15

MANERAS DE PREVENIR EL DELITO EN EL ÁMBITO VIRTUAL

Alberto Nava Garcés

FGR
FISCALÍA GENERAL DE LA REPÚBLICA
INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

15 maneras de prevenir el delito en el ámbito virtual

Instituto Nacional de Ciencias Penales
Magisterio Nacional núm. 113,
Col. Tlalpan, Alcaldía Tlalpan,
C.P. 14000, Ciudad de México

Primera edición, 2022

ISBN: 978-607-560-134-2

Contenido

Volver al índice

Utiliza los títulos del índice de contenidos para navegar a través del libro

Introducción

Para prevenir el delito es importante, en principio, tener un diagnóstico e identificar las conductas y las circunstancias que dan lugar a que este ocurra. En el ámbito virtual, el desconocimiento de la red y su potencial en muchas ocasiones propician que sea el propio usuario quien se coloque en una posición vulnerable. No siempre es así, pero bien podría minimizarse la posibilidad de ser víctima del delito.

Los altos índices de delincuencia e impunidad han sido un problema constante en nuestro país. Desde hace varios años es una constante apreciar el aumento en la comisión de delitos en México, lo cual ha provocado reacciones diversas por parte de actores sociales para afrontar el fenómeno criminal.

Debemos apostar por otro tipo de medidas que ayuden a reducir la criminalidad y el beneficio que se obtiene de él, siendo una de ellas la prevención, pero entendida esta no desde una instancia gubernamental o que tenga que articu-

larse por parte de agentes estatales, sino desde nuestra esfera personal.

Siempre ha existido el riesgo de ser víctima de un delito. Sin embargo, ¿qué tanto influye mi conducta para propiciar la comisión de delitos?, ¿vale la pena ostentar mis pertenencias en la vía pública o redes sociales?, ¿puedo evitar ser víctima de un delito modificando algunas actividades?

Es cierto que los índices de criminalidad son altos. También lo es que la mayoría de los delitos que se cometen en México son de naturaleza patrimonial y se pueden prevenir con acciones simples y concretas.

Por ello, el INACIPE presenta *15 maneras de prevenir el delito en el ámbito virtual*, en el que se dan a conocer medidas y acciones cotidianas que ayudarán a reducir la comisión de delitos y su impacto en la sociedad.

1

¿Qué son los delitos informáticos?

Los delitos informáticos son aquellas conductas que, mediante el uso de las nuevas tecnologías, atentan contra las personas, su información, sus datos, su patrimonio. También son conocidos como ciberdelitos.

Hace algunos años se consideraban meros medios comisivos de delitos clásicos, sin embargo, con el desarrollo de nuevas tecnologías, plataformas, redes sociales, aplicaciones, etcétera, los delitos informáticos cobraron una nueva dimensión y su futuro próximo lo encontraremos en el metaverso, porque lamentablemente el delito está asociado a la condición humana desde siempre.

Más ampliamente, los delitos informáticos son una subespecie de los delitos electrónicos que tiene como denominador común el uso de la computadora o dispositivos tecnológicos para realizar actividades criminales que, en un primer momento, los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo,

fraude, falsificaciones, daños, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las computadoras ha propiciado, a su vez, la necesidad de regulación por parte del derecho para sancionar conductas como las señaladas.

El delito informático se puede ver como el medio utilizado para cometer el delito y también como el fin cuando su objeto de ataque es otro dispositivo electrónico.

¿Puedo ser víctima de un delito informático?

Con el uso indebido de tecnologías nuevas o de punta y bajo el empleo de la ingeniería social, se abre un espacio para facilitar conductas reprochables. Entre las primeras tenemos el robo de información, el hackeo, el bloqueo a instrumentos o programas, clonación de tarjetas, usurpación de identidad, mientras que en las segundas se encuentran el denominado *grooming* o ciberacoso infantil, el fraude informático y el *phishing*, entre otras conductas, basadas esencialmente en el engaño.

La inmadurez de los menores de edad y el desconocimiento por parte de quienes los acercan a las nuevas tecnologías han dejado ese espacio en el que un depredador virtual puede actuar.

Si se conoce la forma en que actúan los delincuentes informáticos es posible prevenir los llamados delitos informáticos en su mayoría.

Ahora sirve preguntar: **¿puedo no ser víctima de un delito?**

La respuesta es *sí*. En un gran porcentaje, el usuario de nuevas tecnologías puede ponerse a salvo si sigue algunos pasos que no son tan complicados, solo es cuestión de entender el dispositivo que se utiliza, la página web a la que se accede o la plataforma que se descarga.

Algunos proveedores de servicios, de manera responsable, han desarrollado buenas prácticas para evitar el robo de identidad o el aprovechamiento indebido de datos y comunicaciones, por ejemplo, al establecer una doble forma de autenticación del usuario o a través de tarjetas inteligentes que no muestran abiertamente el número de cuenta o el nombre completo del poseedor de una tarjeta de crédito.

¿En qué consiste un ataque a un dispositivo conectado a la red?

Lo más común es que si, una persona no tiene cuidado con el uso de sus datos y la protección mínima de sus equipos y dispositivos, estos sean atacados por hackers, que sus equipos atraigan lo que se denomina *malware* y esto produzca no solo un mal funcionamiento, sino la pérdida de información. Por supuesto,existen ataques a distintas escalas, desde personas y usuarios individuales hasta instalaciones o actividades estratégicas para un país.

Un ataque ocurre cuando el usuario no utiliza de manera adecuada su equipo o dispositivo y se coloca en un estado vulnerable. La falta de contraseñas, de un software que prevenga la infección de virus o que terceros accedan a la computadora sin autorización son ejemplos de los actos más comunes.

Poner una contraseña débil (123456..., mary74, juanXXIII, o "contraseña", etcétera) es igual a no contar con un freno a una intrusión no autorizada, que es una primera parte de la protección. Lo mismo ocurre cuando, habiendo establecido una contraseña, esta se utiliza para todos los equipos, páginas web, aplicaciones o plataformas en las que se requiere de una.

Una contraseña sólida o resistente a ataques, a guisa de sugerencia, se basa en el establecimiento de una serie de elementos intercalados: números, signos, letras mayúsculas y minúsculas.

¿Qué es el robo de información?

Un dato es solo la referencia a algún aspecto, característica o elemento que, de manera aislada, no tiene mayor representación o peso en la vida cotidiana. La suma de datos constituye información.

