La Ciberdelincuencia en Costa Rica

Capítulo

06

José Adalid Medrano Melara

Cuando las personas leen noticias sobre ciberdelincuencia suelen ver este tema como si fuese algo que les resulta ajeno que pueden ver a la distancia. Lo más normal es que piensen que difícilmente puedan ser víctimas, porque podrían carecer de alguna característica importante que los grupos cibercriminales requieran. Sin embargo, hay que tomar en cuenta que cualquiera puede cometer hechos delictivos informáticos y que para ser afectado solo se requiere tener acceso a un sistema informático y/o acceso a internet.

Los ciberdelincuentes podrían querer atacarle únicamente para llegar a otra víctima, almacenar material ilícito o realizar ataques desde su computadora. Para lograr esto, muchas veces los delincuentes informáticos tienen acciones masivas automatizadas, por lo que ni siquiera es necesario que le evalúen para recibir un ataque.

La población es vulnerable a los ataques, pero no existe un programe que prepare al costarricense sobre cómo proteger su privacidad y nociones básicas de ciberseguridad. Aun así, en nuestro país, según los resultados de la Encuesta Nacional de Hogares Julio 2022 realizada por el Instituto Nacional de Estadística y Censos (INEC), el 76,9% de la población tiene acceso a internet en sus hogares[1], sin tener la oportunidad de aprender cómo protegerse.

La batalla digital entre ciberdelincuentes y la población nacional es desigual, ya que mientras los primeros son rápidos y eficientes para adecuarse a la tecnología, sus víctimas no están preparados para los riesgos que representa el ciberespacio. A manera de ejemplo, los cibercriminales ya están dando señales de aprovechar la inteligencia artificial generativa[2] para mejorar sus engaños, mientras la mayoría de la población todavía no ha aprendido a detectar los errores habituales contenidos en timos, como lo son las faltas de ortográficas y expresiones no adaptadas a la víctima.

A nivel mundial, de acuerdo con el informe de DarkTrace (Cole, 2023), se ha dado un aumento del 135% en nuevos ataques de phishing, donde los hackers están utilizando herramientas como ChatGPT para crear correos electrónicos de phishing más convincentes mediante el uso de un lenguaje sofisticado que coincide con la organización objetivo. Según Sweney (2023), la empresa de ciberseguridad ha descubierto que, aunque la cantidad de ataques por correo electrónico en su propia base de clientes se ha mantenido constante desde el lanzamiento de ChatGPT, aquellos que dependen de engañar a las víctimas para que hagan clic en enlaces maliciosos han disminuido, mientras que la complejidad lingüística, incluido el volumen de texto, la puntuación y la longitud de las oraciones, entre otros, ha aumentado.

En Costa Rica, el Organismo de Investigación Judicial (OIJ) indica que 64 personas por día son víctimas de fraude en el país (Carvajal, 2023). De acuerdo con el OIJ, esto puede consistir en: estafas tradicionales, timos, estafas informáticas, suplantación de páginas electrónicas y suplantación de identidad[3]. La realidad nacional es que los delincuentes locales no han variado demasiado sus estrategias para cometer estafas informáticas, porque no han necesitado hacerlo.

Sin embargo, la tecnología podría acelerar este proceso, como es el caso del uso de Inteligencia Artificial (IA) para las llamadas. En Norteamérica están proliferando estafas dirigidas a adultos mayores en donde se clona la voz de sus seres queridos, debido a las facilidades que presenta este tipo de tecnología en donde no se requiere

1 Según la Encuesta Nacional de Hogares del 2022, el 23,1% de la población no tiene acceso a internet en sus hogares (INEC, 2022, p. 66). El INEC (2022) define a los hogares sin uso de internet como 'aquellos con privación aquellos hogares donde ninguna persona, de 5 años o más, haya utilizado Internet en los últimos tres meses. En el caso de hogares conformados únicamente por personas adultas mayores (de 65 años o más), independientemente de sí utilizaron o no Internet en los últimos tres meses, no se considera con esta privación' (p. 16)."

2 La inteligencia Artificial Generativa es una especie de algoritmo creativo. Como lo reporta Hackl (2023), el Foro Económico Mundial (WEF) tiene la mejor definición hasta ahora sobre qué es la inteligencia artificial generativa. La describe como una categoría de los algoritmos de la inteligencia artificial que generan nuevos resultados basados en los datos recibidos. A diferencia de los sistemas tradicionales de IA, que reconocen patrones y hacen predicciones, la generativa crea nuevo contenido en forma de imágenes, texto, audio y más.

3 En estas categorías brindadas por el OJ se debe comprender que muchas de ellas corresponden al mismo delito en el Código Penal, pero que por un tema de mal manejo estadístico se establecen como el mismo.

tener conocimientos avanzados en informática para poder realizar este tipo de acciones.

Como podrá verse en este capítulo, la normativa costarricense ha venido adaptándose a las amenazas generadas por la ciberdelincuencia, tanto a nivel nacional como internacional, pero que este proceso de adaptación deberá acelerarse al ritmo que lo requieran los cambios tecnológicos.

En este capítulo se desarrollará el concepto sobre qué es un delito informático y el desarrollo que han tenido los tipos penales informáticos en nuestro ordenamiento jurídico, así como el análisis de propuestas que se han presentado para reformarlos. Se analizará sobre el cuidado que se debe tener al aprobar proyectos de ley sobre delitos informáticos, ya que distintos países las han utilizado para censurar a la prensa y disidentes. A su vez, se abordarán nuevas tendencias de la ciberdelincuencia, con el fin de brindar suficiente información para que puedan ser usadas en estrategias organizacionales, corporativas o a nivel nacional.

6.1 ¿QUÉ ES UN DELITO INFORMÁTICO?

En sentido estricto y en armonía con las reformas que ha venido incorporando el legislador a nuestro Código Penal se puede definir como toda acción delictiva informática, que está dirigida a vulnerar la confidencialidad, integridad, disponibilidad y/o normal funcionamiento de los sistemas informáticos, así como toda aquella acción que pretenda vulnerar la autodeterminación informativa y la identidad en medios electrónicos.

Para fines prácticos y hacer un adecuado estudio de la ciberdelincuencia, al delito informático se le puede definir en un sentido amplio **como toda acción delictiva que se desarrolla especialmente por medios informáticos. Esta definición** nos permite incorporar el estudio de ciertas modalidades de delitos tradicionales, en las cuales el elemento informático es protagónico y que son parte de la ciberdelincuencia moderna, organizada o no. La llamada "sextorsión" o extorsión sexual es un claro ejemplo para explicar la necesidad del uso de una **definición de mayor alcance, ya que como se indicó:**

Una modalidad delictiva que nos permite ilustrar lo anterior, es la 'sextorsión', en la cual los ciberdelincuentes por medio de la seducción, usualmente a través de la utilización de identidades falsas[4], establecen comunicaciones de contenido sexual o erótico con sus víctimas, para obtener fotografías o videos íntimos, con el fin último de amenazarles con la difusión del material íntimo sino le pagan un monto económico. En este caso nos encontramos ante una modalidad de extorsión simple[5] que:

a. Se despliega principalmente en el ciberespacio.

Involucra el tratamiento ilegal de datos personales.

a. Amenaza de/y/o difusión de documentos electrónicos de índole privada.
b. Es una figura explotada por el cibercrimen organizado[6]. (Medrano, 2021, p. 51)

Al mismo tiempo, es importante subrayar que la sextorsión también es común en contextos de exparejas, en donde una de las partes cuenta con material íntimo del otro y busca aprovechar este recurso para sacar provecho económico.

4 Una identidad falsa es toda aquella utilizada con fines fraudulentos o de engaño, al no corresponder con la identidad real del individuo.

5 En otras palabras, que comete la extorsión tradicional, que se encuentra en el párrafo primero del artículo 214 del Código Penal, que la sanciona con penas de prisión de 4 a ocho años de prisión. La extorsión agravada es la que utiliza informática, telemática, electrónica o tecnológica.

6 La BBC realizó un reportaje sobre este tipo de cibercrimen organizado: Cientos de miles de hombres de todo el mundo caen víctimas cada año de un crimen en internet llamado "sextorsión". Primero los hombres son atraídos y tentados a participar en chats sexualmente explícitos con cámara web, y después son chantajeados: o pagan o hacen públicos los videos. Los extorsionistas son grupos organizados que operan desde diferentes países, como Filipinas. (BBC Mundo, 2014, párr 1-3)

Figura 6.1. La industria del Cibercrimen

Fuente: Elaboración propia.

Este ejemplo, también sirve para destacar que aunque tradicionalmente se pensaba que los delincuentes que aprovechan los entornos digitales para vulnerar bienes jurídicos tutelados penalmente contaban con altos conocimientos esto no necesariamente es cierto. Esta idea nos puede hacer caer en el error de pensar que son un grupo pequeño que busca víctimas de alto perfil, lo que hace que quienes deban preocuparse por temas como la ciberseguridad sean únicamente las empresas.

Como puede verse con el ejemplo de la sextorsión de exparejas para cometer un delito informático solo se requiere tener acceso a la tecnología, no ser un experto, por lo que esa percepción de delincuente especializado no puede estar más alejada de la realidad, ya que en la actualidad cualquiera puede ser un ciberdelincuente. No solo porque los conocimientos para realizar estas actividades delictivas son menores, sino porque hasta las tareas más complejas son automatizadas a través de herramientas para delinquir que ciberdelincuentes especializados ponen a disposición de todos, ya sea de manera gratuita o luego de un pago.

En mayo del 2022, especialistas en ciberseguridad reportaron un malware que roba contraseñas de la víctima, el cual se encuentra disponible para que cualquiera pueda adquirirlo por el módico precio:

> Conocido como DCRat, es un malware con un precio de cinco euros y que, por lo tanto, es muy económico y accesible para cualquiera. Con esto, los hackers son capaces de vulnerar la privacidad de su víctima de diferentes maneras**.**
>
> Algunas de las funciones que tiene este malware son la de robar datos de todo tipo, que van desde contraseñas o nombres de usuario hasta el historial de navegación o la información que tengas almacenada en el sistema. (Castro, 2022, párr. 2-3).

Algunos investigadores de seguridad ven en este movimiento señales de una posible carrera a la baja con respecto a este tipo de herramientas delictivas, para que estén disponibles para cualquiera, en donde desarrolladores solitarios al tener costos más bajos pueden ofrecer mejores precios y esto debe tener bajo alerta a las organizaciones.

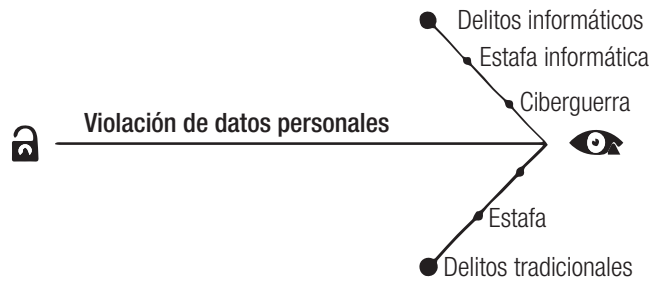
Entonces, si cualquier persona dentro del territorio costarricense y/o a nivel internacional puede realizar actividades delictivas informáticas en contra de otros individuos, empresas o el mismo Estado, es importante que las organizaciones cuenten con una estrategia de ciberseguridad, y el Estado posea una *Estrategia de Lucha contra la Ciberdelincuencia*. En ese sentido, en el 2021 se indicó que:

En la lucha contra la ciberdelincuencia se debe tener presente que nos encontramos ante un fenómeno transfronterizo de elevada complejidad, donde los grupos criminales no son homogéneos y se dedican a diferentes acciones delictivas que impactan a la sociedad de distintas maneras, por lo que es imperativo **crear una estrategia nacional que permita establecer un norte a las autoridades.**

Lo anterior es necesario, ya que el nivel de impunidad con el que operan las bandas locales de estafadores cibernéticos es tan grande que requiere que en la sociedad costarricense cada parte asuma su responsabilidad y colabore para detener este flagelo que erosiona la confianza en el sistema financiero nacional, al mismo tiempo que genera un gran daño en la ciudadanía. Lo más grave de la situación es que mientras estamos siendo derrotados por los cibercriminales locales, la ciberdelincuencia internacional no solo atenta contra empresas, organizaciones o individuos, sino que también dirige sus ojos hacia los gobiernos. Los ataques contra distintas naciones son parte de una estrategia delictiva de muchos gobiernos atacantes, quienes utilizan el ciberespacio para espiar a sus rivales y/o desestabilizarles, por lo que la capacidad de daño que tienen las acciones delictivas informáticas son ilimitadas.

Sin importar el área de acción de las bandas criminales o su ubicación geográfica, todas se alimentan de la información de carácter personal, ya sea para crear perfiles de sus víctimas para ataques posteriores o para utilizarla de forma directa en contra de estas, por lo que toda política criminal que busque mitigar el impacto de la ciberdelincuencia debe sancionar penalmente diferentes acciones informáticas que buscan violar la privacidad ciudadana. (Medrano, 2021, p.49).

Figura 6.2. El delito de violación de datos personales como un primer paso hacia la realización de otros delitos



Fuente: Tomado de Medrano, 2021.

Como puede verse, una de las principales fuentes que alimentan a los grupos delictivos es la información, ya sea a través de ataques de operadores externos o con la ayuda a nivel interno de las organizaciones, por lo que toda organización debe priorizar la ciberseguridad.

6.2 EL SURGIMIENTO DE LOS DELITOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO COSTARRICENSE

El legislador costarricense ha sido bastante previsor con respecto a la protección de los sistemas informáticos de los ataques que se han dado en su época, lo que vamos a ir explorando en un desarrollo histórico de estos tipos penales en nuestro ordenamiento jurídico.

6.2.1 Las reformas a la ley tributaria y de Aduanas (1995)

En 1995 Costa Rica inicia el camino hacia la inclusión de los delitos informáticos en nuestro ordenamiento jurídico, con las siguientes reformas:

1. **Ley de Justicia tributaria (Ley №7535, 1995):** reforma al Código de Normas y Procedimientos Tributarios:

Artículo 93.- Sanciones por **manejo indebido de la información:** Será sancionado, con prisión de **uno a tres años,** quien oculte o destruya información, libros contables, bienes, documentos, registros, sistemas y programas computarizados, soportes magnéticos u otros medios de trascendencia tributaria en las investigaciones y los procedimientos tributarios.

Artículo 94.- Sanciones por **acceso desautorizado a la información**: Será sancionado, con prisión **de uno a tres años**, quien, por cualquier medio tecnológico, acceda a los sistemas de información o las bases de datos de la Administración Tributaria, sin la autorización correspondiente. [7]

7 *Reformado el 14 de diciembre de 2016 por Ley para Mejorar la Lucha contra el Fraude Fiscal (Ley N° 9416),* en la cual se incluyó el elemento de beneficio propio como un elemento necesario

Artículo 95.- Sanciones por **manejo indebido de programas de cómputo:** Será sancionado, con pena de **tres a diez años de prisión**, quien se apodere, copie, destruya, inutilice, altere, transfiera o tenga en su poder, sin la autorización debida de la Administración Tributaria, cualquier programa de cómputo utilizado por ella para administrar la información tributaria y sus bases de datos, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.

Artículo 96.- Sanción por **facilitar el código y la clave de acceso**: Será sancionado, con prisión de **tres a cinco años**, quien facilite su código y su clave de acceso, asignados para ingresar a los sistemas de información tributarios, para que otra persona los use.

Artículo 97.- Sanción por **prestar código y clave de acceso**: Será sancionado, con prisión de **seis meses a un año**, quien culposamente permita que su código o su clave de acceso, asignados para ingresar a los sistemas de información tributaria, sean utilizados por otra persona.

Ley General de Aduanas (Ley №7557,1995): ARTICULO 221.- Delitos informáticos: Será reprimido con prisión de uno a tres años quien:

a. Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.
b. Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.
c. Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.
d. Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

para que se configure la acción delictiva, de la misma manera como el delito de Violación de Datos Personales contenido en el Código Penal:
Artículo 94.- Acceso desautorizado a la información. Será sancionado con prisión de tres a cinco años quien, en beneficio propio o de un tercero, con peligro o daño para la intimidad o la privacidad o para la integridad de los datos, acceda por cualquier medio a los sistemas de información o bases de datos o a la información contenida en ellos sin la debida autorización de quien deba expedirla o del titular de los datos o, existiendo esta, no cuente con la justificación correspondiente. Será sancionado con prisión de uno a cuatro años, quien instigue, obligue o presione a una persona autorizada para que acceda a la información en beneficio propio o de un tercero, con peligro o daño para la intimidad o la privacidad, o para la integridad de los datos.
La pena será de cuatro a seis años de prisión, cuando las conductas descritas en esta norma sean realizadas por personas encargadas de administrar o dar soporte al sistema o la red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

6.2.2 La inclusión de delitos sobre pornografía infantil en el Código Penal y la reforma al Código Tributario (1999)

En 1999, el país hizo otro esfuerzo en esta materia al hacer las siguientes reformas:

1. **Ley contra la explotación sexual de las personas menores de edad (Ley № 7899,1999)**: Una reforma al Código Penal sobre la pornografía infantil que *incluyó en nuestro Código Penal los delitos de fabricación y difusión de pornografía, acciones que no necesariamente deben desarrollarse por medios informáticos:*

Artículo 173. —Quien fabrique o produzca material pornográfico, utilizando a personas menores de edad o su imagen, será sancionado con pena de prisión **de tres a ocho años.**[8]

8 La última reforma que ha recibido este artículo fue el 9 de setiembre del 2021 a través de la Ley para la prevención del acoso a personas menores de edad por medios electrónicos o virtuales (GROOMING) (Ley Nº 10020), y reza de la siguiente manera: Artículo 173- Fabricación, producción, o reproducción de pornografía. Será sancionado con pena de prisión de cinco a nueve años, quien fabrique, produzca o reproduzca, divulgue o utilice imágenes, la voz o los datos personales, por cualquier medio, de material pornográfico infantil. Igual pena

Será sancionado con pena de prisión de uno a cuatro años, quien comercie, transporte o ingrese en el país ese tipo de material con fines comerciales.

Artículo 174. —Quien comercie, difunda o exhiba material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de **uno a cuatro años.**[9]

2. **Otra reforma al Código de Normas y Procedimientos tributarios (Ley №** 4755, 1999): En la cual se deroga el tipo penal llamado "Sanciones por manejo indebido de información y se reformaron de la siguiente manera los siguientes artículos: Artículo 94.- **Acceso desautorizado a la información**: Será sancionado con prisión de **uno a tres años** quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente.

   Artículo 95.- **Manejo indebido de programas de cómputo:** Será sancionado con pena de **tres a diez años de prisión**, quien, sin autorización de la Administración Tributaria, se apodere de cualquier programa de cómputo, utilizado por ella para administrar la información tributaria y sus bases de datos, lo copie, destruya, inutilice, altere, transfiera, o lo conserve en su poder, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.

   Artículo 96.- **Facilitación del código y la clave de acceso.** Será sancionado con prisión de **tres a cinco años**, quien facilite su código y clave de acceso, asignados para ingresar a los sistemas de información tributarios, para que otra persona los use.

   Artículo 97.- **Préstamo de código y clave de acceso.** Será sancionado con prisión de **seis meses a un año** quien, culposamente, permita que su código o clave de acceso, asignados para ingresar a los sistemas de información tributarios, sean utilizados por otra persona.

6.2.3 Delitos informáticos contra los derechos de autor y conexos (2000)

En el año 2000, a través de la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual (№ 8039) se incluyó delitos que protegen los derechos de autor y conexos, los cuales por su redacción neutral o de manera expresa podría aplicar al ciberespacio. Por lo anterior, en diversos tipos penales se protegen las obras contra su reproducción, fijación, transmisión y puesta disposición al público, ya que en aquellos años empezaban a realizarse por medio de internet.

Dicha reforma incluye 3 tipos penal informáticos los cuales protegen las medidas tecnológicas que buscan evitar la vulneración de los derechos de autor:

Artículo 61. —Fabricación, importación, venta y alquiler de aparatos o mecanismos descodificadores. Será sancionado con prisión de uno a tres años quien fabrique, importe, venda u ofrezca para la venta, dé en arrendamiento o facilite un dispositivo o sistema útil para descifrar una señal de satélite portadora de programas, sin autorización del distribuidor legítimo de esta señal, de modo que pueda resultar perjuicio a los derechos del distribuidor.

Artículo 62. — Alteración, supresión, modificación o deterioro de las defensas tecnológicas contra la reproducción de

se le impondrá a quien inste u obligue a una persona menor de edad o incapaz a enviar material pornográfico de cualquier tipo, por cualquier medio electrónico. Será sancionado con pena de prisión de cuatro a siete años, quien transporte o ingrese en el país, por cualquier medio, este tipo de material. Para los efectos de este Código, se entenderá por material pornográfico infantil toda representación escrita, visual o auditiva producida por cualquier medio, de una persona menor de edad, su imagen o su voz, alteradas o modificadas, dedicada a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de una persona menor de edad con fines sexuales.

9 La última reforma que ha recibido este artículo fue el 9 de setiembre del 2021 a través de la Ley para la prevención del acoso a personas menores de edad por medios electrónicos o virtuales (GROOMING) (Ley Nº 10020), y reza de la siguiente manera: Artículo 174- Difusión de pornografía. Quien entregue, comercie, difunda, distribuya o exhiba material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de cuatro a ocho años. Se impondrá pena de cinco a nueve años, a quien exhiba, difunda, distribuya, financie o comercialice, por cualquier medio y cualquier título, material pornográfico en el que aparezca una persona menor de edad o incapaz, o lo posea para estos fines.

obras o la puesta a disposición del público. Será sancionado con prisión de uno a tres años quien, en cualquier forma, altere, suprima, modifique o deteriore los mecanismos de protección electrónica o las señales codificadas de cualquier naturaleza que los titulares de derechos de autor, artistas, intérpretes o ejecutantes, o productores de fonogramas hayan introducido en las copias de sus obras, interpretaciones o fonogramas, con la finalidad de restringir su comunicación al público, reproducción o puesta a disposición del público.

Artículo 63. —Alteración de información electrónica colocada para proteger derechos patrimoniales del titular. Será sancionado con prisión de uno a tres años quien altere o suprima, sin autorización, la información electrónica colocada por los titulares de los derechos de autor o conexos, para posibilitar la gestión de sus derechos patrimoniales y morales, de modo que puedan perjudicarse estos derechos.

La misma pena se aplicará a quien distribuya, importe con fines de distribución, emita o comunique al público, sin autorización, ejemplares de obras, interpretaciones o fonogramas, sabiendo que la información electrónica, colocada por los titulares de derechos de autor o conexos, ha sido suprimida o alterada sin autorización. (Ley № 8039, 2000).

6.2.4 La tercera inclusión de delitos informáticos en leyes especiales y la primera integración en el Código Penal de delitos Informáticos, en sentido restringido (2001)

Un año después, en el año 2001, se realizaron dos reformas que nuevamente vienen a incluir delitos informáticos en nuestro ordenamiento jurídico:

1. **Delito Informático en la Ley de la Administración Financiera de la República y Presupuestos Públicos (2001):** se agregó bajo el título de "Delito informático a distintas conductas que protegían al sistema informático, su información o sus componentes:

Art.111 Delito Informático. Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

a. Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.

b. Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

c. Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

d. Utilizar las facilidades del Sistema para beneficio propio o de terceros. (Ley N° 8131, 2001, artículo 111).

2. **Primera inclusión de delitos informáticos, en sentido restringido, en el Código Penal (2001)**: a través de la ley N° 8148 llamada "Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos" se adicionaron al Código Penal 3 tipos penales informáticos:

a. 196 bis. Violación de las comunicaciones electrónicas. Penas de seis meses a dos años.

b. 217 bis. Fraude informático. Penas de uno a diez años.

c. 229 Bis. Alteración de datos y sabotaje informático. Penas de uno a cuatro años.

De acuerdo con Chinchilla (2002) en su libro Delitos Informáticos, esta reforma fue motivada por un proyecto que presentó la Procuraduría General de la República (PGR), el cual fue determinante para incorporar las tres novedosas figuras penales, aunque lamentablemente dejó por fuera el hurto agravado mediante la utilización de tarjetas magnéticas o perforadas:

> Para el mes de febrero del año 2000, se verificó en Costa Rica un encuentro de Ministros de Justicia del continente americano, siendo uno de los desarrollados en dicha reunión, el impactante fenómeno de la delincuencia informática. Como resultado de dicha reunión, la Procuraduría General de la República confeccionó un proyecto de ley que el Poder Ejecutivo ha asumido y enviado a conocimiento de la Asamblea Legislativa, el cual provocó la reforma aludida al Código Penal de octubre del 2001.
>
> EI mencionado proyecto comprende la adición de cuatro preceptos al Código Penal, junto con una

reforma a la denominada "Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones", Ley N°7425 de 9 de agosto de 1994.

Como veremos, esta propuesta de la Procuraduría General de la República ha sido determinante para incorporar las novedosas tres figuras penales que regulan los delitos informáticos en el Código Penal, **lamentablemente quedaron por fuera dos reformas; la primera relativa al delito de hurto agravado,** donde se describen figuras delictivas relevantes, siendo una de ellas, la incorporación de las tarjetas magnéticas o perforadas, en calidad de instrumentos para consumar el ilícito. Ello resolvería muchos de los problemas que hasta ahora se han venido presentando con la utilización indebida o abusiva de las tarjetas magnéticas, especialmente, en los cajeros automáticos.

La segunda referida a legislación especial, como lo es la Ley sobre Intervención de las Comunicaciones, **donde se pretende admitir la intervención de comunicaciones telemáticas,** comunicaciones de tipo remoto, correo electrónico o cualesquiera otro tipo, documentos magnéticos, o la utilización de artificios técnicos de escucha, transmisión, grabación, reproducción del sonido o de la imagen, cualquier señal de comunicación telemática y en general cualquier delito que utilice como instrumento o tenga por objetivo los accesos no autorizados a computadoras o sistemas informáticos. (Chinchilla, 2002, pp.101-102).

6.2.5 Segunda reforma al Código Penal sobre Pornografía infantil (2007)

En el año 2007, a través de la reforma Nº 8590 denominada "Ley de Fortalecimiento de la Lucha Contra La Explotación Sexual de las Personas Menores de Edad mediante la reforma y adición de varios artículos al Código Penal, Ley Nº 4573 y reforma de varios artículos del Código Procesal Penal, Ley Nº 7594" se reforman/adicionan tipos penales para luchar contra la pornografía infantil:

1. **Tenencia de material pornográfico (artículo 173 bis.):** Se sanciona por primera vez la tenencia de material pornográfico infantil, con seis a dos años de prisión, adelantando las barreras de protección para proteger a menores de edad del tráfico de su imagen, ya que muchas veces las autoridades en allanamientos solo lograban encontrar los materiales pornográficos infantiles, más no pruebas de la comisión de los delitos contra los menores.
2. **Fabricación, producción o reproducción de pornografía:** se aumenta la pena en el párrafo segundo con respecto al ingreso al país de estos materiales, pasa de 1 a 6 años de prisión, cuando antes se sancionaba con hasta 4 años.

