que significa que la gran mayoría de estos delitos quedan impunes. Es fundamental que las autoridades trabajen en la mejora de los recursos y herramientas disponibles para combatir este tipo de delitos, y se fomente una mayor colaboración entre los diferentes organismos encargados de hacer cumplir la ley. Asimismo, es necesario que se implementen políticas y medidas de seguridad adecuadas en las empresas y organizaciones, y se eduque a los usuarios para que tomen medidas de seguridad adicionales para proteger sus datos y su privacidad en línea.

Tabla 2: relación de casos esclarecidos

Tipo de hecho conocido	Nº de casos	Nº de casos esclarecidos	Tasa de esclarecimiento
Abuso sexual	151	156	103,311258
Acceso ilegal informático	2024	224	11,0671937
Acoso sexual	136	73	53,6764706
Amenazas	10943	7039	64,3242255
Amenazas a grupo étnico cultural o religioso	10	5	50
Ataques informáticos	1373	42	3,0589949
Calumnias	368	210	57,0652174
Coacciones	1829	849	46,4188081
Contra la propiedad industrial	110	78	70,9090909
Contra la propiedad intelectual	87	52	59,7701149
Corrupción de menores/con discapacidad/diversidad funcional	183	115	62,8415301
Daños	100	21	21
Delito de contacto mediante tecnología con menor de 16 años con fines sexuales	456	183	40,1315789
Descubrimiento/revelación de secretos	1967	770	39,1459075
Estafa bancaria	40788	2418	5,92821418
Estafas con tarjetas de crédito, débito y cheques de viaje	88934	2855	3,2102458
Exhibicionismo	39	13	33,3333333
Falsificación de moneda, sellos y efectos timbrados	31	1	3,22580645
Injurias	1054	611	57,9696395
Otras estafas	62653	13439	21,4498907
Otros relativos al mercado/consumidores	13	4	30,7692308
Pornografía de menores	751	549	73,10253
Provocación sexual	58	37	63,7931034
Usurpación de estado civil	4244	1097	25,8482564
TOTAL	218302	30841	14,1276763

Fuente: elaboración propia según datos del Ministerio del interior (2021)

La resolución de delitos cometidos a través de la red es un asunto complejo debido a la dificultad para rastrear las actividades ilegales que se llevan a cabo en servidores remotos y a la eliminación de registros para evitar su seguimiento. Esta situación dificulta

enormemente la labor de las fuerzas y cuerpos de seguridad encargados de su resolución, lo que explica las bajas tasas de resolución de este tipo de delitos, que en ningún caso son consideradas altas.

Es fundamental tener en cuenta que los delitos cometidos a través de la red pueden tener un impacto negativo importante en la vida de las víctimas, incluyendo posibles secuelas emocionales y financieras. Por esta razón, es importante prestar especial atención a las víctimas y proporcionarles el apoyo y la ayuda necesaria para mitigar los efectos del delito y conseguir resarcirlas del perjuicio que han sufrido.

Es necesario que las autoridades adopten medidas efectivas para combatir la delincuencia en línea, incluyendo la creación de unidades especializadas en la investigación de delitos informáticos y la mejora de los recursos y herramientas disponibles para las fuerzas y cuerpos de seguridad encargados de la resolución de estos delitos. Además, es importante concienciar a los usuarios de internet sobre las posibles amenazas y riesgos que pueden encontrarse en línea y fomentar el uso responsable y seguro de la red. Solo así podremos reducir el número de delitos cometidos a través de la red y mejorar la seguridad y protección de los usuarios.

4 Las implicaciones de la inteligencia artificial en las ciber víctimas

La inteligencia artificial (IA) es una tecnología que ha ido evolucionando rápidamente en las últimas décadas y ha encontrado numerosas aplicaciones en diferentes campos, desde la industria hasta la atención médica y la educación. Sin embargo, su uso también ha planteado importantes desafíos y riesgos en términos de ciberseguridad y ciber víctimas.

La IA se ha convertido en una herramienta valiosa para los ciberdelincuentes, ya que les permite realizar ataques más sofisticados y difíciles de detectar. Según un informe de la consultora Gartner, se espera que para el año 2022 el 30% de los ciberataques se realicen mediante el uso de la IA. Los hackers pueden utilizar la IA para automatizar tareas repetitivas y obtener acceso no autorizado a sistemas y datos, lo que puede poner en riesgo la privacidad y la seguridad de los usuarios.

