cap cit

Consell Assessor del Parlament sobre Ciència i Tecnologia

Informe de ciberseguridad y privacidad para el Parlament de Catalunya

Resumen ejecutivo

Este documento responde a una petición del Consejo Asesor del Parlament sobre Ciencia y Tecnología (CAPCIT) con el objetivo de realizar un informe sobre ciberseguridad y privacidad para el Parlament de Catalunya. Este informe no pretende dar información exhaustiva ni rigurosa bajo un punto de vista analítico de los diferentes tipos de ataques y mecanismos para protegernos, sino que intenta ofrecer una visión general que no requiera una formación específica en el ámbito de las ingenierías de las TIC.

El documento se estructura en dos grandes bloques: el primero correspondiente a la ciberseguridad y el segundo dirigido a la privacidad. Posteriormente, se añade una guía de buenas prácticas y unas conclusiones.

Respecto al bloque de ciberseguridad, se realiza una clasificación de los tipos de ataques más comunes (ingeniería social, vulnerabilidades en las aplicaciones, APT, *software* de secuestro), indicando las características, el impacto y los mecanismos para poder mitigar estos ataques. También se ha añadido a petición del solicitante información sobre el ataque Pegasus.

Respecto al bloque de privacidad, en primer lugar, se ha establecido una clasificación de los datos en función de su sensibilidad y se han introducido de forma sencilla las tecnologías que se utilizan para proteger la privacidad. Posteriormente, se ha indicado cuáles de estas tecnologías deben utilizarse en las diferentes etapas del ciclo de vida de la información. Por último, se indica cuáles son las leyes que permiten regular la privacidad en nuestro entorno.

Introducción

La ciberseguridad consiste en la protección de sistemas, redes y datos digitales contra ataques informáticos. Se trata de una disciplina crítica e indispensable que protege nuestros datos, nuestra privacidad y nuestra sociedad en su conjunto. Los ataques a la ciberseguridad pueden ser realizados por una amplia gama de actores, incluidos *hackers* éticos, ciberdelincuentes, grupos de *hackers* estatales y otros. Así pues, la ciberseguridad se convierte en una necesidad vital para empresas, gobiernos e individuos.

La sociedad actual depende cada vez más de las TIC y esto obliga a poner más foco en la resiliencia. Mientras que la ciberseguridad tradicional se focaliza en proteger la información, la ciberresiliencia, entendida como la habilidad para prepararse, responder y recuperarse de un ciberataque, será básica para limitar el impacto de los ciberataques y garantizar la continuidad de los servicios esenciales.

La ciberseguridad es una responsabilidad compartida: tanto los individuos como las organizaciones deben tomar medidas para protegerse de los ataques informáticos. El gasto mundial en ciberseguridad durante 2022 ha sido superior a 260.000 millones de euros y se espe-

ra que tenga un crecimiento del 15% anual hasta 2025. El aumento de los presupuestos en ciberseguridad se debe a la relevancia que este ámbito está alcanzando en el desarrollo de la sociedad digital.

Un ciberataque es una acción o serie de acciones realizadas por un atacante con el objetivo de comprometer o dañar un sistema informático, una red, un dispositivo o los datos que se almacenan en él. Existen varios tipos de clasificaciones de ciberataques en función de su objetivo, metodología o impacto. Según el objetivo, estos ataques pueden tener diferentes finalidades, como el acceso no autorizado, el robo de información, el sabotaje o la destrucción de datos, la denegación de servicio, entre otros. Desgraciadamente, ningún sistema es inmune a los ataques. Cualquier entidad que gestione, transmita, almacene o manipule datos de alguna otra forma debe instituir y aplicar mecanismos para monitorizar su entorno informático, identificar vulnerabilidades y tapar los agujeros de seguridad tan pronto como sea posible. Pero no solo las instituciones deben tomar medidas para velar por la ciberseguridad; a nivel individual también pueden realizarse una serie de acciones para proteger los datos y dispositivos, como pueden ser utilizar contraseñas fuertes y únicas, mantener el *software* actualizado, evitar hacer clic en enlaces o abrir archivos de fuentes desconocidas, utilizar un programa antivirus de confianza y ser consciente de los riesgos de la ciberseguridad.

Una disciplina complementaria a la ciberseguridad e íntimamente ligada es la privacidad. La privacidad es el derecho de una persona a controlar la información sobre sí misma. Este derecho incluye el derecho a decidir quién tiene acceso a la información personal, cómo se utiliza y si debe compartirse. La privacidad es un derecho fundamental que protege la libertad, la seguridad y la dignidad de las personas en un mundo cada vez más digital y conectado. Mantener el equilibrio entre la utilización de datos para fines legítimos y la protección de la privacidad es un reto importante para la sociedad actual.

La privacidad es importante por una serie de razones. En primer lugar, permite a los individuos proteger su intimidad. En segundo lugar, promueve la libertad de expresión. En tercer lugar, protege los derechos humanos básicos, como el derecho a la libertad de opinión y el derecho a la protección contra la discriminación. La privacidad puede verse amenazada por la recogida y compartición de datos entre entidades, la venta de datos personales a terceros y los ataques informáticos que pueden robar datos personales.

Existen una serie de leyes y regulaciones de privacidad que protegen los derechos de privacidad de las personas, que establecen requisitos para las entidades sobre cómo pueden recopilar, utilizar y compartir datos personales.