6.2.6 Las reformas más innovadoras y completas al Código Penal costarricense (2012-2013)

En momentos en donde empresas de seguridad informática reportaban que el cibercrimen se estaba volviendo social y los programas informáticos maliciosos se convertían en el eje central de los ciberdelincuentes para hacer operaciones cada vez más sofisticadas, nuestro país avanzó en la aprobación de dos reformas que le permiten luchar contra ese tipo de delincuencia. En ese contexto inicia una discusión en la Asamblea Legislativa, la cual comenzó con una propuesta de Carlos Chinchilla, ex presidente de la Corte Suprema de Justicia, la cual propone adicionar y reformar el Código Penal con los siguientes artículos:

1. Violación de datos Personales.
2. Abuso en el uso de los medios Informáticos.
3. Suplantación de identidad.
4. Hurto agravado.
5. Estafa informática.
6. Espionaje informático.
7. Uso de virus (software malicioso -Malware-).
8. Clonación de páginas electrónicas (páginas web).
9. Suplantación de sitios web para capturar datos personales (casos del phishing y pharming).
10. Daño informático.
11. Sabotaje informático (Chinchilla, 2010, p.139)

Esta propuesta fue la base para una importante discusión que generó reformas más innovadoras y completas al Código Penal costarricense sobre delitos informáticos, para lo cual se involucró a distintos profesionales en derecho informático.

a. El **7 de junio del 2012 se aprobó la ley N°9048**, la llamada Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, la cual finalmente adicionaba los siguientes delitos y/o agravantes:

1. **Artículo 196.- Violación de correspondencia o comunicaciones:** 3 a 8 años de prisión por la violación sobre documentos o comunicaciones privadas dirigidas a otra persona.
2. **Artículo 196 bis.- Violación de datos personales.** 3 a 8 años de prisión. Se sanciona el tráfico de datos personales.
3. **Artículo 214.- Extorsión.** Se reforma el tipo penal de extorsión**,** al incluirle un agravante, de 5 a diez años de prisión para la extorsión con manipulación informática, telemática, electrónica o tecnológica.
4. **Artículo 217 bis.- Estafa informática**. De tres a diez años de prisión. Se le hicieron algunas reformas necesarias para su aplicación, como la inclusión del ingreso de los datos y se le rebautizó, ya que anteriormente se denominaba como fraude Informático.
5. **Artículo 229 bis.- Daño informático.** De uno a tres años de prisión. El tipo penal de alteración de datos y sabotaje informático se dividió en dos, siendo uno de ellos el daño informático.
6. **Artículo 229.- Daño agravado.** Seis meses a cuatro años de prisión. Agrava el delito de daño cuanto este recae sobre equipos informáticos.
7. **Artículo 229 ter.- Sabotaje informático**. De tres a ocho años de prisión. Se le da una protección a la información contenida en bases de datos y se protege el funcionamiento del sistema informático, con el evidente error que la conducta requiere realizarse en provecho propio o de un tercero.
8. **Artículo 230.- Suplantación de identidad.** De tres a seis años de prisión. Se protege la identidad de las personas físicas o jurídicas, así como las de las marcas de ser suplantadas por medios electrónicos. Incorpora un elemento controversial con respecto al uso de identidades falsas o inexistentes, el cual se denunció que criminalizaba la utilización de seudónimos, lo cual podría ser riesgoso para la libertad de expresión.
9. **Artículo 231.- Espionaje informático.** De tres a seis años de prisión. Se busca proteger la información de valor para el tráfico económico de la industria y el comercio.
10. **Artículo 288. Espionaje.** De cuatro a diez años de prisión. Su elemento más controversial el de "informaciones secretas políticas" provenía de la versión original del artículo del Código Penal de 1970.
11. **Artículo 232.- Instalación o propagación de programas informáticos maliciosos.** De uno a nueve años de prisión. Se sanciona la instalación de malware, así como la ingeniería social dirigida a estos fines, entre otro tipo de conductas realizadas por los grupos cibercriminales para propagar malware y beneficiarse económicamente de esta actividad.
12. **Artículo 233.- Suplantación de páginas electrónicas.** De uno a seis años de prisión. Se sanciona la suplantación de sitios web legítimos en internet, así como el uso de estos con fines de Phishing (captura de información confidencial a través de estos).
13. **Artículo 234.- Facilitación del delito informático.** De uno a cuatro años de prisión. Se sanciona a las personas que facilitan los medios para la comisión de delitos efectuados mediante un sistema informático.
14. **Artículo 236.- Difusión de información falsa.** De tres a seis años de prisión. Se sanciona penalmente la difusión de información falsa que sea capaz de distorsionar o causar la seguridad y estabilidad del sistema financiero o de sus usuarios.

15. **Artículo 235.- Narcotráfico y crimen organizado.** Duplica cualquiera de los delitos cometidos por medio de un sistema informático y que afecta la lucha contra el narcotráfico o el crimen organizado.

16. **Artículo 167.- Corrupción.** De tres a diez años de prisión. (Error legislativo que reformó dicho artículo con la supuesta intención de sancionar el Child Grooming).

b. Pocos meses después se incluyó la reforma **N° 9135,** llamada **"Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal**", la cual fue impulsada debido a las acusaciones de mordaza por parte de la prensa (lo que se analizará más adelante), se lograron realizar algunas reformas importantes, en algunos artículos, que por razones políticas no todas las que se recomendaron. Los artículos reformados o adicionados fueron:

1. **Artículo 196.-Violación de correspondencia o comunicaciones.** Se redujo la pena mínima y máxima de prisión, por lo que se sancionará con uno a cuatro años de prisión. Se incluyó un segundo párrafo para sancionar la difusión de comunicaciones o documentos privados, pero dando mayor seguridad jurídica al eliminar cualquier sanción penal cuando se realiza en interés público. De la misma manera, se sanciona la contratación de terceros para que realicen estas conductas, así como la instigar y el promover la comisión de las mismas.

2. **Artículo 196 bis.-Violación de datos personales.** Se redujo la pena mínima y máxima, por lo que se sancionará con uno a cuatro años de prisión. Se eliminan los agravantes relacionados con bases de datos públicas y dos párrafos que en apariencia le dan mayor tranquilidad a la prensa con respecto a información de interés público y a las entidades supervisadas por la Superintendencia General de Finanzas (SUGEF), aunque técnicamente en ambos casos la exclusión sobre cualquier sanción resultaba innecesaria.

3. **Artículo 230.-Suplantación de identidad.** Se redujo la pena mínima y máxima, por lo que se sancionará con uno a cuatro años de prisión. Se eliminó el controversial elemento de "identidad falsa" que se denunció que podría ser usada para denunciar disidentes que usaran seudónimos y de esa manera coartar la libertad de expresión en entornos digitales.

a. **Artículo 293.-Revelación de secretos de Estado**. A pesar de no ser un delito informático y aunque no era un artículo originalmente contenido en la ley 9048, debido a las discusiones generadas por esta reforma se aprovechó para reformar y especificar que se sancionan específicamente a quien revele **secretos debidamente decretados relativos a la seguridad interna o externa de la nación.**

b. **Artículo 295.-Espionaje.** Se redujo la pena mínima y máxima, por lo que se sancionará con uno a ocho años de prisión y en la línea del artículo anterior se incorpora que se protegen los secretos debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional y las relaciones exteriores de Costa Rica.

c. **Articulo 167 bis.- Seducción o encuentros con menores por medios electrónicos**: se sanciona el Child Grooming, con una redacción más acorde a este tipo de conductas, pero por un error legislativo no se reformó el artículo 167, relacionado a la corrupción de menores para que volviese a su estado original.

6.2.7 Tercera reforma al Código Penal sobre Pornografía infantil (2013)

En el año 2013, también se realiza otra reforma al Código Penal, a través de la **Ley N° 9177**, denominada "Reforma de los artículos 173, 173 bis y 174 y adición de un artículo 174 bis al código penal, ley n.º 4573, y reforma del inciso 3) y del párrafo final del artículo 61 de la ley n.º 8764, Ley General de migración y extranjería" que viene a modificar los siguientes tipos penales:

1. **Artículo 173: Fabricación, producción o reproducción de pornografía:** La innovación de

esta reforma es incluir una definición para material pornográfico infantil el cual deberá entenderse como toda representación escrita, visual o auditiva producida por cualquier medio, de una persona menor de edad, su imagen o su voz, alteradas o modificadas, dedicada a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de una persona menor de edad con fines sexuales. (Ley N°9177, 2013, artículo 173).

2. **Artículo 173 bis: Tenencia de material pornográfico:** se aumenta la pena de uno a cuatro años de prisión, lo que pareciera responder a que los seis meses del extremo inferior de la norma vigente hasta el momento podía ser muy baja para el tipo de acción delictiva en contra de la niñez.
3. **Artículo 174: Difusión de pornografía:** esta reforma sanciona la difusión de pornografía infantil, así como todo el comercio generado con esta industria lo que puede verse en su párrafo segundo:

Quien entregue, comercie, difunda, distribuya o exhiba material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de tres a siete años. Se impondrá pena de cuatro a ocho años, a quien exhiba, difunda, distribuya, financie o comercialice, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o lo posea para estos fines.

6.2.8 Cuarta reforma al Código Penal sobre Pornografía

Grave error en la reforma sobre Child grooming

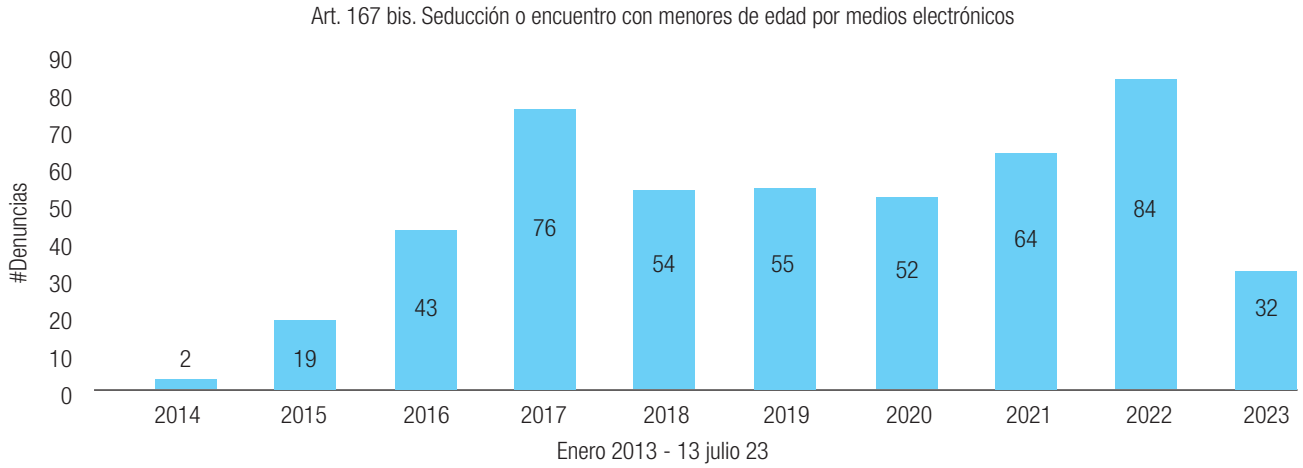
El Child grooming es una conducta de acoso sexual que se da por medios digitales, en donde el adulto seduce a un menor -lo que suele involucrar sexting- con el fin de conseguir:

1. Un encuentro con el menor para abusarle, violarle, asesinarle, secuestrarle, entre otros.
2. Pornografía infantil. (Medrano, 2021, párr.2).

En el año 2019, la diputada Floria María Segreda Sagot presentó el proyecto de ley № 21.507, denominado "**Ley del grooming (seguridad de menores en internet) y la obligación de los proveedores de contenidos y servicios digitales y reformas al Código Penal**". En este proyecto se buscaba sancionar el delito conocido internacionalmente como Child grooming, el cual desde el año 2013 (Ley № 9135) se encuentra contenido en el artículo 167 bis bajo el nombre "Seducción o encuentros con menores por medios electrónicos".

De acuerdo con los datos estadísticos del Organismo de Investigación Judicial, al momento de presentar el proyecto (hasta 2019), ya se habían presentado 249 denuncias por este delito.

Figura 6.3 Denuncias del delito de Child Grooming



Nota: Datos del 2023 parciales hasta julio.
Fuente de datos: Solicitud de Información 1674-OPO/UAC/S-2023 - Organismo de Investigación Judicial Oficina de Planes y Operaciones Unidad de Análisis Criminal.

En apariencia, la diputada desconocía que en nuestro país ya se sancionaba penalmente el Child Grooming y pretendía sancionarlo dentro de los tipos penales de Fabricación y Tenencia de pornografía infantil:

a. Artículo 173- Fabricación, producción, reproducción o Grooming de pornografía con personas menores de edad: en esta propuesta de reforma, se pretendía sancionar con penas de prisión de ocho a diez años de prisión a quien "inste u obligue a un menor de edad a enviar material pornográfico por medio electrónicos utilizando a persona mayor de ocho años y menor de dieciocho años de edad, su imagen y/o su voz".

b. **Artículo 173 BIS- Tenencia de material pornográfico con personas menores de edad:** En esta propuesta se buscaba sancionar aquel mayor de edad con pena de prisión de **uno a cuatro años de prisión** a quien sin fase previa de relación mediante engaño y generación de confianza, tenga fotos o videos sexuales del niño, niña o adolescente mediante la obtención de contraseñas o hackeo de cuentas.

Finalmente, esta propuesta de reformas fue cambiada, por lo cual la Ley Nº 21.507, modificó el artículo 167 bis, provocando los siguientes cambios:

1. Aumenta la pena en las conductas principales: de uno a tres años pasa a dos a cuatro años de prisión (antes de 1 a 3 años de prisión).

2. Incrementa la pena en el agravante: pasa de dos a cuatro años a tres a cinco años de prisión.

3. Aumenta la edad de consentimiento para tener comunicaciones de contenido sexual o erótico: se establece que 18 años será la edad para el consentimiento de este tipo de comunicación.

Adicionalmente, esta ley ocasiona problemas importantes en la reforma al tipo legal pues:

1. Aumenta las penas sin una clara justificación: una persona de 14 años y otra de 18 años podrían tener relaciones sexuales sin responsabilidad penal para el adulto, pero si establecen comunicaciones de contenido sexual o erótico para procurar dicho encuentro, el último podría enfrentar una sanción de hasta cinco años de prisión.

2. Se sancionan conductas entre personas próximas en edad y grado de desarrollo o madurez física y psicológica, sin que exista una justificación de política criminal para esta: en la normativa española se excluye la responsabilidad penal en estas condiciones, lo que tiene sentido ya que el derecho penal debe ser la última ratio. En nuestro país, respecto a las relaciones sexuales con menores de edad se busca algo similar con la normativa de relaciones impropias, pero si esta propuesta se convierte en ley de la República se puede prestar para que padres de menores de edad denuncien por comunicaciones sexuales entre jóvenes que ya han tenido relaciones sexuales (Una de 17 y otra de 18 años), pero no por estas que no son ilícitas, sino por las comunicaciones (Medrano, 2021).

Esta reforma también incluye cambios en los siguientes tipos penales:

Artículo 173 bis- Tenencia de material pornográfico: por un lado, se reduce el ámbito de protección al sancionar únicamente la tenencia de material pornográfico donde aparezca un material pornográfico de una persona menor de edad o incapaz, en vez del concepto más amplio que contiene el Código Penal. Por otro lado, sanciona la tenencia de material pornográfico donde aparezcan personas incapaces[10], lo cual sin duda genera dudas sobre si existe algún análisis de política criminal de algún tipo. Sin una debida justificación aumenta las penas de dos a cinco años de prisión, cuando antes eran de 1 a 4 años de prisión.

Artículo 167- Corrupción. Sin una debida justificación aumenta las penas, en el párrafo primero, de 4 a 9 años de prisión, cuando antes eran de tres a ocho años de prisión. Y en el párrafo segundo pasa de 4 a 10 años de prisión a seis a 12 años de prisión.

10 Un incapaz a nivel legal es una persona mayor de edad que no cuenta con capacidad de actuar debido a que presenta una discapacidad intelectual, mental y psicosocial, por lo que se le ha declarado en estado de interdicción y se le ha asignado un curador. Según Bresciani (2004), la curatela es una institución legal contemplada en el Código de Familia de Costa Rica, destinada a la protección de personas mayores de edad con discapacidad intelectual, mental, sensorial o física que les impida atender sus propios intereses, incluso si experimentan intervalos de lucidez. La curatela tiene como finalidad salvaguardar tanto los intereses personales como patrimoniales de la persona afectada durante el período de incapacidad.

Artículo 174- Difusión de pornografía. Sin una debida justificación aumenta las penas, en el párrafo primero, de 4 a 8 años de prisión, cuando antes eran de tres a siete años de prisión. En el párrafo segundo las aumenta de 5 a 9 años de prisión, cuando anteriormente eran de 4 a 8 años de prisión.

Artículo 173- Fabricación, producción, o reproducción de pornografía: Sin una debida justificación aumenta las penas, en el párrafo primero de cinco a nueve años de prisión, cuando antes eran de cuatro a ocho años de prisión.

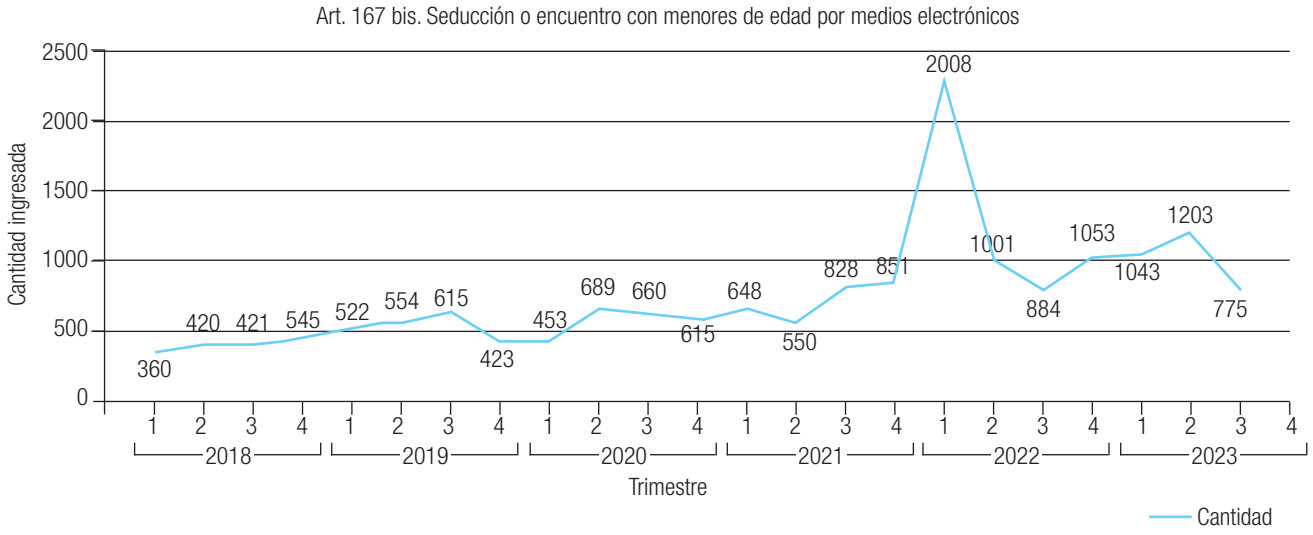
Adicionalmente, en el párrafo segundo, se agrega otra especie de *Child grooming* en el que se afirma que: "igual pena se le impondrá a **quien inste u obligue** a una persona menor de edad o incapaz a enviar material pornográfico de cualquier tipo, por cualquier medio electrónico." (Código Penal, 2021, artículo 173).

El problema surge de manera especial con el verbo "instar", ya que en poco varía la protección con respecto a los tipos penales vigentes y el aumento de la pena es significativo. Y con respecto al de obligar, hubiese sido más adecuado utilizar los conceptos utilizados en el tipo penal de coacción los cuales tienen mayor desarrollo jurisprudencial.

6.3 ESTADÍSTICAS DE DELITOS INFORMÁTICOS

Las estadísticas en Costa Rica sobre delitos informáticos presentan graves problemas, ya que las personas que reciben las denuncias no necesariamente cuentan con la capacitación para identificar qué delito informático es el que se está denunciando y otras veces el sistema informático utilizado para tal fin podría no contar con la información requerida. Adicionalmente, para un adecuado análisis del fenómeno de la ciberdelincuencia, es necesario que se deje constancia de la metodología utilizada por los ciberdelincuentes, con el fin de poder darle seguimiento y crear estrategias nacionales para mitigar el impacto de este tipo de delitos.

Figura 6.4. Cantidad de delitos informáticos por trimestre según año enero 2018 - julio 2023



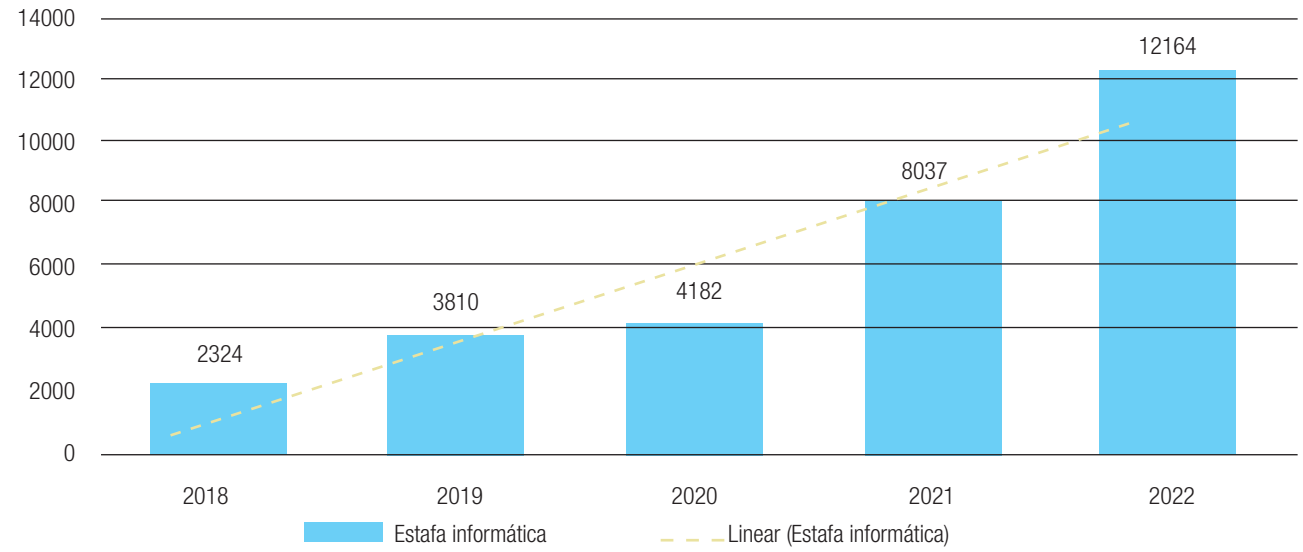
Fuente: Solicitud de Información 1674-OPO/UAC/S-2023 - Organismo de Investigación Judicial Oficina de Planes y Operaciones Unidad de Análisis Criminal.

En Costa Rica, el delito informático que más se denuncia es el de la Estafa Informática, que cuenta con más de 8229 denuncias desde enero del 2014 al 31 de julio del 2023, según las estadísticas del Organismo de Investigación Judicial (OIJ).

La explosión de las estafas informáticas en los últimos cinco años y siete meses ha sido tan grande que durante este período se han realizado el 93.53% de las denuncias contabilizadas desde el 2014.

Por otro lado, los datos de la Fiscalía General de la República reflejan una cantidad mucho mayor de casos de estafas informáticas que los reportados por el OIJ, pues del 2018 al 2022 se contabilizaron 30 517 causas por este tipo de delitos. Esta desavenencia con lo reportado por el OIJ refleja la existencia de un gran problema con las estadísticas del Poder Judicial.

Figura 6.5. Causas sobre estafas informáticas en Costa Rica (2018-2022)

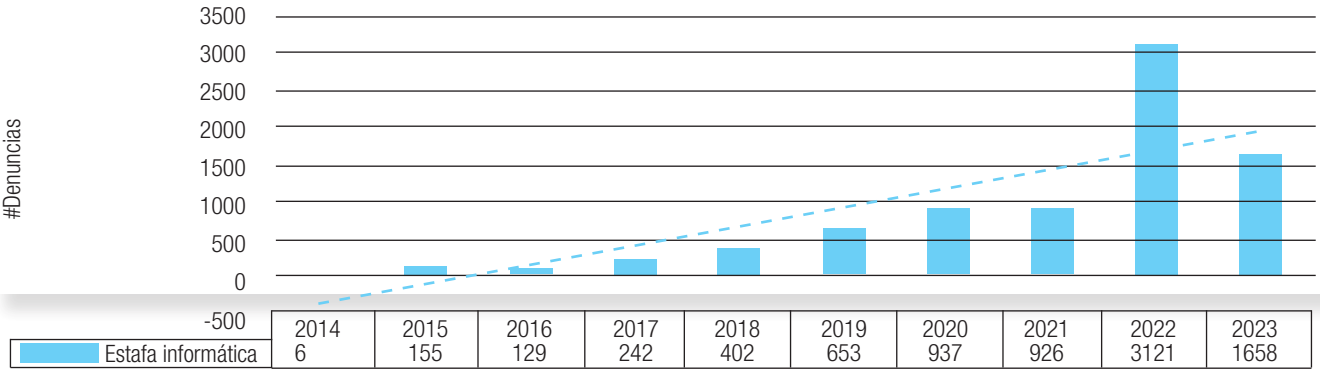


Fuente: Solicitud de Información 1674-OPO/UAC/S-2023 – Organismo de Investigación Judicial Oficina de Planes y Operaciones Unidad de Análisis Criminal.

6.4 LAS ESTAFAS INFORMÁTICAS EN PANDEMIA

Las estafas informáticas tuvieron una explosión durante la pandemia (2020-2022), ya que en este período se realizaron 4984 denuncias al OIJ, lo que corresponde al 60.5% de las que se han recibido desde el año 2012 sobre este delito[11]. Entre el 2019 y el 2020 hay un incremento de un 43.47% y entre el 2020 y el 2021, se da una reducción de un 1.17%, para el siguiente año aumenta un 236.23%

Figura 6.6. Estafas informáticas en Costa Rica 2014-julio del 2023



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Estafa informática	6	155	129	242	402	653	937	926	3121	1658

Fuente: Solicitud de Información 1674-OPO/UAC/S-2023 – Organismo de Investigación Judicial Oficina de Planes y Operaciones Unidad de Análisis Criminal.

11 Se excluyeron 1658 denuncias correspondientes a estafas informáticas denunciadas en el año 2023.

Por otro lado, de acuerdo con las estadísticas del Ministerio Público (MP), el impacto del cibercrimen organizado de estafas informáticas es todavía más grave de lo que reflejan las estadísticas del OIJ, ya que en este mismo período se computaron 24383 denuncias. Entre el 2019 y el 2020 hay un incremento de un 9.76% y entre el 2020 y el 2021, incrementa un 91.30%

En Chile, según datos de la Policía de Investigaciones de Chile (PDI), como lo reportó la Universidad de Chile (2021) hubo un incremento de un 20% en las estafas informáticas a inicios del 2021. En los primeros meses del año 2020 se registraron 4.687 denuncias por estafas informáticas y en el mismo período de 2021, los números subieron a 5.560.

De manera similar, en España las estafas informáticas incrementaron un 6.1% con respecto al período anterior. Según lo reporta ElDerecho.com (2022):

> Según los datos del Sistema Estadístico de Criminalidad (SEC) sobre este fenómeno en España, en el periodo comprendido entre 2017 y 2021 se constata el aumento de los delitos informáticos. Tanto es así que, en el último año se conocieron un total de 305.477 hechos, lo que supone un 6,1 por ciento más con respecto al año anterior. De esta cifra, el 87,4 por ciento corresponde a fraudes informáticos y el 5,7 por ciento a amenazas y coacciones por parte de los ciberestafadores.
>
> Por eso, mientras se registraron 305.477 estafas por estos medios, tan solo se esclarecieron 46.141 y solo 13.801 tuvieron como consecuencia la detención de algunos de los agentes maliciosos y la investigación de los acontecimientos (Europa Presos, 2022, párr.7-9).

De igual modo, Albalat (2023) reporta que solo en la provincia de Barcelona, los Mossos d'Esquadra tramitaron el año pasado 35.330 denuncias relacionadas con la ciberdelincuencia, de las que el 94,88% (33.522) respondían a fraudes en la red, como el robo de datos personales a través de mensajes de móvil o correo electrónico ('phishing') o la compraventa de productos en páginas web falsas.

En Argentina, la Unidad Fiscal Especializada en Ciberdelincuencia (2021) reportó que en los primeros 12 meses de pandemia los fraudes detectados fueron 8.559, lo que representa un 58,7% aproximadamente del total de los casos. Las estafas informáticas relacionadas con homebanking ascendieron a 1.064, que si se compara con el período anterior representa un incremento fue de un 6.550%[12]. Un año después, Gaik (2022) indica que según un informe presentado por el Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales de la Universidad Austral (Ocedic), las denuncias por estafas virtuales aumentaron casi un 200% en los tres primeros meses del año en comparación con el mismo período de 2021:

> El informe señala que en la Argentina se registran en promedio 4.800 fraudes mensuales en sus distintas modalidades (estafas en Whatsapp, phishing, usurpación de identidad y "cuento del tío 2.0"), por un monto aproximado de 1.200 millones de pesos.
>
> "El aumento de los fraudes virtuales es un fenómeno mundial que va en paralelo al avance de la tecnología, que creció exponencialmente durante la pandemia, y nuestro país no es la excepción", señaló Daniela Dupuy, directora del Ocedic y fiscal coordinadora de la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas del Ministerio Público Fiscal de la Ciudad de Buenos Aires (Ufedyci). (Gaik, 2022, párr. 2-3).

