ÉTICA, LEGISLACIÓN Y PROFESIÓN

CONTENIDO DE LA CHARLA

Facultad de Informática

Grupo Alto Mando
Patricio Álvarez Castillo
Jonathan Carrero Aranda
Pablo Márquez Fernández
Pablo Martín Atienza
Mario Michiels Toquero
Pedro Sánchez Ramírez
Cristian Pinto Lozano

Introducción

En primer lugar, presentamos, a modo de seguir la lectura del documento mientras se realiza el visionado, el *enlace* desde donde puede verse la presentación.

Estructuramos la charla de forma que fuese lo más dinámica posible para aquellos alumnos que no poseyeran conocimiento técnicos en el área informática o, generalizando un poco más, en las TIC. A pesar de ello, debe tenerse en cuenta que, para conocer los peligros en la web, es necesario dar algunas pinceladas que nos ayuden a conocer la causa del problema, lo que conlleva y qué podemos hacer para evitarlo.

Entrando en contenido, comenzaremos con una pequeña introducción en la que, esencialmente, responderemos a una pregunta a la que la mayoría de la gente no suele darle la importancia debida: *¿Por qué debo preocuparme de mi privacidad en Internet?*

Nos centraremos en un bloque básico que afecta a todo usuario dentro de Internet, sea o no del ámbito jurídico: *La navegación web*. Veremos qué son las cookies, cómo borrar nuestro rastro tras la navegación o qué problemas puede acarrear el hecho de no limpiar nuestro sistema asiduamente.

Entraremos en el mundo de las redes WiFi, de los problemas que pudieran surgir si no tomamos medidas de precaución y veremos soluciones para navegar de forma segura a traveś de ellas. También conoceremos técnicas que emplean los delincuentes para intentar engañarnos con web falsas y que piquemos el anzuelo de la estafa.

También daremos un rodeo para enseñarte cómo proteger la información que llevas en tu USB, proporcionando software que te ayudará a la protección de tus datos más confidenciales.

Además, echaremos un ojo al Código Penal para conocer de primera mano qué penas conlleva el mal uso de las TIC o cómo podríamos nosotros saber qué es lítico y qué no lo es.

Por último, y para corroborar la respuesta con la que comenzamos esta charla, mostraremos imágenes reales de casos en los que, precisamente, no se dio la importancia necesaria a toda esa información.

¿Por qué preocuparse por la privacidad en Internet?

Por Patricio Álvarez Castillo

¿Debo preocuparme por mi privacidad en Internet? Es una buena pregunta para empezar, y la respuesta es sencilla: Si; todos los datos personales de un usuario pueden ser utilizados por terceros de forma arbitraria e irresponsable, con las consecuencias que aquello implica.

La otra frase tan frecuente dicha es “No tengo nada que ocultar” o “No tengo nada que pueda interesarle a un atacante” o “No soy un delincuente ni un terrorista”. Bien, si alguien opina que no tiene nada que ocultar, debería plantearse las siguientes preguntas:

- ¿Compartirías información sobre tu ubicación con un extraño?
- ¿Compartiría fotos tuyas o de tus familiares con desconocidos?
- ¿Compartiría información relacionada con tu trabajo, tus asuntos financieros o de salud con ajenos?
- ¿Compartiría información sobre tu rutina diaria o la de tus hijos con un desconocido?
- ¿Permitiría que alguien con acceso a dicha información lo compartiera con cualquiera?

Ahora es el momento de preguntarse nuevamente: *¿Tengo algo que ocultar?*

Historial de navegación

Por Pablo Martín Atienza y Pablo Márquez Fernández

Las prácticas que se nombran a continuación tienen explicaciones (algunas de ellas bastante técnicas) sobre cómo se llevan a cabo y qué repercusiones exactas tienen sobre nosotros. En cualquier caso, se han omitido con el objetivo de no entrar en muchos detalles e ir a lo que verdaderamente nos interesa. Estas son algunas de las prácticas que llevan a cabo las grandes empresas:

- Facebook: aunque elimines tu cuenta, los datos siguen estando almacenados en los servidores, la única forma de borrarlos sería eliminar foto por foto, comentario por comentario, etc.
- Facebook: utilizan cookies (más tarde sabremos qué son) para rastrear tus gustos y así ofrecerte publicidad sobre cosas que puedan llegar a interesarte (ropa, móviles, viajes…).
- Facebook: los contenidos públicos pueden ser indexados por cualquier buscador y, aunque tu datos (sí, los propios datos) sean eliminados, es posible que esa información ya haya sido capturada por un tercero. Con lo cual, es imposible controlar el alcance que tendrá tu información pública.
- Google: supongamos que tienes dos ventanas abiertas en el navegador; en una de ellas tienes abierta tu sesión de Gmail y en la otra realizas cualquier búsqueda (hoteles en Calpe, por ejemplo). Pues bien, Google asocia la información que buscas directamente con tu perfil de Google.
- Google: también guarda información sobre los dispositivos que usaste para conectarte a cualquiera de sus servicios.
- Google: almacena toda la actividad de una cuenta determinada (conversaciones, dispositivos, registros de audio y de vídeo, calendarios, documentos subidos a Google Drive…). Si alguien tiene curiosidad, puede consultar la actividad que Google ha recolectado sobre su cuenta en el siguiente *enlace*.
- Google: también almacena un historial de geolocalización (esto ocurre, entre otras cosas, cuando una aplicación de Android no pide permiso para acceder a nuestra geolocalización). De nuevo, si alguien tiene curiosidad puede visitar el siguiente *enlace*.

Podríamos estar muchísimo tiempo destapando cosas que, no olvidemos, hemos aceptamos al usar los servicios de estas grandes empresas (hemos nombrado quizá las dos más conocidas, pero esto ocurre con muchas otras: Twitter, Instagram, Snapchat…), pero tan solo pretendemos dar una visión global de todo lo que ocurre y de cómo las empresas ganan tantísimas cantidades de dinero gracias nuestra información personal.

Cookies

Las cookies son pequeños ficheros de texto que guardan información enviada por el navegador del usuario. Normalmente se utilizan para facilitar al usuario la tarea de

interactuar con los servicios en Internet. Cuando decimos que guardan información nos referimos a que almacenan cosas como:

- Información referente a la sesión de un usuario en un determinado sitio web (Google, Facebook, Forococches…).
- Patrones de comportamiento del usuario, es decir, si cuando entras en la página web del Decathlon (por ejemplo) te gusta visitar la parte de tiro con arco, surf o lo que sea. De ahí que en muchas páginas aparezca lo típico de "Te recomendamos…".
- Las cookies también pueden guardar información que te identifique personalmente. Esta información personal, como por ejemplo nombre, correo electrónico, domicilio, domicilio de tu puesto de trabajo o número de teléfono, es la que se puede usar para identificarte o contactar contigo. Sin embargo, un sitio web solo tiene acceso a la información personal que tú le proporcionas (en ese botón que nadie se lee llamado "Acepto los términos de blah, blah, blah").

Historial de descargas y descargar en el ordenador

El historial de navegación es un fichero que guarda todas las páginas web que se visitan a lo largo del tiempo, mientras que el historial de descargas es un fichero que guarda el lugar de origen y destino de todos los archivos descargados.

Con lo cual si juntamos las ideas del historial de navegación y de las cookies nos damos cuenta de que puede ser algo peligroso. Dado que cualquiera puede recolectar nuestra información sin que nosotros nos percatamos de ello, bien sea de las páginas que visitamos, de sesiones que dejemos iniciadas. Lo mismo que ocurre con el historial de navegación, ocurre con el historial de descargas, con la diferencia de que el historial de descargas no necesita de las cookies para ser algo peligroso. Si no nos encargamos de eliminar cualquier referencia a nuestras descargas, corremos el riesgo de que algún documento privado, caiga en manos de cualquier persona que haga uso del ordenador y al que le puedan llegar interesar nuestros datos o quiera hacer un mal uso de los archivos.

Dentro de los navegadores tenemos la posibilidad de que a partir de una descarga realizada con anterioridad, aunque se haya eliminado el archivo descargado, se pueda volver a descargar, ya que los navegadores guardan la información de la página web desde donde se realizó las descarga.