Tipos de ataques más comunes

En la actualidad la variedad de los ataques existentes es muy diversa, y cada vez, más compleja, ya que, a medida que los sistemas de protección van mejorando, los atacantes se van profesionalizando y dedican ingentes cantidades de tiempo a formarse y aprovechar el mínimo error para poder realizar sus actos cibercriminales. Muchos de estos atacantes se han profesionalizado hasta el punto de crear estructuras y sistemas de gestión propias de regímenes militares o empresariales.[1] Así pues, nos encontramos ante una nueva era, donde el cibercrimen organizado debe tomarse muy en serio.

A pesar de este avance que ha sufrido el cibercrimen, cabe remarcar que generalmente pueden observarse patrones repetibles en los ataques, por lo que en la práctica de la gran diversidad existente se acaban observando ataques relativamente similares.

Así, todavía hoy en día los tipos de ataques más usados están basados en ingeniería social y en errores de seguridad en las aplicaciones utilizadas. Por eso este capítulo se centra en la descripción de los ataques por ingeniería social, para continuar con una detallada explicación de los ataques causados por vulnerabilidades del *software*, pasando después la discusión sobre dos derivadas de estos ataques más básicos, los ataques con *software* de secuestro (*ransomware*) y Pegasus, que no dejan de ser una combinación de los anteriores.

Ingeniería social

Aunque en una primera instancia podría pensarse que la ingeniería social no es un ataque, en realidad los efectos que puede conseguir hace que deba replantearse esta premisa. Con ingeniería social se logra violar uno de los primeros pilares de la ciberseguridad, la privacidad, y esto se logra a través de uno de los puntos más importantes cuando se habla de entornos ciberseguros, la recogida de información de la víctima.

¿Qué es la ingeniería social? Es el ataque por el que se engaña a la víctima a través de trucos psicológicos para, a través de una falsa sensación de urgencia, revelar información sensible o forzar a la víctima a compensar económicamente al atacante.

La ingeniería social es considerada uno de los vectores de ataque más comunes actualmente. Tanto es así que la ingeniería social se considera el ataque más utilizado durante el 2022, especialmente con una de las formas

1. https://www.kelacyber.com/wp-content/uploads/2022/03/KELA-Intelligence-Report-ContiLeaks-1.pdf

más comunes, el *phishing*, que se estima que causa el 33% del total de ataques realizados. Cabe mencionar que la ingeniería social raramente es el fin de un ataque, más bien es el medio, para posteriormente poder obtener un rédito de esta información obtenida.

Por lo general un atacante buscará información personal de alguien para:

- **Impersonar** a la víctima para lucrarse económicamente o bien para poder utilizarla como palanca para conseguir más información de otro.
- Conseguir que la víctima realice alguna **acción**, como efectuar una transferencia bancaria u otorgar permiso para permitir que el atacante pueda realizar alguna operación, generalmente económica.

Características e impacto

Existen muchos tipos y variantes de ingeniería social dependiendo del mecanismo utilizado para ganarse la confianza de la víctima y así conseguir realizar el ataque. Los mecanismos más típicos son:

- ***Phishing***: donde el atacante envía un mensaje haciéndose pasar por algún conocido. El conocido puede ser alguien de nuestra agenda de contactos, pero puede ser también algún proveedor de servicios. En esta categoría son conocidos[2] los mensajes haciéndose pasar por una entidad bancaria, alguna empresa de entrega de mercancías o una oficina de correos. Existen varios tipos de *phishing* y cada vez son más evolucionados. El más peligroso es el *spear phishing*, donde el atacante previamente hace un análisis exhaustivo de la víctima o su organización, y crea entonces un mensaje personalizado, incluso suplantando a alguien conocido de la víctima, que es mucho más creíble que un correo genérico de alguna entidad externa. Tenemos ejemplos conocidos de este tipo de ataques como el que sufrió el Ayuntamiento de Barcelona, donde, a través de la impersonación de un proveedor, se logró cambiar el número de cuenta de sus pagos por uno controlado por un atacante, consiguiendo desviar sobre unos 350.000 euros.
- ***Whaling***: es una variante del *phishing* muy común donde el objetivo son los directivos de empresas o jefes políticos. En este caso, el atacante, a través del correo electrónico, se hace pasar por otro ejecutivo o político de alto rango de otra entidad. El mensaje generalmente contiene alguna emergencia falsa o una gran oportunidad que va a durar poco tiempo y que requiere una acción rápida de la víctima. Generalmente el objetivo es conseguir información sensible.
- ***Honey trap***: esta variante típicamente utiliza redes sociales conocidas, como Instagram, WhatsApp o Telegram. El objetivo es enviar un mensaje impersonando a alguien que quiere mantener una relación sentimental y, una vez ganada la confianza, pedir algún tipo de ayuda inmediata para un problema inventado, pidiendo urgencia para no dar tiempo a pensar en la veracidad del mensaje.
- ***Baiting***: el objetivo en este caso es obtener información sensible de la víctima, por eso se busca que la víctima rellene algún cuestionario o documento con esta información o la redirige a una página de inicio de sesión de Google o Microsoft falsas para robarle sus credenciales.
- ***Pretexting***: el atacante crea un escenario ficticio, por ejemplo, pretendiendo ser del servicio técnico de alguna empresa y diciendo que, para poder arreglar un problema, también ficticio, la víctima debe proporcionar datos personales, como tarjetas de crédito o contraseñas, para poder continuar utilizando un servicio.