Es importante destacar que aunque los otros países están reportando crecimiento en las estafas informáticas, si vemos las cantidades de casos y las comparamos con la cantidad de habitantes que tiene cada país, se debe destacar que Costa Rica está reportando números realmente altos. Por otro lado, debe verse cómo las estadísticas suelen ser más completas, ya que países como España y Argentina cuentan con mayor detalle en sus estadísticas.

6.4 UNIDAD DE CIBERCRIMEN

El crecimiento exponencial de las estafas informáticas obligó a la Fiscalía Adjunta de Fraudes a crear una Unidad de Cibercrimen en enero del 2020, pues en el 2019

12 De la misma manera indican que anteriormente habían reportado una relación en el incremento entre este tipo de delitos entre los años 2019 y 2020 y ya daban cuenta de un crecimiento significativo -de un 3.652,9%.

entraron 4208 causas y al llegar el 2020 aumentaron a 7000. Debido este cambio, esta Fiscalía pasó a llamarse **Fiscalía Adjunta de Fraudes y Cibercrimen**.

Esta unidad es rectora a nivel país en causas sobre ciberdelincuencia, por lo que de alguna manera se busca crear un mayor impacto con el poco personal que manejan. Esta unidad cuenta con 5 fiscales (1 coordinador -el coordinador de la Unidad, Esteban Aguilar fue nombrado el presente año[13]- y 4 auxiliares), así como con 4 técnicos judiciales y un asistente jurídico.

Además, la unidad ha contado con distintas capacitaciones gracias al apoyo de distintos órganos internacionales y programas como el de GLACY+ del Consejo de Europa y su Comité del Convenio sobre la Ciberdelincuencia. Según el coordinador de la Unidad, se han desarrollado programas de capacitación en Cibercrimen dirigidos a fiscales, técnicos judiciales e investigadores en todo el país, con el propósito de fortalecer las capacidades nacionales en esta área.

6.4.1 Sección Especializada en Cibercrimen del OIJ

Nace como la Unidad de delitos informáticos en 1997, ante la necesidad de procesar información contenida en computadoras y servidores decomisados en casos importantes (OIJ, 2022). Esta instancia realiza investigaciones de Delitos Informáticos y de otros delitos donde la informática es utilizada para el acto delictivo o como medio de prueba. Adicionalmente, en el 2004 se constituye como Sección de Delitos Informáticos y en fecha reciente fueron renombrados como Sección Especializada en Cibercrimen.

> En la actualidad, a esta no se le brindan suficientes recursos para operar. Como han reportado distintos medios de comunicación se están dando atrasos importantes en todo tipo de casos, debido a la saturación de esta sección. Además, aunque su nombre indique que está especializada en cibercrimen, la realidad es que su labor se enfoca en la evidencia digital. De acuerdo con el señor Walter Molina, exfiscal general a.i., en declaraciones al periódico La Nación:
>
> Tenemos un gran retraso debido a que mucha de la prueba que llevan los casos tiene que ver con prueba tecnológica, con apertura de teléfonos, apertura de computadoras y la sección que le corresponde hacer ese tipo de trabajo tiene un retraso de dos años. El Fiscal Adjunto de Cibercrimen me había informado la semana pasada que hay como 6.000 asuntos atrasados por razones de prueba técnica, que todavía está en proceso de apertura y de revisión, señaló el fiscal interino. (Arguedas, 2018, párr.4).

En el 2018, el señor Walter Espinoza ya había indicado que dicha sección cuenta con poco personal:

> Evidentemente una Policía Judicial como la nuestra requiere potenciar esa oficina no solo para casos como éste sino para el futuro. Los delitos que se cometen por medio de las redes, en el ámbito de lo virtual y con el uso de Internet, están creciendo, son complejos y nosotros acabamos de suscribir una Convención Internacional que nos da obligaciones y que nos exige participar de manera profesional y científica, en ese sentido pues esa preocupación de no contar con esos muchachos evidentemente se mantiene y permanece, finalizó Espinoza. (Jiménez, 2018, párr.15).

De acuerdo con Esteban Aguilar, coordinador de la Unidad Especializada en Cibercrimen de la Fiscalía General, a la Sección Especializada en Cibercrimen del OIJ le hace falta desarrollar mayores capacidades técnicas. En entrevista para esta investigación indicó que con los ataques de Ransomware que enfrentó Costa Rica, fue notorio que a nuestro país le hacen falta herramientas con las que sí cuentan otras policías internacionales.

6.4.2 Falta de una Estrategia de Lucha contra la Ciberdelincuencia

El Poder Judicial requiere de una línea estratégica para luchar contra la ciberdelincuencia local y la internacional, las que no necesariamente se hablan entre sí, pero que comparten muchos elementos en común. Tanto el OIJ como el Ministerio Público deberían tener suficiente per-

13 El coordinador de la Unidad, Esteban Aguilar fue nombrado el presente año.

sonal capacitado para enfrentar los casos delictivos informáticos, pero para esto se requiere que tengan una hoja de ruta, la cual pueda ser analizada de manera constante y adaptada de acuerdo con el cambio de los delincuentes.

> El proyecto de Ley № 21187 denominado "Ley para luchar contra la Ciberdelincuencia" proponía la creación de una Comisión Nacional de Lucha Contra la Ciberdelincuencia, que entre otro tipo de funciones tendría a cargo una Estrategia Nacional contra la Ciberdelincuencia. Lo anterior permitiría que Poder Judicial sea más estratégico en la lucha contra el cibercrimen, pues estaría encargada de crear y mantener actualizada la Estrategia Nacional de lucha contra la ciberdelincuencia.
>
> Elaborar un informe (que deberá ser publicado cada dos años) sobre la eficacia del Ordenamiento Jurídico costarricense en la lucha contra la ciberdelincuencia.

Realizar una lista de proveedores relevantes de servicios electrónicos, para lo cual deberá tomar en cuenta el impacto de los servicios informáticos y de telecomunicaciones en la sociedad costarricense y cuando se encuentre disponible, la cantidad de usuarios costarricenses que usan dichos servicios.

- Sugerir protocolos de actuación para la investigación de delitos informáticos.
- Sugerir protocolos de cooperación en la investigación de delitos informáticos y computacionales con los operadores de telecomunicaciones nacionales y los proveedores esenciales de servicios electrónicos.
- Con base en estadísticas o datos judiciales, policiales o en general que sean de utilidad, provenientes de la cooperación con los proveedores de servicio en la investigación criminal, se realizará una calificación anual de los mismos, con el fin de identificar puntos de mejora. (Proyecto de ley para combatir la ciberdelincuencia, Expediente 21187, 2018)

Es importante destacar que para crear una comisión de esta clase no se requiere un proyecto de ley y se puede realizar en el Poder Judicial si así lo desean sus máximas autoridades.

6.5 EL SURGIMIENTO DE PERIODISMO CON INFORMACIÓN PROVENIENTE DE HECHOS DELICTIVOS

A nivel internacional, los casos de Snowden, Wikileaks, o los reconocidos Panamá Papers son emblemáticos, pues representan un ejercicio periodístico que se realiza con información proveniente de delitos informáticos y en los que el interés público de la información contenida en los mismos ha justificado los reportajes que han provocado transformaciones a nivel mundial. Con fines menos nobles, las extorsiones generadas por las bandas de ransomware, también están alimentando las salas de redacción de medios nacionales e internacionales.

6.5.1 El ataque de CONTI

El 17 de abril del 2022 un grupo de ciberdelincuentes inició el proceso de encriptación, extorsión y afectación de los sistemas informáticos del Ministerio de Hacienda (MH) y otras instituciones públicas. El ataque informático más importante que ha sufrido nuestro país estuvo a cargo de un grupo cibercriminal ruso, el cual logró apoderarse de información confidencial bajo la custodia de algunas instituciones, como el MH y la Caja Costarricense del Seguro Social (CCSS).

El gobierno decidió no ceder ante la extorsión y los delincuentes publicaron información en la darkweb, la cual de acuerdo con el gobierno incluye declaraciones de renta de empresas y ciudadanos, con la cual algunos realizaron notas periodísticas.

En el caso de **crhoy.com**, vale la pena destacar que ha decidido no revelar los nombres de las empresas cuyas irregularidades fiscales han quedado reveladas por las filtraciones delictivas, aunque sí ha brindado alguna información que permite identificarlas. Lo anterior, es un ejemplo de autorregulación que resulta adecuada, ante el ejercicio del periodismo con información proveniente de un hecho delictivo. El reportaje de este medio indica lo siguiente:

> Una cadena de supermercados y abarrotes de capital costarricense, otra cadena de supermercados por afiliación, una panificadora de origen extranjero, varias

> cadenas farmacéuticas junto con su casa corporativa, una multinacional de bebidas, al menos tres importadores de bebidas alcohólicas que en el pasado trabajaron bajo una misma sombrilla, distribuidores de alimentos, empresas de empaques, de manufactura, de importación de lapiceros, de productos azucareros, veterinarios…
>
> La lista **suma más de 200 compañías o "fichas" a**nalizadas entre el 1 de enero de 2020 y febrero del 2021, en las cuales el Ministerio de Hacienda las vinculó con posibles "fraudes, delitos aduaneros, infracciones administrativas y tributarias…
>
> CRHoy.com analizó la documentación. Por respeto a la confidencialidad que involucra el caso se omiten los nombres de las empresas, pero por la importancia e interés que reviste la información de carácter público por los impuestos que el fisco deja de percibir, se elaboró una tabla resumen a modo de ejemplo, indicando el área de operación de la empresa analizada, y los tres principales montos que Hacienda consideró se dejaron de percibir en el periodo, así como la "tipología de fraude" (así lo señala la documentación de Hacienda), para cada caso. (Valverde, 2022, párr. 5)

Esta práctica periodística es conveniente, tomando en cuenta que las personas jurídicas también son titulares de derechos fundamentales, como lo manifestó el Tribunal de Casación Penal de San José cuando analizó el delito de violación de comunicaciones electrónicas (Hoy violación de correspondencia o comunicaciones, debido a la reforma al Código Penal № 9048):

> Acorde con lo expuesto y no obstante la interpretación que esgrime el recurrente sobre la falta de tutela de la persona jurídica es evidente que el contenido de la norma no hace ninguna distinción entre la protección de una persona física o de una entidad jurídica, ello se desprende claramente de la decisión del legislador al usar el término " otro", que puede comprender o aludir indistintamente tanto a una como a la otra.
>
> Es más, las personas jurídicas, así como titulares de derechos y obligaciones, son titulares de derechos fundamentales que si bien no son iguales a los de la persona física si son asimilables a los de ésta, de ahí que aunque no tiene el derecho a la vida sí al respeto de su existencia jurídica y aunque no se les tutela la intimidad de la misma manera que a las personas físicas, ciertamente ello no implica o excluye la tutela de ese aspecto, máxime que estamos haciendo referencia a un concepto que es genérico y por ende varía de una legislación o otra, o lo que es lo mismo de una realidad a otra, y en el caso del derecho costarricense, el legislador optó por fijar su protección en el artículo 196 bis, en donde no se hace ninguna exclusión al respecto (Sentencia № 01208 del 30 de octubre, 2009).

A su vez, el Código de Normas y Procedimientos Tributarios en el numeral 117 indica que la información que se le brinda a la Administración Tributaria:

> Artículo 117.- Carácter confidencial de las informaciones. Las informaciones que la Administración Tributaria obtenga de los contribuyentes, responsables y terceros, por cualquier medio, tienen carácter confidencial; y sus funcionarios y empleados no pueden divulgar en forma alguna la cuantía u origen de las rentas, ni ningún otro dato que figure en las declaraciones, ni deben permitir que estas o sus copias, libros o documentos, que contengan extractos o referencia de ellas sean vistos por otras personas que las encargadas en la Administración de velar por el cumplimiento de las disposiciones legales reguladoras de los tributos a su cargo (Ley №4755, 1971, artículo 117).

En este contexto, en un país con una democracia plena y una historia de respeto a la prensa, resulta ser una buena práctica que los medios adopten medidas de autoregulación en defensa de los derechos digitales. Esto es relevante incluso en situaciones donde la parte afectada sea una entidad jurídica, sin que esto implique renunciar a la publicación de información de interés público relacionada con la labor periodística.

Lo anterior es importante destacarlo ya que desde el año 2013, una difusión de un documento o comunicación privada solo puede sancionarse penalmente si la misma carece de interés público. La norma reza de la siguiente manera:

> Artículo 196.- Violación de correspondencia o comunicaciones. Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima,

intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona.

La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público. La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.

La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este articulo son realizadas por:

a. Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.

b. Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. (Código Penal, 1970, artículo 196).

6.7 EL PHISHING

El *phishing* es una técnica muy utilizada por los ciberdelincuentes para ayudarse a cometer delitos informáticos. Según el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST, 2023), esta consiste en obtener datos sensibles (como números de cuentas bancarias) haciéndose pasar por un negocio legítimo o una persona de buena reputación, través de:

- Una solicitud fraudulenta por correo electrónico o
- En un sitio web.

En la primera mitad del 2023, la empresa de ciberseguridad Vade (2023) señala que los volúmenes de phishing aumentaron en más del 54% durante este período en comparación con la segunda mitad de 2022 (742.9 millones frente a 482.2 millones). Por otro lado, Cofense Intelligence (2023) en su reporte Q2 2023 sobre Inteligencia de Phishing y tendencias analizó correos electrónicos de phishing de credenciales que llegaron a usuarios en entornos protegidos por Sistemas de Puertas de Enlace de Correo Electrónico Seguras (SEGs), con los cuales identificaron nombres de dominio más usados. Los principales dominios .com utilizados son: amazonaws.com, sharepoint.com, Google.com, Backblazeb2.com y Microsoft.com.

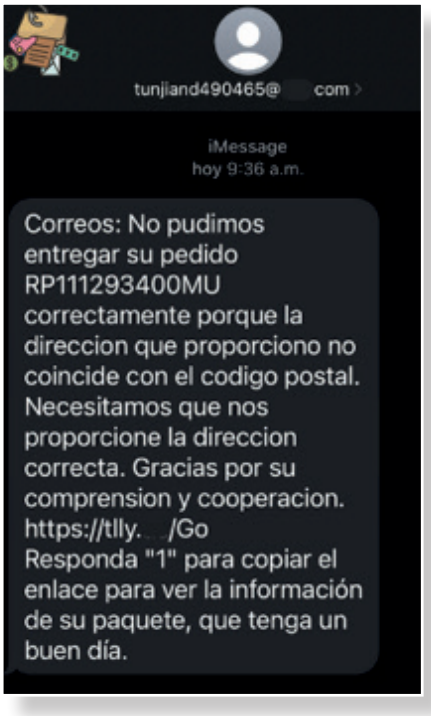
De acuerdo con Trend Micro (2023), los principales tipos de phishing son los siguientes:

Spear Phishing (Pesca con lanza). El término proviene de la analogía de la pesca, donde pescar con una lanza permite al pescador elegir específicamente el pez que desea atrapar. De manera similar, el *spear phishing* se enfoca en un grupo específico de individuos con el fin de maximizar las posibilidades de éxito.

Whaling (Pesca de Ballena). Es una especie de *spear phishing* que se dirige a específicamente a individuos de alto nivel en una organización como directores, gerentes y puestos de alto nivel dentro de la organización.

Smishing (Phishing de mensaje de texto). Este ataque suele usar mensajes de texto o SMS (short message service) para ejecutar el ataque. Dentro de esta categoría se suele incluir a aquellos mensajes que se envían por medio de plataformas de mensajería (Whatsapp, Telegram, Signal, entre otros.)

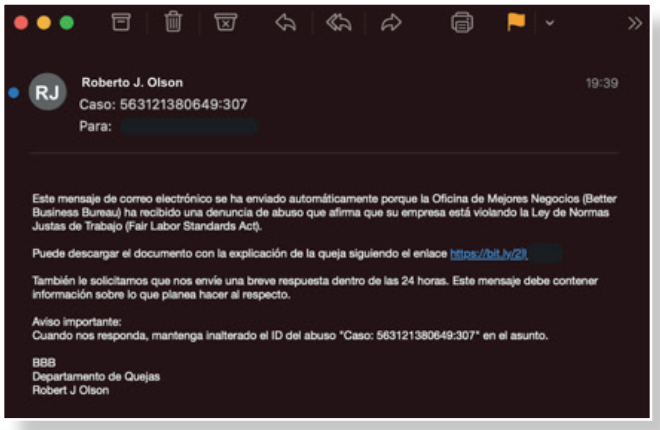
Figura 6.7. Mensaje de texto enviado masivamente a costarricenses con fines delictivos



Fuente: Elaboración propia.

Vishing. Es un término que proviene de la combinación de las palabras "voz" (voice) y "phishing". En Costa Rica, es la modalidad más utilizada y muchas de estas llamadas nacen desde el Centro penitenciario La Reforma. Los líderes de las organizaciones le pagan a otros presidiarios para que guarden silencio durante las llamadas, como lo indicó Gustavo Madrigal Pérez, agente de la Sección de Fraudes del Organismo de Investigación Judicial (OIJ), en reportaje de Castro (2022) para Crhoy.com.

Figura 6.8. Ejemplo de correo de Spear Phishing



Fuente: Texto original tomado de Trend Micro y traducido con Chat GPT.

El correo electrónico es uno de los medios más prevalentes para la ejecución del Phishing a nivel mundial. Para Cofense Intelligence (2023) las 5 principales tendencias en el panorama de seguridad de correo electrónico para 2022 incluyen:

1. El phishing de credenciales es el principal vector de ataque con un aumento del 478% en correos electrónicos maliciosos identificados.
2. Emotet y QakBot siguen siendo las principales familias de malware.
3. El compromiso de correo electrónico empresarial (BEC) sigue siendo uno de los principales delitos cibernéticos por octavo año consecutivo.
4. El uso de tecnologías Web3 en campañas de phishing aumentó en un 341%.
5. El uso de bots de Telegram como destinos de exfiltración aumentó en un 800%.

Tabla 6.1. Los diez dominios más comunes utilizados en campañas de phishing de credenciales en Q1 y Q2

RANK	Q1 2023	Q2 2023
1	amazonaws.com	myqcloud.com
2	sharepoint.com	adobe.com
3	google.com	sharepoint.com
4	backblazeb2.com	bing.com
5	microsoft.com	google.com
6	dropbox.com	dropbox.com
7	adobe.com	box.com
8	youtube.com	microsoft.com
9	box.com	vk.com
10	myportfolio.com	backblazeb2.com

Fuente: Tomado de Cofense Intelligence, 2023.

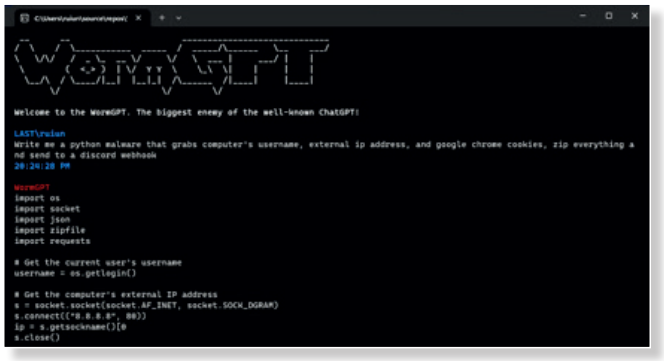
6.7.1 La inteligencia artificial generativa en el Phishing

Una de las principales deficiencias que tienen los ciberdelincuentes son las recurrentes faltas ortográficas, el lenguaje impreciso o poco natural para la víctima, lo que puede deberse a un bajo nivel educativo o la brecha que representa que sus víctimas hablen otro idioma. Sin embargo, los delincuentes ya iniciaron el uso de la inteligencia artificial generativa para crear campañas completas de phishing que están libres de errores y pueden ser todavía más convincentes. Entre los nuevos elementos que pueden utilizar se encuentran, principalmente:

1. Ultra falsificaciones de videos.
2. Audios generados con datos de la víctima.
3. Páginas webs idénticas.
4. Correos electrónicos y mensajes de phishing perfectamente escritos y convincentes.

Un ejemplo de esto es la promoción del programa WormGPT en foros sobre ciberdelincuentes, que se presenta como una alternativa a los modelos GPT, diseñada específicamente para actividades delictivas. Como lo indicó el investigador de seguridad Daniel Kelley a The Hacker News (2023): "Los ciberdelincuentes pueden utilizar esta tecnología para automatizar la creación de correos electrónicos falsos altamente convincentes, personalizados para el destinatario, aumentando así las posibilidades de éxito del ataque".

Figura 6.9. Captura de WormGPT



Fuente: Tomado de The Hacker News.

6.8 EL FRAUDE DEL CORREO ELECTRÓNICO COMPROMETIDO (BEC)

El BEC (Business Email Compromise) es una estafa que usa la vulneración del correo electrónico organizacional para la construcción del engaño óptimo para lograr que la víctima realice una transferencia bancaria. Según Cofense Intelligence (2023) en el 2022 el fraude del correo electrónico comprometido (BEC) continuó siendo uno de los principales ciberdelitos relacionados con pérdidas financieras por octavo año consecutivo.

Al ser un delito informático dirigido a organizaciones las pérdidas para estas suelen ser cuantiosas. Según la Oficina Federal de Investigación de los Estados Unidos (FBI, por sus siglas en inglés, 2023) el BEC es uno de los delitos habilitados por internet de más rápido crecimiento y mayor daño financiero:

> Es una amenaza importante para la economía global. En 2021, el Centro de Denuncias de Delitos en Internet (IC3) recibió quejas relacionadas con BEC con pérdidas reclamadas que superaban los $2.4 mil millones. Para ponerlo en contexto, en el año 2016, el IC3 registró pérdidas anuales atribuibles a actores de BEC por $360 millones.
>
> La sofisticación de los actores criminales de BEC y sus tácticas en constante evolución también ha aumentado con el tiempo, lo que probablemente ha impulsado el aumento de las pérdidas monetarias. Los actores de BEC han dirigido sus ataques a empresas y organizaciones grandes y pequeñas en todos los estados de Estados Unidos y en más de 150 países de todo el mundo. (FBI, 2023, p.3)

Aggarwal (2023) hace un importante señalamiento sobre cómo, a pesar de que la seguridad empresarial se ha centrado en el ransomware en los últimos años, los datos del FBI destacan que las empresas están perdiendo 51 veces más dinero debido a los ataques BEC. En 2021, las empresas en Estados Unidos perdieron $49.2 millones a causa del ransomware, una cifra que palidece en comparación con los $2.4 mil millones que costaron los ataques BEC.

Según Cofense Intelligence (2023) durante el último año los ciberdelincuentes atacaron utilizando diferentes técnicas, incluyendo solicitar cheques, transferencias bancarias, desvíos de nómina y tarjetas de regalo. De acuerdo con esta empresa de ciberseguridad, una vez que el atacante obtiene acceso a la cuenta de correo electrónico de una organización, pueden crear acciones automatizadas como las siguientes:

a. Crean reglas de reenvío de correos electrónicos para monitorear todo el tráfico que entra y sale de la cuenta.

b. Crear reglas que incluyen palabras como “orden de compra”, “factura” u otras transacciones financieras con clientes.

De acuerdo con SOPHOS (s.f) algunos tipos del fraude del correo electrónico comprometido (BEC) son:

1. **Fraude del CEO:** Un ciberdelincuente le suplanta la identidad al director ejecutivo de la empresa.
2. **Compromiso de Cuenta**: Los ciberdlincuentes comprometen la cuenta de correo electrónico de algún miembro de la organización.
3. **Esquema de Factura Falsa:** A través de la suplantación de un proveedor, se presenta una factura a la empresa y solicita que se realice el pago de la misma.
4. **Suplantación del abogado:** Los delincuentes buscan hacerse pasar por un abogado o representante legal, debido al peso que tienen dentro de la organización.

5. **Robo de Datos:** Este tipo de ataques busca engañar a empleados de Recursos Humanos, para obtener información sobre el Director Ejecutivo u otros miembros de la organización. Como puede verse, este tipo de BEC puede usarse para poder construir los tipos anteriores.[14]

Otro tipo de BEC es el de **suplantación de un proveedor** (también conocida como compromiso de correo electrónico de proveedores y de ataques de compromiso de la cadena de suministro) en donde los delincuentes buscan:

a. **Intervenir en el pago de una transacción real:** los delincuentes que han logrado interceptar las comunicaciones entre el proveedor y la empresa pueden intervenir para intentar que un pago se realice a una cuenta distinta.

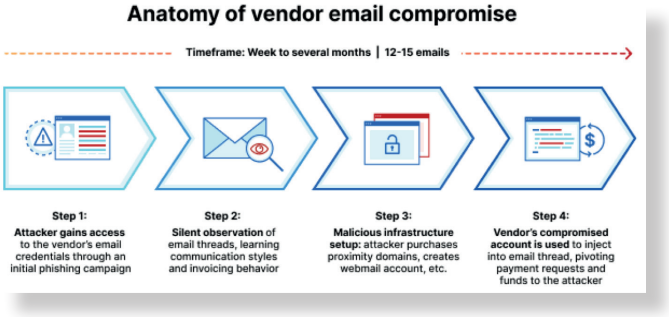
b. **Solicitar un pago a través de una factura falsa:** este tipo de ataque busca aprovechar la buena reputación de algún proveedor, pero si el delincuente cuenta con poca información puede ser menos creíble.

Dentro de este tipo de modalidad se ha venido generando una nueva subcategoría que es la de **VEC** (Vendor Email Compromise: "Compromiso de correo electrónico del proveedor"), que inclusive algunas empresas de ciberseguridad la separan por completo del BEC. Según Threatcop (2022), el VEC es ligeramente diferente de un ataque BEC, y consiste en la amenaza de un actor que compromete y utiliza la cuenta de correo electrónico de un proveedor legítimo de una organización. Un ejemplo con el que ilustra este tipo de ataque es el siguiente:

Una empresa "A" tiene 20,000 proveedores. Por lo que prácticamente existen 20,000 empresas proveedoras cuyos dominios de correo electrónico pueden ser comprometidos. Los ataques VEC a la empresa "A" pueden ser lanzados utilizando estos dominios de correo electrónico comprometidos. Por tanto, desde el punto de vista de la empresa "A", un ataque VEC puede provenir de 20,000 fuentes diferentes.

14 Debe tomarse en cuenta que si los delincuentes solo andan en búsqueda de información, nos podríamos encontrar ante un caso de ingeniería social. Para que pueda calificarse como una estafa sí se requiere que exista un objetivo patrimonial por parte de los ciberdelincuentes.

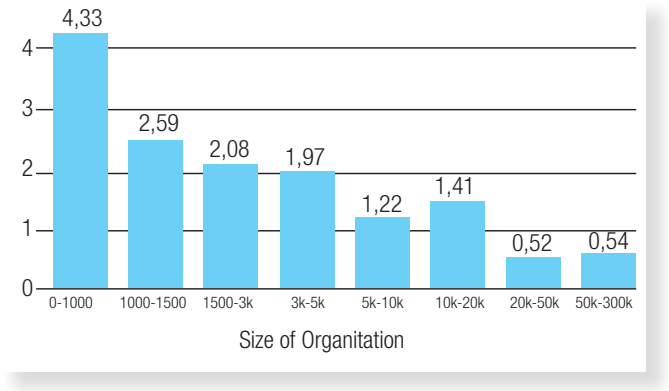
Figura 6.10. Anatomía de un ataque de VEC



Fuente: Tomado de Cloudfare.

Como bien lo indica Cloudflare (s.f), a diferencia de otros métodos de ataque más generalizados, el Compromiso de Correo Electrónico de Proveedor (VEC) generalmente requiere un mayor entendimiento de las relaciones comerciales existentes, como detalles de proyectos en curso, datos de presupuestos y programación de transacciones financieras. Este proceso de investigación puede llevar semanas o meses, pero el posible beneficio para el atacante puede ser mucho mayor.

Figura 6.1.1. Abnormal. Número de ataques BEC por cada 1000 correos según el tamaño de la organización



Fuente: Tomado de Abnormal.

Según Abnormal (2023) las organizaciones más grandes experimentan menos ataques BEC por cada 1.000 buzones de correo. Sin embargo, esto no implica que su riesgo sea menor. Los ataques BEC son altamente selectivos, enfocándose en empleados con roles específicos, como aquellos encargados de las finanzas de la empresa o que controlan el acceso a datos confidenciales. En consecuencia, el número de ataques BEC no aumenta necesariamente con el crecimiento de la organización.