Además, la IA también puede ser utilizada para crear ataques de "phishing" más efectivos. Los ataques de "phishing" son una de las técnicas de ciberataque más comunes y consisten en enviar correos electrónicos fraudulentos que parecen legítimos para engañar a las víctimas y obtener información confidencial. Con la ayuda de la IA, los atacantes pueden personalizar estos correos electrónicos de manera más efectiva y engañar a las víctimas con mayor facilidad.

Otro riesgo relacionado con la IA y la ciberseguridad es la creación de "deepfakes". Los "deepfakes" son videos o imágenes manipuladas con tecnología de IA que pueden parecer muy realistas, pero que en realidad son falsos. Estos pueden ser utilizados para difundir información falsa o dañina, lo que puede tener consecuencias graves en términos de seguridad nacional o reputación empresarial. La creación de "deepfakes" también puede ser utilizada para la suplantación de identidad y la difusión de noticias falsas.

Por último, la IA también puede ser utilizada para desarrollar malware y otras herramientas de ciberataque. Por ejemplo, los atacantes pueden utilizar la IA para analizar los sistemas informáticos de una empresa y encontrar vulnerabilidades que puedan ser explotadas. Esto puede poner en riesgo la seguridad de los datos y sistemas informáticos de una empresa.

La IA ha traído consigo importantes avances en muchos campos, pero también ha creado nuevos riesgos y desafíos en términos de ciberseguridad y ciber víctimas. Es importante que las empresas y organizaciones tomen medidas para protegerse contra estos riesgos y trabajar en conjunto con expertos en ciberseguridad para estar preparados ante cualquier eventualidad.

5 *La IA y su ayuda a la prevención de la ciber victimización*

La ciberdelincuencia es un problema cada vez más grave y sofisticado, y las posibilidades de convertirse en víctima son muy reales. La inteligencia artificial (IA) puede ser una herramienta poderosa para ayudar a prevenir la ciberdelincuencia y proteger a los usuarios en línea.

La IA se puede utilizar para analizar grandes cantidades de datos y detectar patrones, lo que puede ser especialmente útil para detectar amenazas cibernéticas. Por ejemplo, las empresas pueden utilizar la IA para analizar el comportamiento de los usuarios y detectar patrones sospechosos, como intentos de phishing o acceso no autorizado a cuentas.

Además, la IA también se puede utilizar para predecir posibles ciberataques y tomar medidas preventivas antes de que ocurran. Por ejemplo, los sistemas de IA pueden analizar patrones de tráfico de red y detectar comportamientos anómalos que indiquen un posible ataque.

La IA también puede ayudar en la educación de los usuarios sobre las prácticas seguras en línea. Los chatbots de IA pueden proporcionar información sobre los riesgos cibernéticos y ofrecer consejos para protegerse.

Sin embargo, también hay desafíos en el uso de la IA para la ciberseguridad. La IA no es infalible y también puede ser vulnerable a los ataques de los ciberdelincuentes. Además, la implementación de la IA puede ser costosa y requiere una capacitación especializada.

En resumen, la IA puede ser una herramienta efectiva para prevenir la ciberdelincuencia y proteger a los usuarios en línea. Pero, es importante reconocer que no es una solución perfecta y se deben abordar los desafíos que pueden surgir en su implementación.

Según Kshetri (2018), el uso de la tecnología blockchain en combinación con la IA puede mejorar la seguridad y la transparencia en la cadena de suministro, lo que puede ayudar a prevenir la ciberdelincuencia. Además, Mendes, et. al., (2018) desarrollaron un sistema inteligente de detección de phishing que utiliza técnicas de aprendizaje automático y análisis de texto para identificar correos electrónicos de phishing.

El uso de la IA puede ser una herramienta valiosa para prevenir la ciberdelincuencia y proteger a los usuarios en línea. Sin embargo, también es importante abordar los desafíos en su implementación y considerar soluciones integrales que incluyan la educación de los usuarios, la tecnología y la legislación adecuadas..

6 Ingeniería social y la ciberseguridad en las víctimas en la red

La ingeniería social es una técnica que utilizan los ciberdelincuentes para manipular a las personas y hacer que revelen información sensible o realicen acciones perjudiciales para ellas mismas o para sus empresas. Esta técnica se ha vuelto cada vez más sofisticada con el paso del tiempo, y la inteligencia artificial (IA) ha permitido una mayor automatización y personalización en las técnicas de ingeniería social. Sin embargo, la IA también puede ser utilizada para detectar y prevenir ataques de ingeniería social y proteger a las ciber víctimas.