El impacto que tienen este tipo de ataques es difícilmente cuantificable, principalmente porque muchas de las víctimas, bien por vergüenza o por falta de información, no denuncian el acto. Sin embargo, como puede observarse en el informe del Internet Crime Complaint Center (IC_3), se calcula que durante 2022 se realizaron más de 300.000 ataques.

Aparte de esto, y como punto crítico de los ataques por ingeniería social, cabe mencionar que es uno de los vectores de ataque más habituales por grupos de ciberdelincuentes organizados para conseguir un acceso inicial dentro de un sistema. Una vez dentro, trata de expandirse a toda la red antes de realizar un ataque coordinado contra la víctima. Un ejemplo de esto lo tenemos en el ataque que sufrió la Universidad Autónoma de Barcelona, en el que los atacantes inicialmente utilizaron *phishing* para conseguir las credenciales de un empleado para posteriormente efectuar un ataque con *software* de secuestro (*ransomware*).

Cómo mitigar los ataques por ingeniería social

Existen varias formas de poder mitigar, o al menos minimizar, el impacto de este tipo de ataques, pero esto siempre implica dos pilares fundamentales: por un lado, es necesario disponer de las herramientas tecnológicas necesarias, generalmente aplicativos de monitorización de la seguridad de nuestros sistemas, pero también, e igualmente importante, concienciando a los empleados y usuarios de nuestros sistemas sobre cómo actuar y cómo detectar este tipo de fraude. Esta concienciación generalmente pasa por proporcionar a los empleados cursos de ciberseguridad con casos prácticos para poder observar de primera mano el funcionamiento de este tipo de ataques.

2. Campañas de suplantación de entidades bancarias con falsos cargos y bloqueo de cuentas

Esta concienciación generalmente pasa por la verificación de una lista de puntos a considerar antes de publicar cualquier tipo de información en la red. Los más importantes son:

- **Determinar** si el correo recibido es del interlocutor que dice ser. Por eso se recomienda observar con detalle el dominio desde el cual se ha enviado el correo. Esto es, desde la «@» del correo hasta el final: allí hay que ver exactamente el dominio esperado, sin ningún error ni letra diferente a lo que debería (no es lo mismo user@microsoft.com que user@micosoft.com).
- **Sospechar** de cualquier interlocución, especialmente si no se conoce al emisor del mensaje.
- **Evitar** descargar adjuntos de los correos cuando vengan de fuentes desconocidas y contengan aplicaciones. Para saber si un adjunto es una aplicación, es necesario ver el tipo de archivo. Las aplicaciones son: archivos EXE, MSI e incluso VBA.
- **Asegurarse** de la corrección de los enlaces de los correos. Esto debe observarse pasando el ratón por encima del enlace y ver cuál es el dominio al que llevará el enlace: debe inspeccionarse que el dominio apunte hacia donde toca. Para ello es necesario observar todo el contenido de la URL, especialmente desde «https://» hasta la primera «/» del nombre; así, el dominio de la URL https://www.gencat.cat.in/noticies/2023-07-22/ no apunta a la web de la Generalitat. Por eso se recomienda que, en vez de clicar en los enlaces, se acceda a la página web tecleando directamente en el navegador la página que desea visitarse.
- **Verificar** la identidad del interlocutor a través de métodos alternativos, tales como con una llamada telefónica o validando la libreta de direcciones.

Para poder hacerse una idea de la concienciación de los empleados o usuarios de las TIC conviene de vez en cuando realizar campañas de ataques de *phishing* controlados para permitir que los empleados aprendan a detectarlos y a actuar en consecuencia, sobre todo creando un clima en el que pueda reportarse libremente si algún ataque de estas características se ha producido, sin represalias para la posible víctima, que puede esconder el hecho por vergüenza o por miedo a consecuencias disciplinarias.

Ataques causados por vulnerabilidades en las aplicaciones

Teniendo en cuenta la gran cantidad de dispositivos que actualmente están conectados a Internet, la gran cantidad de *software* que poseen y la enorme cantidad de usuarios, es normal que este *software* pueda contener errores. Estos errores pueden ser funcionales, en los que la aplicación no actúa como se espera, pero otros pueden ser sencillamente errores de programación o configuración que no son perceptibles por los usuarios, pero que pueden ser aprovechados por un atacante malicioso para forzar que la aplicación se comporte de forma no esperada, causando así una potencial exfiltración de información o permitiendo al atacante tomar control de los recursos afectados.

Este segundo grupo de errores se conocen como vulnerabilidades y son una enorme fuente de ataques, especialmente con aplicaciones no actualizadas o aplicaciones no validadas que pueden contener muchos de estos errores.

Características

Si bien los ataques por ingeniería social implican una acción por parte de uno o más usuarios, las vulnerabilidades de aplicaciones, por el contrario, se manifiestan a través de fallos de una aplicación que permiten al atacante realizar acciones maliciosas en el equipo de la víctima, sea un móvil, un ordenador de escritorio o el servidor hospedado en un centro de datos. Esto implica que muchas veces este tipo de ataques no requieren ninguna acción por parte de la víctima. Solo hace falta un atacante con suficientes conocimientos técnicos y un equipo vulnerable conectado a la red.

Procedencia de los ataques

Generalmente estos ataques vienen a través de dos vías: a través de ataques automáticos o bien a través de ataques dirigidos.