Frente a esto, tenemos un par de soluciones para evitar el problema ya explicado:

- Podemos o bien borrar el historial de descargas, o podemos conectarnos a internet a través de la navegación privada.

Una vez hayamos borrado el historial de descargas, tenemos que prestar también atención a cómo borramos los propios archivos del ordenador. Para ello tendremos que revisar la papelera de reciclaje. Para ello existen varias formas que dependen del sistema operativo:

- Para Windows:
    - Borrar el archivo como normalmente lo haríamos para después visitar la papelera y vaciarla.
    - Borrar el archivo haciendo uso de los comandos(Shift + Supr) que eliminarían el archivo sin necesidad de tener que vaciar la papelera.
- Para Mac:
    - Borrar el archivo como normalmente lo haríamos para después hacer un vaciado de forma segura de la papelera.
    - Borrar el archivo haciendo uso de los comandos(Alt + Comando + Supr o Alt + Comando y pulsando sobre la opción eliminar permanentemente.

Para finalizar este apartado, como recomendación personal, durante el uso de un ordenador, ya sea bien público o bien privado, sería conveniente el uso de la navegación privada para evitar todo lo comentado hasta ahora en relación a las cookies y al historial de navegación, teniendo solo que prestar atención a la forma de borrar las descargas realizadas.

Peligros en redes WiFi

Por Mario Michiels Toquero y Pedro Sánchez Ramírez

En el acceso a redes, especialmente de líneas Wifi abiertas o compartidas, hay que evitar utilizar información personal o acceder a sitios de donde pones en compromiso tu privacidad, ya sea bancos, correo, etc.

¿Por qué? Pues porque al igual que me puedo conectar yo, se puede conectar un atacante que intercepte nuestra comunicación y nos robe nuestros datos personales, por ejemplo pueden usar sniffers o el ataque The man in the middle. Los métodos más comunes son:

Man in the middle (Arp spoofing)

El principio del ARP Spoofing es enviar mensajes ARP falsos a la Ethernet esto lo hace poniendo el gateway de tu dispositivo(víctima) apuntando a la MAC del atacante, así todo lo que envía tu dispositivo pasa primero por el dispositivo del atacante(half routing).
En el caso de que también se envenene (spoofing) al router para hacerle creer que la mac destino (víctima) de un paquete eres tú, es full routing.

Con arp spoofing se puede hacer:

- Sniffer http sin monitor mode: editar las peticiones http y enviarlas cambiadas, redirigir http, etc.
- Inyectar código maligno en los navegadores (inyección JavaScript).

Una de las mejores soluciones consiste en usar WiFi Protector, el cual protege, sobre todo, de full routing. Para poder hacer uso es necesario, como root, instalar KingRoot (ojo, se pierde la garantía).

Fake Wifi hotspot (Evil Twin)

Esta técnica es parecida al man in the middle, pero en este caso particular nuestro dispositivo realmente actúa como el router. Por tanto los problemas son los mismos que en man in the middle, solo que sin ser necesario el arp spoofing.

Las soluciones a esta técnica consiste en desactivar WiFi cuando no lo usemos (porque si no intentará conectarse a los WiFis abiertos automáticamente) y, si dudamos si es el hotspot correcto, podemos consultar el siguiente *enlace*.

Acceso remoto a nuestro dispositivo (ssh y demás protocolos, troyanos, etc)

Con el acceso remoto a nuestro dispositivo nos podrían robar cualquier tipo de información, desde nuestro material audiovisual, como nuestras cuentas o secuestrarnos la sesión guardada (cookies).

Las soluciones que recomendamos son el uso de Firewall, antivirus y la navegación en modo incógnito.

Sniffer paquetes

Los sniffers son unas herramientas muy utilizadas hoy en día para analizar y capturar los paquetes que circulan por nuestra red. Este tipo de programa es utilizado tanto por técnicos de redes como por posibles atacantes.