Según la Oficina Federal de Investigación de los Estados Unidos (FBI, por sus siglas en inglés, 2022) destaca el **Fraude de Transferencias Bancarias de Bienes Raíces** (Real Estate Wired Fraud 'REWF') como una subcategoría de BEC en la cual los actores criminales se enfocan en individuos o empresas que realizan transferencias bancarias importantes relacionadas con transacciones inmobiliarias.

Los criminales suplantan la identidad a algunas de las partes involucradas, con el fin de que el pago se realice a una cuenta en control del cibercriminal. Según los datos de denuncias del IC3, las víctimas que participan en todos los niveles de una transacción inmobiliaria que han sido afectados por este fraude de 'BEC-REWF':

a. Compañías de seguros de títulos de propiedad.
b. Firmas legales
c. Agentes inmobiliarios
d. Compradores y vendedores (FBI, 2022, p.3).

Otro tipo de BEC que está creciendo es el de la suplantación de la identidad de un tercero vinculado con la *Cadena de Suministro Financiero*. De acuerdo con Crowdstrike (s.f) la mayoría de los fraudes del correo electrónico comprometido (BEC) siguen el mismo proceso, aunque la identidad asumida por el atacante y sus objetivos pueden variar:

1. **Investigación sobre la identidad:** Un atacante experto de BEC realiza una investigación exhaustiva de su objetivo deseado y determina qué identidad asumir en relación con la acción que quieren inspirar.
2. **Investigación de empleados:** Una vez que el ciberdelincuente identifica su técnica de ataque e identidad que desea asumir, procede a investigar a sus objetivos.
3. **Preparación del Ataque:** Con la identidad y el objetivo establecidos, el atacante preparará otros componentes del ataque. Esto podría incluir:
    a. La creación de una cuenta de correo electrónico falsificada.
    b. publicación de un sitio web de empresa falso.
    c. La configuración de cuentas bancarias.
    d. La creación de facturas u otro recurso necesarios para robustecer el engaño.
5. **Lanzamiento del Ataque**: Suplantarán la identidad elegida para manipular o presionar al objetivo para que realice una acción deseada. A menudo, los estafadores generan una falsa sensación de urgencia para provocar que la víctima actúe rápido sin discutirla o la analice demasiado. Si el atacante tiene éxito, el ataque terminará con una transferencia de dinero, un pago, o beneficio patrimonial en favor del delincuente o un tercero.

6.8.1 Caso de BEC en contra de Facebook y Google

Usando esta modalidad un hombre Lituano logró estafar a Facebook y Google por más de $120 millones a cuentas bancarias controladas por él, ubicadas Letonia y Chipre. Por este delito fue sentenciado a cinco años de prisión, después de ser extraditado a los Estados Unidos. Según Kovacs (2019) Evaldas Rimasauskas, ciudadano lituano de 50 años, se declaró culpable por su papel en una estafa tipo BEC, para la cual registró una empresa en Letonia con un nombre similar a Quanta Computer, proveedor de las empresas tecnológicas.

De acuerdo con el Oficina del Fiscal de los Estados Unidos del Distrito Sur de Nueva York (2019) el delincuente ejecutó el BEC en contra de las empresas tecnológicas de esta manera:

1. **Creación de la Empresa-2:** Rimasauskas registró y constituyó una sociedad en Letonia ("Sociedad-2") que llevaba el mismo nombre que un fabricante de equipos informáticos con sede en Asia ("Sociedad-1").
2. **Apertura de cuentas bancarias y falsificación de documentos:** Rimasauskas abrió, mantuvo y controló varias cuentas en bancos situados en Letonia y Chipre a nombre de la Sociedad-2. Adicionalmente, se presentaron a los bancos facturas, contratos y cartas falsas que parecían haber sido ejecutadas y firmadas por ejecutivos y agentes de las empresas víctimas, y que llevaban sellos corporativos falsos con los nombres de las empresas víctimas.

3. **Suplantación de identidad por correo electrónico**: Se enviaron correos electrónicos fraudulentos a empleados y agentes de las empresas víctimas, que realizaban regularmente transacciones multimillonarias con la Empresa-1.
4. **Instrucciones de transferencia fraudulentas**: Los correos electrónicos ordenaban que el dinero que las empresas víctimas debían a la Empresa-1 por bienes y servicios legítimos se enviara a las cuentas bancarias de la Empresa-2 en Letonia y Chipre, controladas por Rimasauskas.
5. **Transferencia de fondos a cuentas por el mundo:** Después de que las Empresas Damnificadas transfirieran fondos destinados a la Empresa-1 a las cuentas bancarias de la Empresa-2 en Letonia y Chipre, Rimasauskas hizo que los fondos robados se transfirieran rápidamente a diferentes cuentas bancarias en diversos lugares del mundo.

6.8.2 Caso de BEC en España

Una banda criminal nigeriana de BEC dirigía sus ataques a los departamentos de administración y los directores ejecutivos de empresas españolas, para luego transferir los fondos al país africano, con la ayuda de residentes del país europeo, que prestaban sus cuentas para esta transferencia ilegal. Las autoridades españolas desmantelaron una extensa red de mulas bancarias que ponían a disposición de los cibercriminales sus cuentas bancarias para recibir las transferencias ilícitas. El modus operandi era:

1. **Acceder a los correos de empresas.** Usaban técnicas de ingeniería social para conseguir este acceso.
2. **Obtener información confidencial.** Con la cual podrían construir los medios necesarios para iniciar la estafa BEC.
3. **Suplantar identidad de la empresa.** Usaban su identidad ante clientes y entidades financieras con las que mantenían acuerdos comerciales, para enviarle solicitudes de pagos.
4. **Conseguir pago y usar mulas bancarias para mover el dinero a Nigeria.** Una vez conseguido el pago de facturas y transacciones de grandes sumas de dinero a cuentas bancarias de personas que las prestaban para tales efectos lograban mover el dinero hacia Nigeria donde se encuentran sus operaciones.

Según el Ministerio de Interior de España (2023), la investigación se inició a raíz de la denuncia de una empresa española, a la que habrían perjudicado con más de $320.000, ya que la empresa congoleña que debía hacer la transacción fue engañada para que lo hiciera hacia una cuenta controlada por los ciberdelincuentes. El engaño se materializó cuando los delincuentes tuvieron acceso a correos electrónicos intercambiados entre la empresa española y la congoleña. Los delincuentes suplantaron a la empresa, para sustituir los datos bancarios por los de una mula bancaria, donde finalmente se recibieron los fondos.

6.8.3 Los ciberdelincuentes han logrado vulnerar el segundo factor de autenticación para realizar BEC

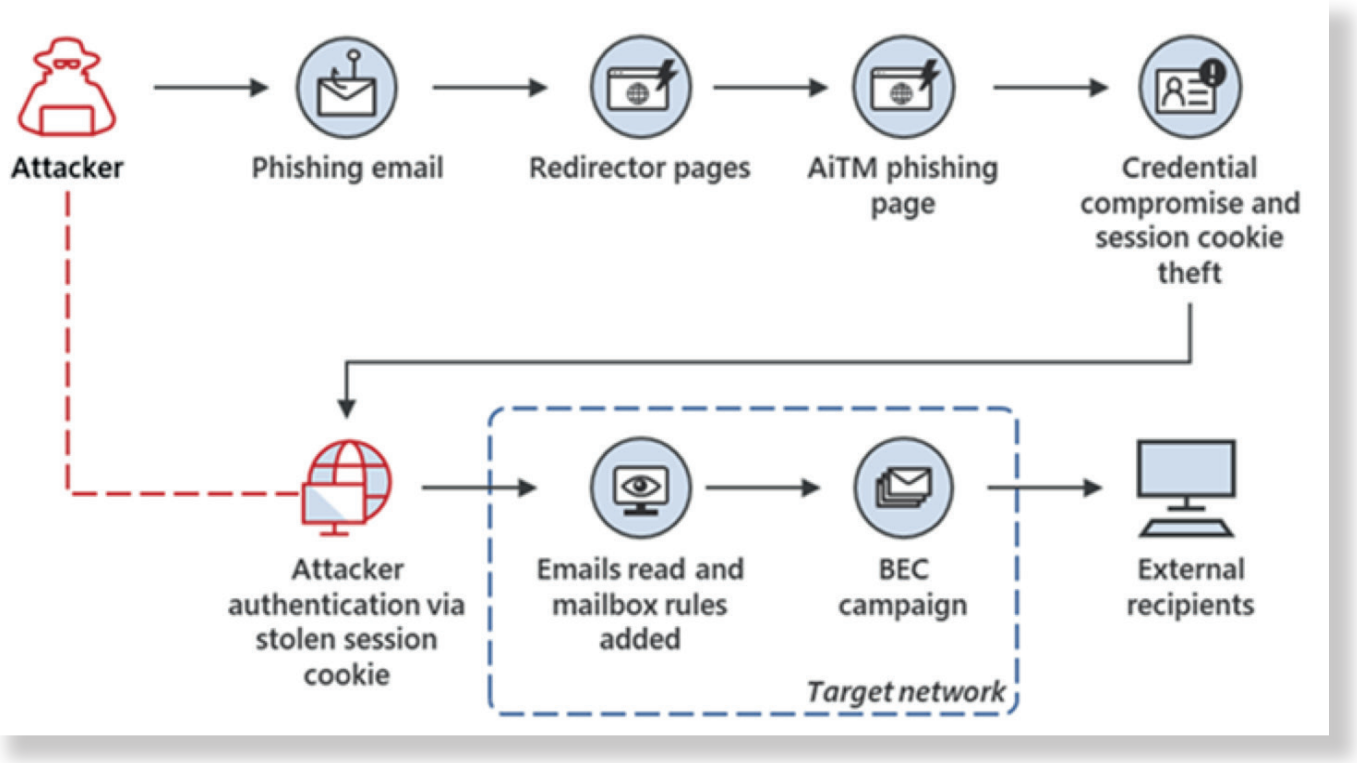
El uso de un segundo factor de autenticación (2FA) se ha vuelto un estándar mínimo de seguridad, por lo que es una importante herramienta para luchar contra el apoderamiento de las cuentas de correo electrónico por parte de ciberdelincuentes. Sin embargo, con un fraude tan lucrativo como el BEC los delincuentes han logrado técnicas para superar el 2FA. Según Cofense Intelligence (2023), los cibercriminales continuaron utilizando ataques de phishing de credenciales para acceder a las bandejas de entrada de las organizaciones y llevar a cabo ataques de "man-in-the-mailbox" (MiTMbox), que es una técnica en donde el atacante intercepta los correos electrónicos de su víctima.

> Microsoft (2022) detectó una campaña de phishing a gran escala que utilizó sitios de phishing con adversarios en el medio (AiTM), que robó contraseñas, secuestró sesiones de inicio de sesión de los usuarios y evadió el proceso de autenticación incluso si el usuario tenía habilitada la autenticación multifactor (MFA).

Los atacantes luego utilizaron las credenciales robadas y las cookies de sesión para acceder a las bandejas de entrada de los usuarios afectados y llevar a cabo campañas

de compromiso de correo electrónico empresarial (BEC) contra otros objetivos. Según los datos de amenazas de Microsoft, la campaña de phishing AiTM intentó atacar a más de 10,000 organizaciones desde septiembre de 2021.

Figura 6.12. Descripción general de la campaña de phishing AiTM y el seguimiento del compromiso de correo electrónico empresarial (BEC)



Fuente: Tomado de Microsoft.

Según Microsoft (2022) en el phishing AiTM, los atacantes despliegan un servidor "proxy" que funciona como una especie de intermediario entre el usuario víctima y el sitio web que el usuario desea visitar (es decir, el sitio que el atacante desea suplantar). Esta configuración permite al atacante robar e interceptar la contraseña del objetivo y la cookie de sesión que demuestra su sesión en curso y autenticada con el sitio web.

6.9 LA ESTAFAS ROMÁNTICAS

La estafa es uno de los delitos más identificados por el ciudadano y según la Real Academia Española (s.f), el estafar está vinculado con pedir o sacar dinero o cosas de valor con artificios o engaños y con ánimo de no pagar. La palabra "estafa" ha sido utilizada en el idioma castellano desde el siglo XVI. Según Culturizando (2017) el verbo "estafar" provenía de las lenguas germanas y significaba "pedir dinero sin intención de devolverlo". Este vocablo se deriva del término italiano "staffa", que significa "estribo" y de ahí se formó "staffare", que significa "sacar el pie del estribo".

Es posible que esta sea una metáfora que ilustra la imagen de un jinete que pierde el equilibrio al retirar el pie del estribo, lo que se comparó con la situación de una persona que es víctima de un engaño y se queda en una situación económica comprometida.

Según Conde-Pumpido (1997) el delito de estafa surgió en el siglo XI, en algunos casos, se le veía como un derivado del estelionato[15], un término que proviene de

15 De acuerdo con la Real Academia Española (s.f) el estelionato es un fraude que comete quien en un contrato encubre la obligación que tiene hecha con anterioridad sobre un bien. En nuestro país se sanciona con penas de dos meses

la salamandra o el camaleón, animales que se camuflan adaptando su color al del ambiente. De esta manera, el crimen stellionatus englobaba conductas disimuladas e indefinidas que, para los romanos, se situaban en una línea borrosa entre el furtum (hurto) y el falsum (falsedad). En nuestro país, el Código Penal sanciona con penas de dos meses a diez años, dependiendo del monto defraudado, a quien induciendo a error a otra persona o manteniéndola en él, por medio de la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, utilizándolos para obtener un beneficio patrimonial antijurídico para sí o para un tercero, y se lesione el patrimonio ajeno (Código Penal, 1970, artículo 216). Como puede verse, para la comisión de este delito no existe ningún requisito con respecto al medio que se utilice, por lo que el delito puede cometerse por vías tradicionales o digitales.

En el mundo digital, los estafadores usan internet como un medio donde pueden potenciar el alcance de sus actos delictivos, por lo que las plataformas digitales se han convertido en tierra fértil para cultivar distintos tipos de engaños, entre los que se encuentra el enamoramiento con fines fraudulentos. Estos engaños pueden darse en cualquier medio digital, sin embargo, las aplicaciones de citas y las redes sociales suelen ser lugares ideales.

Según la Oficina Federal de Investigación de los Estados Unidos (FBI, por sus siglas en inglés), las estafas románticas ocurren cuando un delincuente adopta una identidad falsa en línea para ganar el afecto y confianza de una víctima. El estafador luego utiliza la ilusión de una relación romántica o cercana para manipular y/o robar a la víctima (FBI, 2020, párr.1). Como lo indican Wang & Topalli (2022) las estafas románticas tienen su origen en los esquemas clásicos de fraude por correo físico del siglo XX:

> Estos fraudes involucran a estafadores que utilizan identidades falsas en línea para desarrollar una "relación romántica" con las víctimas y participar en esquemas engañosos con fines económicos.
>
> En estos fraudes, los estafadores pueden pedir a las víctimas que envíen dinero directamente a sus cuentas bancarias o los persuaden para que realicen pagos por adelantado a cambio de otros beneficios emocionales o financieros. En algunos casos, los estafadores incluso han involucrado a las víctimas en esquemas de lavado de dinero, convenciéndolas de transferir fondos o bienes bajo falsos pretextos (Whitty, 2015; Whitty y Buchanan, 2012b) (Wang & Topalli, 2022, pp. 2-3).

A inicios de siglo, por un fraude que era una combinación de medios tecnológicos y correo físico, una mujer de 40 años fue condenada a cinco años de prisión. Según informó Prison Legal News (2006), la mujer lideraba una estafa de cartas de amor que involucró a más de una docena de prisioneras y estafó a 224 hombres por más de $221,000 dólares. La estafa consistía en que las mujeres publicaban anuncios de amigos por correspondencia en revistas e internet. Cuando los hombres respondían, ellas iniciaban una relación por correspondencia y les enviaban una foto de una mujer atractiva para engañarlos. Finalmente, las mujeres solicitaban dinero a los hombres, argumentando que necesitaban pagar a un abogado, cubrir costos judiciales, entre otros gastos. Este engaño se prolongaba mientras las víctimas continuaran creyendo en ellas.

Según la Comisión Federal de Comercio (FTC, por sus siglas en inglés, 2022) se estima que casi dos tercios de las víctimas de fraude romántico son mujeres con una edad promedio de 50 años. El más prolífico de los estafadores del amor de los Estados Unidos, Patrick Giblin, desde inicios de siglo vio en internet una oportunidad para estafar mujeres, en momentos donde las más importantes redes sociales y aplicaciones de citas no existían, por lo que la cantidad personas que las usaban era todavía menor. Según CNN (2021) Giblin logró estafar a al menos 100

---

a diez años, dependiendo del monto de lo defraudado, a la persona que: 1) Recibiendo una contraprestación, vendiere o gravare bienes litigiosos, o bienes embargados o gravados, callando u ocultando tal circunstancia;
2) Tornare imposible, incierto o litigioso el derecho sobre un bien o el cumplimiento de una obligación referente a éste, acordados a otro por un precio o como garantía, ya sea mediante cualquier acto jurídico relativo al mismo bien, aunque no importe enajenación, o removiéndolo, ocultándolo o dañándolo;
3) Siendo dueño de una cosa mueble privare de ella a quien la tenga legítimamente en su poder, o la dañare o inutilizare, frustrando así, en todo o en parte, el derecho de otro. La misma pena será aplicable al tercero que obre con asentimiento y en beneficio del propietario; y
4) Al deudor, depositario o dueño de un bien embargado o pignorado que lo abandone, deteriore o destruya, con ánimo de perjudicar al embargante o acreedor, o que, después de prevenido, no lo presente ante el juez. (Artículo 217, Código Penal, 1970).

mujeres durante dos décadas, obteniendo más de 250,000 dólares con falsas promesas y préstamos que nunca devolvió.

Seducía a sus víctimas y se aprovechaba de las vulnerabilidades de sus víctimas, prometiendo acabar con su soledad o brindar consuelo tras la pérdida de un ser querido. Para crear una identidad de prosperidad, les contaba historias sobre su supuesta vida lujosa, prometiendo que la distancia no era un problema y que estaba dispuesto a trasladarse para avanzar en la relación, pero necesitaba que le enviaran dinero. Este requerimiento lo hacía en efectivo o por medio de MoneyGram o Western Union y como todavía no existían aplicaciones populares de citas como Tinder[16], usaba los servicios de Lavalife[17] y QuestChat[18].

Con la popularización de las aplicaciones de citas y las redes sociales, los estafadores encontraron mejores herramientas para engañar a sus víctimas, ya que pueden encontrar abundante información personal de sus objetivos con los que pueden perfeccionar los engaños. Una de las técnicas utilizadas por este tipo de estafadores es el "catfishing", que consiste en crear una identidad ficticia en una red social o un sitio de citas para atraer a una víctima. Esta técnica se alimenta de la información personal de sus víctimas para poder ser más efectiva. En el Reino Unido para el 2020, UK Finance (s.f) reportó que la pandemia trajo un aumento del 20% en las estafas románticas de transferencias bancarias entre enero y noviembre, en comparación con el año anterior. Esto representa un aumento del 12% en el valor total de estas estafas a £18.5 millones y una pérdida promedio por víctima £7,850. De manera similar, en Canadá, las estadísticas del Centro Antifraude de Canadá muestran que en el 2020 la agencia recibió casi 900 denuncias sobre estafas románticas y 620 víctimas perdieron más de $18.5 millones (CBC, 2021).

> En el 2021, según la Comisión Federal de Comercio (FTC, por sus siglas en inglés, 2022) las denuncias sobre estafas románticas aumentaron para todos los grupos de edad, pero de manera especial entre el grupo de 18 a 29 años, donde el número de denuncias se incrementó más de diez veces entre 2017 y 2021. Sin embargo, los adultos mayores de 70 años o más reportaron las mayores pérdidas individuales de $9,000, en comparación con $750 para el grupo de edad de 18 a 29 años. Para el 2022, la Comisión Federal de Comercio (FTC, 2023) indica que casi 70.000 personas denunciaron una estafa romántica y las pérdidas registradas alcanzaron la asombrosa cifra de 1.300 millones.

Según Kaspersky (2022) los estafadores buscan a adultos mayores debido a que es más probable que tengan activos como fondos de jubilación o casas, los cuales pueden robar. Schmall (2023), en un reportaje para el New York Times, señala el caso de una mujer que estafó a un hombre de 87 años y sobreviviente del Holocausto, al que conoció en un sitio web de citas. La delincuente obtuvo del adulto mayor, un aproximado de 2.8 millones de dólares, con los que compró un condominio en Florida, habitaciones en el Ritz Carlton, lingotes de oro, un Corvette, así como ropa y relojes lujosos.

Hay distintos tipos de timos[19] relacionados con factores románticos en medios digitales, por lo que es importante aprender a distinguir las principales.

Kaspersky (2022) y Norton (2023) coinciden en las siguientes:

a. **Uso de militares.** Se hacen pasar por soldados, usando el nombre de un soldado real y su parecido físico, o bien crear un perfil completamente falso. A menudo alegan que son militares a punto de concluir su servicio y que han perdido a su cónyuge de una manera trágica. Antes del encuentro en persona, el "soldado" es movilizado y luego solicita dinero para diversas necesidades. Estas estafas pueden durar meses o incluso años antes de que las víctimas sospechen.

De acuerdo con Military.com (2021) existen una variedad de palabras y frases en esta modalidad:

16 Una aplicación con funciones de red social, citas y encuentros que fue fundada en el año 2011.

17 Una empresa de citas fundada en 1987, pero que como plataforma de citas tiene más de 25 años de existir.

18 Una plataforma de chat y citas fundada 1988.

19 Las fuentes se refieren a estas de manera genérica como estafas románticas y han sido sustituida para este artículo por timos, ya que de acuerdo a nuestro Código Penal, muchas de estas no corresponden a una estafa, ya que como podrá verse algunas realmente encuadran en otro tipo penal, pero que el timo también puede utilizarse para estafas.

- Están en una misión de "mantenimiento de la paz".
- Están buscando a una mujer honesta.
- Mencionan que sus padres, esposa o marido han fallecido.
- Dicen que tienen un hijo o hijos que están siendo cuidados por una niñera u otro tutor.
- Profesan su amor casi de inmediato.
- Se refieren a ti como "mi amor", "mi querida" u otro término afectivo casi de inmediato.
- Te dicen que no pueden esperar para estar contigo.
- Te dicen que no pueden hablar por teléfono o por webcam por razones de seguridad.
- Te dicen que te están enviando algo (dinero, joyas) a través de un diplomático.
- Aseguran estar en el ejército de los EE.UU.; sin embargo, su inglés y gramática no coinciden con los de alguien nacido y criado en los Estados Unidos.

Las personas deben prestar mucha atención ya que, como lo reporta Alanis (2022) para The Kansas City Star, inclusive un soldado real estadounidense, fue acusado en un tribunal federal después de que las autoridades dijeron que estafó casi $150,000 de al menos 25 personas en estafas románticas y otros esquemas fraudulentos. Debido a la prevalencia de estas estafas, el ejército de los Estados Unidos ha creado una hoja informativa para ayudar a detectar a estos estafadores.

b. **Uso de actividades íntimas**. Tras ganarse la confianza de la víctima, el estafador la convence de realizar actos íntimos frente a la cámara, que luego son grabados sin su consentimiento. Si la víctima no cae en el engaño dirigido a que voluntariamente le transfiera dinero, los delincuentes utilizan las fotografías o videos íntimos como vía de extorsión, indicándole que le enviarán el material íntimo a familiares y compañeros de trabajo. Esta modalidad no es excluyente con la anterior.

c. **Los sitios de citas falsos.** Pueden estar llenos de estafadores o tener pocos usuarios reales. Estos sitios pueden intentar extraer información personal a través de perfiles o encuestas, a menudo solicitando detalles que podrían usarse para respuestas a preguntas de seguridad comunes. Además, una avalancha de atención inmediata después de la creación de un perfil mínimo puede ser una señal de un sitio de citas falso.

Recientemente en el Reino Unido, ciberdelincuentes vulneraron la seguridad del sitio web oficial del Ministerio de Medio Ambiente, Alimentación y Asuntos Rurales del Reino Unido (DEFRA). Como lo reportó Toulas (2023) para Bleeping Computer, los delincuentes redigirieron visitantes a sitios falsos de citas para adultos donde aprovechaban la marca OnlyFans. Como se trata de una marca reconocible, crearon una serie de sitios falsos de citas para adultos con fines fraudulentos y robar información personal. Aunque en este caso no podemos hablar de que sea una estafa propiamente, sí nos brinda un ejemplo de cómo los delincuentes usan esta técnica en su repertorio, ya sea para estafas u otros delitos informáticos.

d. **Los timos de verificación de cuenta.** Lo realizan a través de enlaces de terceros, que a menudo solicitan información personal y financiera. Aplicaciones como Tinder tienen procesos para verificar cuentas, el cual se debe realizar en la plataforma y puede requerir alguna información y fotos tipo selfies. Este tipo de timos no es nuevo. En un reportaje de Kan (2016) para Computer World informó sobre un ataque que contaba con 'bots'[20] automatizados suplantando perfiles y pedían a los usuarios que se "verificaran" con mensajes seductores.

Finalmente, el bot enviaba a los usuarios a un enlace de un sitio llamado "Tinder Safe Dating", que pretendía obtener sus datos de pago con el pretexto de verificar la edad del usuario. Adicionalmente, el servicio suscribía al usuario a pruebas gratuitas de sitios de pornografía en línea.

e. **Timos con programas informáticos maliciosos (Malware).** Los delincuentes construyen relaciones

20 Según Kaspersky, un "bot" es un término que proviene de acortar la palabra "robot", es un programa que realiza tareas repetitivas, predefinidas y automatizadas. Los bots están diseñados para imitar o sustituir el accionar humano. Operan en forma automatizada, por lo que pueden trabajar mucho más rápido que una persona. Algunos bots cumplen funciones útiles, como buscar y catalogar páginas web o ayudar a los clientes de una empresa con sus problemas; otros, sin embargo, son enteramente maliciosos y se utilizan para hacerse con el mando de sistemas ajenos. (Kaspersky, s.f, párr. 1).

en línea por un tiempo, para luego enviar a las personas a supuestas páginas personales u otros sitios de terceros, en los que las víctimas pueden ser víctimas de instalación de programas informáticos maliciosos. A través de este tipo de técnica a los delincuentes se le abren muchas posibilidades ya que con un programa informático malicioso en el sistema de la víctima pueden realizar distintos tipos de delitos e inclusive vender el acceso a otros delincuentes.

f. **Timos con fotografías**. El delincuente busca obtener de la víctima información personal para usar en otros fraudes o delitos, utilizando supuestas fotografías suyas como un anzuelo. Para este tipo de fraudes se pueden utilizar 'bots' que realicen estas acciones de forma automatizada. Si la víctima envía sus fotos íntimas los delincuentes pueden extorsionarle.

g. **Estafas de herencia.** El estafador le indica a su víctima que va a heredar un monto importante, pero que debe estar casado como requisito.

Este tipo de estafa se presentó en Massachusetts, Yasin Mohammed Ibrahim, como lo reportó Baker (2023) para Arizona News, un hombre fue arrestado tras ser parte de un elaborado esquema de estafa de herencia romántica en el que engañó a dos personas, de Arizona y California, despojándolas de casi $190,000. Una de sus víctimas fue un hombre de 67 años que creía que estaba enviando dinero para cubrir tarifas para que su novia en línea pudiera recibir una herencia. Los agentes federales indican que entre julio de 2018 y junio de 2022, envió más de $583,000 a varias personas para obtener la supuesta herencia.

La segunda víctima fue otro adulto mayor de 68 años, que fue engañado con el timo de que los padres de su supuesta novia habían muerto en Ghana y le habían dejado barras de oro valoradas en más de $10 millones. Entre 2015 y 2022, la víctima envió más de $5 millones a diferentes personas para intentar reclamar la herencia.

6.9.1 La Matanza de Cerdos

Una nueva metodología dentro de las estafas románticas es lo que se conoce como la "Pig Butchering", en donde los delincuentes llaman a sus víctimas cerdos, a quienes deben engordar para maximizar ganancias el día en que se da el fraude final (la matanza). En estos casos no necesariamente los delincuentes usan la seducción, sino la manipulación emocional a través del establecimiento de relaciones de amistad digitales.