Ataques automáticos

Un ataque automático hace referencia a aquellos ataques en los que el atacante, en vez de buscar activamente a una víctima para atacarla, pone un sistema automático que busca errores conocidos en el *software* de todas las máquinas conectadas a Internet. Este ataque sistemático trata de identificar estas vulnerabilidades y, una vez encontradas, avisa al atacante indicando la lista de equipos vulnerables que se han encontrado. Una vez hecho esto, el atacante aprovecha esta vulnerabilidad para tomar control del equipo que tiene el *software* vulnerable.

Como puede observarse, este tipo de ataques no van dirigidos a alguien en particular, sino que van dirigidos a usuarios con aplicaciones vulnerables independientemente de quiénes son y qué hacen.

Ataques dirigidos

Otro tipo muy importante de ataques que aprovechan errores del *software* es cuando un atacante se fija en una víctima y, una vez decidido a atacarla, se realiza un análisis personalizado en el que se estudian todos sus

recursos públicos. Una vez identificados todos, se ve lo que se conoce como *superficie de ataque*, que hace referencia al conjunto de recursos atacables de un individuo o empresa. Una vez identificada esta superficie de ataque, se realiza un estudio de qué sistema se utiliza y se intenta de forma personalizada atacar cada uno de estos recursos. En este punto se pone a prueba la seguridad y la configuración de toda la infraestructura que la víctima tiene en el sistema.

Objetivos aprovechando vulnerabilidades en las aplicaciones

Si bien existen muchas posibles clasificaciones de formas de aprovecharse de vulnerabilidades, una de las más relevantes es la que considera la víctima del ataque, que principalmente puede ser un usuario final o bien el propio servicio ofrecido por una empresa.

Ataques contra los usuarios

Generalmente, este tipo de ataques se benefician de acciones incorrectas realizadas por usuarios aprovechando problemas en la aplicación que utilizan. En esta categoría pueden encontrarse, por ejemplo, problemas en el navegador o problemas en aplicaciones empresariales, como Microsoft Office u otros.

Aquí el objetivo es hacer que el usuario realice alguna acción que hace que la aplicación en cuestión se comporte de forma incorrecta.

Un ejemplo clásico es cuando la víctima abre un adjunto que ha recibido de un correo electrónico. Este adjunto contiene un documento Word con un contenido forjado por un atacante que hace que la aplicación se comporte de forma inadecuada, por ejemplo, abriendo una conexión hacia el exterior que permite al atacante tomar el control de la máquina de la víctima. Esto se conoce como ataque de tipo *backdoor*.

Otro caso clásico es cuando un atacante malicioso consigue que la víctima abra un enlace con el navegador, que está forjado de forma que permite robar las galletas del navegador, lo que, en la práctica, significa que el atacante tendrá acceso a todos los recursos *online* a los que la víctima accede desde ese navegador.

Como puede observarse, este tipo de ataques, al contrario de lo que se ha observado en los ataques automáticos, requiere acciones concretas por parte de los usuarios.

Para hacernos una idea, desde la creación del navegador Google Chrome en 2009, se le han encontrado un total de **3.243 vulnerabilidades**,[3] de las cuales, en los primeros ocho meses de 2023, ha habido un total de **31**. Esto no quiere decir que este navegador esté mal implementado, lo que significa es que es uno de los más usados y, por tanto, hay mucho interés en encontrarle errores que permitan a los atacantes tener éxito en sus ataques.

Ataques contra los servicios

En el caso de ataques realizados contra servicios, el objetivo generalmente es conseguir los datos que hay detrás del servicio en particular, pero la gran diferencia con los ataques contra usuarios es que en este caso la víctima no debe realizar ninguna acción. Lo que procura el atacante en estos casos es enviar datos inválidos al servicio o analizar su funcionamiento buscando alguna mala configuración que le permita acceder al sistema.

El envío de datos inválidos suele provocar un mal funcionamiento de la aplicación, que en según qué casos puede proporcionar acceso total al atacante. Este tipo de vulnerabilidades tienen el mismo impacto que las de los ataques contra usuarios, en el sentido de que son errores de programación que podrían arreglarse. De nuevo, cuanto más conocida y usada es una aplicación, más errores se encuentran y mayor impacto potencial tienen contra nuestros sistemas.

Tenemos ejemplos de este tipo de ataques con gestores de contenido (conocidos como *Content Management Systems – CMS*), que son aplicaciones que permiten la introducción de forma muy sencilla en páginas web para gestionar su contenido por usuarios no expertos. Estos sistemas siempre han sido el foco de ataques, ya que están presentes en casi todas partes. Uno de los más famosos es WordPress, del que, desde su creación en 2003, se han reportado un total de **6.830 diferentes vulnerabilidades**, algunas de las cuales han tenido impacto mediático, como el caso de los Papeles de Panamá,[4] que en 2016 llevaron a lo que se conoce como la mayor filtración periodística de la historia.

Sin embargo, cabe mencionar que, al igual que con los ataques contra aplicaciones de usuarios, las empresas detrás de estas aplicaciones, generalmente, tienen equipos de desarrolladores grandes, dedicados exclusivamente a resolver estos errores en el menor tiempo posible.

En cuanto a los errores en la configuración del sistema, típicamente hay sistemas con contraseñas por defecto o muy fáciles de adivinar, páginas de administración accesibles por todos o servicios innecesarios con acceso abierto para posibles atacantes.