En el apartado técnico vemos que la tarjeta wifi soporta el monitor mode, por lo que no hace falta el arp spoofing para ver toda la información que transcurre por nuestra red, por lo que podrían ver desde nuestra contraseña hasta las imágenes o datos que circulen por la red.

Las soluciones más utilizadas para estos casos es el uso del protocolo https y los certificados de seguridad, que podemos verlos dándole arriba a la izquierda en el navegador, al lado de la url se puede ver

Suplantación de identidad, robo de cuentas y encriptación USB

Por Mario Michiels Toquero y Pedro Sánchez Ramírez

La suplantación de identidad en internet es cada vez más frecuente, esto se debe a varios factores, como el aumento del uso de redes sociales que ofrecen información variada, al igual que el aumento de técnicas para realizar dicha suplantación. A esto hemos de añadirle la gran desinformación general del usuario sobre internet y las nuevas tecnologías.

Pero… ¿Qué datos relevantes nos pueden robar?

Pues prácticamente toda información que utilicemos en internet, desde nuestras fotos, mensajes, datos personales, nuestras cuentas o incluso el secuestro de nuestras sesiones guardadas (cookies).

Los métodos más comunes para la suplantación de identidad:

- Correos falsos: esta técnica permite pasar a un atacante por una organización, banco o empresa.
- Personal: cualquier persona maliciosa podría obtener información que escuchó o vio de parte suya que le garantiza acceso a algún recurso valioso.
- Ataque organizado: cualquier atacante podría intentar superar la seguridad de un banco, empresa u organización para obtener información personal de los clientes para luego acceder a algún recurso de esa empresa.
- Ataque a servidores de almacenamiento de información online: el atacante puede tratar de obtener datos de un servidor de almacenamiento de datos en la nube; obteniendo contraseñas, DNI, cuentas bancarias, etc.

Una técnica bastante utilizada es la de MAC Spoofer, en la que los suplantadores de identidad intentan sustituir nuestra MAC por la suya, y sabiendo que la MAC es nuestro identificador único dentro de una LAN, cualquier acto cometido por el suplantador quedaría como si lo estuviéramos realizando nosotros mismos.

Consejos para un uso más seguro de internet:

En primer lugar siempre tener un Firewall o antivirus instalado en nuestro dispositivo, ya que estos monitorizan que ningún intruso acceda a nuestro dispositivo o lo infecte con malware. Pero este nivel de seguridad es insuficiente ya que hay muchas formas de poner en riesgo nuestra seguridad.

Dependiendo de la situación en la que nos encontremos deberemos tomar diferentes precauciones, por ejemplo si nos encontramos conectados a una wifi pública no debemos utilizar información relevante, como contraseñas, etc. Pero sin duda la mejor práctica para esta situación es el uso de la tecnología VPN, de la cual hablaremos más tarde.

Si en cambio la situación se diera en nuestra propia wifi lo más recomendable es hacer un filtrado de la red para evitar que alguien desconocido se conecte sin nuestro permiso.
El robo de cuentas es otro de los grandes problemas de seguridad de nuestro tiempo ya que al igual que la suplantación esté se ha vuelto muy frecuente.

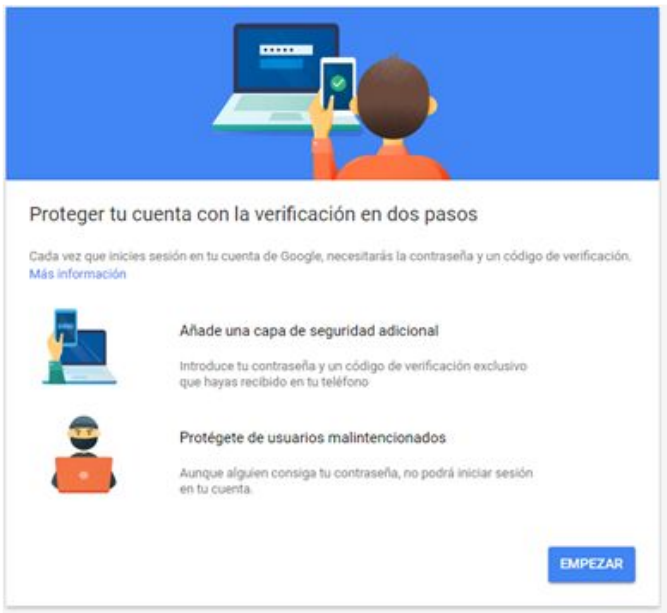
Los métodos más comunes para el robo de cuenta:

- La fuerza bruta: El ataque de fuerza bruta consiste en intentar descifrar una contraseña mediante la repetición, es decir, a base de ensayo y error.
- Diccionario del hacking: Este método también se podría considerar un ataque de fuerza bruta pero, en este caso, un software se encarga automáticamente de descifrar la contraseña.
- Ataque Spidering: es un bot que inspecciona automáticamente las páginas web.
- Phishing: en este caso se engaña al usuario para que rellene un formulario falso con sus credenciales de inicio de sesión.

Pero… ¿Qué podemos hacer para protegernos de este tipo de ataques que ponen en compromiso nuestra seguridad?, pues os damos varios consejos.

- Usar siempre el protocolo HTTPS que cifra nuestra información

- Activar la verificación de dos pasos: Al habilitar la **verificación** en **dos pasos** se añade una capa de seguridad adicional a la cuenta. De esta manera, inicias sesión con un dato que conoces (tu contraseña) y con un dato que tienes (un código que recibes en tu teléfono). Este tipo de verificación se puede usar para tu cuenta google, para whatsapp, etc.



VPN (Virtual Private Network)

Sustituye nuestra identidad (ip de nuestra casa) por la ip del servidor VPN. Se crea un canal encriptado: tu isp no ve la información, el server VPN sí lógicamente. Pero debería ser privada la información. Conflicto, qué prefieres, que tu isp pueda ver lo que haces vs que los dueños del server VPN puedan ver lo que haces.

Supuestamente algunos no recopilan logs(lo cual es muy dudoso más cuando aún te piden tus datos para sus servicios de pago)

¿Acciones legales de tu isp? ¿Acciones legales para obtener los datos al VPN?

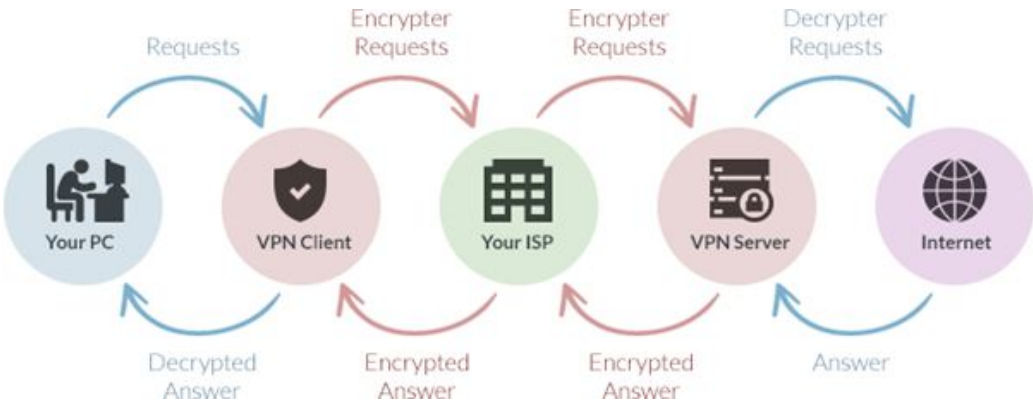
Son un tipo de red en el que se crea una extensión de una red privada, como la red local que tienes en casa, sobre una red pública como internet, permitiendo que los dispositivos conectados puedan enviar y recibir datos como si estuvieran conectados a una red local.

¿Cómo usarla?

En primer lugar necesitamos un cliente VPN el cual deberemos configurar para el acceso a nuestra VPN, indicando el servidor al que te quieres conectar, el tipo de encriptación de la VPN y la autenticación.
Sin embargo, existen muchos servicios en internet que te permiten descargar un cliente que te ahorra todos esos pasos de configuración. ¿Cuáles?