La IA puede ser utilizada por los ciberdelincuentes para realizar ataques de ingeniería social de manera más efectiva y a gran escala. Por ejemplo, los ataques de phishing pueden ser más sofisticados al utilizar técnicas de generación de texto basadas en IA para crear correos electrónicos que parezcan más auténticos y persuasivos para las víctimas potenciales (Mendes et al., 2018). Asimismo, la IA puede ser utilizada para crear perfiles falsos en redes sociales y plataformas de citas, para contactar a las víctimas y obtener información personal (Chauhan et al., 2021).

Además, la IA puede ser utilizada para automatizar la recolección de información

personal en las redes sociales y otras fuentes en línea, lo que puede ser utilizado para crear perfiles más detallados y precisos de las víctimas potenciales. Esto puede ser utilizado para crear ataques de ingeniería social más personalizados, como el spear phishing, en el que los atacantes utilizan información personal para crear correos electrónicos o mensajes de texto que parecen provenir de amigos o colegas (Chauhan et al., 2021).

Sin embargo, la IA también puede ser utilizada para detectar y prevenir ataques de ingeniería social. Por ejemplo, se han desarrollado técnicas de detección de phishing basadas en IA que analizan el contenido de los correos electrónicos y utilizan técnicas de aprendizaje automático para identificar patrones que sugieren que el correo electrónico es malicioso (Mendes et al., 2018). Además, la IA también puede ser utilizada para identificar perfiles falsos en las redes sociales y otras plataformas en línea, lo que puede ayudar a prevenir ataques de ingeniería social antes de que se produzcan.

En conclusión, la ingeniería social es una técnica sofisticada y en constante evolución utilizada por los ciberdelincuentes para engañar a las víctimas y obtener información personal o realizar acciones perjudiciales. La IA puede ser utilizada tanto por los atacantes como por los defensores para detectar y prevenir ataques de ingeniería social. Por lo tanto, es importante que las empresas y los individuos estén al tanto de los riesgos de la ingeniería social y adopten medidas de seguridad adecuadas para protegerse. .

7 Prevención y mitigación de ciber ataques y sus víctimas

La prevención y mitigación de los ciberataques es un aspecto crítico en el mundo actual altamente conectado. Estos ataques pueden causar daños significativos no solo a las organizaciones, sino también a las ciber víctimas individuales que pueden sufrir pérdida de datos, daño a la reputación, fraude financiero y otros efectos negativos. Por lo tanto, es esencial adoptar estrategias adecuadas para prevenir y mitigar los ciberataques, que incluyan medidas tanto preventivas como reactivas.

Las medidas preventivas deben ser proactivas y están diseñadas para evitar que se produzcan ataques. Estas medidas incluyen la implementación de políticas y prácticas de seguridad sólidas, la formación y educación continua del personal en seguridad cibernética, la actualización constante del software y la eliminación de vulnerabilidades conocidas, y el uso de medidas de autenticación fuertes, como la autenticación de dos factores. Estas medidas pueden ayudar a reducir significativamente la probabilidad de un ciberataque exitoso.

Además, es fundamental contar con medidas reactivas que permitan detectar y responder rápidamente a los ciberataques en caso de que ocurran. Estas medidas incluyen la implementación de sistemas de monitoreo y detección de amenazas, la configuración de alertas de seguridad, la realización de pruebas de penetración regulares y la preparación de planes de respuesta a incidentes. Estas medidas pueden ayudar a minimizar el daño que se produce después de un ciberataque.

Es importante destacar que, a pesar de estas medidas, la posibilidad de un ciberataque nunca se puede eliminar por completo. Por lo tanto, es fundamental contar con medidas de recuperación y resiliencia, como la realización de copias de seguridad regulares y el almacenamiento fuera de línea de información crítica, para minimizar el impacto de un ciberataque.

Las estrategias para prevenir y mitigar ciberataques deben ser integrales y abarcar tanto medidas preventivas como reactivas, así como medidas de recuperación y resiliencia. Adoptar estas medidas puede ayudar a proteger tanto a las organizaciones como a las ciber víctimas individuales de los ciberataques.

8 Conclusiones

El aumento exponencial de la ciberdelincuencia y su variedad de formas constituyen un motivo de preocupación a nivel global (Atienza & Bermejo, 2020). Los ciberdelincuentes no solo pueden vulnerar los datos más íntimos de personas y organizaciones, sino que también pueden actuar en contra de los intereses de sus víctimas, generando graves riesgos e incluso tensiones y conflictos sociales, como los procesos de radicalización (Atienza & Bermejo, 2020).