Por ejemplo, de nada nos sirve saber el número de páginas de un libro o cuándo fue realizado si no tenemos más datos que, reunidos, nos proporcionen información valiosa: título, autor, texto, editor, año y lugar de impresión, etcétera. Lo mismo ocurre con la información que sirve para realizar cualquier actividad profesional, comercial o doméstica.

De manera más específica, los datos que en su conjunto refieren las características con las que se identifica a una persona cobran tal relevancia que se conocen como datos personales y su protección está prevista por la Constitución.

La información, es entonces, un bien valioso para las personas y por ello también se convierte en un objeto que

puede resultar atractivo para los delincuentes, quienes buscan apropiarse de información importante para usarla de manera indebida. Por ejemplo, pueden utilizar información para hacer compras con una tarjeta de crédito ajena, hacer transacciones no autorizadas por su titular, obtener bienes y servicios, cambiar registros bancarios o comerciales y hasta apropiarse de bienes inmuebles.

En los medios digitales la información es susceptible de ser copiada, borrada o alterada. Por ese motivo, dichas acciones deberían considerarse como delito en todas las legislaciones locales, lo que no ocurre hoy en día y, por tanto, independientemente de ser una tarea para el legislador, el usuario debe considerar la protección de la información que posee en sus distintos dispositivos electrónicos, ya sea con contraseñas seguras que impidan el acceso a los equipos, así como con la realización de respaldos con los que se procure evitar la pérdida de información.

Cuide su información y no olvide denunciar si ha sido víctima de algún delito relacionado con esta. La cultura de la denuncia es algo que todos debemos procurar.

¿Qué pasa si proporciono mis datos a través de un correo electrónico?

Existen diversas formas mediante las cuales los delincuentes informáticos "enganchan" a sus víctimas.

Piense, ¿cuáles son sus intereses en la red?, ¿bienes?, ¿servicios? Pues en la red puede existir el ofrecimiento falso de los mismos. Es por ello que la cultura de la compra en la red no debe inhibirse, sino realizarse con responsabilidad, a través de medios de pago que garanticen el reembolso en caso de que no se cumplan con las expectativas de la transacción.

¿Qué buscan los delincuentes que fingen proveer un servicio o la venta de algún bien?

A través de la llamada ingeniería social (que es un conocimiento sobre el actuar de las personas utilizado para explotar su ignorancia, ambiciones, deseos o hasta sus preocupaciones al realizar extorsiones virtuales o secuestro de información, etcétera) se hacen pasar por instituciones falsas, de loterías, centros de caridad o cuestiones que des-

pierten el interés por participar de los usuarios a los que les dirigen sus mensajes.

Para estos casos, basta con solicitar el auxilio de la Policía cibernética (local o federal) para reestablecer la computadora, sin embargo, ocurre que a veces las personas, los usuarios, piensan a qué páginas accedieron y consideran que no es necesario recurrir a la autoridad.

Es como un reconocimiento de culpas por las páginas que visitan y donde, con seguridad, fueron enganchados con algún programa para encriptar su computadora y limitar el acceso. Lo ideal sería que no se pagaran rescates para recuperar el control del equipo, pues nada asegura que realmente lo recuperen o que, probablemente, vuelvan a ser motivo de un acto reprobable como lo es el secuestro de información. Conclusión: llame a la Policía.

En estos tiempos, los temas de caridad, búsqueda de alimentos y medicinas, consulta de padecimientos, ofertas de último momento, ofertas de empleo que ofrecen grandes ingresos y que no exigen mayores requisitos (salvo una cooperación económica, como supuesta inversión), serán sin duda un motivo para tratar de enganchar a las víctimas potenciales. **Procure no ser una de ellas.**

Los pequeños saben mucho de las tecnologías actuales, sin embargo, ¿pueden ser víctimas de algún delito sin salir de casa?

Hoy en día, los menores de edad están cada vez más tiempo conectados a través de un dispositivo, pero hay varios riesgos o peligros en Internet para los niños, niñas y adolescentes. Y antes de dejar que los usen solos (aunque lo ideal es que estén siempre bajo vigilancia), hay que advertirles de esos peligros. Recordemos que la experiencia virtual deriva de la educación e información que tengamos de las plataformas, aplicaciones y redes sociales.

En la red hay depredadores sexuales, pedófilos, redes con contenidos que pueden causar mucho daño. Los casos más frecuentes tienen que ver con pornografía, acoso sexual (*grooming*), atentado sexual, violencia, abuso sexual, prostitución infantil, tráfico con propósitos sexuales, turismo sexual, pero también existe el peligro de que se vuelvan adictos a juegos de azar en línea o padezcan de acoso ciber-

nético (*cyberbullying*), este último de creciente incidencia en los jóvenes y adolescentes.

Cada uno de estos delitos tiene diferentes modalidades por Internet. Por ejemplo, los niños pueden exponerse a recibir o ver **pornografía** a través de páginas Web engañosas, que al abrirlas presentan fotos y videos con contenido pornográfico.

Todo comienza en el buscador, con la investigación inocua de palabras simples y propias de una tarea escolar. Por ejemplo: "Saturno", puede ser que al principio aparezcan las referencias técnicas y visuales del planeta referido, pero si se avanza en otras páginas, pudiera ocurrir que el contenido no sea académico sino más bien propio de negocios y más delante de sucesos o páginas no aptas, por su contenido, para ser vistas por menores.

También pueden darse acercamientos de adultos, a través de Internet, que intentan **seducir a niños, niñas y adolescentes**. Estos acercamientos se pueden hacer a través de las plataformas o redes sociales más populares como Facebook, Tiktok, Instagram, Snapchat, Whatsapp, Zoom, Google Meet y otros.

Es de suma importancia acompañar a los menores en su navegación por la red y, paulatinamente, supervisar sus actividades.

Más allá del ámbito tecnológico resulta de especial relevancia crear un ambiente de confianza con los menores para que estos a su vez puedan reportar cualquier anomalía que surja mientras utilizan sus dispositivos.

Quiero conocer a mucha gente, ¿qué tan confiables son las redes sociales?

Uno de los temas más interesantes respecto al uso de las nuevas tecnologías, sin duda alguna, es el de las llamadas redes sociales en Internet.

Pero las redes sociales no son en sí el delito; pueden ser, en cambio, el medio para su comisión, tal como ocurre en el que llamamos mundo real (es que el mundo virtual y sus alcances son tan reales que ya la clasificación está un poco obsoleta).