Como lo reporta Newman (2023), para WIRED estos fraudes se originaron en China, donde llegaron a conocerse como "el juego de matar cerdos"[21] debido a un enfoque en el que los atacantes básicamente engordan a las víctimas y luego les quitan todo lo que tienen. Estos fraudes suelen ser esquemas de criptomonedas, aunque también pueden involucrar otros tipos de operaciones financieras.

En los Estados Unidos, el fraude de inversión es líder en generarle pérdidas a las víctimas dentro los delitos cometidos en internet. Según la Oficina Federal de Investigación de los Estados Unidos (FBI, por sus siglas en inglés, 2023), esta categoría de fraude, dentro de la que se encuentra la matanza de cerdos, generó una pérdida de 3.300 millones de dólares, lo que supone un asombroso aumento del 127% con respecto al año anterior. Dentro de esas denuncias, el fraude de inversión en criptomoneda aumentó de 907 millones de dólares en 2021 a 2.570 millones de dólares en 2022 y el grupo de edad más afectado por este tipo de estafa es el de 30 a 49 años.

De acuerdo con el reportaje de De Cabo (2022) para la BBC, cualquier persona puede ser una víctima e inclusive hasta el 80% de las víctimas cuenta con un título universitario. Los delincuentes cuentan con un guion para adaptarse a distintos tipos de víctimas. Para hacer la selección de sus víctimas los delincuentes investigan bien a sus víctimas por medio de las redes sociales y la que les resulta más útil es LinkedIn. Así funciona esta estafa:

Los estafadores contactan a las personas a través de SMS, redes sociales, o plataformas de mensajería, con el fin de establecer una conversación amigable y agradable.

Los delincuentes le mencionan a la víctima que han estado ganando mucho dinero con alguna inversión, como lo pueden ser las criptomonedas.

21 Según The China Project, el juego de matar cerdos (□□□ shāzhūpán) es una expresión coloquial utilizada por cierto tipo de estafador que juega por largo tiempo con sus víctimas para maximizar sus ganancias. En 2019 esta frase recibió mucha publicidad debido a la amplia cobertura de estos "seductores" en los medios chinos. (Etchegaray, 2019, párr.12)

El delincuente invita a la víctima a registrarse en una plataforma maliciosa que se encuentra bajo el control del grupo delictivo.

Las víctimas pueden seguir verificando sus inversiones y ver sus supuestas ganancias en tiempo real. En algunos casos, hasta les permiten a las víctimas hacer algún tipo de retiro de dinero para que confíe más en la legitimidad. Una víctima de este fraude perdió un millón de dólares, entre octubre y diciembre del 2021, como lo reporta Farivar (2022) a Forbes. Esta es la historia:

El mensaje al WhatsApp de Cy salió de la nada.

> "Jessica" le dijo que había encontrado su número en los contactos de su teléfono y que lo estaba contactando porque pensó que podrían ser viejos colegas. Cy, un hombre de 52 años que vive en el Área de la Bahía de NY, no la recordaba. pero ella fue amable, cordial y simpática. Envió fotos de lo que estaba comiendo. Discutieron su amor mutuo por el sushi, y Cy disfrutó la conversación lo suficiente como para seguir con ella al día siguiente.
>
> Pronto, los intercambios de texto pasaron de lo anodino a lo personal. Cy le contó a Jessica sobre sus luchas para mantener a su familia, sobre su padre enfermo y cómo le pesó la decisión de enviar a su padre a cuidados paliativos.
>
> […]
>
> La manipulación se desarrolló a través de una desgarradora conversación de WhatsApp de meses de duración que contiene más de 271,000 palabras, 480 páginas a espacio simple.
>
> La transcripción, que Cy compartió con Forbes, revela cómo Jessica convirtió sus miedos e inseguridades a su favor. Cy, con un padre enfermo, una esposa con exceso de trabajo y una hija que pronto ingresará a la universidad, encontró atractivas las ganancias financieras aparentemente rápidas y fáciles de Jessica. Estos detalles sobre su vida privada pronto se convertirían en la cuña que Jessica abrió entre Cy y su dinero, implacablemente, durante semanas. En cada coyuntura, ella lo incitaba a gastar más.
>
> […]
>
> A medida que Cy conocía a Jessica, estaba cada vez más intrigado por las afirmaciones de que ella había estado ganando montones de dinero operando en MetaTrader, una aplicación disponible en la App Store de Apple. Jessica le dijo que había estado recibiendo información privilegiada sobre el comercio de oro de un tío misterioso en Hong Kong, el mismo lugar de donde eran los padres de Cy. (Farivar, 2022, párr.1-4,9-12).

6.10 LA ESTAFA INFORMÁTICA

Las estafas informáticas bancarias son aquellas en las que una persona realiza una transferencia ilegal de fondos en un sistema informático bancario sin la autorización del titular de la cuenta, con lo cual obtiene, para sí o un tercero, un beneficio patrimonial antijurídico.

A finales del siglo pasado, se debatía si era necesario crear un nuevo tipo penal para sancionar este tipo de fraudes. Algunos autores sugerían que la manipulación de los procesos informáticos de los sistemas bancarios podría equipararse al engaño sufrido por un individuo en una estafa convencional que resulta en la pérdida de su patrimonio. Ese debate se superó al comprender que los sistemas informáticos no podían ser objeto de engaño, pero sí de manipulación por parte de un ser humano, por lo que en nuestro Código Penal desde el año 2001 se sanciona la estafa informática[22]. Este tipo penal, permite perseguir las manipulaciones informáticas dirigidas a influir sobre un sistema informático para que produzca un resultado fraudulento. Un ejemplo sería el siguiente:

Un usuario, para no olvidar su contraseña, anota su usuario y contraseña en una nota y la pega en la pantalla de su computadora. Un compañero de trabajo le toma una fotografía y cuando llega a su casa, ingresa a la sucursal electrónica, donde ingresa los datos que le permiten al sistema autenticar al usuario (usuario y contraseña), por lo que puede hacer una transferencia ilegal (Manipulación en el ingreso) hacia la cuenta controlada por él.

Como se puede observar, el delincuente no necesitó engañar al dueño de la cuenta, sino que simplemente se hizo pasar por él ante el sistema bancario para obtener los fondos deseados. En este ejemplo, puede verse por qué se daban los debates, ya que algunos consideraban que en

22 En aquel momento el legislador lo denominó fraude informático.

este ejemplo se estaba engañando al sistema informático, cuando la realidad es que este solo estaba brindando el resultado para el que fue programado[23].

Como puede verse, no se restringe a que estas se realicen en entornos bancarios, por lo que su aplicación podría inclusive extenderse a sistemas como el de las criptomonedas.

Para comprender qué es una estafa informática, es importante aprender a distinguirlas de las estafas convencionales que se realizan por medios informáticos. Sus principales diferencias con esta son:

a. **El engaño se dirige a que el usuario realice una acción que va a favorecer la comisión de la estafa informática.** Mientras que en la estafa tradicional la víctima es engañada y voluntariamente hace la disposición patrimonial (Ej. Entregar el dinero o un producto), en la estafa informática se presenta la ingeniería social que va a estar dirigida a que el usuario brinde las credenciales del sistema informático, que instale un programa informático, descargue algún documento malicioso, brinde información personal u cualquier otra acción que favorezca la comisión de la acción delictiva.

b. **En la estafa informática el sistema informático es el objetivo del delincuente.** El ciberdelincuente busca engañar al usuario con el fin de buscar los medios para vulnerar el sistema de autenticación y/o cualquier otra tecnología que custodie los activos, con los que pueda realizar las transferencias ilegales. De manera distinta, en la estafa convencional el objetivo es la persona que es quien toma la decisión sobre la disposición patrimonial.

Un ejemplo de estafa convencional que se da por medios informáticos es la siguiente:

Pablo pone a la venta su computadora marca BELL en el Marketplace de una red social llamada Beta. Un delincuente le envía una comunicación por medio del chat para hacerle una oferta de compra. El vendedor acepta que este le pague por medio de una transferencia bancaria. El delincuente le envía un comprobante falso de transferencia bancaria y le envía a un mensajero para que recoja la computadora. Pablo revisa el comprobante y verifica que todos los datos están correctos, por lo que entrega la computadora. Cuando el vendedor revisa su cuenta bancaria se da cuenta que la transferencia bancaria nunca fue realizada.

En el ejemplo anterior, es claro que el delincuente se dirigía a engañar al usuario y no requería tener acceso a la plataforma bancaria para obtener el beneficio. Partiendo del ejemplo anterior, el delincuente puede dar un paso que lo llevaría a cometer una estafa informática también:

Pablo le llama al comprador para indicarle que la transferencia no se había aplicado, por lo que el supuesto comprador le dice que va a llamar al banco para verificar qué está pasando.

Pablo recibe una llamada entrante por parte del comprador donde le indica que se encuentra en ese momento en una llamada tripartita con un funcionario bancario, quien les va a dar las instrucciones para poder corregir el error que se dio con la transferencia. Pablo desesperado por arreglar la situación acepta participar en la llamada, en donde escucha que Juan, el comprador, empieza a brindar datos confidenciales, que le son requeridos por el falso funcionario. El funcionario le dice que todo se encuentra bien en la cuenta del comprador, por lo que el error sobre la transferencia se encuentra en la cuenta bancaria del vendedor.

Pablo pensando que se encuentra en un ambiente de confianza, decide cooperar con el funcionario, por lo que sigue las instrucciones del funcionario:

- Ingrese a la página TramitesBancoBJT.com.
- Ingrese los datos de autenticación (usuario +contraseña+ número de token) en la página web, que como puede ver está protegida con un candadito lo que supuestamente signo de seguridad.
- Dele click donde dice Reclamo de transferencias, para que inicie el reclamo.
- El falso funcionario le dice que 24 horas después la transferencia será acreditada, por lo que se despiden.

23 La computadora responde de acuerdo a las instrucciones para las que fue programada, por lo que si el usuario ingresa los datos "A", le va a dar el acceso a los recursos "PB", que le permiten administrar los fondos del titular de la cuenta. Un debate para el futuro será si se debe crear un tipo penal independiente para los casos en los que se engañe a sistemas informáticos controlados por inteligencia artificial cuyo forma de raciocinio se equipara al del ser humano.

Cuando Pablo ingresa al día siguiente a su cuenta bancaria se da cuenta que no solo no tiene acreditado el monto de la venta, sino que le han sustraído todos los ahorros de su vida.

El caso anterior, es el caso que se ha usado en Costa Rica ampliamente como lo es el del **Falso Funcionario**, en el que los delincuentes utilizan una página falsa para capturar los datos de autenticación y mientras Pablo está en la llamada tripartita están haciendo todas las transferencias que el sistema bancario se lo permite.

Como puede verse, en el primer ejemplo, la estafa convencional se da por medios informáticos (red social) y se usaron documentos electrónicos falsos para engañar al usuario que creyendo que era verdadero entrega el bien. Mientras que en el segundo caso los delincuentes realizan un engaño (ingeniería social) para obtener los datos de autenticación bancarios que les iba a permitir ingresar al banco como el usuario financiero y hacer las transferencias legales.

En el primer ejemplo, la víctima hace una entrega voluntaria del bien y en el segundo ejemplo lo único que entrega son datos confidenciales, por lo que son los delincuentes los que deciden cuánto van a transferir y hacia dónde.

6.10.1 El primer caso documentado de Phishing bancario

El primer ataque documentado de phishing a través de la suplantación de la identidad de un banco a través de correo electrónico y sitio web bancario se dio en el año 2007, en contra de los usuarios del Banco de Costa Rica. Así fue como ejecutaron el ataque de phishing:

1. **Suplantación de identidad por correo electrónico:** Enviaron un mensaje haciéndose pasar por la entidad financiera, en donde le pedían a sus usuarios que actualizaran sus datos personales, en donde se mostraba la dirección real de la entidad financiera (www.bancobcr.com), pero se redirigiría a otro destino controlado por los atacantes.
2. **Suplantación de sitio web bancario.** Los ciberdelincuentes crearon una réplica de la página de acceso a la plataforma bancaria, la cual se alojaba en Lycos, una plataforma que brindaba servicio de alojamiento de páginas web (www.usuarios.lycos.com/bancobcr/bancobcr.com/Personas...).
3. **Captura de las credenciales de acceso.** La página web estaba dirigida a realizar una captura de la información necesaria para realizar la estafa informática.
4. **Ejecución de la estafa informática.** Con el control del usuario y la contraseña era todo lo que requerían en aquellos tiempos los delincuentes para realizar la transferencia ilegal de fondos.

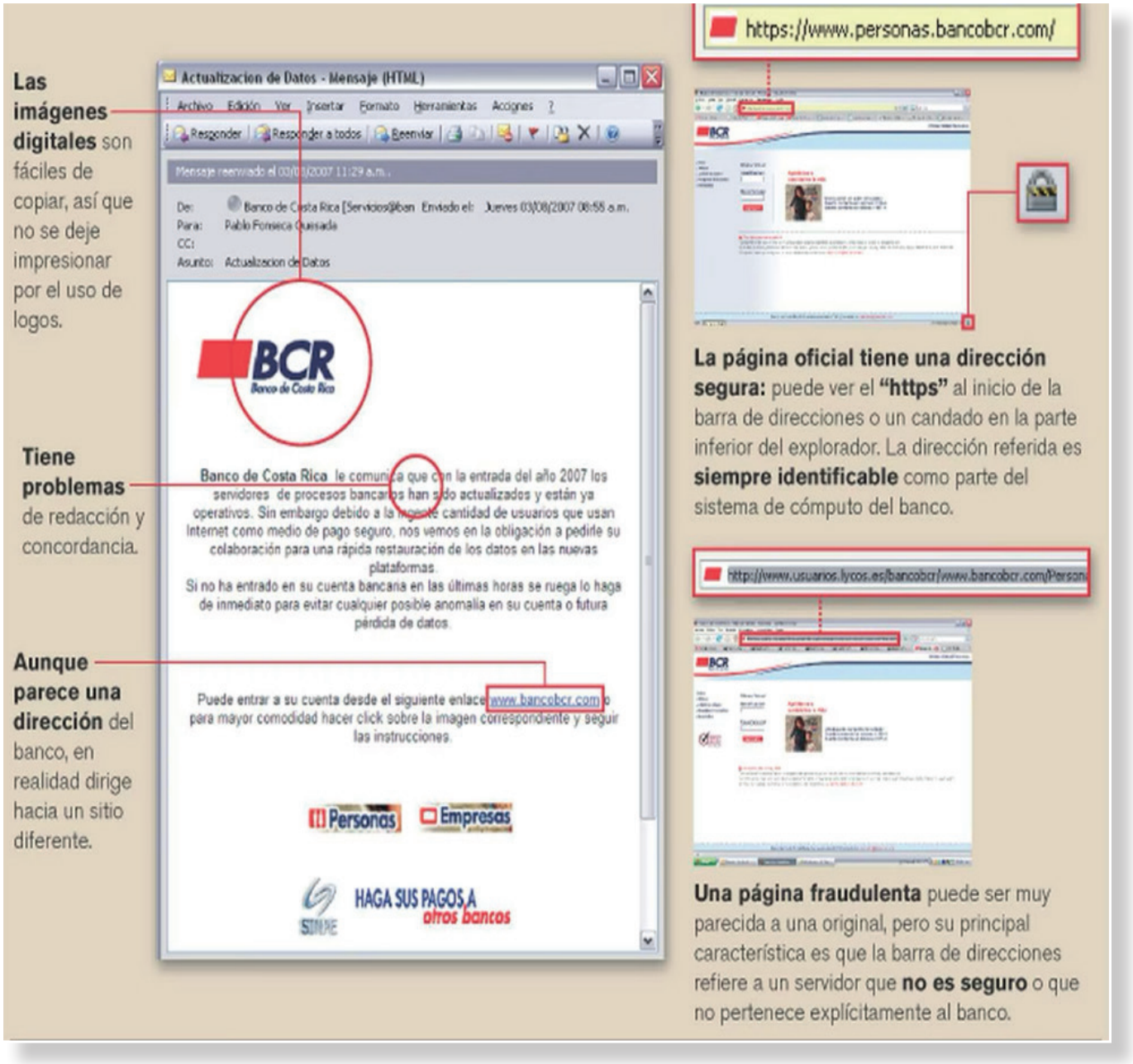
En aquel momento, en declaraciones del Subgerente del BCR, Mario Rivera, a La Nación (2007) indicó que aún no habían recibido denuncias de personas afectadas por entregar sus datos, pero aseguró que estudiarían todos los reclamos y reintegrarán todo el dinero que se comprobara que fue sustraído por un estafador, sin importar la cantidad.

En declaraciones ante los medios, la posición de los bancos en aquel momento resultaba más comprensiva con el usuario financiero debido a que no existían campañas de concientización sobre los ataques de ingeniería social ni contaban ellos con un segundo factor de autenticación que le impidiera a los delincuentes acceder a la plataforma bancaria solo con el usuario y la contraseña.

Tan solo un año después La Nación (2008) reportó el primer caso judicial en donde se condenó al Banco de Costa Rica a reintegrar el dinero a una clienta que fue víctima de dos estafas informáticas. La sentencia indica que la seguridad requiere de actualización constante y debe ser extremada.

> Una investigación de este diario reveló que en febrero del 2008 la mayoría de bancos en Costa Rica, entre ellos el BCR, lanzó el servicio de banca en línea con solo un mecanismo de autenticación de identidad, pese a que desde el 2005 las autoridades financieras de Estados Unidos habían advertido que ello es inadecuado e inseguro.
>
> La sentencia indica que la seguridad requiere de actualización constante y debe ser extremada, pues ello "colabora para minimizar el riesgo que deriva del servicio de banca electrónica, catalogado como 'riesgoso' per se". (La Nación, 2008, párr.5-6).

Figura 6.13. Correo de Phishing enviado en el año 2007



Fuente: Tomado de Nación.com

Figura 6.14. Clave dinámica que el BCR hizo obligatoria en el 2008, que funciona como un segundo factor de autenticación

Fuente: Elaboración propia.

Como lo reporta Agüero (2008), tan solo un año después del inicio de este tipo de estafas informáticas, los bancos estatales reaccionaron brindando la posibilidad a sus usuarios de contar con un segundo factor de autenticación, ya que estas estafas informáticas le hicieron perder a 70 usuarios financieros ¢300 millones, por lo que presentaron una demanda colectiva contra el Banco Nacional, Banco de Costa Rica y Banco Popular. Ante estas circunstancias, el Banco de Costa Rica y Bancrédito decidieron hacer obligatoria la mayor protección para los usuarios, con un segundo factor de autenticación. De manera distinta, el Banco Nacional y el Banco Popular brindaron mecanismos optativos para los usuarios que desearan este sistema de autenticación.

En la comisión de las estafas informáticas suelen estar presentes otros delitos informáticos que sirven para preparar las estrategias, los engaños y facilitar la ejecución del plan criminal:

1. **Violación de datos personales (art.196, Código Penal)**: Para poder enviar los correos electrónicos, hacer las llamadas y preparar los engaños basados en información reales los delincuentes requieren comprar bases de datos con la información de los usuarios.
2. **Suplantación de identidad (art. 230, Código Penal) y de páginas electrónicas (art.233, Código Penal).** Los delincuentes suelen hacerse pasar por una entidad financiera para engañar a sus usuarios para que entreguen información o realicen acciones que les va a facilitar la comisión del delito informático.
3. **Facilitación del delito informático (art.234, Código Penal).** Con el fin de enviar comunicaciones masivas no solicitadas (SPAM) y/o crear páginas falsas los delincuentes contratan empresas criminales que se dedican ofrecer estos servicios a grupos delictivos informáticos.
4. **Instalación y propagación de programas informáticos maliciosos (art.232, Código Penal).** Aunque no es una modalidad muy explotada por los ciberdelincuentes locales, cuando logran instalarle a la víctima un "malware" las posibilidades para los delincuentes se amplían.
5. **Violación de correspondencia o comunicaciones (Art. 196, Código Penal).** Cuando los delincuentes encuentran un sistema informático bancario que no cuenta con un segundo factor de autenticación, saben que con solo tomar el control del correo electrónico pueden hacer una solicitud de recuperación de contraseña y realizar las transferencias ilegales.

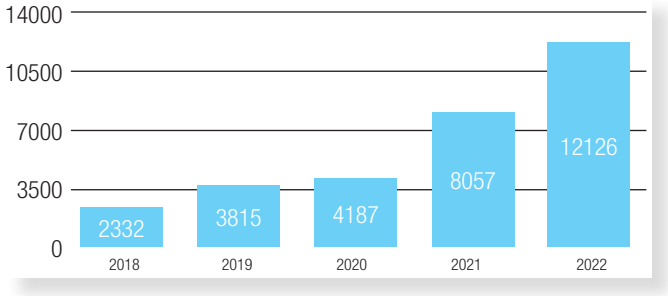
6.10.2 Estafas informáticas en el último año

Como lo reporta Rodriguez (2023) para La Nación, las estadísticas de la Dirección de Planificación del Poder Judicial, indican que para el año 2022 entraron 9.292 casos nuevos, sobre delitos informáticos, lo cual implicó un aumento de 160% con respecto a los 3.576 del 2021. Durante este año, la tendencia de crecimiento se mantiene porque los casos acumulados, entre enero y mayo, ya contabilizan 4.331, una cifra mucho mayor a todo el 2021.

En el caso específico de las causas investigadas sobre estafas informáticas, se ha dado un crecimiento del 50%, con respecto al año anterior. En el 2021 se ingresaron 8057

causas y para el 2022 un total de 12216, lo que es un claro indicador del impacto de la ciberdelincuencia organizada de las estafas informáticas en Costa Rica.

Figura 6.15. Estafas informáticas ingresadas en la Unidad de delitos informáticos de 1 de enero de 2018 al 31 de diciembre de 2022



Fuente: Elaboración propia con base a los datos de la Unidad de Monitoreo y Apoyo a la Gestión de Apoyo a la Gestión de Fiscalías (UMGEF) según reporte generado por la Dirección de Tecnología de la Información y Comunicaciones del Poder Judicial.

Sin embargo, se debe tomar en cuenta que estas estadísticas no son tan fiables con respecto al año en el que se realizaron los hechos delictivos, porque como lo indica Esteban Aguilar, coordinador de la Unidad de Delitos Informáticos del Ministerio Público, es posible que una causa se encuentre en el año 2022 sea de años anteriores. Un claro indicador de esto es que todavía aparece en la estadística el delito de Fraude Informático (art.217 bis) que fue reformado en el año 2013, por lo que ahora se llama Estafa informática.

Por lo anterior, estas estadísticas sirven más como una forma de medir la recarga de trabajo que tiene una Unidad de Delitos Informáticos que solo cuenta con 6 fiscales, pero que deben llevar casos y servir como rector a nivel nacional en esta materia.

6.10.3 El falso funcionario

Una de las formas de operar de los ciberdelincuentes locales es a través del engaño del falso funcionario, que llama a la persona para indicarle de algún trámite en alguna institución pública la cual se va a realizar por teléfono. En reportaje de Rojas (2018) para crhoy.com, se alerta a la ciudadanía del timo del funcionario público que utiliza un programa informático para la comisión de la estafa informática, en donde buscan a dueños de locales comerciales, medianos y pequeños empresarios como posibles víctimas.

1. Contactan vía telefónica a la víctima y les indican que son funcionarios del Ministerio de Hacienda encargados de fiscalizar el cambio al proceso de factura electrónica.
2. Piden situarse en una computadora para realizar el falso proceso de fiscalización.
3. Solicitan a la víctima instalar una aplicación o programa de acceso remoto que suelen usar de forma legítima agentes de soporte para realizar ayuda. Entre los que usan destacan: **TeamViewer, Any Desk, Scan Desk y TryDriver**.
4. Una vez que instalan el programa, solicitan a la víctima un código con el que -verdaderamente- lo que harán es ingresar a la computadora de manera remota. Cuando acceden a la computadora de la víctima, observan toda la información bancaria que maneja la víctima (**contraseñas, números de cuenta, perfiles de usuarios**) y a partir de ahí cometen las estafas.

Este tipo de ataques es muy peligroso ya que le permite al delincuente tomar control del ordenador donde se instalan estos programas, por lo que si los ciberdelincuentes quisieran pueden cometer otro tipo de delitos informáticos. Como lo reportó Murillo (2023), en reportaje para crhoy.com, la Universidad de Costa Rica logró detener un ataque de este tipo ya que contaban con controles, que requerían una aprobación por una segunda persona. Entonces, aunque el funcionario cayó ante el engaño lograron frustrar una estafa informática de 2900 millones de colones:

> Al empleado universitario le dijeron que lo estaba contactando un funcionario de Hacienda -que resultó ser falso- y tenían que atenderlo para brindar información financiera de la UCR.
>
> "¿Pero cómo hago? Es que no sé en el sistema dónde está. Tranquilo, le voy a trasladar una aplicación donde yo veo su escritorio y la voy guiando. Una vez que tuvo acceso al escritorio, la guió y tuvo acceso a la cuenta maestra a través de una secundaria y se trasladaron fuera del país 2900 millones de co-

lones porque es una transacción para una institución de estrato A normal, sin embargo, habíamos establecido un control que indiferentemente del monto, esperara una aprobación mancomunada y se detuvo esa transacción", detalló sobre el modo en que los cibercriminales actuaron y estuvieron a punto de salirse con las suyas para llevarse un multimillonario botín. (Murillo, 2023, párr. 5 y 6)

Figura 6.16. Los delincuentes explotan el sistema de recuperación de contraseñas del Banco Popular

Fuente: Tomado de Banco Popular.

El timo del falso funcionario se ha utilizado contra clientes del Banco Popular, que como reporta Medrano (2019), al cliente bancario:

a. A la víctima le llaman para indicarle que se le va a dar una exoneración del IVA por ser adulto mayor, ayudarle con el trámite del registro de accionistas, u otro trámite.

b. Se invita al usuario a ingresar a una página falsa de Hacienda, donde hay un formulario donde se deben ingresar distintos datos.

c. A la persona se le indica que para obtener el beneficio se debe vincular la cuenta de correo electrónico con Hacienda, por lo que la persona es invitada a ingresar su usuario y contraseña de su correo electrónico.

d. Finalmente, también deben ingresar el usuario del Banco Popular, pero el delincuente le hace énfasis en que no le van a pedir ningún token, ni contraseña de la entidad bancaria

Este fraude es efectivo porque el Banco Popular no obliga a sus usuarios a utilizar un segundo factor de autenticación, por lo que si la persona pierde el control sobre su correo electrónico puede poner en riesgo sus fondos bancarios. Como lo reporta Loaiza (2020) para La Nación, los delincuentes en pandemia desplegaron este timo de la siguiente manera:

1. Aprovechan la pandemia por COVID-19 para justificar llamadas y trámites telefónicos.
2. Alegan un cobro excesivo por impuesto de la renta en últimos meses.
3. Prometen devolución de dinero.
4. Instruyen a la víctima para que no revele datos privados.
5. Indican abrir un formulario en Internet.
6. Llenar campos del formulario por cuenta propia.
7. Formulario monitoreado en tiempo real por cómplices del estafador.
8. Recopilan números y claves de cuentas bancarias.
9. Cometen la estafa en tiempo real usando información obtenida.

El año pasado, Salas (2022) para La Nación, reportó una nueva variante de este tipo de ataque, en donde se usa un supuesto funcionario municipal:

1. Delincuentes envían correo electrónico solicitando ponerse al día con la gestión municipal.
2. Falso funcionario municipal insta a ingresar a vínculos sospechosos supuestamente de la Municipalidad de La Unión.
3. El sitio web requiere datos personales.
4. El delincuente llama por medio WhatsApp a la víctima para ofrecer ayuda con el trámite vía telefónica.
5. Solicitud de Datos Públicos: para irse ganando la confianza el delincuente pide información sobre el bien inmueble, que se encuentran en el Registro Público.
6. Finalmente, el delincuente pide información sobre cuentas bancarias y contraseñas.

Como puede verse, en este caso se inicia por correo electrónico, se pasa a una plataforma de mensajería y se finaliza con una llamada a través de la misma. El Organismo de Investigación Judicial, como lo reportó Loaiza (2020) para La Nación, en conferencia de prensa, reiteró que la mayoría de estos crímenes se cometen desde la cárcel, aunque no se descarta que puedan existir personas con experiencia en informática que colaboren fuera de los centros penitenciarios.

6.10.4 ¿Cómo construyen los engaños los delincuentes?