La ley, al no poder aplicarse retroactivamente, siempre va por detrás de los delitos cibernéticos y solo puede legislar a posteriori (Peñaloza, 2019). Esto puede generar situaciones de indefensión para las víctimas. Sin embargo, los sistemas jurídicos alrededor del mundo están tratando de adaptarse a las nuevas corrientes y demandas de la sociedad y a los nuevos delitos cibernéticos (Peñaloza, 2019).

Es esencial no dejar desamparada a la víctima del ciberdelito, ya sea por la falta de programas de prevención de la ciberdelincuencia, por la falta de legislación pertinente o por la falta de medidas para reparar el daño (Gorostidi, 2020). En muchos casos, la afectación a la víctima es tan grave que puede llevar a la ruina y al desamparo.

Es necesario investigar nuevas vías para prevenir los ciberdelitos y caracterizar e intervenir sobre la ciberdelincuencia a nivel policial y procesal para llenar los vacíos legales existentes (Calderón et al., 2019). También es fundamental considerar el tratamiento de las víctimas del ciberdelito a nivel psicosocial y comunitario para garantizar su protección y bienestar.

En resumen, la ciberdelincuencia es un problema global que debe ser abordado de manera integral y coordinada, involucrando a diversos actores y considerando las necesidades y derechos de las víctimas del ciberdelito.

Referencias

CARRERA CALDERÓN, FRANKZ ALBERTO; QUILLIGANA BARRAQUEL, JOEL ESTUARDO; AGUILAR MARTÍNEZ, MARIO DANILO; y FIALLOS BONILLA, SANTIAGO FERNANDO. (2019). Desafío de la ciberseguridad ante la legislación penal. *Dilemas contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v31i1.1236

CENTENO, DAVID. (2015). "El ataque se puede producir desde cualquier ubicación del mundo". El País. Recuperado de https://elpais.com/tecnologia/2015/01/27/actualidad/1422371877_899702.html

CHAUHAN, ANKUR KUMAR, SANJEEV & SANYAL, SUGATA. (2021). Intelligent phishing detection system using machine learning. International Journal of Advanced Science and Technology, 30(4), 488-496. https://doi.org/10.48175/IJARSCT-3801

CHEN, XIAOMING ZHOU, WEI & WANG, HONGXIN. (2021). *A survey on artificial intelligence in cyber security.* Journal of Cybersecurity, 7(1), 1-25. https://doi.org/10.1093/cybsec/tyaa018

CHOU, SAM, & CHOU, JONATHAN. (2015). Cybersecurity: The essentials. CRC Press.

CRUZ-BELTRÁN, JOSÉ. LUIS y LIZ-RIVAS, LENNY (2019). El perfil del ciberterrorista: la utilización de medios informáticos con fines terroristas, en; "El conflicto y su situación actual: del terrorismo a la amenaza híbrida", coord. por Carlos Espaliú Berdud, CIVITAS, pp. 159-173.

CURTIS, PAUL. (2011). The construction of the cyberspace: Metaphors and narratives of the web. In S. S. Yu & X. In (Eds.), Proceedings of the 2011 International Conference on Information Science and Applications (pp. 1-5). IEEE. https://doi.org/10.1109/ICISA.2011.5772305

DELGADO MORÁN, JUAN JOSÉ. (2023). Políticas públicas de seguridad en España.

Análisis desde perspectivas criminológicas. *Revista Opinião Jurídica, Fortaleza*, v. 21, n. 37, p. 183- 211, maio/ago. http://dx.doi.org/10.12662/2447-46641oj.v21i37.p183-211.2023

DE LA CUESTA ARZAMENDI, JUAN LUIS y SAN JUAN, CARLOS. (2010). *La cibercriminalidad.* Derecho penal informático, 57-78.

DE LA CUESTA ARZAMENDI, JUAN LUIS y PÉREZ MACHÍO, ANA ISABEL. (2010) *Ciberdelincuentes y ciber víctimas*. Derecho penal informático, 99-120

DE LA CUESTA ARZAMENDI, JUAN LUIS, PÉREZ MACHÍO, ANA ISABEL y SAN JUAN, CARLOS. (2010) *Aproximaciones criminológicas a la realidad de los ciberdelitos.* Derecho penal informático, 79-88.

FRIEDMAN, BATYA & KAHN, PETER. (2018). Human values, ethics, and design. In The Routledge Handbook of Philosophy of Engineering (pp. 408-419). Routledge.