Es la red social un lugar de intercambio, donde las personas depositan pensamientos, ideas, rutinas, lugares frecuentados, comidas, antojos, viajes, relaciones personales, gustos; de modo tal que, sin darnos cuenta, quienes consultan un perfil pueden observar patrones de conducta que permiten ofertar bienes y servicios, muy al gusto de las personas, quienes pueden ser seducidas por la propia información que han dado, lo que dará lugar a que, a cambio del objeto ofertado, proporcionen datos personales o números de cuenta

de banco. El golpe está hecho, las distancias entre el lugar donde reside el delincuente y la víctima pueden estar separados no solo por todo un océano, sino por leyes que no terminan de empatar y que al final generan impunidad.

Cierto, hay que reconocer que se han dado soluciones locales para un problema global, pero también es importante reforzar la cultura de lo que pasa en la red para evitar, en lo posible, ser víctima de un ataque o un delito que pudimos prevenir con el uso del sentido común.

8

¿Qué es la usurpación de identidad?

¿Qué pasaría si alguien tomara mis datos?, ¿podría generarme algún problema legal o económico?

Resulta ya un lugar común referirse a los datos como el petróleo del siglo XXI. Para las generaciones pasadas los datos personales no parecen tener mayor relevancia más allá de establecer características singulares que distinguen a una persona de otra, y para las futuras generaciones habrá que explicarles qué significaba el petróleo en el siglo XX. Pero ¿realmente tenemos que preocuparnos por cuidar de nuestros datos?

Hoy en día existe una alta posibilidad de que llegue al domicilio una tarjeta de crédito no solicitada o diversa correspondencia que, sin bien está dirigida al habitante del domicilio, no deja de inquietar cómo ocurrió, en qué momento las empresas procesaron información para hacer llegar sus mensajes.

Lo mismo ocurre con los usuarios de la red, cuando descubren que la publicidad (*Ads*) pareciera estar pensada en sus necesidades, lo cual es cierto. El uso, las búsquedas, el tiempo que uno se detiene en las cosas que llaman la atención, las páginas abiertas, entre otros hábitos, forman una bitácora que tanto las redes sociales como los buscadores en Internet comparten para una explotación comercial (de ello dan cuenta los avisos de privacidad y contratos de uso, cuyas cláusulas pasamos inmediatamente, motivados por la ansiedad de iniciar la aplicación o entrar a la red).

9

¿Qué es el *smishing*?

Los usuarios, por diversas razones, depositamos ingentes cantidades de datos personales en Internet: edad, domicilio, estado civil, teléfonos, ingresos, lugar de trabajo, dependientes económicos, número de cédula, licencia, pasaporte, credencial para votar, CURP, números de tarjetas de crédito, NIP, fechas de vencimiento, número de seguridad social, placas de vehículos, claves catastrales, predio, identificador de contrato telefónico, contrato de cable y hasta contraseñas, entre muchos otros. Con estos datos estamos dotando a quien los recibe de una información que puede ser utilizada para cualquier fin.

De igual modo, quienes roban la identidad lo pueden hacer desde un trabajo aparentemente inocuo, por ejemplo, un encuestador que solicita no solo que la persona describa alguna preferencia, sino que le pide alguna identificación o, en los casos más comunes, hay quienes revisan la basura en

busca de datos. Así que la próxima vez que pretenda tirar un estado de cuenta a la basura, piense en cuántos datos contiene y el mal uso que puede hacerse de estos.

> Los ciberdelincuentes pretenden obtener información sensible por medio de mensajes de texto y la descarga de una aplicación.
>
> La nueva modalidad es el conocido "smishing", una nueva vertiente del "phishing", mediante el cual un sujeto intenta conseguir los datos de una persona para sustraer el dinero de sus cuentas bancarias.
>
> Usando técnicas de ingeniería social, se manda un mensaje de texto alarmante precisando la fecha y hora de una supuesta operación, comúnmente retiro de efectivo, se indica la cantidad y si señala si se reconoce o no la misma responder.
>
> Al responder la víctima, los ciberdelincuentes inician el contacto vía telefónica fingiendo ser personal bancario, argumentando la cancelación de la transacción falsa. Haciendo preguntas básicas, los ciberdelincuentes obtienen el nombre completo, fecha de nacimiento, número telefónico, datos de la cuenta y la última transacción.[1]

En el ámbito digital, Nico Sell ha publicado algunos consejos para la destrucción de datos y mantener comunicaciones seguras:

1 Coronado, Jesús, "¿Qué es el *smishing*"?, *idc Online*, 22 de julio de 2020, disponible en https://idconline.mx/corporativo/2020/07/22/que-es-el-smishing

1. Afirma que es necesario desinformar a las redes sociales, por ejemplo Facebook, respecto a datos como la fecha de nacimiento.
2. "Debes tener cuidado con las personas y los sitios que te piden información. ¿Por qué necesitan mi número de Seguridad Social? ¿Por qué necesitan mis señas?".
3. "Hay que acabar con la geolocalización". Aplicaciones como Twitter, Instagram y Foursquare, que piden información sobre la ubicación del usuario, pueden ser utilizadas para obtener información personal a través de la ingeniería social o incluso para averiguar el mejor momento para robar una casa.
4. Hay que leer los tediosos acuerdos de privacidad.
5. No confíe en ninguna aplicación médica. Se refiere al número de datos que hay que proporcionar y lo delicado de su contenido.[2]

Esta modalidad pone en grave peligro varios bienes jurídicos, entre ellos la identidad de las personas.

Los datos son muy importantes, la suma de ellos implica información. La información personal da lugar a un uso indebido y, aunque sea un delito, lo más importante es la prevención.

2 Redacción RT, "6 consejos de un importante 'hacker' para evitar el robo de identidad", RT español, 7 de julio de 2014, disponible en http://actualidad.rt.com/sociedad/view/133269-consejos-privacidad-hacker-robo-datos

10

¿Cómo puedo saber si el correo que recibo es peligroso?

Es altamente probable recibir correos cuyo único objetivo es causar algún daño al usuario, ya sea en su información o patrimonio; de modo tal que se debe estar atento a los remitentes. ¿Puede alguien ganarse la lotería sin haber comprado un boleto? El remitente nos escribe de manera cariñosa, pero ¿no sabe nuestro nombre (a menos que esté implícito en la dirección de correo electrónico: "maria@", "josé@", etcétera)? ¿Qué pasa con los mensajes que piden caridad o explotan el interés de ganar *dinero inmediato* por parte de alguien que no conocemos? Es evidente que se trata de un engaño.