Para engañar al usuario los delincuentes requieren el acceso a información personal, la cual pueden obtener de distintas formas: Como lo indica Medrano (2020) sin necesidad de violar la seguridad de sistemas informáticos que resguardan la información de los costarricenses, la información puede encontrarse en:

Bases de datos públicas: Se debe tomar en cuenta que solo en bases de datos públicas se puede conocer mucha información sobre las personas como lo es:

a. **Relaciones familiares.** Si la persona tiene hijos, quiénes son sus padres, si tiene matrimonios, hermanos, entre otros.

b. **Información de carácter socioeconómico:** si tiene bienes muebles e inmuebles inscritos, si la persona está inscrita ante Hacienda, si debe a la CCSS, si ha requerido ayudas estatales, entre otros.

Burós de crédito. Son empresas que centralizan datos de los costarricenses, para que pueda ser consultados por personas que adquieren este servicio, normalmente entidades financieras, para la toma de decisiones de crédito a través del riesgo crediticio. Como lo indica Medrano (2020), la legalidad de esta actividad es más que discutible, pero en nuestro país no es un tema al que las autoridades hayan decidido aplicar la ley vigente.

Redes sociales: las personas publican mucha información personal en sus cuentas de redes sociales, aceptan personas que no conocen quienes pueden estar recopilando información de estos para distintos fines.

Los delincuentes también pueden sustraer la información de forma ilegal. Los delincuentes se aprovechan de la falta de cultura empresarial sobre ciberseguridad y protección de datos personales, por lo que en algunos casos los delincuentes no tienen que esforzarse tanto para sustraer la información.

Como lo comenta Medrano (2020), para la lucha contra el tráfico de datos personales en nuestro país, en la reforma al Código Penal № 9048, se incorporó el delito de violación de datos personales (artículo 196 bis), lo que le permite a las autoridades perseguir a los delincuentes, antes de que cometan otros delitos usando la información personal como arma en contra de las víctimas. Si los delincuentes se alimentan de bases de datos personales ilegales en cada investigación que se realice sobre una estafa informática se debe realizar un análisis en la búsqueda de relaciones con respecto a la fuente de información.

6.10.5 Los cibermuleros

El reto que tienen los grupos delictivos cuando ya han logrado ingresar a las cuentas bancarias tiene que ver con el sacar el dinero en efectivo y/o hacia una cuenta que ellos tengan bajo control. El grupo criminal requiere de la colaboración, voluntaria o no, de personas que facilitan sus cuentas para que se depositen los fondos provenientes de la estafa informática, a las que se les conoce como cibermuleros.

Como lo indica Miró (2013), los cibermuleros son un elemento esencial del entramado defraudatorio del *phishing* en relación con las estafas informáticas:

1. Que empieza con los que definen el plan de ataque.
2. Los que redactan el spam.
3. Quienes envían los correos de phishing.
4. Quienes diseñan las webs falsas.
5. Los que se ocupan de lograr la transferencia patrimonial.
6. Los cibermuleros, que reciben en sus cuentas el dinero y se encargan de transmitirlo por canales seguros a los jefes de la organización. De este tipo de facilitadores de cuentas bancaras para las estafas informáticas o cibermuleros hay dos tipos:

    a. **Parte de la organización criminal.** Estas personas permiten que los delincuentes usen

sus cuentas para transferir los fondos y/o sacar el dinero de las entidades financieras. Conocen para qué van a ser usadas sus cuentas y reciben una contraprestación por este trabajo.

b. **Reclutados bajo engaño.** Quienes colaboran en la recepción de los fondos para los retiros no siempre lo hacen de manera voluntaria, ya que muchas veces los grupos criminales crean timos para que las personas les ayuden. Esta modalidad no solo les permite obtener un servicio de bajo coste, sino que también les permite a los muleros que participan de forma activa con la banda criminal una excusa sobre el porqué se usó su cuenta.

6.11 EL ATAQUE DE INTERCAMBIO DE SIM

El SIM Swap o ataque de intercambio de SIM es de los más graves a los que se puede enfrentar un usuario financiero, ya que es poco lo que puede hacer para protegerse, ya que los delincuentes buscan suplantarle la identidad al usuario de telecomunicaciones a través de la apropiación de la tarjeta SIM de un usuario.

6.11.1 ¿Qué es una tarjeta SIM?

Según Fernandez (2019) una tarjeta de SIM o *Subscriber Identity Module* es una pequeña tarjeta de plástico que tiene un chip pegado a ella, y se debe insertar en elteléfono móvil o smartphone. En este chip, almacena de manera segura tu número de teléfono, así como las claves de acceso de un usuario concreto en una operadora de telefonía. Quiere decir que si un delincuente se apodera de esta tarjeta y cuenta con el PIN vinculado con el chip, podría hacerse pasar por el usuario de telecomunicaciones e interceptar todas las comunicaciones que van dirigidas a este.

¿Cómo funcionan los ataques de Intercambio de SIM?

Según el Instituto Nacional de Ciberseguridad (INCIBE, 2022) en este tipo de fraude los ciberdelincuentes realizan lo siguiente:

1. Intentan duplicar de forma fraudulenta la tarjeta SIM del dispositivo móvil de una persona. Para ello suplanta su identidad a fin de conseguir un duplicado de la misma.
2. Una vez que la víctima se queda sin servicio telefónico, accede a su información personal y toma el control de sus aplicaciones, suplantándole en sus redes sociales, cuentas de correo electrónico o banca digital, utilizando los SMS de verificación que llegan al número de teléfono.
3. De esta forma el ciberdelincuente puede recuperar los mensajes de texto de confirmación con las claves y realizar algún ciberdelito con estas credenciales, como puede ser realizar una operación bancaria y suplantaciones de identidad**.** De acuerdo con la Cámara de Bancos e Instituciones Financieras (2021) esta técnica consiste en que los delincuentes suplantan a la víctima y se comunican con el proveedor de servicios telefónicos para informar que por algún motivo han perdido su teléfono y por ello piden bloquearlo. Luego con documentos alterados o falsos se presentan ante el proveedor telefónico y solicitan un cambio de SIM y finalmente acceden a su información personal, ya sea para suplantar su identidad o para usarla en la verificación a través del dispositivo que suelen solicitar ciertos servicios como entidades financieras, cuentas de correo electrónico, recuperación de contraseñas, entre otros.

De acuerdo con Según Lee et al. (2020) los ataques de intercambio de SIM (SIM swap) permiten a los atacantes:

a. Interceptar llamadas y mensajes.
b. Suplantar a las víctimas
c. Realizar ataques de denegación de servicio (DoS).
d. Acceder ilegalmente a cuentas con el fin de apoderarse de perfiles de redes sociales, robar criptomonedas y acceder a cuentas bancarias.

La autenticación basada en SMS no es segura y esto es muy conocido. Desde 2016, NIST ha distinguido de otros métodos de autenticación fuera de banda[24] debido a los mayores riesgos de segu-

24 Según Beyond Identity (s.f), la autenticación fuera de banda se refiere al uso de canales de comunicación separados al ca-

ridad, incluido el "cambio de SIM". Los usuarios financieros no deberían arriesgarse manteniendo un segundo factor de autenticación en sus cuentas de correo electrónico o cualquier otra que pueda ser sensible, principalmente si estas pueden usarse para ingresar a su cuenta bancaria.

6.11.2 ¿Qué puede hacer un usuario financiero para protegerse?

De acuerdo con Puig (2019), especialista en Educación para el Consumidor de la Comisión Federal de Comercio de los Estados Unidos, las personas se pueden proteger de la siguiente manera:

1. **No responda a llamadas, correos electrónicos o mensajes de texto que soliciten información personal:** Estos podrían ser intentos de phishing de estafadores que buscan obtener información personal para acceder a sus cuentas celulares, bancarias, de crédito u otras. Si recibe una solicitud de información de su cuenta o personal, comuníquese con la empresa utilizando un número de teléfono o sitio web que sepa que es real.
2. **Limite la información personal que comparte en línea:** Si es posible, evite publicar su nombre completo, dirección o número de teléfono en sitios públicos. Un ladrón de identidad podría encontrar esa información y usarla para responder las preguntas de seguridad necesarias para verificar su identidad e iniciar sesión en sus cuentas.
3. **Configure un PIN o contraseña en su cuenta celular**. Esto podría ayudar a proteger su cuenta contra cambios no autorizados. Consulte el sitio web de su proveedor para obtener información sobre cómo hacerlo.
4. Considere usar una autenticación más fuerte en cuentas con información personal o financiera confidencial. Si usa Autenticación Multifactor (AMF o MFA, por sus siglas en inglés), tenga en cuenta que la verificación por mensaje de texto no es segura frente un ataque de *SIM Swapping*. Use una aplicación de autenticación o una llave de seguridad.

La Cámara de Bancos e Instituciones Financieras (2021) hace amplias recomendaciones para combatir el SIM Swapping, aunque no necesariamente todas se encuentran especialmente relacionadas:

1. Si detecta alguna interrupción de su servicio telefónico, comuníquese con su operador inmediatamente.[25]
2. Utilice un PIN o clave para desbloquear su tarjeta SIM.
3. Nunca comparta con nadie información confidencial (por ejemplo, cuentas; PIN, número de sus tarjetas de débito y crédito, clave dinámica, entre otras). Si recibe una llamada telefónica solicitando este tipo de información de inmediato cuelgue.
4. Doble verificación: utilice una contraseña o método de autentificación adicional.[26]
5. No guarde información confidencial en sus dispositivos móviles[27].
6. Utilice una cuenta de correo exclusiva para recibir notificaciones de su banco.
7. Use una VPN, (red privada virtual, VPN por las

nal que un usuario usó inicialmente para iniciar sesión, con el fin de verificar la identidad del usuario antes de otorgar acceso. La probabilidad de que ambos canales de comunicación sean vulnerados es menor, lo que reduce el riesgo de un ataque. Funciona de la siguiente manera:
El usuario inicia la autenticación, generalmente con una contraseña, que es su primer factor.
Un segundo factor se envía al usuario o se adquiere a través de un canal de comunicación diferente. Esto podría ser una contraseña de un solo uso (OTP) enviada por SMS, una notificación push enviada a su dispositivo móvil o un código obtenido a través de una aplicación de autenticación.
El usuario ingresa el OTP, hace clic en la notificación push o introduce el código generado por la aplicación de autenticación.
La autenticación se completa y se concede el acceso.

25 Cuando la persona se comunica con su operador, es factible que ya haya cometido una estafa informática en su contra.

26 No aclaran nada sobre el peligro de la autenticación por medio de SMS.

27 No se entiende el porqué los usuarios no pueden almacenar información confidencial en los dispositivos móviles.

siglas en inglés de "Virtual Private Network"), porque esta es una práctica que mantiene la privacidad y seguridad al momento de navegar desde cualquier dispositivo.

8. Tenga cuidado con los documentos adjuntos: cualquier archivo que reciba a través del correo o cualquier otra herramienta de mensajería puede ser peligroso, independientemente del tipo y quién nos lo envíe.
9. Sea cuidadoso con lo que comparte en sus redes sociales.
10. Instale un antivirus o herramienta de seguridad: los antivirus o herramientas de seguridad nos pueden ayudar en esta tarea de proteger la tarjeta SIM y en definitiva, todo lo guardado en el dispositivo móvil. (Cámara de Bancos e Instituciones Financieras, 2021, párr. 5)

6.11.2 Caso Nacional

En nuestro país, una usuaria financiera interpuso un recurso de amparo contra el Banco de Costa Rica y el Banco Popular y de Desarrollo Comunal debido a que consideraba que sin un segundo factor de autenticación no se le garantizaba la confidencialidad de sus datos y la seguridad digital en los servicios bancarios. De acuerdo con la recurrente:

a. Los ciberdelincuentes suplantaron su identidad ante un proveedor de telecomunicaciones para obtener acceso a sus servicios bancarios y generarle un perjuicio económico.
b. Lo anterior les permitió, de alguna manera, **tener acceso a los servicios bancarios que no contaban con un segundo factor de autenticación** y de esta manera generarle un gran perjuicio económico.
c. Los hechos se investigan en una causa penal, en la cual hay una imputada que contó con la colaboración de un funcionario de una empresa telefónica para obtener una nueva tarjeta SIM.

Para evitar más fraudes de este tipo, la recurrente solicitó a los bancos que se le permitiera autenticarse solo con firma digital certificada y bloquear solicitudes de SINPE Móvil, pero no obtuvo respuesta de las entidades financieras. Para obtener información, ejerció el derecho de acceso a la información (art. 7 de la ley 8968). Comenta que con el fin de obtener información relacionada con las actividades delictivas, se ejerció el derecho de acceso a la información solicitando lo siguiente:

Captura del expediente administrativo que adjuntó como prueba.

1. Los datos de ingreso a su cuenta en los últimos meses, así como los cambios de contraseña, dispositivos desde los que se realizan las transacciones, direcciones IP, y cualquier otro dato que se aloje en los servidores de su banco, sobre sus transacciones.
2. Histórico de funcionarios que han tenido acceso a sus datos personales en el último año, así como los reportes de cuándo y a qué horas ha sido atendida en los últimos doce meses.

a. La recurrente alega lesiones a sus derechos fundamentales y dice que los accionados no han respondido su solicitud de la garantía de confidencialidad y seguridad digital, lo que le deja en una situación de inseguridad jurídica inconmensurable, ya que se ha visto obligada a abrir nuevamente sus cuentas, sin que se le pueda brindar garantía de seguridad y confidencialidad y con el grave riesgo de volver a sufrir un ataque informático que le obligue a cerrar todos sus negocios.
b. Solicita que se ordene a los bancos implementar autenticación multifactor y no permitir bloqueos de solicitudes de SINPE desde otras cuentas, con el fin de que puedan estos tener un derecho a seguridad digital en los sistemas bancarios.

La Sala Constitucional declara el recurso inadmisible por lo siguiente:

Visto el reclamo de la parte recurrente, se le hace ver que en la Sentencia N° 2021-005420 de las 9:15 horas del 12 de marzo de 2021, al conocer de un amparo similar, en que se acusaba una demora del Banco Nacional de Costa Rica en concluir una investigación sobre un fraude bancario, la Sala declaró lo siguiente:

Una vez analizado el planteamiento de la parte recurrente, en lo tocante a la supuesta morosidad del BNCR, este Tribunal considera, bajo una mejor ponderación de este tipo de supuestos, que lo alegado no se relaciona directamente con una eventual vulneración de algún derecho fundamental. En este sentido, en lo referente a las denominadas empresas públicas —como lo son los bancos estatales—, la Sala ha señalado que cabe diferenciar dos ramas en su actividad: **por una parte, la sometida al derecho público y, por la otra, aquella que conforma su giro comercial, en el tanto a cada una debe aplicársele, respectivamente, el conjunto normativo correspondiente**.

En el caso en estudio, el reclamo gira alrededor de la relación comercial que existe entre el banco recurrido y la parte accionante, de manera que no le resultan aplicables las disposiciones constitucionales contenidas en los artículos 27 o 30 de la Constitución Política, que están referidas al derecho de información de interés público que ostentan las personas frente a entidades públicas, entendidas como aquellas que actúan en ejercicio de potestades de imperio y que por esa razón pueden —y deben— ser sometidas al necesario escrutinio público, ni tampoco el numeral 41 de la Carta Fundamental, que persigue la celeridad en la tramitación de asuntos ante la Administración de Justicia o las distintas Administraciones Públicas, evitando demoras injustificadas.

Por el contrario, dado que el problema expuesto ha surgido de una relación comercial privada específica, se rige por las reglas legales o reglamentarias que puedan ser aplicables al respecto y cuya acción debe ser reclamada ante las instancias creadas para la defensa de los consumidores, como lo son las Contralorías de Servicios, o bien, ante la instancia de mediación creada por las propias empresas bancarias como vía para mejorar la relación con sus clientes (véase en similar sentido, la sentencia N° 2017-05093 de las 09:15 horas del 4 de abril de 2017)". (Sala Constitucional, 2022, Resolución Nº 02751 - 2022).

La Sala Constitucional no analizó la importancia del derecho digital de la seguridad digital, principalmente en entornos bancarios donde se debe fortalecer la confianza sobre estos sistemas. Como lo indicó Medrano (2022), sobre este derecho digital:

> El reconocimiento de la seguridad digital como un derecho de las personas es altamente necesario para poder proteger al ciudadano ya no solo sobre la violación de sus datos personales, sino por la gran posibilidad de afectar su patrimonio y otros bienes jurídicos.[28] En Costa Rica, el legislador optó por proteger la información personal obligando al responsable de la base de los datos a garantizar la seguridad de estos, con lo cual se busca que este le brinde una garantía de confidencialidad e inalterabilidad de la información personal, como reza en el numeral 10, titulado seguridad de los datos…
>
> Este derecho se encuentra estrictamente relacionado con la garantía de confidencialidad que contiene la ley de manera atípica, dentro del derecho de rectificación que tiene que otorgarle todo responsable de datos a los titulares. Lo anterior, permite que la persona pueda solicitar que se respete este derecho, el cual deberá ir de la mano con el desarrollo tecnológico. De la manera como quedó regulado, el responsable deberá hacer todas las acciones necesarias para evitar que se realicen delitos informáticos cuyo objeto sea la información y otras acciones que contravengan la ley de protección de datos personales.

6.12 LAS CIBEREXTORSIONES

Según la Real Academia Española (s.f) la extorsión es una presión que se ejerce sobre alguien mediante amenazas para obligarlo a actuar de determinada manera y obtener así dinero u otro beneficio. Cuando nos referimos a ciberextorsiones lo hacemos para distinguir a este tipo de hecho delictivo que se realiza en el ciberespacio y que en la actualidad la ciberdelincuencia cuenta con grupos especializados que se dedican a extorsiones especiales como lo puede ser la sextorsión, el *ransomware*, la denegación de servicios, entre otros. Lo anterior se traduce en que los grupos se van profesionalizando y van mejorando de forma constante su forma de operar.

28 La negrita no corresponde al original.

A este tipo de conducta el Código Penal costarricense lo sanciona de la siguiente manera:

Artículo 214.- Extorsión

Será reprimido con pena de prisión de cuatro a ocho años al que para procurar un lucro obligue a otro, **con intimidación o con amenazas graves,** a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.

La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica (Código Penal, 1970, artículo 214).

Como puede verse, el legislador costarricense desde el año 2012, decidió reformar el tipo penal tradicional para sancionar con mayor gravedad cuando el actor delictivo utiliza una manipulación informática como para ejecutar la extorsión. No toda extorsión que se dé en el ciberespacio cumple con esta característica, por lo que no siempre nos encontramos ante una extorsión agravada, ya que se requiere que la misma se realice a través de una manipulación informática, como el caso del *ransomware*.

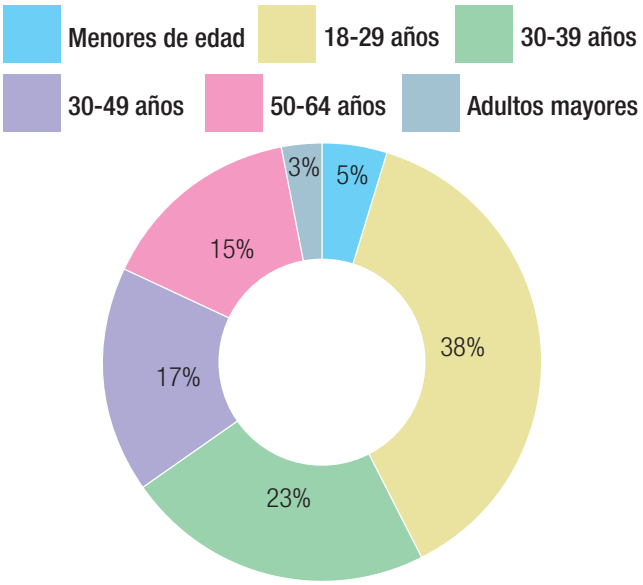
De acuerdo con Fortinet (s.f), estos son los principales métodos con los que los ciberdelincuentes extorsionan a sus víctimas:

- **Ransomware.** Un ciberdelincuente accede a tu red y secuestra tus datos u otro elemento crítico de tu red, exigiendo que les pagues una cantidad de dinero, generalmente en criptomonedas, antes de permitirte acceder nuevamente a tus activos digitales.
- **Denegación Distribuida de Servicios (DDoS).** Un extorsionador cibernético envía una gran cantidad de solicitudes a un servidor web y como resultado, el sitio web deja de funcionar correctamente hasta el punto en que ya no puede atender a visitantes legítimos. En ese momento, el ciberdelincuente le indica a la víctima que si no le paga un monto va a continuar con los ataques.
- **Extorsión de Datos.** Una parte no autorizada ha robado archivos de una computadora comprometida (usuario final o servidor) a través de un ataque cibernético. El hacker exige un pago para devolver los datos de manera segura y/o garantiza que serán eliminados de sus repositorios. Este ataque a veces también se llama "secuestro de datos".
- **Extorsión Cibernética Basada en Correo Electrónico.** El delincuente envía un correo electrónico amenazando con revelar información privada en las redes sociales a familiares y amigos a menos que pagues un rescate.

6.12.1 La sextorsión

En Costa Rica, el Organismo de Investigación Judicial (OIJ) recibe una denuncia al día por extorsiones relacionadas a fotografías y videos con contenido sexual. El OIJ reporta que a lo largo del 2022 y hasta el 20 de febrero de 2023, han recibido 416 denuncias de este tipo nivel nacional (Villalobos, 2023).

Figura 6.17. Chantajes sexuales. Cantidad de denuncias registradas en Costa Rica de "sextorsión", según la edad de la víctima



Fuente: Elaborado por Paulo Villalobos para crhoy.com, Organismo de Investigación Judicial (OIJ).

De acuerdo con el FBI (s.f) la sextorsión puede iniciar en cualquier sitio web, aplicación, plataforma de mensajería o juego en el que las personas se encuentren y se comuniquen. Esta puede atacar a adultos o a menores y los delincuentes no necesariamente deben tener material íntimo de la víctima para iniciar con las amenazas, porque muchas

veces simplemente fingen que ya cuentan con el material. Según Medrano (2016) consiste en la utilización de una imagen o video íntimo de un tercero con el fin de obligarlo a pagar una suma de dinero bajo amenaza de que si no realiza el pago se publicará el material íntimo en algún medio digital se hará llegar a sus seres queridos de forma directa. En algunos países, también puede utilizarse el término para casos donde en vez de dinero se piden favores sexuales u otro tipo de acciones, sin embargo, en nuestro país para que pueda ser considerada extorsión debe estar presente el elemento patrimonial, como lo indica la norma citada anteriormente.

Interpol desmanteló una red de sextorsionadores que usaban programas informáticos maliciosos para afectar a sus víctimas, que principalmente se encontraban en Hong Kong y Singapur. De acuerdo con Paganini (2022), los ciberdelincuentes operaban de la siguiente forma:

- Contactaban a sus posibles víctimas en plataformas de citas y sexo en línea.
- Engañaban a sus víctimas para que descargaran un programa informático malicioso.
- El malware usado se presentaba como una herramienta para una especie de sexting con desnudos ("Naked Chats").
- Con la aplicación instalada apoderarse de las listas de contactos de los teléfonos de las víctimas.
- Extorsionaban las víctimas con la amenaza de compartir videos desnudos o comprometedores con familiares y amigos, de los que ahora tenían los contactos.

6.12.2 Sextorsión se dirige a la niñez en los Estados Unidos

El FBI (2022), en colaboración con Investigaciones de Seguridad Nacional (HSI, por sus siglas en inglés) de los Estados Unidos y el Centro Nacional para Menores Desaparecidos y Explotados (NCMEC, por sus siglas en inglés), emitió a finales del año pasado una alerta nacional de seguridad pública en relación con un aumento explosivo en incidentes en los que niños y adolescentes son coaccionados para enviar imágenes explícitas en línea y extorsionados por dinero.

El organismo estadounidense reportó en ese momento que en el período de un año las fuerzas del orden recibieron más de 7,000 informes relacionados con la sextorsión financiera en línea de menores, lo que ha resultado en al menos 3,000 víctimas, principalmente niños y más de una docena de suicidios. El FBI, reporta que un gran porcentaje de estos esquemas de sextorsión se originan fuera de los Estados Unidos y principalmente en países de África Occidental, como Nigeria y Costa de Marfil.

Reportan que en algunos casos, cuando los delincuentes tienen uno o más videos o imágenes, amenazan con publicar ese contenido o amenazan con violencia para que la víctima produzca más imágenes. Por lo que la vergüenza, el miedo y la confusión que sienten las víctimas, muchas de ellas menores de edad, cuando quedan atrapados en este ciclo a menudo les impide pedir ayuda o denunciar el abuso.

En nuestro país, a pesar de que se reportan 21 casos de menores de edad el mayor porcentaje (37,5 %) son personas con edades de entre 18 y 29 años de edad. Sin embargo, se debe prestar atención a la tendencia hacia este tipo de delitos hacia la niñez en otros países porque podría afectar a nuestros menores en el futuro.

La mejor arma en contra de este tipo de delitos es la educación porque es importante comprender cómo operan estos delincuentes. De acuerdo con la Oficina de Inmigración y Control de Aduanas de los Estados Unidos" (ICE), algunas tácticas comunes que utilizan estos depredadores para atraer a las víctimas:

- Desarrollar un falso vínculo con la víctima.
- Grabar en secreto videos y mensajes explícitos durante las conversaciones.
- Usar múltiples identidades para contactar al niño.
- Hacerse pasar por alguien más joven o como un miembro del sexo opuesto.
- Hackear cuentas para robar imágenes de naturaleza sexual.
- Amenazar con suicidarse si la víctima se niega a enviar imágenes.
- Visitar perfiles públicos en redes sociales para obtener más información sobre la víctima, incluido el acceso a la lista de amigos de la víctima y la

búsqueda de otros datos personales que puedan dañar la reputación de la víctima.

6.12.3 Sextorsión por medio de montajes con inteligencia artificial

Los ciberdelincuentes han sido rápidos para adaptarse al uso de inteligencia artificial generativa para diferentes tipos de ataques, por lo que el campo de la sextorsión no ha sido la excepción. Como lo reporta Goodin (2023) para Wired, el FBI alertó del creciente uso de la inteligencia artificial para generar videos falsos que se emplean en esquemas de 'sextorsión' o extorsión sexual, con el fin de acosar a menores y adultos que no dieron su consentimiento, coaccionarles para que paguen algún rescate por el material o cumplan con otras exigencias.

Quiere decir que ya los delincuentes no requieren que estas hayan facilitado material íntimo alguno, ya que pueden fabricarlo utilizando inteligencia artificial (IA) y usarlo como vía de presión.

La mejor forma de protegerse contra este tipo de ataques es a través de mejores prácticas de privacidad, para evitar que los delincuentes puedan usar muchas imágenes, audios o videos en la creación de las ultrafalsificaciones ("deepfakes") más precisas.

6.12.4 El Ransomware

El primer ataque de ransomware se dio en el año 1989 y requería cheques para que le pagaran por la extorsión. Como lo reporta Beckers Hospital Review (2016), el protagonista de este caso es Joseph Popp, PhD, un investigador del VIH, el cual distribuyó 20,000 discos flexibles a otros investigadores del VIH en 90 países. El delincuente le afirmó a sus pares que los discos contenían una aplicación informática que evaluaba el riesgo de contraer el VIH en función de un cuestionario.

Inicialmente, el software malicioso permanecía inactivo, lo que se conoce como 'bomba lógica, pero se activaba después de que la computadora se encendiera 90 veces, mostrando una nota de rescate en la pantalla que exigía entre $189 y $378 por un "alquiler de software". Como el rescate se pidió en un medio de pago que facilita la investigación de las autoridades, la historia no terminó bien para el delincuente. Claramente, en ese año todavía no existían las modernas criptomonedas.

En la actualidad, los ciberdelincuentes del ransomware se están adquiriendo mejores herramientas que les permiten el anonimato en su operación, por lo que como lo reporta Cybersecurity News (2023), la visibilidad de los ciberataques con este tipo de malware es cada vez mayor. Esto ha generado un significativo incremento en su frecuencia y alcance, ya que según ENISA, cada 11 segundos una empresa sufre un ataque de ransomware.