3. https://www.opencve.io/cve?product=chrome&vendor=google
4. https://www.xataka.com/seguridad/un-plugin-de-wordpress-y-un-drupal-antiguo-causantes-de-la-filtracion-de-los-papeles-de-panama

Tipo de vulnerabilidades por antigüedad

La última clasificación que se mostrará en este documento es la clasificación de las vulnerabilidades en función de la antigüedad. Esto es especialmente importante, ya que, en la práctica, para poder resolver un problema, hay que conocer su existencia. Por eso, distinguimos dos tipos: las vulnerabilidades conocidas –o «antiguas»– y los ataques de día cero (*0-day*), que son las vulnerabilidades que todavía no están reportadas y que, por tanto, todavía no son conocidas por los desarrolladores.

Vulnerabilidades conocidas

Hay equipos de empresas grandes y conocidas y otros expertos *freelance* que dedican su tiempo a buscar vulnerabilidades. Cuando se encuentra una, esta es reportada a los desarrolladores y se les da un tiempo antes de hacerla pública. Este procedimiento sirve, por un lado, para obligar a los desarrolladores a resolver los problemas y, por otro, darles tiempo suficiente para que nadie que no conozca la vulnerabilidad pueda aprovecharse mientras se resuelve. En cualquier caso, resolver la vulnerabilidad no es suficiente; falta que los administradores de las aplicaciones las actualicen a la versión segura lo antes posible.

La base de datos de vulnerabilidades conocidas se llama Common Vulnerabilities and Exposures (CVE)[5] y es una lista realizada por Mitre y financiada por el gobierno de Estados Unidos. Actualmente, tiene un total de **211.265** entradas de todas las aplicaciones existentes desde la creación de la base de datos, en septiembre de 1999.

0-day

Si las vulnerabilidades conocidas y registradas pueden traernos muchos problemas, con los ataques de día cero (*0-day*) el problema es aún mucho mayor, ya que, como ya se ha dicho, los ataques de día cero son vulnerabilidades recientemente descubiertas, bien por expertos reconocidos o atacantes maliciosos.

Cuando quien descubre la vulnerabilidad es un atacante malicioso, este puede aprovechar el error encontrado durante mucho más tiempo, ya que la víctima y los desarrolladores de las aplicaciones no son conocedores del mismo. Así, son un tipo de vulnerabilidades extremadamente delicadas. Durante la historia ha habido ataques de día cero famosos, pero el más conocido recientemente, como se verá más adelante en este documento, es la aplicación Pegasus, que se aprovecha de errores en el sistema de mensajería de IOS en el iPhone para descargar la aplicación de forma totalmente transparente al usuario del dispositivo móvil.

Impacto

Junto a los ataques por ingeniería social, los ataques que aprovechan vulnerabilidades de *software* son los más habituales actualmente. Hay numerosos estudios que tratan de cuantificar el impacto de este tipo de ataques, pero todos coinciden en que el impacto económico y de prestigio en la víctima de estos ataques es enorme.

En 2023,[6] según IBM, el coste medio en Estados Unidos de un ataque se cuantifica en **4,45 millones** de dólares, lo que supone un incremento del 2,3% respecto al 2022.

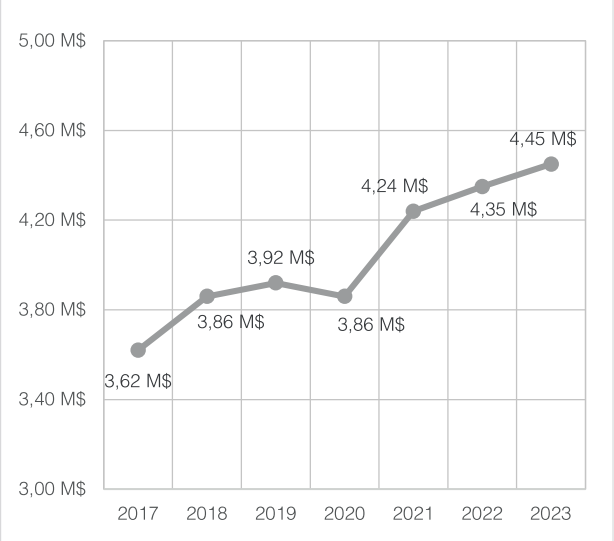

Figura 1: Evolución del coste (millones de dólares)[5]

Por otro lado, el mismo informe pone de manifiesto que de media las empresas tardan **182 días** a ser conscientes de que se ha realizado un ataque de forma exitosa, y casi **60** a solucionar el problema. Esto pone de manifiesto la gran necesidad de tener un buen equipo de ciberseguridad en la empresa, así como conocimiento de las herramientas necesarias para poder mitigar este tipo de ataques y solucionarlos.

Un punto importante a tener en cuenta es que este impacto económico considera, entre otras cosas, el impacto en la reputación de la empresa, que, por lo general, se ve muy afectada con la pérdida de clientes y con la publicidad negativa que supone; pero también considera el coste que supone el filtrado o la destrucción de información que puede realizar el atacante. Más adelante, se verán los ataques con *software* de secuestro (*ransomware*), que en muchos casos se benefician de vulnerabilidades en las aplicaciones para ganar acceso a la información de la víctima.