Así que se sugiere, además de usar el sentido común, seguir simples pasos para detectar esta clase de correos:

- Comprobar el remitente. Distinguir si se trata de alguien conocido o no.

- Revisar el correo remitente. Ya que en ocasiones los delincuentes se hacen pasar por personas o instituciones, pero el correo electrónico no concuerda con la persona o institución o varían letras como la "L" minúscula y la "I" mayúscula que pueden pasar inadvertidas. Revise con cuidado este dato.
- Si se trata de alguien desconocido, corroborar el asunto del correo.
- Si pudiera parecer familiar el tema del asunto, verificar la información en el texto del mismo. No se deje llevar por el tono amenazante o por la solicitud de que debe contestar urgentemente.
- En ocasiones, el texto es una mera traducción (notoriamente deficiente), por lo que con seguridad se trata de información engañosa.
- Si tiene archivos adjuntos, deben tener una liga a un sitio seguro, ya sea que se identifique por un candado minúsculo o por el "https//", que significa que ha sido verificado. Un correo electrónico que se abre o se contesta con premura puede contener *malware* o ser el inicio de una estafa informática.

11

¿Las mujeres y niñas corren algún peligro con las nuevas tecnologías?

Sobre este particular se ha avanzado mucho en materia legislativa: el acoso, la pornovenganza, la violencia digital han sido atendidas de manera paulatina. La Asociación para el Progreso de las Comunicaciones (APC) elaboró la siguiente tipología que da cuenta de 13 formas distintas de agresión contra las mujeres a través de las tecnologías.

1. "Lo que entendemos por 'violencia en línea' es en realidad la práctica diversa que, a través de la vigilancia, el control o la manipulación de la información o de los canales de comunicación tienen como objetivo hacerte daño". Cuando una persona controla, vigila y supervisa las comunicaciones privadas (y no se trata

de menores, cuya atención es necesaria) se está ejerciendo violencia.[1]

2. El estar siguiendo a una persona, de manera que no le permita hacer libremente sus actividades, es otra forma de violencia.
3. Del uso inadecuado de las tecnologías, o derivado de otro delito, mujeres y menores pueden ser objeto de otros delitos, como la difusión de sus imágenes íntimas.

   No hay forma de aconsejar a un adulto que no mande por mensajes material gráfico personal, pero sí habría que advertir que enviar material íntimo ajeno, sin consentimiento y de manera paulatina es considerado un delito.

   Si alguien roba un celular y encuentra fotos íntimas entre los archivos, es posible que escriba un mensaje para pedir dinero a cambio de no publicarlas. No se debe ceder. Es posible que decida ponerlas en línea con una etiqueta.[2]

1 Luchadoras, "13 formas de agresión relacionadas con las tecnologías contra las mujeres", 23 de noviembre de 2017, disponible en https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/

2 Para la elaboración de esta tipología se revisaron los tipos de ataques en línea contra las mujeres enunciados por organizaciones como la Asociación para el Progreso de las Comunicaciones, Artículo 19, Cimac, Digital Rights Foundation, Women's Media Center, y Women Action Media, así como de procesos como Coming Back to Tech de Tactical Tech Collective. Véase también https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/

Para prevenir habría que recordar lo siguiente:

- Lo que se coloca en la red social o en Internet o se trasmite a través del celular, de manera potencial, se puede hacer público.
- Tener respaldo de la información del celular.
- Activar, de ser posible, el rastreo GPS del celular.
- Que este se active solo a través de una contraseña, de preferencia de carácter biométrico (reconocimiento de huella o rostro).
- Tener activada la aplicación para borrar la información de manera remota.
- No tener mucha información sensible en un objeto que puede ser robado o perdido.
- Denunciar el robo es importante. No debemos olvidar la cultura de la denuncia. Así, también, denunciar si ocurren actos posteriores que lastimen a la persona o divulguen su intimidad.
- Y, por otro lado, no difundir esta clase de material sin consentimiento.

12

¿Qué pasa si difundo los mensajes que me llegan por correo o por mensajería?

Podemos pensar en muchas formas por las que el equipo del usuario puede ser instrumentalizado: por un ataque, la inserción de un virus y, en esos casos, si la persona carece de una buena contraseña o un *firewall* en su equipo, ni cuenta podría darse de que este contribuye a la comunicación de grupos delincuenciales.

Pero hay otra forma, y es preocupante porque puede parecer inocua y hasta de buena fe. Nos referimos a la propalación de mensajes que llegan por correo o a través de las distintas redes sociales: las *fake news*.

Las noticias falsas son el *spam* de hoy, y lo peor es que muchas veces se contribuye sin conocimiento a la desinformación y a propalar alarma en la población.

Se esparcen noticias que solo sirven para acrecentar la polarización de la sociedad, a crear incertidumbre, generar

rumores, dar noticias que llenen de falsas esperanzas o alienten el encono contra algún sector o persona en particular.

Al final del día, una noticia falsa siempre envenenará a la sociedad a la que va dirigida. La forma de no contribuir a ello es verificando la fuente, así como el contenido de la propia nota. La red es un lugar donde se pueden alojar sin problema supuestas empresas o noticieros, es importante verificar su trayectoria, su intención y hacia dónde va la noticia difundida.

13

¿Qué es la *Deep Web*?

Por otra parte, existe la denominada *Deep Web*, que no es otra cosa sino una red construida para compartir o transmitir material ilícito, primordialmente. Esta red utiliza un sistema muy complejo para eludir la persecución de las autoridades encargadas de prevenir y combatir el delito, de modo tal que logran utilizar equipos de personas que navegan en la red sin mucho cuidado y hacer de sus equipos un instrumento para ocultar sus movimientos.

Y a la pregunta sobre lo qué podemos hallar en la *Deep Web:*

> ... la respuesta varía según se den por ciertos mitos que no llegan ni a realidad virtual. La respuesta más osada podría incluir sitios web de sectas satánicas, información clasificada y/o secreta de gobiernos, grupos terroristas, etc. Sin llegar a tanta ciencia ficción, pero sí a un alarmante

> inframundo virtual basado en el inframundo real, es cierto que en la web profunda normalmente se encuentran sitios con pornografía infantil, material censurado por cuestiones de decoro y ética periodística (videos explícitos de violencia sin censura como asesinatos o torturas), sitios de comercio electrónico de efectos ilegales, etc.[1]

No, no es ciencia ficción, por lo que es importante contar con programas que impidan que los equipos sean utilizados para estos fines: antivirus, firewalls, que son programas que de manera popular se encuentran en el mercado para evitar esta conducta.