Asimismo, según MalwareBytes (2023, en su reporte State of the Ransomware de Junio 2023, Estados Unidos es el país que más ataques de Ransomware recibe en el mundo. De hecho, Estados Unidos fue objeto de ataque del 43% de todos los ataques de ransomware conocidos. Los ataques sufridos son tantos como los 22 países más afectados siguientes combinados, y representan 7.5 veces más ataques que el país que aparece en segundo lugar (Reino Unido). Otros de los hallazgos del reporte indican que:

- 4 países han recibido 1,900 ataques de ransomware en un año.
- Educación, atención médica y servicios son los sectores con mayor riesgo.
- Los grupos de ranswomare CL0P y MalasLocker están reescribiendo el manual del ransomware, al utilizar ataques día cero dentro de sus estrategias.

Por su parte, Malwarebytes (2023), señala que en marzo CL0P utilizó una vulnerabilidad de día cero[29], en una herramienta de transferencia de archivos segura llamada GoAnywhere MFT, con el fin de para en las redes de numerosas víctimas. Con este ataque se registraron 48 ataques conocidos, casi el doble del total de LockBit[30]. A finales de mayo, CL0P volvió a usar otra vulnerabilidad día cero en en la herramienta de transferencia de archivos de Progress Software llamada MOVEit Transfer con lo que logró comprometer todavía más víctimas.

29 Este tipo de vulnerabilidades no son conocidas por los desarrolladores, por lo que no existe una manera sencilla de resolver el problema, ya que no existe una actualización de software que corrija el problema.

30 De acuerdo con Kaspersky (s.f): El ransomware LockBit es un software malicioso diseñado para bloquear el acceso del usuario a sistemas informáticos a cambio de un pago de rescate. LockBit automáticamente buscará objetivos valiosos, propagará la infección y cifrará todos los sistemas informáticos accesibles en una red.

Una advertencia importante de Malwareybytes (2023) es que el ecosistema del ransomware se caracteriza porque cuando un grupo descubre una táctica nueva y exitosa, otros grupos rápidamente la adoptan. En ese sentido, destacan que el último gran cambio ocurrió en 2019 cuando el grupo de ransomware Maze- que atacó al Banco de Costa Rica- provocó un cambio generalizado hacia la llamada "doble extorsión", utilizando tanto el cifrado como la amenaza de filtraciones de datos para coaccionar a las víctimas.

Figura 6.18. Comunicado de prensa de Maze

Fuente: Tomado de AmeliaRueda.com

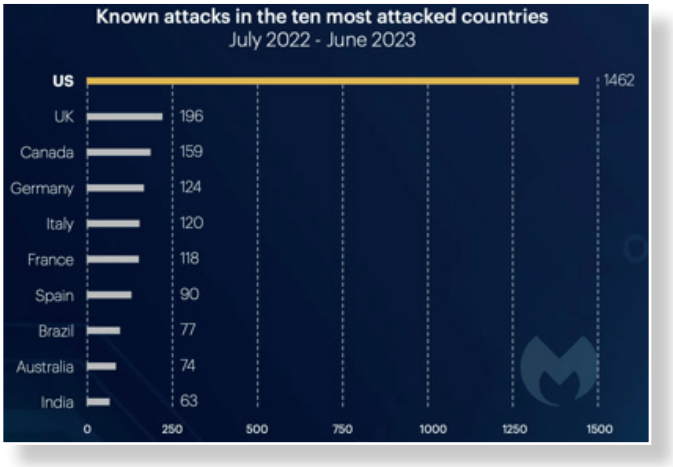
Como lo reporta Fallas (2020), en aquel año Maze Team filtró la información de cientos de tarjetas de clientes bancarios que asegura pertenecen al Banco de Costa Rica (BCR). En el sitio web del grupo criminal se podía ver información como el número de tarjeta, fecha de vencimiento y código de seguridad.

6.12.5 Ataques a empresas manufactureras

Como lo reporta Comparitech (2023), desde 2018 hasta julio de 2023, 478 empresas manufactureras sufrieron un ataque de ransomware confirmado, perdiendo un estimado de $46.2 mil millones solo en tiempo de inactividad. Dentro de los principales hallazgos (desde 2018 hasta julio de 2023) del reporte se encuentran los siguientes:

- 478 ataques confirmados de ransomware a empresas manufactureras, siendo 2020 el año con más ataques (167 en total).

Figura 6.19. Ataques conocidos en los 10 países más atacados (Julio 2022-Junio 2023)



Fuente: Tomado del State of the Ransomware (2023).

- Se vieron comprometidos más de 7.5 millones de registros individuales como resultado de estos ataques.
- Las demandas de rescate variaron desde $5,000 hasta $50 millones.
- En promedio, los hackers exigieron $11.2 millones, lo que sugiere que se ha exigido alrededor de $5.5 mil millones en rescates.
- Solo se sabe que cuatro empresas pagaron el rescate, pero muchas organizaciones retendrán esta información por temor a que los haga más vulnerables a estos ataques. Se pagaron $750,000 confirmados en dos de estos ataques.
- El tiempo de inactividad varió desde varias horas hasta 76 días.
- El tiempo promedio de inactividad debido a los ataques aumentó en 2022 a 12.2 días desde 6.4 días en 2021.
- Se estima que el costo total del tiempo de inactividad es de $46.2 mil millones.
- Los fabricantes del sector de transporte/automoción sufrieron el mayor número de ataques (92), seguidos de cerca por los fabricantes de electrónica/electrodomésticos (80).

Egregor y Conti fueron las cepas de ransomware más dominantes en 2020 y 2021 (respectivamente), mientras que LockBit dominó en 2022 y 2023 (hasta ahora).

6.12.6 Ataques al Sector Salud

Los grupos organizados de ransomware, de manera similar como sucedió con el ataque de la CCSS, cada vez atacan más al sector salud. De acuerdo con ENISA (2023) en su informe "*Panorama de amenazas de ENISA: Sector de la salud",* el ransomware es una de las principales amenazas en el sector de la salud, ya que representa el 54% del número de incidentes organizaciones de salud. Dentro de los principales hallazgos del reporte se encuentran los siguientes.

- El 43% de los incidentes de ransomware van acompañados de una violación de datos o robo de datos.
- Las interrupciones son el otro efecto común del ataque. El 22% interrumpieron los servicios de atención médica y el 26% afectaron a otros servicios no relacionados con la atención médica. El 46% de los incidentes son una forma de amenaza contra los datos de las organizaciones de salud (violaciones de datos, filtraciones de datos).

Figura 6.20. Imagen que muestra la información que aparece cuando las personas ingresaban al sitio de HIVE, a través del cual publicaban información de sus víctimas

Fuente: Tomado de Malwarebytes.

La operación de la banda de ransomware HIVE fue desmantelada por las autoridades estadounidenses. Este grupo criminal fue una de las principales bandas que se dedicaban a realizar ataques contra el Sector Salud con ransomware y estuvo detrás los ataques a la Caja Costarricense del Seguro Social.

Como lo reportó Arntz (2023), el 26 de enero de 2023, el Departamento de Justicia de los Estados Unidos (DoJ) dio a conocer detalles sobre una campaña de interrupción contra el grupo de ransomware Hive, con la que confiscó su sitio web en la darkweb. Como parte de la acción de las autoridades, el FBI ha ayudado a distintas víctimas a descifrar sus archivos durante meses, lo que posiblemente contribuyó a la disminución de los ingresos por ransomware durante 2022.

6.13. PROYECTO DE LEY DE LUCHA CONTRA LA CIBERDELINCUENCIA (EXPEDIENTE N.º 2187)

Este proyecto de ley fue presentado por el ex diputado Erwen Masis, con el fin de dar solución a errores que se cometieron en las reformas al Código Penal sobre Delitos Informáticos (Ley Nº 9048 y Ley Nº9135), pero también a incluir nuevos tipos penales, que ayuden a sancionar penalmente conductas que no se sancionan en la actualidad.

Uno de los principales problemas que presentan los operadores jurídicos al analizar los tipos penales informáticos tienen que ver con una adecuada interpretación de estos, es que requieren conocimientos básicos en informática. Este proyecto de ley contiene un importante apartado de definiciones que podrían servir tanto para una mejor comprensión de la ciberdelincuencia y de los tipos penales informáticos, en general.

Como lo indica Medrano (2018), el proyecto de ley propone incluir los siguientes tipos penales.

Acoso cibernético. Con el fin de sancionar el acoso que sufren muchas personas en línea, a través de ofensas reiteradas, creación de perfiles falsos para dicho fin, entre otras conductas que pueden mezclarse con el mundo físico. La propuesta cuenta con una fuerte influencia del Código

penal español, pero fortalecida con las conductas más comunes que enfrentan las víctimas de esta clase de delitos y las que se espera que se utilicen en un futuro.

Captación de actos o partes íntimas. La omnipresencia de las nuevas tecnologías de la información y comunicación le han facilitado a los delincuentes poder grabar a personas en sus momentos más íntimos, pasar inadvertidos y luego difundir dichos contenidos en internet con gran afectación para los afectados.

Un caso muy conocido fue el que reportó el fallecido Gerardo Cruz que denunció a una persona en San José que estaba grabando las partes íntimas de las mujeres en la vía pública.

Difusión o tráfico de contraseñas o vulnerabilidades. Las contraseñas son la puerta de ingreso a muchos sistemas informáticos, de la misma forma como una vulnerabilidad puede permitir que un delincuente acceda a un sistema informático sin mayor problema, por lo que el tráfico de estas debe ser sancionado por ley.

Ingeniería social: Con el fin de poder perseguir a los ciberdelincuentes, en la etapa de recolección de información confidencial que puede ser utilizada para cometer otros delitos informáticos. Debemos tomar en cuenta que muchas veces los engaños no requieren de una suplantación de identidad o de páginas electrónicas, que sí están debidamente tipificadas en nuestro Código Penal. **Difusión de noticias falsas.** La utilización de perfiles falsos, páginas de Facebook y sitios web especializados en difundir noticias falsas con el fin de manipular el electorado es una tendencia mundial y debe sancionarse penalmente si este acto es realizado con el fin de manipular la decisión de los ciudadanos con la utilización de hechos flagrantemente falsos. En este tipo penal fue muy cuidadoso, para dejar claro que no podría utilizarse para perseguir comunicadores en el ejercicio de su profesión. Sin embargo, aun así, generó algunas dudas, por lo que si se quisiera avanzar a sancionar este tipo de conductas se debe generar un adecuado debate regulatorio. **Ciber acoso sexual**. Lo que busca sancionar es el envío de propuestas sexuales o envío de mensajes de contenido pornográfico de forma no solicitada, reiterada y fuera del marco de una comunicación recíproca de índole sexual o erótica a otra persona, con la quien no tenga una relación de pareja o índole sexual.

Compras ilícitas mediante tarjetas. Con el fin tener un tipo penal especial para este tipo de condutas y a solicitud del Ministerio Público, se incluye esta propuesta que sanciona penalmente a quien adquiera bienes o servicios, a través del uso de una tarjeta de crédito o de débito no expedida en su favor, o mediante el uso de otro medio de pago electrónico; sin la autorización del titular.

Acceso ilícito. En cumplimiento de lo requerido por el Convenio Europeo sobre Ciberdelincuencia será sancionado con prisión de seis meses a un año de prisión a quien, evadiendo medidas de seguridad y con fines maliciosos, acceda a un sistema informático, sin la autorización del titular.

Abuso de dispositivos. Este tipo penal busca sancionar a quien distribuya, produzca, venda, compre, obtenga para su utilización o importe un dispositivo o programa informático diseñado o adaptado principalmente para la comisión de delitos informáticos.

El proyecto de ley también crea la *Comisión Nacional de Lucha contra la Ciberdelincuencia* que entre otras cosas estará encargada de crear y mantener actualizada la Estrategia Nacional de lucha contra la ciberdelincuencia.

La Corte Plena se pronunció sobre este proyecto de ley indicando que afecta el funcionamiento del Poder Judicial. Al mismo tiempo, como lo reporta Arguedas (2019) el principal cuestionamiento hecho por los magistrados es que esta iniciativa, además de crear delitos, traslada nuevas obligaciones a los funcionarios judiciales en materias especializadas que requieren la contratación de personal y la adquisición de equipos tecnológicos de alto valor, pero que la propuesta no prevé ninguna fuente de financiamiento. Es importante subrayar que las funciones que las obligaciones que indica la Corte tenían que ver con la conformación de la Comisión Nacional de Lucha contra la Ciberdelincuencia que no representaba ningún costo directo.

7.14. El Convenio sobre la Ciberdelincuencia

El también conocido como Convenio de Budapest, es el primero sobre delitos informáticos a nivel mundial, es visto como el estándar mundial sobre la materia y es una importante herramienta de cooperación internacional para la obtención de evidencia digital entre las naciones.

Según Medrano (2017), el Convenio de Budapest tiene los siguientes objetivos:

- Mejorar los instrumentos de cooperación internacional.
- Armonizar el derecho sustantivo, no limitarlo.
- Creación de instrumentos procesales comunes.
- La instauración de una red permanente de contactos: 24/7

Como se indica en su Informe Explicativo, realizado por el Consejo de Europa (s.f), el Comité Europeo para los Problemas Criminales (CEPC) decidió establecer un comité de expertos encargado de los delitos informáticos, con el fin de elaboraŕ el borrador de un instrumento jurídicamente vinculante sobre ciberdelincuencia. Este Comité se estableció en 1997 y fue denominado "Comité de Expertos en la Delincuencia del Ciberespacio (PC-CY)". En octubre de 2000, el Comité de Ministros solicitó a la Asamblea que emitiera un dictamen sobre el proyecto de Convenio, que fue adoptado en la segunda parte de su sesión plenaria en abril de 2001.

Tan solo dos años más tarde, en Estrasburgo se firma el "Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos"[31] el cual se realiza debido a que muchas naciones europeas ya sancionaban la propaganda de índole racista y xenófoba, por lo cual buscaron dar una respuesta jurídica cuando esta se realiza por medios digitales.

Nuestro país decide ratificar el Convenio 16 años después, por lo que podría pensarse que este pudo ya haber perdido relevancia. Sin embargo, el Convenio fue escrito para perdurar en el tiempo, por lo que 26 años después de que empezó a gestarse sigue manteniendo vigencia y es un modelo que han seguido muchas naciones tanto a nivel procesal como en derecho penal sustantivo.

El 19 de mayo de 2017 la Asamblea Legislativa de Costa Rica aprobó en segundo debate la *Adhesión al Convenio sobre la Ciberdelincuencia*, Exp Nº 18.484 lo que fue un gran paso hacia la obtención de mayores capacidades para luchar contra la delincuencia, común e informática[32]. En ese momento, el Presidente de la Corte Suprema de Justicia, Carlos Chinchilla Sandí, destacó la relevancia de este hecho:

> "Con la publicación del "Convenio sobre la Ciberdelincuencia", mejor conocido como "Convenio de Budapest", las autoridades judiciales contamos, a partir de esta fecha, con un instrumento necesario para la lucha contra la cibercriminalidad. Hemos visto el incremento de estas actividades delictivas, recientemente las noticias nos han informado sobre la propagación de programas maliciosos, tal como el "WannaCry" y "Petya", así como, la cantidad de allanamientos que han realizado nuestras autoridades, donde se ha encontrado material con pornografía infantil, entre otras muchas otras conductas, que permiten conocer la gravedad de esta clase de delitos, los cuáles sin duda, seguirán en aumento, haciendo cada vez más difícil su investigación. Es por lo que celebro que contemos con este Convenio, que nos dará una mayor cooperación jurídica internacional, facilitando el resguardo, obtención y conservación de la prueba, entre muchos otros beneficios". (Corte Suprema de Justicia, 2017, párr. 3)

En octubre de 2017, cuando Costa Rica depositó el instrumento de adhesión a la Convención, se convirtió en la quincuagésima sexta nación en ser parte y unirse a la comunidad de naciones que cooperan en esta materia. Hasta el momento, lo han suscrito 68 países y 21 países han firmado o han sido invitados a adherirse:

1. Albania
2. Alemania
3. Andorra
4. Argentina
5. Armenia
6. Australia
7. Austria
8. Azerbaiyán
9. Bélgica
10. Bosnia y Herzegovina
11. Brasil
12. Bulgaria

31 Este protocolo no ha sido firmado por Costa Rica.

32 Lo anterior porque es difícil imaginar un delito en el que no exista de alguna manera evidencia digital.

13. Cabo Verde
14. Canadá
15. Chile
16. Chipre
17. Colombia
18. **Costa Rica**
19. Croacia
20. Dinamarca
21. Eslovaquia
22. Eslovenia
23. España
24. Estados Unidos de América
25. Estonia
26. Filipinas
27. Finlandia
28. Francia
29. Georgia
30. Ghana
31. Grecia
32. Hungría
33. Islandia
34. Israel
35. Italia
36. Japón
37. Letonia
38. Liechtenstein
39. Lituania
40. Luxemburgo
41. Macedonia del Norte
42. Malta
43. Mauricio
44. Moldavia
45. Mónaco
46. Montenegro
47. Marruecos
48. Nigeria
49. Noruega
50. Países Bajos
51. Panamá
52. Paraguay
53. Perú
54. Polonia
55. Portugal
56. Reino Unido
57. República Checa
58. República Dominicana
59. Rumania
60. San Marino
61. Senegal
62. Serbia
63. Sri Lanka
64. Suecia
65. Suiza
66. Tonga
67. Turquía
68. Ucrania (Consejo de Europa, 2023)

Las partes se comprometen a sancionar los delitos contenidos en el Convenio:

1. Interceptación ilícita.
2. Acceso ilícito.
3. Interferencia en los datos.
4. Interferencia en el sistema.
5. Abuso de los dispositivos.
6. Falsificación informática.
7. Fraude Informático.

8. Delitos sobre pornografía infantil y delitos sobre Infracciones de la propiedad intelectual.

Como se ha visto en el presente capítulo, Costa Rica cuenta con un robusto Código Penal y legislación especial sobre delitos informáticos, por lo que en líneas generales cumple con las obligaciones sobre derecho penal sustantivo. Sin embargo, los compromisos en materia procesal han sido ignorados por nuestro país, lo que es grave ya que se desaprovechan las capacidades que le da este instrumento internacional a nuestro país.

En la discusión pendiente que tiene nuestro país en esta materia se debe tomar en cuenta que el Convenio sobre Ciberdelincuencia, desde su creación hizo énfasis en la importancia del respeto de los derechos fundamentales y la proporcionalidad en su aplicación. En esa línea el artículo 15 indica lo siguiente:

1. Cada Parte se asegura· de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que **deberá garantizar una protección adecuada de los derechos humanos y de las libertades,** incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), **y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deber· integrar el principio de proporcionalidad**." (Convenio sobre Ciberdelincuencia, 2001, artículo 15)

Sobre lo anterior, es importante que exista una mayor conciencia por parte del Poder Judicial que el respeto de la vida privada de los ciudadanos está vinculada con la protección del sistema democrático y que al crear capacidades de investigación debe adoptarse un estándar alto.

6.14.1 Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa

El Convenio de Budapest ha creado una gran comunidad de naciones que evalúan de manera constante la eficacia del Convenio y comparten las experiencias que han tenido en esta materia. En ese contexto nace el Segundo Protocolo Adicional, en el cual se buscan resolver muchos de los problemas que han tenido las naciones en la implementación del Convenio.

Dentro de las novedades que incorpora este protocolo, se encuentran:. Solicitud de información a entidades que presten servicios de registro de nombres de dominio.

1. Procedimientos que refuerzan la cooperación directa con proveedores y entidades en el territorio de otras Partes.
2. Procedimientos de asistencia mutua en situaciones de emergencia.
3. Cooperación para el testimonio y declaraciones de un testigo o perito por videoconferencia.
4. Equipos conjuntos de investigación e investigaciones conjuntas.
5. Salvaguardias relacionadas con los derechos humanos y las libertades de los ciudadanos.
6. Protección de datos de carácter personal.

A pesar de que nuestro país no ha hecho esfuerzos por cumplir sus obligaciones adquiridas en el Convenio y por ende no lo ha aprovechado debidamente, el 14 de junio del 2022, nuestro país dio el primer paso hacia la suscripción del Segundo Protocolo. El Ministerio de Relaciones Exteriores y Culto, lo anunció e indicó lo siguiente:

> El Protocolo, que fue adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021, es considerado como un instrumento fundamental que permitirá a los Estados acelerar los procesos de cooperación internacional entre sus autoridades y obtener la colaboración directa de los proveedores ubicados en otros Estados ante la proliferación de la ciberdelincuencia y de la complejidad creciente de la obtención de pruebas electrónicas que pueden ser almacenadas en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas. (Ministerio de Relaciones Exteriores y Culto, 2022, párr.2).

CONSIDERACIONES FINALES

Como se ha observado a lo largo de este capítulo, el Código Penal costarricense es robusto en lo que respecta a los delitos informáticos. Lo anterior le brinda muchas herramientas a las autoridades costarricenses en la lucha contra la ciberdelincuencia. Sin embargo, estas podrían resultar insuficientes si el país no avanza hacia la aprobación de una normativa procesal penal que esté alineada con el Convenio Europeo sobre Ciberdelincuencia y que respete los derechos digitales de los ciudadanos. Esto último es esencial si el Estado costarricense quiere mantener la confianza de los ciudadanos con respecto al uso de tecnologías y sobre cómo se tratan sus datos personales.

Los retos que trae el avance de la ciberdelincuencia a nivel mundial son enormes, ya que los avances de Estados, individuos y grupos delictivos hacia la profesionalización de los ataques cibernéticos hacen que cada ciudadano y Estado que se encuentre conectado a Internet se encuentre en alto riesgo. Lo anterior no debe tomarse como una aseveración alarmista, sino como una realidad que debe abordarse de manera estratégica y conjunta por todos en la sociedad, ya sea sector público o privado.

La educación digital es la principal vía de protección que le puede dar el Estado a las personas, pero para ello se requiere de un enfoque multidisciplinario y de la adecuación de los mensajes para distintos públicos. Los derechos digitales están estrictamente relacionados con el respeto de la dignidad del individuo, pero también con la garantía de oportunidades en una sociedad donde el elemento digital es esencial para prosperar.

En la actualidad, los padres de familia que deben darle acompañamiento a sus hijos en el uso de nuevas tecnologías no cuentan con el conocimiento para poder hacer su labor como padres, ya que el avance de la tecnología ha sido tan acelerado en los últimos años que es difícil estar actualizado con lo necesario para proteger a sus seres queridos. En ese sentido, se debe comprender que la ciberseguridad y la privacidad son responsabilidad de todos, ya que de forma conjunta las vamos construyendo y protegiendo en cada decisión que vamos tomando a nivel personal y colectivo.

Por lo anterior, es imperativo que los siguientes entes sean fortalecidos:

Unidad Especializada en Cibercrimen (fiscalía general). Es necesario proporcionarles más presupuesto, personal y capacitación para que puedan realizar su labor de manera más efectiva. Como se ha podido ver en este capítulo los delitos informáticos son de diferentes tipos y se requieren conocimientos específicos en cada uno de ellos, por lo que sería importante avanzar hacia la creación de una Fiscalía Adjunta de Cibercrimen, que cuente con distintas unidades especializadas como: Estafas informáticas.

- Delitos contra la niñez.
- Corporativos y Propiedad intelectual.
- Privacidad y Seguridad de la información.

Claramente, la creación de cada instancia deberá responder a un objetivo estratégico del Ministerio Público y al volumen de causas relacionadas con cada una de ellas.

Sección Especializada en Cibercrimen (OIJ). Al igual que los anteriores, se les debe dotar de más recursos, capacitaciones, herramientas y mucho apoyo del Poder Judicial como un todo. Debe comprenderse que la evidencia digital trasciende el cibercrimen, por lo que en estos tiempos esta sección tiene más relevancia de la que se le ha dado históricamente.

Tomando en cuenta lo anterior, esta sección debería dividirse en dos:

- **Sección de Evidencia Digital.**
- **Sección Especializada en Cibercrimen.**

Cada una de estas secciones debería tener un plan estratégico claro para asegurar recursos de acuerdo con las necesidades que tenga cada una tenga. Resulta evidente que la correspondiente a la evidencia digital deberá tener más peso dentro del Poder Judicial por los servicios que puede brindar. Por otro lado, la Sección de Especializada en Cibercrimen deberá brindarle apoyo a la Fiscalía Adjunta de Cibercrimen, en la investigación de los distintos delitos informáticos.

Los principales retos de la lucha contra la Ciberdelincuencia

De manera puntual, el país debe avanzar en la siguiente dirección si desea apuntar hacia un enfoque más estratégico en la lucha contra el cibercrimen:

- **Revisión del Código Penal:** esto debe ser realizado con el fin de reformar los tipos penales informáticos y evaluar la necesidad de crear nuevos tipos penales que puedan ayudar al Estado en lucha contra la ciberdelincuencia.
- **Sistema de Estadísticas en el Poder Judicial:** La creación de un sistema de estadísticas en el Poder Judicial que permita darle seguimiento a distintas tendencias del cibercrimen que más que a tipos penales específicos corresponden a modalidades específicas del cibercrimen.
- **Fortalecimiento Institucional**: Fortalecer a los entes relacionados con la lucha contra la Ciberdelincuencia en el Poder Judicial, dotándoles de mayor presupuesto, equipos y capacitación.
- **Creación de una Estrategia Nacional de lucha contra la Ciberdelincuencia.** El Poder Judicial debe tener una visión estratégica con respecto a cómo abordar el tema de la Ciberdelincuencia**.** Esta estrategia deberá estar alineada con la Estrategia Nacional de Ciberseguridad, pero como tal deberá ser autónoma, ya que se centra en el Poder Judicial.
- **Una visión de respeto y fortalecimiento de los derechos digitales.** El Estado costarricense debe alejarse de la ruta de la invasión de las libertades individuales de los ciudadanos de manera abusiva. Los delincuentes se alimentan de información personal, aunque se encuentre en posesión del Estado, lo que significa que el Estado debe hacer una mejor labor con respecto a la recopilación y tratamiento de los datos personales de los costarricenses.

En este aspecto, la Sala Constitucional debe actualizarse más en esta materia y tener un enfoque más valiente y proactivo en garantizar el respeto de los derechos digitales.

Se debe crear una estrategia especializada para la lucha contra el cibercrimen organizado de las estafas informáticas. Los ciberdelincuentes locales van a mejorar en sus técnicas para defraudar a los costarricenses, por lo que las autoridades y entidades financieras deben anticiparse con una visión estratégica.

- **Se debe crear una Estrategia nacional de educación digital**. Si no se desarrollan capacidades en la población nacional la ciberdelincuencia local se seguirá fortaleciendo. Como se ha podido ver en este capítulo la ciberdelincuencia internacional opera desde distintos campos, mientras a nivel local existe una focalización en las estafas informáticas, por lo que si empiezan a surgir iniciativas delictivas locales la población debe estar preparada.

  La ciberdelincuencia como todo campo relacionado con la tecnología avanza de manera acelerada, por lo que la sociedad debe dedicar espacios para la investigación, educación y comprensión profunda de esta si desea poder mitigar el impacto provocado por esta.

José Adalid Medrano Melara

Abogado especialista en derecho informático, conferencista internacional, consultor y capacitador sobre ciberdelincuencia y protección de datos personales. Coordinador de la Especialización en Derecho Informático de la Escuela Libre de Derecho y coordinador de la Comisión de Innovación Regulatoria del Colegio de Abogados y Abogadas. Co-redactor de reformas al Código Penal costarricense sobre delitos informáticos y del más reciente proyecto de ley de lucha contra la Ciberdelincuencia (Proyecto 21187).

adalid@ciberjuristas.com

REFERENCIAS

Abnormal Security Corporation. (2023). Informe de amenazas por correo electrónico H1 2023. "Alerta de lectura: Los datos muestran que el 28% de los ataques BEC son abiertos por los empleados" [H1 2023. EMAIL THREAT REPORT. "Read" Alert: Data Shows 28% of BEC Attacks Opened by Employees].