- *HotspotShield*
- *TunnelBear*
- *SpotFlux*

Cada una de estas tiene una versión gratuita y otra de pago, dependiendo de las necesidades de cada uno. También tenemos la un versión de software libre *OpenVPN* para configurar tu propia VPN.



Encriptación USB

Por Cristian Pinto Lozano

En muchas ocasiones, una memoria USB se transforma en una verdadera oficina portátil, con datos de vital importancia. Si se produce una pérdida del dispositivo, con el cifrado de datos reducimos el estrés de saber que nuestra información puede ser utilizada con fines perversos.

Es prácticamente imposible mantener el 100% de nuestra privacidad bajo control, pero sí hay algo que podemos hacer: cifrar o encriptar nuestros datos. No los ocultaremos a las miradas de los servicios de Internet que nos los exigen para ofrecer dichos servicios gratuitos, pero si bloquearemos a los espías no autorizados: malware, software espía, apps maliciosas, rastreos rutinarios gubernamentales, hackers, etc.

Si encriptas un dispositivo nadie podrá ver lo que contiene. Ten en cuenta que es un sistema de seguridad mucho más fuerte que una contraseña en la pantalla de inicio del móvil o el PC, que sólo protege el acceso, pero no los datos. Basta con extraer el disco duro de un PC y usarlo en otro ordenador para romper la contraseña de acceso de Windows, y hay herramientas para arrancar el móvil en modo root y acceder a su contenido. La encriptación evita esto porque cada fichero, cada dato, están encriptados.

Sin embargo, si pierdes la contraseña de encriptación o el disco duro se corrompe o falla, perderás el acceso a todos los datos. Además en dispositivos con poca potencia de proceso la encriptación ralentiza el acceso a los datos, pues deben ser encriptados y desencriptados en tiempo real.

Existen diversos programas de cifrado de datos que nos pueden ayudar a proteger la información confidencial que tenemos almacenada en nuestra memoria USB. Entre ellos , Mohos mini Drive es una aplicación de código abierto, gratuita, que funciona “on-the-fly” (sobre la marcha) y de contrastada seguridad.

Su funcionamiento básico consiste en crear un ‘volumen secreto virtual’ en un archivo, que una vez montado funciona como una partición más en el USB, con su propio sistema de archivo.

El montaje y acceso a esta partición virtual de tamaño personalizado requiere una contraseña establecida por el usuario, combinada con un keyfile como segunda contraseña, eligiendo cualquier archivo para ello haciendo casi imposible su acceso a desconocidos. Hay que tener en cuenta que, con independencia de lo fuerte que sea la encriptación de datos, el nivel de seguridad vendrá también dado por la contraseña elegida.

Casos Reales

Por Patricio Álvarez Castillo

A continuación podemos ver el historial de navegación completo de uno de los trabajadores. Historial que permite saber a cualquiera que acceda a ese equipo -su superior sin ir más lejos- qué páginas ha visitado.

Ver diapositiva 26.

Sesiones con cuentas de Google abiertas, las cuales permiten acceder a todos los servicios de Google (Drive, Gmail, Google+...).

Ver diapositiva 27.

Sesiones abiertas pertenecientes al correo interno de la empresa. Se observan correos con contenido jurídico importante y, por supuesto, comprometido.

Ver diapositiva 28.

Archivos almacenados en ordenadores después de ser descargados o transferidos. Pueden verse convenios, acuerdos, designaciones, cartas de oficio, interrogatorios… De nuevo, información altamente comprometida.

Ver diapositiva 31.

Podría pensar que una solución sería hacer hincapié en que las personas tomen consciencia de que realmente la privacidad de los datos importan y de que debemos llevar a cabo unos sencillos procedimiento para minimizar problemas que pudieran surgir. Pero a veces, ni siquiera es suficiente con advertir de las consecuencias que conlleva…

Ver diapositiva 39.

Ver diapositiva 36.

Información referente a los delitos informáticos en España

Por Jonathan Carrero Aranda

En la Ley-Orgánica 10/1995 del 23 de noviembre (BOE número 281) viene la base de toda la información referente a los delitos informáticos. Esta Ley fue modificada por la Ley-Orgánica 1/2015 el día 30 de marzo. Si bien es cierto que la ley del año 2015 introdujo algunos cambios importantes, la mayoría proviene de la ley del año 1995.