1 Grover Dorado, John, "La web profunda y sus desafíos legales", *El Tribuno*, 3 abril de 2016, disponible en http://www.eltribuno.info/la-web-profunda-y-sus-desafios-legales-n695933, consultado el 5 de abril de 2016, 18:52 hs.

14

¿De qué se aprovechan los ciberdelincuentes para enganchar a sus víctimas?

Muchos ciberdelincuentes utilizan, por ejemplo, una llamada de atención, bajo el contexto de la pandemia, para contactar con los usuarios a través de redes sociales y correo electrónico.

Se ofrecen medicinas, tratamientos, equipo médico, mascarillas, cubrebocas, guantes, así como ingentes ofertas de entretenimiento. Es importante verificar el origen, pues en no pocas ocasiones se han detectado (por instituciones como el INCIBE, en España) varias campañas de envío de correos electrónicos con archivos adjuntos que contienen programas maliciosos, conocidos como *malware*.

Es muy aconsejable en estos tiempos reforzar la contraseña del correo, procurar tener un antivirus actualizado y contar con un *firewall* en los equipos. La contraseña debe incluir signos de puntuación, letras mayúsculas y minúsculas, números y símbolos, lo que dificultará su descifrado.

Es importante mantener la información a salvo y no abrir ofertas de procedencia desconocida ni proporcionar datos ante ofertas de último minuto.

Así mismo, es importante tener el antivirus al día y revisar que las contraseñas sean verdaderamente un muro ante cualquier ataque. **Si el dispositivo fuese objeto de inmovilización (extorsión virtual) no hay que dudar en avisar a las autoridades.** Con frecuencia la información es recuperada.

Es importante evitar el uso de señales gratuitas de *wifi* que nos ofertan en diversos lugares, ya que al acceder a este tipo de señales el equipo o dispositivo del usuario se coloca en una situación vulnerable o puede ser que se haya conectado a una red de donde tomarán sus datos.

Así que, si lo anterior es un tema que hay que tomar con las debidas precauciones, **con mayor razón** hay que evitar acceder a una red pública si la intención es ingresar a nuestra cuenta bancaria.

15

¿Están legislados los delitos informáticos?

De manera amplia están legislados los delitos informáticos en el Código Penal Federal, y en algunas legislaciones locales (ya que cada entidad federativa cuenta con su propio código penal) se contemplan diversas figuras como la pornografía infantil, el robo de identidad, el robo de información, la clonación de tarjetas de crédito, etcétera.

Y aunque ya algunos estados han legislado sobre cuestiones como el ciber acoso sexual infantil (*grooming*) o la pornovenganza, que consiste en subir a la red o compartir contenido de índole sexual de alguna pareja o expareja sin su consentimiento, está en vías de legislarse en todo el país este tipo de conductas.

Pero también han existido distintos intentos por sancionar la colocación de *memes*, parodias o críticas en la red, lo

que no es otra cosa sino una forma de censura. Hasta ahora esos intentos no han prosperado.

De modo tal que debemos colocar el énfasis en la prevención de las conductas que pudieran afectar la fama de las personas, su dignidad, su patrimonio y por supuesto su información.

Glosario

Ciberdelitos

Su denominación correcta, considero, debe ser delitos informáticos, ya que las referencias al ciberespacio son en realidad un derivado de una obra de ficción y del término acuñado como ciberespacio.

La primera dificultad teórica que suscita este sector del derecho informático surge de su propia denominación. En sentido estricto se entienden por delito las conductas tipificadas como tales por la ley penal. No obstante, bajo el rótulo del *delito informático*, se suele incluir también a las conductas criminales que, por su gravedad, encajan en los tipos delictivos. Aquellas que por su menor trascendencia no rebasan la esfera de las meras faltas.

Junto a estos tipos penales, la expresión *delito informático* se utiliza muchas veces con referencia a las infracciones administrativas (por ejemplo, los atentados contra las normas de protección de datos personales informatizados) o

los ilícitos civiles (tales como la consabida piratería del *software*). Incluso para contribuir a la mayor indeterminación y equivocidad conceptual del delito informático, dado el retraso de la respuesta jurídica a muchos supuestos criminales de incidencia informática.

Los *delitos informáticos* son actividades criminales que, en un primer momento, los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo o hurto, fraude, falsificaciones, daños, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las computadoras ha propiciado, a su vez, la necesidad de regulación por parte del derecho para sancionar conductas como las señaladas. Correa destaca el aspecto evolutivo del delito informático y al respecto señala:

> A través de los años se ha ido produciendo una evolución del concepto de protección de datos determinada por dos aspectos fundamentales: la evolución de las técnicas de información y la nueva configuración de derecho a la vida privada.
>
> En los primeros años de aplicación de las leyes de protección de datos la discusión se centraba en la antítesis vida privada *versus* computadoras. En el actual estado tecnológico la protección de datos es una síntesis de los intereses individuales y sociales en juego.[1]

1 Sieghart, Paul (citado por Correa), *Legislation and data protection*, Proceedings of the Roma Conferencia on Problems Relating to the Development and Aplication of Legislation on Data Protection, Council

> La evolución de las técnicas informáticas hace necesario hablar de sistemas de información en lugar de ficheros y tener en cuenta las contradicciones que existen entre la vida privada y otras libertades esenciales.[2-3]

Al respecto, debemos puntualizar que la evolución recae en las tecnologías de la información y no en sus técnicas, toda vez que estas pueden entenderse como los procesos o la pericia que alguien posee en un arte u oficio.

Sin embargo y luego de la siguiente disquisición, Correa acepta el concepto que, veremos, establece Sieber y es recogido también por Palazzi:

> El uso de las computadoras, y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso del computador. Si bien no existe aún una medida exacta de la importancia de estas trasgresiones, es probable que su incidencia se acentúe con la expansión del uso de computadoras y redes telemáticas. Los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas, tal como la interferencia en una red bancaria para obtener, mediante una orden electrónica,

of Europa, Camera dei Deputati, Roma 1983, p.16.

2 Lenoir, Nôelle, (citada por Correa), *Legislation and data protection,* p. 26.

3 Correa *et al., Derecho Informático,* Ediciones Depalma, Buenos Aires, Argentina, 1987, p. 249.

un libramiento ilegal de fondos o la destrucción de datos. El tema plantea, además, complejos perfiles para el Derecho Internacional cuando el delito afecta a más de una jurisdicción nacional.[4]

En el ámbito internacional se considera que no existe una definición propia de *delito informático*, sin embargo, muchos han sido los esfuerzos de expertos que se han ocupado del tema y, aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Ahora, uno de los problemas que ha enfrentado nuestro tema es que en la mayoría de los casos se ha tratado por juristas ajenos al derecho penal.