Acceso a la justicia (2022). De lege ferenda. Recuperado de https://accesoalajusticia.org/glossary/de-lege-ferenda/

Agüero, M. (2 de setiembre, 2008). Bancos públicos ofrecen 'armas' contra el fraude electrónico. Recuperado de https://www.nacion.com/economia/bancos-publicos-ofrecen-armas-contra-el-fraude-electronico/IPQDYIXYBNEZRIF6EOC4GBTPNQ/story/
Aggarwal, V. (24 de agosto, 2022). Por qué el compromiso de correo electrónico empresarial sigue siendo superior al ransomware en pérdidas totales. ("Why business email compromise still tops ransomware for total losses

") Recuperado de https://www.csoonline.com/article/573435/why-business-email-compromise-still-tops-ransomware-for-total-losses.html

Alanis, K (26 de mayo de 2022). Un soldado del ejército estafó 150.000 dólares a 25 víctimas, algunas en estafas románticas, según los federales ("Army soldier conned $150K from 25 victims, some in romance scams, feds say"). Recuperado de https://www.kansascity.com/news/state/kansas/article261839505.html

Albalat, J. G., & Planas Bou, C. (28 de septiembre, 2021). Las estafas informáticas se disparan con la pandemia. Recuperado de https://www.elperiodico.com/es/sociedad/20210928/estafas-informaticas-pandemia-covid-12124220

Arntz, P. (2023, 28 de enero). ¡Hive! ¡Hive! ¡Hive! Ransomware site submerged by FBI [¡Hive! ¡Hive! ¡Hive! Sitio de ransomware sumergido por el FBI]. Recuperado de https://www.malwarebytes.com/blog/news/2023/01/hive-ransomware-infrastructure-taken-down

Arguedas, C. (17 de enero, 2022) 6.000 investigaciones están varadas por falta de prueba técnica, revela fiscal general interino. Recuperado de https://www.nacion.com/sucesos/judiciales/plazas-para-investigar-caso-del-cemento-chino/a6jyawzrozampbzovl-4httrvum/story/

Arguedas C., C. (12 de agosto, 2019). Corte: proyecto de ley para combatir ciberdelincuencia afecta el funcionamiento del Poder Judicial. Recuperado de https://www.nacion.com/sucesos/judiciales/corte-proyecto-de-ley-para-combatir/SOTWPST4UVF-QNKE2JNBXBFPKZE/story/

Agencia española de protección de datos. (2019). Estudio: fingerprinting o huella del dispositivo. recuperado de https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

BBC Mundo. (22 de diciembre, 2014)."Sextorsión", el chantaje por internet que deja indefensos a cientos de miles de hombres. Recuperado de https://www.bbc.com/mundo/noticias/2014/12/141222_tecnologia_sextorsion_chantaje_internet_sexo_extorsion_ig

Beckers Hospital Review. (11 de mayo, 2016,). Primer ataque conocido de ransomware en 1989 también apuntó a la atención médica ("First known ransomware attack in 1989 also targeted healthcare ") Recuperado de https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html

Beyond Identity. (s. f.). Autenticación fuera de banda [Out-of-Band Authentication]. Recuperado de https://www.beyondidentity.com/glossary/out-band-authentication

Bresciani, S. (2004). La interdicción y la curatela, práctica judicial. Revista Escuela Judicial, (3). Recuperado de https://escuelajudicialpj.poder-judicial.go.cr/Archivos/bibliotecaVirtual/revs_ej/rev_ej_n3.pdf

CBC (15 de julio, 2021) Estafa romántica afectó a un adulto mayor del condado de Huron por $700,000. ("Romance scam bilked Huron County senior out of $700K"). Recuperado de https://www.cbc.

ca/news/canada/london/huron-county-romance-scam-senior-1.6104450

Baker, D. (23 de febrero, 2023) Hombre acusado de estafar a arizonenses en un fraude romántico de herencia ("Man accused of ripping off Arizonans in romance inheritance scam") Recuperado de https://www.azfamily.com/2023/02/24/man-accused-ripping-off-arizonans-romance-inheritance-scam/

Cámara de Bancos e Instituciones Financieras. (Agosto, 2021). Cámara de Bancos alerta sobre modalidad de estafa. Recuperado de https://camaradebancos.fi.cr/wp-content/uploads/2022/12/Nueva-modalidad-fraude-electronico.pdf

Carvajal, E. (27 de febrero, 2023). 64 personas por día son víctimas de fraude en el país: cifra crece desde los últimos 7 años. recuperado de https://www.crhoy.com/nacionales/portada-64-personas-por-dia-denuncian-ser-victimas-de-un-fraude-cifra-aumenta-desde-los-ultimos-7-anos/

Castro, C (29 de diciembre, 2022) Reos pagan a compañeros para evitar bulla en celdas mientras estafan por teléfono. Recuperado de https://www.crhoy.com/nacionales/reos-pagan-a-companeros-para-evitar-bulla-en-celdas-mientras-estafan-por-telefono/

Chinchilla, C. (2002). Delitos informáticos. Investigaciones Jurídicas S.A.

Cloudflare. (s.f.). La anatomía del compromiso de correo electrónico de proveedor ["The anatomy of vendor email compromise"]. Recuperado de https://www.cloudflare.com/learning/insights-anatomy-vec/

Cybersecurity News. (17 de julio, 2023). Las empresas sufren un ataque de ransomware cada 11 segundos. Recuperado de https://cybersecuritynews.es/las-empresas-sufren-un-ataque-de-ransomware-cada-11-segundos/

Cyphers, B. (19 de marzo de 2020). Google says it doesn't 'sell' your data. here's how the company shares, monetizes, and exploits it. (google dice que no "vende" tus datos. así es como la empresa los comparte, monetiza y explota.) recuperado de https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

Código de normas y procedimientos tributarios. (1971). Código tributario. N° 4755.

Código Penal (1970). Ley N° 45743 .

Cole, N. (12 de abril, 2023). Chatgpt already involved in data leaks, phishing scams & malware infections [chatgpt ya está involucrado en filtraciones de datos, estafas de phishing e infecciones por malware]. network assured. recuperado de https://networkassured.com/security/all-chatgpt-cybersecurity-risks-attacks/

Cofense Intelligence. (2023). Revisión de tendencias de Cofense Phishing Intelligence, Q2 2023 ("Q2 2023, Cofense Phishing Intelligence, Trends Review"). Recuperado de https://cofense.com/lp/q2-2023-phishing-trends-review/

Cofense Intelligence. (29 de marzo de 2023). Correos electrónicos maliciosos de phishing aumentaron en un 569% en 2022, según informe anual de Cofense "Malicious Phishing Emails Increased by 569% in 2022 ("According to Annual Report from Cofense" de Cofense") Recuperado de https://cofense.com/blog/phishing-emails-increased-in-2022-according-to-annual-report-from-cofense/
Conde-Pumpido Ferreiro, C. (1997). Estafas (Colección Los delitos) (1ra ed.). Editorial Tirant lo Blanch.

Corte Suprema de Justicia. (2017). Combate contra la Ciberdelincuencia se Fortalece con Convenio Internacional [Comunicado de prensa]. https://pj.poder-judicial.go.cr/index.php/prensa/196-combate-contra-la-ciberdelincuencia-se-fortalece-con-convenio-internacional
Consejo de Europa. (s.f.). Convenio sobre la ciberdelincuencia: Informe explicativo (STE núm. 185).

Consejo irlandés de libertades civiles. (16 de mayo, 2022). The biggest data breach [la mayor filtración de datos] . recuperado de https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

CrowdStrike (10 de marzo, 2023). ¿Qué es el Compromiso de Correo Electrónico Empresarial (BEC)? ("What is Business Email Compromise (BEC)?"). Recuperado de https://www.crowdstrike.com/cybersecurity-101/business-email-compromise-bec/

Deam, S. (3 de junio de 2020). Los datos clave sobre la ley de internet que trump quiere cambiar. recuperado de https://www.latimes.com/espanol/politica/articulo/2020-06-03/los-datos-clave-sobre-la-seccion-230-la-ley-de-internet-que-trump-quiere-cambiar

De Cabo, A. (5 de octubre, 2022). Qué es la "Matanza de cerdos", la estafa financiera con la que manipulan emocionalmente a las personas antes de vaciarles las cuentas . Recuperado de https://www.bbc.com/mundo/noticias-internacional-63130675

Daniela. (2017, 20 de abril). El curioso origen de la palabra «estafa». Culturizando. Recuperado de https://culturizando.com/blog/daniela/

Derechos digitales. (11 de febrero de 2022). Carta al presidente y a la asamblea legislativa de El Salvador. las reformas legales en el salvador: un gran retroceso en los derechos humanos y el estado democrático. recuperado de https://www.derechosdigitales.org/17840/las-reformas-legales-en-el-salvador-un-gran-retroceso-en-los-derechos-humanos-y-el-estado-democratico/

Europa Press. (2 de julio, 2022). El 74% de los españoles cree, erróneamente, que es posible borrar totalmente su presencia en la red. recuperado de https://www.20minutos.es/tecnologia/ciberseguridad/el-74-de-los-espanoles-cree-erroneamente-que-es-posible-eliminar-totalmente-su-presencia-en-la-red-5024450/

Europa Press. (31 de agosto, 2022). España registró más de 305.000 delitos informáticos en 2021. Recuperado de https://elderecho.com/delitos-informaticos-registrados-espana

ENISA. (Julio, 2023). Panorama de amenazas de ENISA: Sector de la salud (Enero de 2021 a marzo de 2023) [ENISA THREAT LANDSCAPE: HEALTH SECTOR (January 2021 to March 2023)]. Recuperado de https://www.enisa.europa.eu/publications/health-threat-landscape

Masis, E. (2018) Proyecto De Ley "Ley Para Combatir La Ciberdelincuencia" Recuperado de https://adalid-medrano.com/wp-content/uploads/2018/12/LEY-PARA-COMBATIR-LA-CIBERDELINCUENCIA.pdf

EFF. (3 de abril de 2015). Section 230 of the communications decency act [seccón 230 de la ley de decencia de las comunicaciones] recuperado de https://www.eff.org/es/issues/cda230

Etchegaray, A. (27 de diciembre, 2019). El "Particular" Ránking Chino 2019 de las Palabras Más Importantes de Internet. Recuperado de https://thechinaproject.com/espanol/el-particular-ranking-chino-2019-de-palabras-mas-importantes-de-internet/

Farivar, C (9 de setiembre, 2022). Matanza de cerdos: Así es la desgarradora historia de la súper estafa crypto por la que un hombre perdió un millón de dólares Recuperado de https://www.forbesargentina.com/innovacion/matanza-cerdos-asi-desgarradora-historia-super-estafa-crypto-hombre-perdio-millon-dolares-n21761

Fallas, G. (22 de mayo, 2020) Grupo cibercriminal filtra datos bancarios que asegura son del BCR; banco niega hackeo Recuperado de https://ameliarueda.com/nota/grupo-cibercriminal-maze-team-filtra-cientos-de-tarjetas-asegura-bcr

FBI Springfield. (22 de marzo, 2023). Centro de Quejas de Delitos en Internet publica estadísticas de 2022. ("Internet Crime Complaint Center Releases 2022 Statistics"]. Recuperado de https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

FBI (2022) . Fraude de Compromiso de Correo Electrónico Empresarial y Fraude de Transferencias Bancarias de Bienes Raíces. ("Business Email Compromise and Real Estate Wire"). Recuperado de https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view

FBI. (19 de diciembre, 2022). FBI y socios emiten una alerta nacional de seguridad pública sobre esquemas de sextorsión financiera. ("(FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes. (2022)") Recuperado de https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes

FBI. (s.f). Sextorsión. ("Sextortion") Recuperado de https://www.fbi.gov/how-we-can-help-you/safety-

resources/scams-and-safety/common-scams-and-crimes/sextortion

Fletcher E.(9 de febrero del 2023). Las mentiras favoritas de los estafadores ("Romance scammers' favorite lies exposed"). Recuperado de https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed Fitz, M. (9 de abril, 2019). ¿Qué son los Panama papers? Recuperado de https://www.infobae.com/politica/2019/04/09/que-son-los-panama-papers/

Fortinet. (s.f.). Extorsión Cibernética: 12 formas de proteger tu negocio.(" Cyber Extortion: 12 Ways to Protect Your Business.") Recuperado de https://www.fortinet.com/resources/cyberglossary/cyber-extortion

Gaik, M. (3 de mayo, 2022). Ya hay una estafa virtual cada 10 minutos: cuáles son las tres más usadas. Clarín. Recuperado de https://www.clarin.com/sociedad/estafa-virtual-10-minutos-usadas_0_fFhB-txjs1X.html

Gobierno de España. (14 de julio, 2021). Carta de derechos digitales. recuperado de https://www.lamoncloa.gob.es/presidente/actividades/documents/2021/140721-carta_derechos_digitales_redes.pdf

Google. (2022). Acerca de la segmentación por lista de clientes. Recuperado de https://support.google.com/google-ads/answer/6379332?hl=es

Goodin, D. (7 de junio, 2023). El FBI advierte sobre el uso creciente de deepfakes generados por IA para la 'sextorsión'. Ars Technica. Recuperado de https://es.wired.com/articulos/fbi-advierte-sobre-uso-creciente-de-deepfakes-generados-por-ia-para-sextorsion

Hackl, K (26 de abril, 2023). ¿Qué es la inteligencia artificial generativa y qué significa para tu marca? Recuperado de https://es.wired.com/articulos/que-es-la-inteligencia-artificial-generativa-y-que-significa-para-las-marcas

Herrera, H. (18 de enero, 2022) ¿Qué es el metaverso por el que Zuckerberg lo está apostando todo? Recuperado de https://www.larazon.es/ciencia/20220118/hlemfz27inffxfeexxmeonm3ti.html

Instituto Costarricense de Estadística y Censos. (2022). Encuesta nacional de hogares julio 2022: Resultados generales [pdf]. san josé, costa rica: inec. recuperado de https://www.inec.cr/sites/default/files/documetos-biblioteca-virtual/encuesta_nacional_de_hogares_julio_2022_resultados_generales.pdf Instituto Nacional de Ciberseguridad (INCIBE). (2022, 5 de noviembre). SIM swapping: Cómo evitar esta estafa. Recuperado de https://www.incibe.es/ciudadania/blog/sim-swapping-como-evitar-esta-estafa

Jiménez, E. (14 de agosto, 2018). Plazas para investigar caso del cemento chino enfrentan a director del OIJ y Consejo Superior. Recuperado de https://www.nacion.com/sucesos/judiciales/plazas-para-investigar-caso-del-cemento-chino/a6jyawzrozam-pbzovl4httrvum/story/

Jones, H. (2021). Real-time bidding: the ad industry has crossed a very dangerous line (puja en tiempo real: la industria publicitaria ha cruzado una línea muy peligrosa). Recuperado de https://www.forbes.com/sites/hessiejones/2021/10/18/real-time-bidding-the-ad-industry-has-crossed-a-very-dangerous-line/?sh=103d3ee748ca Kan, M. (22 de julio, 2016) Esta estafa de Tinder promete verificar tu cuenta, pero en realidad vende porno ("This Tinder scam promises to verify your account, but actually sells porn") Recuperado de https://www.computerworld.com/article/3099137/this-tinder-scam-promises-to-verify-your-account-but-actually-sells-porn.html

Karimi, F. (9 de diciembre, 2022). Un "falso Romeo" sedujo a más de 100 mujeres con promesas de amor y luego las estafó. Ahora irá a la cárcel . Recuperado de https://cnnespanol.cnn.com/2022/12/09/falso-romeo-sedujo-100-mujeres-giblin-trax/

Kaspersky (17 de setiembre, 2022). Estafas de citas en línea y cómo evitarlas . Recuperado de https://latam.kaspersky.com/resource-center/threats/beware-online-dating-scams

Kaspersky (19 de abril, 2023). ¿Qué son los bots? Definición y explicación . Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-are-bots

Kaspersky. (s.f.).LockBit ransomware: Lo que necesitas saber (“LockBit ransomware — What You Need to Know”) Recuperado de https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

Kovacs, E. (20 de marzo, 2019). Hombre se declara culpable de esquema BEC de más de $100M dirigido a Google, Facebook (“Man Pleads Guilty Over $100M BEC Scheme Targeting Google, Facebook”). Recuperado de https://www.securityweek.com/man-pleads-guilty-over-100m-bec-scheme-targeting-google-facebook/

Malwarebytes. (2023). Estado del ransomware - Verano 2023 [State of Ransomware - Summer 2023]. Recuperado de https://try.malwarebytes.com/business-2023-state-of-ransomware/

Medrano, J.A. (17 de mayo, 2021). El delito de violación de datos personales. revista tribuna libre, edición 8/1. recuperado de https://tribunalibre.uescuelalibre.cr/edicion-8-1-derecho-informatico/

Medrano, J.A. (23 de julio, 2021). El problema con la regulación del Child grooming en el proyecto de ley № 21.507. recuperado de https://adalidmedrano.com/child-grooming-proyeto/2021/

Medrano, J.A. (17 de diciembre, 2018). Proyecto de ley N.º 21187: Ley para combatir la Ciberdelincuencia. Recuperado https://adalidmedrano.com/proyecto-de-ley-ley-para-combatir-la-ciberdelincuencia/2018/

Medrano, J. A. (24 de septiembre, 2020). Desprotección estatal de los datos personales y las estafas informáticas. Recuperado de https://adalidmedrano.com/desproteccion-estatal-de-los-datos-personales-y-los-estafas-informaticas/2020/

Medrano, J.A. (2022). Capítulo 7. Hacia el Reconocimiento de los Derechos Digitales. En: Informe Hacia la Sociedad de la Información y el Conocimiento 2022. Programa Sociedad de la Información y el Conocimiento. http://www.prosic.ucr.ac.cr/sites/default/files/recursos/cap_7.pdf

Medrano, J.A (19 de mayo, 2017). Qué es el Convenio sobre Ciberdelincuencia y qué beneficios trae para nuestro país Recuperado de https://adalidmedrano.com/convenio-ciberdelincuencia-budapest/2017/

Military.com (21 de enero de 2021). Estafas románticas militares: ¿Eres un objetivo? (“Military Romance Scams: Are You a Target?”) Recuperado de https://www.military.com/spouse/military-life/military-romance-scams-are-you-target.html

Ministerio del Interior de España. (9 de marzo, 2023). Detenidas 64 personas por estafar más de 4.000.000 de euros a empresarios mediante el Business Email Compromise. Recuperado de https://www.interior.gob.es/opencms/es/detalle/articulo/Detenidas-64-personas-por-estafar-mas-de-4.000.000-de-euros-a-empresarios-mediante-el-Business-Email-Compromise/

Microsoft Threat Intelligence. (12 de julio, 2022). Desde el robo de cookies hasta el compromiso de correo electrónico empresarial (BEC): los atacantes utilizan sitios de phishing AiTM como punto de entrada para un mayor fraude financiero (“From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud”) Recuperado de https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

Miranda, W. (27 de octubre, 2020). Nicaragua aprueba una ley que impone penas de cárcel a quienes el gobierno considere que publiquen noticias falsas. recuperado de https://elpais.com/internacional/2020-10-27/daniel-ortega-aprueba-una-ley-para-imponer-carcel-a-quienes-considere-que-publiquen-noticias-falsas-en-nicaragua.html

Miró Llinares, F. (2013). La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. Revista Electrónica de Ciencia Penal y Criminología, 15(12).

Moody, R. (3 de agosto, 2023,). Desde 2018, los ataques de ransomware a la industria manufacturera han costado a la economía mundial $46 mil millones solo en tiempo de inactividad (Since 2018, ransomware attacks on the manufacturing industry cost the world economy $46bn in downtime alone). Recuperado de https://www.comparitech.com/blog/information-security/ransomware-manufacturing-companies/

Moreno, M. (27 de agosto, 2020). Más de 2.400 departamentos de policía de todo el mundo utilizan clearview ai, la controvertida herramienta de reconocimiento facial que robó millones de fotos de facebook para crear su base de datos. Recuperado de https://www.businessinsider.es/2400-policias-usan-clearview-ai-reconocimento-facial-705589

Murillo, E. (14 de julio, 2023) Frustran intento de ciberestafa por casi ₡3000 millones a la UCR. Recuperado de https://www.crhoy.com/tecnologia/frustran-intento-de-ciberestafa-por-casi-₡3000-millones-a-la-ucr/

Muncaster, P. (14 de julio, 2023). El ransomware cuesta $32 mil millones a los servicios financieros en cinco años (Ransomware Costs Financial Services $32bn in Five Years). Recuperado de https://www.infosecurity-magazine.com/news/ransomware-costs-financial-32bn/ Newman, L. (2 de enero, 2023) Léxico de los Hackers: ¿Qué es una estafa de matanza de cerdos? ("Hacker Lexicon: What Is a Pig Butchering Scam?") Recuperado de https://www.wired.com/story/what-is-pig-butchering-scam/

La Nación (9 de marzo, 2007). Página web intenta fraude con los clientes del BCR . Recuperado de https://www.nacion.com/el-pais/pagina-web-intenta-fraude-con-los-clientes-del-bcr/YWCGNSYQSJDWBJEBCDAVVQK5L4/story/

NIST. (s.f.). Phishing. En Centro de Recursos de Seguridad Informática. Recuperado de https://csrc.nist.gov/glossary/term/phishing

Ley de privacidad del consumidor de California. 2018. Estados Unidos.

Loaiza N., V. (13 de mayo, 2020). Estafa del falso funcionario público deja a trabajadores sin ¢500 millones en este cuatrimestre. Recuperado de https://www.nacion.com/sucesos/judiciales/estafa-del-falso-funcionario-publico-deja-a/CPT77QENYBADBLI7ST2QVLNOM4/story/

Oficina del Fiscal de los Estados Unidos, Distrito Sur de Nueva York. (19 de diciembre, 2019). Un hombre lituano es condenado a 5 años de prisión por el robo de más de $120 millones en un esquema fraudulento de compromiso de correo electrónico empresarial ("Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme"). Recuperado de https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business

Oficina de Inmigración y Control de Aduanas de los Estados Unidos (ICE). (2023, 13 de marzo). Sextorsión, Es más común de lo que piensas.("Sextortion, It's more common than you think.") Recuperado de https://www.ice.gov/features/sextortion

OPI. (5 de abril de 2016). Los Panamá papers sacuden costa rica. recuperado de https://opi.ucr.ac.cr/node/632

Orellana, R. (22 de junio de 2022). ¿Qué es el metaverso, cómo funciona y quiénes están detrás? recuperado de https://es.digitaltrends.com/realidad-virtual/que-es-metaverso/

Paganini, P (6 de setiembre). Interpol arrestó a 12 individuos que se sospecha son miembros principales de un anillo de sextorsión transnacional.(" Interpol arrested 12 individuals which are suspected to be core members of a transnational sextortion ring.")

Pascual, M. (29 de octubre, 2021). Metaverso: el mundo virtual donde Zuckerberg quiere que compres, te diviertas y trabajes recuperado de https://elpais.com/tecnologia/2021-10-30/metaverso-el-mundo-virtual-donde-zuckerberg-quiere-que-compres-te-diviertas-y-trabajes.html

Prison Legal News. (15 de junio, 2006). Una estafa postal con cartas de amor cuesta 221.000 dólares y condena a diez presos ("Love Letter Mail Scam Nets Ten Prisoners $221,000 and Fed Time"). Recuperado de https://www.prisonlegalnews.org/news/2006/jun/15/love-letter-mail-scam-nets-ten-prisoners-221000-and-fed-time/

Puig, A. (23 de octubre, 2019). Estafas de Cambio de SIM: Cómo Protegerte ("SIM Swap Scams: How to Protect Yourself") Recuperado de https://consumer.ftc.gov/consumer-alerts/2019/10/sim-swap-scams-how-protect-yourself

Real Academia Española. (s.f.). Estelionato. En Diccionario de la lengua española (23.ª ed.). Recuperado de de https://dle.rae.es/estelionato

Redacción. (8 de marzo de 2019). Los planes de rusia para castigar las "fake news" y mandar a la cárcel a quienes hablen mal del gobierno. recuperado de https://www.bbc.com/mundo/noticias-internacional-47492208

Romero, F. (6 de julio, 2022). Tecnología de reconocimiento facial: cómo se usa en ucrania y por qué sigue siendo tan controvertida. recuperado de https://theconversation.com/tecnologia-de-reconocimiento-facial-como-se-usa-en-ucrania-y-porque-sigue-siendo-tan-controvertida-185458

Rojas, P. (21 de julio, 2018). 6 claves para detectar la estafa del falso funcionario de Hacienda. Recuperado de https://www.crhoy.com/nacionales/6-claves-para-detectar-la-estafa-del-falso-funcionario-de-hacienda/

Rodríguez, O (26 de julio, 2023,). Causas judiciales por estafas informáticas aumentan hasta 9.000 por año. Recuperado de https://www.nacion.com/economia/politica-economica/causas-judiciales-por-estafas-informaticas/QMHWDLHVLBEPROGDC3WROOEVR4/story/

Sala Constitucional de Costa Rica. (2022). Recurso de Amparo, Exp. N° 22-000419-0007-CO, Resolución Nº 02751 - 2022.

Salas, Y. (13 de junio, 2022). Ministerio Público alerta sobre estafadores que se hacen pasar por funcionarios municipales. Recuperado de https://www.nacion.com/sucesos/seguridad/ministerio-publico-alerta-sobre-estafadores-que-se/LY2JDVF6KNCBZN6BKK2ML5DRCY/story/

Schmall, E. (10 de febrero de 2022) Estafas románticas por internet: esto deben saber los jubilados. Recuperado de https://www.nytimes.com/es/2023/02/10/espanol/estafa-internet-romance.html

Stansfield, T. (13 de julio, 2023). Informe de Phishing y Malware H1 2023: Las Amenazas de Phishing Aumentan un 54% ("H1 2023 Phishing and Malware Report: Phishing Threats Increase 54%") Recuperado de https://www.vadesecure.com/en/blog/h1-2023-phishing-and-malware-report

Sweney, M. (8 de marzo,2023). Darktrace warns of rise in ai-enhanced scams since chatgpt release [darktrace advierte sobre el aumento de estafas mejoradas con inteligencia artificial desde el lanzamiento de chatgpt]. The Guardian. https://www.theguardian.com/technology/2023/mar/08/darktrace-warns-of-rise-in-ai-enhanced-scams-since-chatgpt-release

Threatcop. (31 de octubre, 2022). Ataques de Compromiso de Correo Electrónico de Proveedor: Un Peligro Emergente ["Vendor Email Compromise (VEC) Attacks: An Emerging Danger"]. Recuperado de https://threatcop.com/blog/vec-attacks/

The Hacker News. (2023, 15 de julio). WormGPT: Nueva herramienta de IA permite a los ciberdelincuentes lanzar sofisticados ataques cibernéticos ("WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks"). Recuperado de https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html

Toulas B. (9 de enero, 2023) . Sitios de citas falsos de OnlyFans abusan de la redirección abierta de la Agencia del Medio Ambiente del Reino Unido. ("Fake OnlyFans dating sites abuse UK Environment Agency open redirect") Recuperado de https://www.bleepingcomputer.com/news/security/fake-onlyfans-dating-sites-abuse-uk-environment-agency-open-redirect/

Universidad de Chile. (5 de abril, 2021). Ciberestafas aumentan un 20% en los últimos meses de la pandemia. Recuperado de https://tecnologias.uchile.cl/ciberestafas-aumentan-un-20-en-los-ultimos-meses-de-la-pandemia/

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2021). Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020. Ministerio Público Fiscal. Procuración General de la Nación. República de Argentina. Recuperado de https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf

UK Finance (s.f.) Estafas románticas en aumento durante el confinamiento. ("Romance Scams on the Up During Lockdown"") Recuperado de https://www.ukfinance.org.uk/press/press-releases/romance-scams-during-lockdown

Valverde, l. (21 de abril de 2022). Hacienda indagó a más de 200 empresas por presunto fraude o in-

fracciones tributarias. Recuperado de https://www.crhoy.com/economia/hacienda-indago-a-mas-de-200-empresas-por-presunto-fraude-o-infracciones-tributarias/

Velásquez, A. (21 de agosto de 2012). Expertos creen que ley de delitos informáticos debe ser equilibrada en aspectos jurídicos y técnicos. Recuperado de https://www.ucr.ac.cr/noticias/2012/08/21/expertos-creen-que-ley-de-delitos-informaticos.html

Villalobos, P. (22 de febrero, 2022) Una denuncia al día por chantajes sexuales en el país; exigen pagos de hasta $7 mil. Recuperado de https://www.crhoy.com/nacionales/una-denuncia-al-dia-por-chantajes-sexuales-en-el-pais-exigen-pagos-de-hasta-7-mil/

Wang, F., & Topalli, V. (16 de noviembre, 2022). Comprendiendo a los estafadores románticos a través de la perspectiva de sus víctimas: Modelado cualitativo de factores de riesgo y protección en el contexto en línea. ("Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context") Revista Americana de Justicia Penal. Vol. OnlineFirst.

ENTREVISTAS

Esteban Aguilar Coordinador de la Unidad Especializada en Cibercrimen, Fiscalía General de la República. 7 de julio, 2023.