5. https://cve.mitre.org/cve/
6. Informe sobre el coste de la vulneración de datos 2023

Cómo mitigar los ataques por vulnerabilidades del *software*

Cabe mencionar que la mitigación de este tipo de ataques puede impactar a varios niveles. Básicamente pueden verse desde dos puntos de vista, el del desarrollador de la aplicación o el del usuario (bien sea un administrador de sistemas o un usuario final).

Como desarrollador

Detallar las buenas prácticas de desarrollo excede del objetivo de este documento, pero es importante, cuando se utiliza una aplicación, que el usuario tenga en cuenta el histórico de la empresa que la proporciona. Así, hay que mirar si la empresa va mejorando la herramienta y saca nuevas versiones de forma regular, así como cuántas vulnerabilidades críticas se han encontrado en la herramienta y el tiempo que se tarda en resolverlas.

Como usuario final

Estrictamente como usuario final, tanto si es un administrador de un servicio como si es un usuario final sin conocimientos técnicos, la lógica es bastante similar. Como puede verse en informes sobre estadísticas de vulnerabilidades,[7] la inmensa mayoría de ataques (75%) se realizan con vulnerabilidades reportadas desde hace más de seis años, y en casi todos los casos la solución sería tan sencilla como actualizar la aplicación a una versión estable. Esto lleva a la gran buena práctica en este aspecto: un buen usuario debería monitorizar el estado de las herramientas que utiliza y actualizarlas cuando sea necesario. Debido a que esto no es sencillo *a priori*, la mejor forma de hacerlo es a través de herramientas que proporciona el propio sistema operativo, generalmente en la forma de aviso para actualizar o bien el sistema o alguna herramienta que se tiene instalada, y, en la medida que sea posible, tener el sistema al día.

Amenazas persistentes avanzadas

Antes de continuar con otros ataques, esta sección se dedica a ver cómo el crimen organizado está, cada vez más, perpetrando cibercrímenes que cada vez impactan más en la vida de las personas. En particular esta sección se dedica a abordar las amenazas persistentes avanzadas (*Advanced Persistent Threats*, APT).

¿Qué son las APT?

Las APT son grupos organizados de cibercriminales, a menudo autónomos con complejas estructuras empresariales, muchas veces financiados por gobiernos y con objetivos muy diversos, pero generalmente con motivaciones económicas o políticas para llevar la guerra a nivel cibernético.

Las acciones que generalmente realizan estos grupos son, por lo general, robar, espiar o sencillamente perturbar un servicio, equipo o empresa.

Generalmente, en estos ataques realizados por este tipo de grupos, la víctima es cuidadosamente seleccionada, estudiada, y solo cuando se tiene suficiente información se pasa a la ofensiva. Es importante remarcar que un ataque realizado por una APT no es un ataque rápido. Estos tipos de amenazas pueden durar días, semanas o incluso meses, en los que el atacante primero estudia a la víctima. Una vez encontradas posibles vulnerabilidades, se traza un plan de ataque tipo *Land and Expand,* donde primero se trata de tomar control de forma sigilosa de una parte de la infraestructura, para poco a poco ir expandiéndose, hasta que se considera que se ha podido tomar control de todos los recursos de la víctima y se realiza un ataque coordinado. En este punto, dependiendo del objetivo del ataque, pueden ocurrir varias cosas, pero normalmente, y como se verá posteriormente en los ataques con *software* de secuestro, se inhabilitan los servicios que ofrece la víctima y se cifran todos los datos y, si se puede, las copias de seguridad. Una vez llegados a este punto, se informa a la víctima del ataque y de los pasos que debe realizar para recuperar la información. Normalmente, la recuperación pasa por el pago mediante bitcoins u otras criptomonedas para evitar ser encontrados por las autoridades competentes.

Hay que remarcar que generalmente este tipo de grupos de ciberterroristas organizados, una vez pagado el rescate, y por un tema puramente de *marketing*, no vuelven a atacar a la víctima y, en según qué casos, incluso le dan ideas sobre cómo mejorar la seguridad de su sistema.[8] El objetivo es, principalmente, que las futuras víctimas no tengan dudas a la hora de pagar el rescate, dada la seriedad del atacante. Este punto de prestigio ha sido uno de los grandes cambios desde que existen este tipo de cibercriminales organizados.

Con estos grupos de cibercrimen organizado, lo que se ve es que según qué gobiernos los observan como una forma más de ataque contra sus enemigos, y los utilizan cuando es necesario para fines políticos y para tambalear la estabilidad de los países atacados.

Grupos de APT

Los grupos de APT son constantemente monitorizados por empresas y autoridades. Se han identificado más de 250, entre los cuales, en un momento dado, pue-

7. https://www.getastra.com/blog/security-audit/cyber-security-vulnerability-statistics/
8. Grupo de rescate

de haber unos 50 activos. Con el fin de identificarlos, normalmente se les asigna un nombre con la forma **APT[Número]**, donde, por ejemplo, APT1 corresponde a PLA Unit 61398,[9] un grupo cibercriminal chino. Aparte, cada grupo se conoce a sí mismo con algún tipo de seudónimo, por ejemplo Double Dragon[10] (también conocido como APT41), Winnti Group, Barium o Axiom.

Esta diversidad de nombres viene dada por la evolución de estos grupos, que van cambiando de integrantes o de *modus operandi* y se van bautizando a sí mismos utilizando diferentes nombres, a veces por *marketing*, a veces para despistar a las autoridades.