Palazzi señala: "sin establecer una regla genérica, podemos afirmar que una computadora puede constituir un *medio* para cometer un delito o el *objeto* sobre el cual recaiga el mismo".[5] Y, en ese orden de ideas, recoge la definición realizada por un grupo de expertos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE): "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos".[6]

4 *Ibidem, p. 295.*
5 Palazzi, Pablo A., *Delitos informáticos, 1ª ed., Ad Hoc, Buenos Aires, 2000, p. 33.*
6 *Ibidem, p. 39.*

La anterior definición nos obliga a detenernos a recapitular sobre ella porque se aleja de los elementos básicos del delito para formular un concepto genérico, discutible en varios aspectos, sobre todo en lo relativo a una conducta ilegal, la cual consideramos, interpretando en su totalidad la definición, solo redunda en el carácter antijurídico de la conducta que transmite o procesa datos de manera ilegal.

A pesar de todo, consideramos que esta es la acepción más próxima y acertada para establecer los rasgos genéricos del delito informático y al efecto definimos al mismo como "toda conducta ilegal que involucra el procesamiento automático de datos y /o la transmisión de éstos".

El delito informático tiene como fundamento la protección de datos y de información.

Pavón Vasconcelos establece una idea consistente en que en realidad el delito, como noción, puede preexistir a su definición como tal. Así, sobre el particular, Pavón Vasconcelos, en su *Diccionario de Derecho Penal*, escribe:

> Jiménez de Asúa para destacar las dificultades que hay que vencer para definir al delito en cualquier plano, sea este filosófico o natural e inclusive recuerda que 'la cosa debe preexistir a la definición y no ser creada por la definición misma'. A opinión de Jiménez de Asúa, la innecesariedad de una definición en los códigos radica en que 'nada enseña a los doctos y nada aclara a los profanos' como ya lo había señalado Dorado Montero. A su entender, esta afirmación se concreta a las definiciones que se hacen

constar en los códigos, con relación al delito en general, pues la noción de delito puede ser construida científicamente con base en las disposiciones del propio ordenamiento jurídico.[7]

Así, después de describir el objeto materia de este estudio, debemos especificar el ámbito del mismo. Esto nos servirá para apreciar con claridad el hecho que los tratadistas que se han ocupado por definir a los delitos informáticos no han destacado: cuál es el bien jurídico tutelado (que todo delito lleva inmerso en sus fines) y cuál es el alcance del carácter informático.

Claves de acceso (contraseñas)

Las nuevas tecnologías permiten el movimiento de dispositivos y con ello el traslado de datos de un lugar a otro, lo que potencialmente permitiría su sustracción u obtención sin consentimiento. Las claves de acceso son la forma de autenticar a la persona autorizada para conocer de la información que se encuentre ya sea en una computadora o en un dispositivo móvil.

7 Pavón Vasconcelos, Francisco, *Diccionario de Derecho Penal,* 2ª. ed., Porrúa, México, 1999, p. 296, palabra: delito.

Conductas más comunes para enganchar y engañar a los usuarios

Entre esas distintas conductas tenemos las siguientes:

1. *Phishing* de caridad. Haciéndose pasar por organizaciones reales, los delincuentes de la red simulan páginas para que la gente aporte dinero y se obtenga por ese medio el número de cuentas bancarias, así como los números de seguridad para realizar operaciones por Internet. No son pocos los casos que año con año ven los bancos e instancias como CONDUSEF para resolver quebrantos tanto a usuarios como a las instituciones del sistema financiero.
   Y al respecto debemos tomar en cuenta que hay dos quebrantos distintos según la tarjeta utilizada:

   a. Si es una tarjeta de débito, el patrimonio del usuario es el que resiente el daño inmediato. El banco verificará si se llevaron a cabo los protocolos de seguridad del usuario (que tenga en su poder la tarjeta, que no haya trasmitido a un tercero el NIP, y que no se haya usado el chip de la tarjeta en la compra, por ejemplo) para resarcirlo en su patrimonio.
      Sin embargo, este proceso puede ser muy lento. Más vale no prestarse a los engaños que pueden llegar por medio de un correo electrónico o un

mensaje (SMS o por las APPS como WhatsApp, Telegram, etcétera).

b. Si se trata de una tarjeta de crédito, aunque merma la capacidad crediticia del usuario, lo cierto es que el primer afectado es el banco, por lo que este verificará si se llevaron a cabo los protocolos de seguridad del usuario (que el usuario tenga en su poder la tarjeta, que no haya trasmitido a un tercero el nip, y que no se haya usado el chip de la tarjeta en la compra, por ejemplo) para resarcirlo en su capacidad crediticia o cargarle la compra o disposición.

2. Falsas compañías. Correos electrónicos falsos de empresas de "reconocido prestigio" que solicitan información confidencial del usuario (también datos de las tarjetas de crédito), para confirmar que son correctos. Es importante destacar que el usuario debe tomar en cuenta las empresas con los que regularmente mantiene comunicación. Los bancos no le solicitarán datos que la propia institución ya conoce.
3. Se debe tener cierta cautela con los perfiles falsos que abundan en redes sociales y que hacen peticiones de amistad. Más vale tener en cuenta que muchas de estas solicitudes solo entrañan seducir a los usuarios para hacer ventas u obtener datos personales.
4. Se debe evitar, en lo posible, abrir archivos adjuntos que contengan supuestas felicitaciones, pues podrían

ser en realidad un gusano, tanto si van adjuntas en el correo o si van como archivo PowerPoint.

5. Ojo con las ofertas de último momento o que tienen un plazo muy pequeño para responder. En la ingeniería social es común que, si le das poco tiempo a la persona, esta tendrá poca oportunidad de pensar, verificar o consultar a un tercero. Las falsas baratas de marcas de lujo como Gucci y Cartier son la novedad para los incautos en la red, según McAfee.
6. La navegación. La empresa McAfee alerta, de manera regular, sobre la navegación desde ordenadores públicos o redes wifi abiertas, pues los *hackers* aprovechan esas oportunidades para espiar las actividades de los internautas. Se recomienda utilizar navegadores seguros.
7. Halloween, días festivos o la propia Navidad son anunciadas tanto en los correos como en las redes sociales (con virus). Tarjetas vistosas, graciosas tal vez, *wallpapers* o *protectores de pantalla* pueden ser el gancho perfecto para instalar virus.
8. Desempleo. Ofertas increíbles de trabajo se ofrecen en línea y solo tienen la utilidad de robar el dinero o los datos de las personas que buscan desesperadamente un empleo.
9. Herramientas de bajo costo. El robo de contraseñas se convierte en algo habitual durante estas fechas mediante herramientas de bajo costo, como por ejemplo, aquellas que graban las pulsaciones.