GARCÍA-MARTÍNEZ, RAFAEL; GARCÍA-SÁNCHEZ, FRANCISCO; LÓPEZ-CORONADO, MARIO, & BUENO-CRESPO, ANDRÉS. (2021). *Artificial Intelligence and Cybersecurity: A Review of Recent Research*. Electronics, 10(7), 733. https://doi.org/10.3390/electronics10070733

Gartner report (2018). Gartner Says 30 Percent of Companies Will Use Artificial Intelligence to Augment at Least One of Their Primary Sales Processes by 2020.

GOPE, PRASENJIT & BISWAS, GUSTAM. (2020). *An AI-based approach for detecting phishing websites*. Multimedia Tools and Applications, 79(5-6), 4075-4093. https://doi.org/10.1007/s11042-019-08497-9

GOROSTIDI, JOKIN. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. *Estudios de Deusto*, *68*(1), 201-221. https://doi.org/10.18543/ed-68(1)-2020pp201-221

KSHETRI, NRIPENDRA. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

LIZ-RIVAS, LENNY. (2018). Algunas bases neurológicas sobre la violencia y la agresión, en ;"Conflictos y diplomacia, desarrollo y paz, globalización y medio ambiente " coord. Por Emilio José García Mercader, Claudio Payá Santos; César Augusto Giner Alegría (dir.), Juan Jose Delgado Morán (dir.), Thomson Reuters/Aranzadi, pp. 943-955

LUQUE JUÁREZ JOSÉ MARÍA, y LIZ-RIVAS, LENNY. (2021) Factores ligados a la violencia de género, evaluados en la valoración policial del riesgo, en; "Vulnerabilidad de las víctimas desde la perspectiva de género. Una visión criminológica". Víctor Rodríguez González (dir), Ana María Fuentes Cano, Dña. Tara Alonso del Hierro y D. Jonathan Torres Téllez.(coords), Dykinson, pp. 243-256. https://doi.org/10.2307/j.ctv282jjsk.15

MARTÍNEZ ATIENZA, GORGONIO Y FERNÁNDEZ BERMEJO, DANIEL. (2020). *Ciberdelitos*. Ediciones Experiencia.

MAROTTA, ANTONIO & RICCIADI, FEDERICA. (2017). Cybersecurity in SMEs: A literature review. Journal of Business Research, 84, 1-13. doi: 10.1016/j.jbusres.2017.11.011

MENDEZ, ANA MOURA, PAULO & PAULO NOVAIS, PAULO. (2018). Intelligent phishing detection system. International Journal of Information Management, 38(1), 137-147. doi: 10.1016/j.ijinfomgt.2017.09.004

Ministerio del interior (2019). Estudio sobre cibercriminalidad en España. NIPO 126-20-021-2

PAYÁ SANTOS, CLAUDIO. AUGUSTO., y DELGADO MORÁN, JUAN. JOSÉ. (2016). El uso del ciberespacio para infringir el terror. Estudios en Seguridad y

Defensa, 11(22), 91-108.https://doi.org/10.25062/1900-8325.211

PEÑALOZA, BERNARDO. (2019). Mendoza: hacia un Código Procesal Penal adecuado para la investigación de ciberdelitos. In *XIX Simposio Argentino de Informática y Derecho (SID 2019)-JAIIO 48 (Salta)*.

SINDRE, GUNNAR & OPDAHL, ANDREAS. (2011). A threat modelling approach to identification of security requirements. Information and Software Technology, 53(5), 490-503. doi: 10.1016/j.infsof.2010.12.005

SHOUHUAI & SASTRY, SRIRMAN. (2015). Metrics for cyber resiliency evaluation. Computers & Security, 52, 10-23. doi: 10.1016/j.cose.2015.04.005

VERDEJO ESPINOSA, MARIA ANTONIO (2015). *Ciberacoso y violencia de género en las redes sociales.* Universidad Internacional de Andalucía. ISBN: 978-84-7993-281-7

WANG, ZHE; ZHANG, YANCHAO; REN, KUI & LOU, WENJING. (2020). *AI-Supported Cybersecurity in Smart Homes: Challenges and Opportunities*. IEEE Network, 34(1), 88-95. https://doi.org/10.1109/MNET.001.1900275

WHITMAN, MICHAEL & MATTORD, HERBERT. (2016). Management of Information Security. Cengage Learning.

ZUNZUNEGUI, SERGIO. (2008). Pensar la imagen. Akal.