En cuanto a países, China es el lugar donde hay más grupos de APT, seguido de Rusia y los países del este, aunque también existen en Estados Unidos. Un punto importante es que, dada la buena financiación de estos grupos, hoy en día muchos de ellos tienen integrantes en todo el mundo, donde los contratan a través de la web oscura y les pagan con criptomonedas para evitar su seguimiento.

Software de secuestro (*ransomware*)

Los ataques con *software* de secuestro son, sin duda, uno de los tipos de ataques más mediáticos debido al gran incremento de ataques a empresas[11] e instituciones públicas[12, 13] que los han sufrido.

Pero en realidad el ataque con *software* de secuestro es solo la última etapa de un ataque que se ha realizado previamente para ganar acceso a un sistema. Esto generalmente se realiza a través de ingeniería social o bien a través de vulnerabilidades en las aplicaciones existentes en la entidad atacada.

Entonces, el *software* de secuestro es un ataque por el que, una vez el atacante ha ganado acceso a un sistema, cifra todos los datos importantes de la víctima utilizando una clave criptográfica muy robusta y reclama un rescate por los datos. En según qué casos, para forzar el pago del rescate, se amenaza con filtrar y publicar los datos en la web oscura o a través de otros métodos, como Telegram, con el objetivo de sacar rédito económico o político.

Hay que indicar que tanto la ingeniería social como las vulnerabilidades en las aplicaciones vistas anteriormente en muchos casos son tipos de ataques perpetrados por atacantes que normalmente no tienen ningún interés particular en el sitio o la persona atacados; en muchos casos ni siquiera saben de quién se trata y encuentran a la víctima utilizando mecanismos automáticos. En el caso del *software* de secuestro, en general, el ataque tiene un cariz diferente: generalmente se realiza con un objetivo muy claro, donde la víctima ha sido elegida a conciencia por una APT.

Características e impacto

La gran mayoría de ataques que terminan con *software* de secuestro suelen utilizar un vector de ataque bastante similar. En general, primero se investiga a la víctima, tanto desde el punto de vista técnico, mirando los recursos digitales accesibles desde el exterior, especialmente aquellos que tengan potenciales vulnerabilidades, como desde el punto de vista social, investigando e intentando, a través de ingeniería social, obtener credenciales que permitan al atacante iniciar el control de la infraestructura de la víctima.

Una vez que se ha llegado a controlar un recurso de la empresa, el siguiente paso generalmente se basa en tratar de expandir este control a otros recursos. Esto normalmente se realiza a través de sistemas de elevación de privilegios, o sea, el atacante se transforma en administrador y, cuando sea posible, de todo el dominio, y así ir expandiendo el control. Una vez se tiene control sobre gran parte de los sistemas, se realiza un ataque coordinado que generalmente está formado de dos partes: la primera es la exfiltración de datos hacia un equipo externo y la segunda es su posterior cifrado, si es posible incluso de las copias de seguridad para hacer más complicada la restauración de la información.

Una vez realizado el cifrado del sistema, se avisa a la víctima de la acción y se le da un enlace para hacer efectivo un pago que le dará acceso a los datos de nuevo y le restaurará el sistema en el estado original. Normalmente este mensaje contiene también la amenaza por la que, si no se paga el rescate, se publicarán los datos. Sin embargo, la desconfianza con el atacante hace que a menudo la víctima no quiera realizar el pago, lo que ha llevado a los atacantes, en muchos casos, a cambiar su modelo de negocio: ahora dosifican la información que se publica sobre la víctima maximizando así su beneficio. Esto es cada vez más habitual, ya que, en los últimos años, como se ve en la Figura 2, se ha ido reduciendo la cantidad de víctimas que pagan el rescate.

9. https://en.wikipedia.org/wiki/PLA_Unit_61398
10. https://content.fireeye.com/apt-41/rpt-apt41/
11. Ciber ataques a empresas catalanas
12. Ataque informático en la UAB
13. https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona

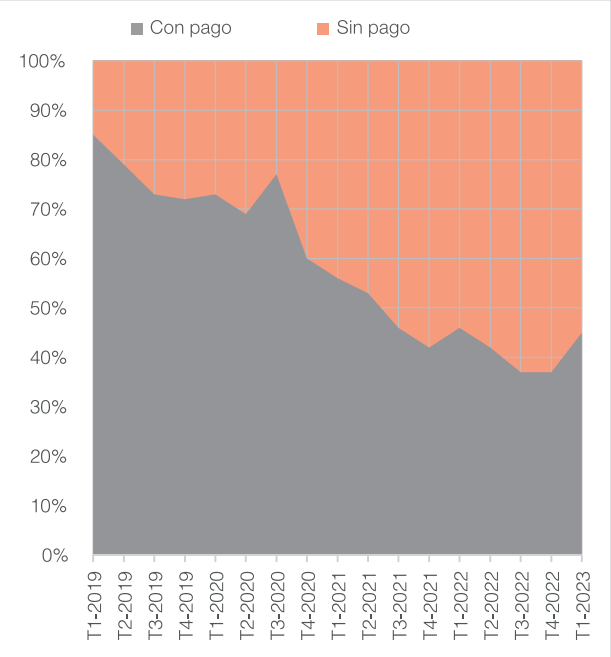

Figura 2: Evolución de los pagos a cibercriminales por rescate de la información [Fuente]

Hay que tener en cuenta que un ataque por *software* de secuestro tiene dos características importantes: por un lado, utiliza otros mecanismos vistos anteriormente para poder realizar el ataque y, por el otro, generalmente está perpetrado por grupos de ciberdelincuentes organizados.