10. Detalles bancarios. Igual que con los supuestos correos de confirmación de empresas, los *hackers* envían un correo supuestamente de bancos. La información que obtienen incluso se vende en el mercado negro.
11. Secuestro en línea de datos, archivos o del arranque de la computadora. Por último, el *secuestro de archivos* propios: el ciberdelincuente encripta los documentos personales del usuario y después pide el pago de un rescate para obtenerlos.[8]

Deep Web

En Estados Unidos se ha propuesto, como medida de control, la creación de una identificación para quien desee navegar en Internet, ya que con esta nueva herramienta la ingeniería social encuentra un medio eficaz para potenciar conductas nocivas, de modo tal que ha dado lugar al desarrollo de la llamada *Deep Web*, que en términos digitales y de la política criminal y la prevención del delito constituyen uno de sus mayores retos.[9]

8 Trexill, News and Stories, disponible en https://www.mcafee.com/enterprise/en-us/about/newsroom.html?article_id=3596

9 "¿Qué es la DeepWeb? Es todo aquello que está en red y que no es accesible por nosotros directamente. Son servicios que están detrás de una autenticación, por lo cual si no tenemos credenciales no podemos ver esos contenidos, explica Vicente Díaz, analista principal de Kaspersky Lab.

La *Deep Web* ha sido una herramienta mediante la cual se difunde información que facilita en gran medida las actividades ilícitas, desde intromisiones no autorizadas hasta flujo de información relativa a pornografía infantil o terrorismo. No solo es la apología del delito, sino la comisión del delito lo que puede cruzar por esa red.

''La Internet Profunda no es accesible desde Google, para ello hace falta la utilización de tecnologías y códigos de programación que generan navegadores específicos para poder acceder a ellas. 'El servicio que siempre se tiene en mente cuando hablamos de DeepWeb son las redes Tor, para las cuales debes poder acceder con un navegador particular' explicó Díaz. ¿Cómo puede afectarme la DeepWeb?
[...]
''Cibercrimen a la carga: de todo pasa en la DeepWeb
Si algo ha evolucionado en esta época de globalización es el hecho de que los cibercriminales ahora son grupos organizados que hasta trabajan como empresas. Un informe de Kaspersky Lab reveló recientemente que los cibercriminales trabajaban en conjunto desde diferentes lugares del mundo para ayudarse a lanzar sus ataques.
Estas comunicaciones se realizan a través de este mercado que se maneja en un submundo en el que simplemente los usuarios comunes no tenemos acceso, e incluso muchas veces ni siquiera las autoridades lo tienen. 'A través de páginas Tor que no son fácilmente accesibles se llevan a cabo estos encuentros', explicó Díaz.
''Aunque en la DeepWeb se puede encontrar también pedofilia, hay un nivel superior de esta Internet profunda, llamado Charter Web, un lugar lleno de hackers, pornografía y depravaciones de todo tipo. En este nivel también se encuentra tráfico de órganos, contratación de sicarios y ejecuciones de extremistas''. Consultado en Salza, César, "¿Qué es la DeepWeb y cómo puede afectar mi vida?", prnoticias.com, 15 de abril de 2016, disponible en http://prnoticias.com/tecnologia/prtecnologia/20151591-deepweb, consultado el 17 de abril de 2016, 21:38 hs.

Geolocalización

El tema de la geolocalización como una herramienta más para la investigación del delito genera polémica porque las nuevas generaciones no están dispuestas a ceder parte de su privacidad y de ese ambiente aparentemente neutro que encuentran en la red mediante dispositivos móviles que existen en el mercado para mejorar las comunicaciones; sin embargo, los teléfonos inteligentes (o *smartphones*) y el ingreso habitual al ciberespacio permiten que el usuario se *autogeolocalice*.

De entre las aplicaciones y redes más comunes hay algunas especializadas en la ubicación, tal es el caso de las que auxilian a encontrar una ruta entre dos puntos (Waze, Navigon, Google Maps, etcétera), las cuales además generan con el uso habitual un patrón de rutas.

De entre esas redes destaca Foursquare (Swarm), creada en 2008 y que realiza el *check-in* de los distintos lugares que el usuario visita (restaurantes, hoteles, aeropuertos, espectáculos, escuelas, supermercados, comercios de distinta índole y nivel) y se autogeolocaliza para los integrantes de su red. Así, también las personas tienen la posibilidad de dejar comentarios e imágenes sobre el lugar visitado, ya sea para recomendarlo o no, y dichas opiniones pueden ser consultadas por quien visite la información de determinado lugar, aun cuando no esté en el mismo grupo.

Por otra parte, la nueva generación de *smartphones* registra la huella del usuario para que este pueda utilizarla

como medio de identificación y acceso a las aplicaciones, o bien, como medio de pago. En cualquier caso, dicha operación permite con un alto grado de certeza contar con un registro.

En ese tenor, la geolocalización proviene del equipo utilizado y se potencia con el uso de las redes, en donde, con más frecuencia, los usuarios deciden compartir su ubicación (existe también que el propio sujeto a localizar utilice algún chip de localización o *software*, como *Trackimo*, para su propia seguridad), motivo por el cual no debería sorprender que la autoridad pretenda regular lo que en otro tiempo ya ocurría, pero sin que pudiese aportarse en juicio por violación a la privacidad.

Grooming

Es el acoso cometido por un adulto contra menores de edad, con el fin de obtener imágenes de contenido erótico o pornográfico. El acosador virtual se oculta gracias a la ingeniería social y con la facilidad que permite el medio electrónico por medio de una falsa identidad, con lo que obtiene que el menor confíe en él y se genere un verdadero vínculo de dependencia y, en consecuencia, el menor no puede librarse por falta de herramientas o madurez suficiente, de modo tal que su voluntad queda sometida al acosador.