Dentro de estas leyes, los distintos escenarios se clasifican a través de *Artículos*. Voy a mezclar las dos leyes: dejaré los artículos del año 1995 que no hayan sido modificados y también pondré los que sí fueron modificados en el año 2015.

Ley-Orgánica 10/1995

Artículo 197

1. El que para vulnerar la intimidad de otro se apodere de sus papeles, correos, cartas o cualesquiera otros documentos o intercepte sus comunicaciones de cualquier tipo, será castigado con penas de prisión de uno a cuatro años.
2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere o modifique, en perjuicio de tercero, datos de carácter personal.
3. Se impondrá pena de prisión de dos a cinco años si se revelan, difunden o ceden a terceros la información de los puntos anteriores.
4. Si los hechos descritos en el apartado 1 y 2 de este artículo lo realizan las personas encargadas o responsables de la información, la pena impuesta será de tres a cinco años.
5. Igualmente, si la información anterior afecta a datos de carácter personal, ideología, religión, salud… Se impondrá las penas previstas en su mitad superior.
6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 197 bis

1. Todo aquel que se introduzca o a introducirse en un sistema de información sin consentimiento del dueño del mismo, será castigado o penado. Pena de 6 meses a 2 años.
2. Todo aquel que intercepte transmisiones de datos no públicos que provienen de un sistema de información. Pena de 3 meses a 2 años.

Artículo 198

La autoridad o funcionario que fuera de los casos permitidos por la Ley y sin causa legal realice cualquier conducta descrita en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199
El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años.

El profesional que, con incumplimiento de su obligación, divulgue secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años y la inhabilitación de la profesión por tiempo de dos a seis años.

Artículo 200
Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201
1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.
2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.
3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el número 4º del artículo 130, el cual cita “Por el indulto”.

Artículo 211
La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212
En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238
Son reos del delito de robo con fuerza los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:
- Escalamiento.
- Rompimiento de pared, puerta o ventana.
- Fractura de armarios o cualquier clase de mueble.
- Uso de llaves falsas.
- Inutilización de sistemas específicos de alarma.

Artículo 239
Se consideran llaves falsas:

- Las ganzúas u otros instrumentos análogos.
- Las llaves legítimas perdidas por el propietario u obtenidas por infracción penal.
- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentamente por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a trescientos euros, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

- Mecanismos instalados para realizar la defraudación.
- Alterando maliciosamente los aparatos contenedores.
- Empleados cualesquiera otros medios clandestinos.

Artículo 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a trescientos euros, será castigado con la pena de multa de tres a doce meses.

Artículo 263

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses si el daño excediere de trescientos euros.

Artículo 264

Será castigado con la pena de prisión de uno a tres años si concurriera alguno de los supuestos siguientes:

1. Impedir que se realicen el libre ejercicio de la autoridad o delito contra funcionarios públicos, bien contra particulares que hayan contribuido a la ejecución de las Leyes o disposiciones generales.
2. Que se cause por cualquier infección o contagio de ganado.
3. Que se empleen sustancias venenosas o corrosivas.
4. Que afecten a bienes de dominio o uso público.
5. Que se arruinen al perjudicado o se le coloque en grave situación económica.

La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 270

1. Será castigado con la pena de prisión de seis a dos años quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica sin el consentimiento de los titulares. La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones.
2. Será castigada también, con la misma pena, la puesta en circulación de cualquier medio técnico o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Artículo 278

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años.
2. Se impondrá la pena de prisión de tres a cinco años si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536

La autoridad o funcionario público que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior.

Ley-Orgánica 1/2015

Artículo 197 bis (se agrega al que ya había)

El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter (también se agrega)
Se castiga con una pena de prisión de seis meses a dos años la producción, adquisición, importación o entrega a terceros de datos de acceso (usuarios y contraseñas) o software desarrollado o adaptado básicamente para cometer cualquiera de los delitos antes citados.