Meme

Son representaciones visuales (imágenes, dibujos, composiciones gráficas) con un mensaje que incide en el momento para abordar noticias, sucesos, citas célebres, recordar frases de políticos, deportistas o artistas, caricaturizar hechos o personas o solamente dejar un texto con ejemplo gráfico. Su carácter coyuntural se aprecia cuanto más se conoce el contexto; con el paso del tiempo son meras referencias sin mayor significado.

Algunos memes, por inocuos que parezcan, hacen uso de imágenes protegidas por derechos de autor.

Phishing y *pharming*

Los ataques de *phishing* son aquellos que se valen de la ingeniería social (redes sociales, chats, correo electrónico), con el propósito de sustraer datos personales y credenciales de cuentas bancarias de las personas.

Esto ocurre de la siguiente manera: mediante el uso de correos falsificados, con el fin de llevar a los consumidores a sitios falsos, creados para que las personas divulguen datos financieros, como son números de tarjeta de crédito, nombres de usuarios de cuenta y contraseñas.

Esto, bajo la falsificación de marcas de bancos, tiendas virtuales y administradoras de tarjetas de crédito; así, de

esta manera los *phishers* logran convencer a los destinatarios a que respondan a dichos engaños.

Señalan que el usuario actualice sus datos, por ejemplo, de una cuenta de banco (y entonces el usuario decide, a ciegas, entrar en la página donde deben proporcionar datos personales, lo cual se podría evitar consultando directamente al banco).

Bibliografía

CASTELLS I. MÁRQUES, Marina, "Drones Civiles", en *Inteligencia artificial*, Tirant lo Blanch, (Col. Derecho y TIC), Valencia, España, 2017.

COELLO COELLO, Carlos A., *Breve historia de la computación y sus pioneros*, FCE, México, 2003.

CORREA, Carlos *et al*., *Derecho informático*, Ediciones Depalma, Buenos Aires, Argentina, 1987.

DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de datos personales en el sector de las comunicaciones electrónicas*, Universidad Comillas, Madrid, 2003.

FÉRAL SCHUHL, Christiane, *Cyberdroit*, 3ª ed., Dalloz, Paris, France, 2002.

GOODMAN, Marc, *Cibercriminalidad*, Vol. 7, Conferencias Magistrales, INACIPE, México, 2003.

LESSIG, Lawrence, *Code and other Laws of Cyberspace*, Basic Books, United States of America, 1999.

LUZ, Clara Bibiana, *Manual de derecho informático*, Editorial Jurídica Nova Tesis, Argentina, 2001.

NAVA GARCÉS, Alberto Enrique, *Análisis de la legislación penal mexicana en informática. Retos y perspectivas* (Colección Los delitos electrónicos en Latinoamérica), UBIJUS, México, 2015.

____, *Delitos Informáticos,* 4ª ed. Universidad de Salamanca, Porrúa, México, 2018.

PALAZZI, Pablo A., *Delitos informáticos*, 1ª ed., Ad Hoc, Buenos Aires, 2000.

ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos,* Comares, Granada, España, 2002.

Legislación

Código Nacional de Procedimientos Penales

Código Penal Federal

Legislation and data protection, Proceedings of the Roma Conferencia on Problems Relating to the Development and Aplication of Legislation on Data Protection, Council of Europa, Camera dei Deputati, Roma 1983.

Hemerografía

NAVA GARCÉS, Alberto E., "Los delitos informáticos y su ausencia en la legislación penal mexicana", en *Derecho Penal*, Universidad de Friburgo, octubre de 2010, dispo-

nible en http://www.unifr.ch/ddp1/derechopenal/articulos/a_20100907_04.pdf

——, "La geolocalización en la regulación procesal penal" en revista *Foro Jurídico*, núm. 135, México, diciembre de 2014, pp. 16–20.

——, "*Grooming* una conducta a tipificar", en revista *Iter Criminis*, núm.10, sexta época, julio–septiembre de 2015, pp. 51–77.

——, "Dos visiones sobre el *grooming*", en revista *El Mundo del Abogado, una revista actual*, Año 17, núm. 199, México, noviembre de 2015, pp. 24–31.

Diccionarios

Diccionario de la Lengua Española, Real Academia Española, 22ª ed., Madrid, 2001.

PAVÓN VASCONCELOS, Francisco, *Diccionario de Derecho Penal*, 2ª ed., Porrúa, México, 1999.

Fuentes electrónicas

Abogados Portaley, "Riesgos de delitos relacionados con criptomonedas", delitos informáticos.com, 17 de febrero de 2021, disponible en http://www.delitosinformaticos.com

Agencias, "Cinco muertos en los disturbios por el precio del alza de la gasolina en México", *El País*, 6 de enero

de 2017, http://internacional.elpais.com/internacional/2017/01/06/actualidad/1483689835_154959.html

CORONADO, Jesús, "¿Qué es el *smishing*"?, *idc Online*, 22 de julio de 2020, disponible en https://idconline.mx/corporativo/2020/07/22/que-es-el-smishing

GROVER DORADO, John, "La web profunda y sus desafíos legales", *El Tribuno*, 3 abril de 2016, disponible en http://www.eltribuno.info/la-web-profunda-y-sus-desafios-legales-n695933, consultado el 5 de abril de 2016, 18:52 hs.

Luchadoras, "13 formas de agresión relacionadas con las tecnologías contra las mujeres", 23 de noviembre de 2017, disponible en https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/

Redacción RT, "6 consejos de un importante 'hacker' para evitar el robo de identidad", RT español, 7 de julio de 2014, disponible en http://actualidad.rt.com/sociedad/view/133269-consejos-privacidad-hacker-robo-datos

SALZA, César, "¿Qué es la DeepWeb y cómo puede afectar mi vida?", prnoticias.com, 15 de abril de 2016, disponible en http://prnoticias.com/tecnologia/prtecnologia/20151591-deepweb, consultado el 17 de abril de 2016.

TheHackerNews, "Troyano bancario copia la forma de propagación de WannaCry", 3 de agosto de 2017, disponible en https://www.seguridad.unam.mx/troyano-bancario-copia-propagacion-de-wannacry

Suprema Corte de Justicia de la Nación, disponible en http:/ www.scjn.gob.mx

Universidad de Freiburg, disponible en http://www.unifr.ch/ derechopenal/

Trexill, News and Stories, disponible en https://www.mcafee.com/enterprise/en-us/about/newsroom.html?article_id=3596

15 MANERAS DE PREVENIR EL DELITO EN EL ÁMBITO VIRTUAL

Edición al cuidado de la Dirección de
Publicaciones y Biblioteca del Instituto
Nacional de Ciencias Penales
Julio 2022

Edición de distribución gratuita