Cómo mitigar los ataques con *software* de secuestro (*ransomware*)

Este tipo de ataques son de los más complicados de evitar, principalmente porque detrás está un equipo organizado con grandes conocimientos y muchas herramientas para poder identificar y explotar posibles fallos o vulnerabilidades del sistema.

Sin embargo, se recomienda tener en cuenta un conjunto de buenas prácticas que pueden minimizar la posibilidad de ser vulnerados:

- Realizar y validar copias de seguridad, dejando alguna siempre fuera de línea para evitar su cifrado
- Concienciar a los usuarios en el uso de los recursos digitales:
  - Tener una buena política de contraseñas
  - Ser observadores con los correos fraudulentos
  - Vigilar a quién se da acceso a los recursos

Impacto político de los ataques con *software* de secuestro (*ransomware*)

Inicialmente los ciberataques eran motivo de prestigio entre los actores maliciosos. Con la aparición del *software* de secuestro se vio rápidamente el cambio hacia un modelo de negocio en el que los ataques podían dar rédito económico rápidamente. Sin embargo, dada la alta especialización y conocimientos de las APT, se está viendo un cambio de motivación en los ataques, donde muchas veces la parte económica es secundaria comparada con la desestabilización que causa el ataque en sí, especialmente cuando el grupo de cibercriminales tiene financiación de gobiernos u otros tipos de ventajas, como por ejemplo protección contra la extradición, como es bien sabido que hace Rusia.[14]

Este cambio de paradigma conlleva que ahora las víctimas de los ataques por *software* de secuestro se busquen entre universidades, hospitales u otras infraestructuras críticas, con el objetivo de desestabilizar gobiernos o ayudar en temas militares, tal y como se observa con la invasión de Ucrania, donde puede verse cómo la cantidad de ciberataques después de la primera ofensiva se multiplicó por 2,5 contra Ucrania y por tres contra los países de la OTAN.[15]

Sin embargo, este cambio de paradigma debería hacer reflexionar a los gobiernos de forma que inviertan en formación de la ciudadanía para tratar de mitigar al máximo posible el impacto de este nuevo modelo de negocio.

Pegasus

Pegasus, si bien ha tenido un eco mediático muy importante desde hace un tiempo, no es un ataque informático *per se*. Sin embargo, como con la gran mayoría de herramientas, siempre puede hacerse un uso incorrecto del mismo. Este documento recoge una visión objetiva de la que proporciona Pegasus y qué características tiene y hasta dónde puede llegar, sin entrar en juicios de la legitimidad del uso que un actor pueda hacer del mismo.

Características

Pegasus es una herramienta que se conoce como de recogida de información (*information gathering*), creada por una empresa israelí llamada NSO Group, que se dedica a conseguir inteligencia de un dispositivo. En este sentido, Pegasus ha sido diseñado por unos expertos en ciberseguridad y se vende a los gobiernos para poder realizar espionaje de delincuentes y personas que potencialmente pueden poner en peligro la seguridad nacional. No es un sistema pensado para su uso con disidentes políticos que no tengan antecedentes penales.

14. Cómo el Kremlin proporciona un puerto seguro para el ransomware
15. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

Esto es así porque Pegasus se aprovecha de vulnerabilidades en sistemas operativos Android e IOS (iPhone), pero también soporta otros sistemas operativos como Blackberry o Symbian (Nokia). Entonces el objetivo final de Pegasus es, de forma personalizada para cada uno de los sistemas operativos y de las víctimas, estudiar el dispositivo y, de forma totalmente transparente para la víctima, instalarle un agente que permite exfiltrar, sin que la víctima se dé cuenta, los datos de su dispositivo. Así, Pegasus es capaz de enviar un gran abanico de información al atacante. Los datos más importantes son:

— Ubicación de la víctima: puede conocerse en todo momento su ubicación
— Todos los datos de aplicaciones: correos electrónicos, imágenes, mensajes de WhatsApp...
— Registro de llamadas
— Audio de las llamadas para poder ser reproducidas por el atacante

Si bien las acciones que realiza Pegasus son muy útiles para el atacante, cabe decir que el punto que lo hace único es la forma que tiene de infectar los dispositivos. Pegasus permite ser instalado prácticamente en cualquier dispositivo móvil de forma transparente y sigilosa y, aprovechando vulnerabilidades de cada uno de los dispositivos, tomar el control del sistema ejecutándose como administrador y, por tanto, permitiendo la adquisición de todos los datos relevantes del sistema.

Para evitar al máximo la detección, Pegasus aprovecha siempre que sea posible lo que se conoce como vulnerabilidades sin clic (*0-click*), que son aquellas vulnerabilidades que no requieren ninguna acción por parte de la víctima para ser infectada. El ejemplo más conocido es una vulnerabilidad existente en el sistema de mensajería MMS de iPhone que permite a Pegasus infectar este tipo de dispositivos. De hecho, vulnerabilidades de este tipo siguen siendo encontradas y explotadas actualmente.[16]

El hecho de que Pegasus prácticamente no deje rastro en los dispositivos lo hace extremadamente difícil de detectar por antivirus u otros sistemas; tanto es así que el propio sistema tiene un mecanismo para desinstalarse del dispositivo cuando el atacante lo decide o cuando está a punto de detectarse.

Cómo mitigar los ataques tipo Pegasus

Siendo realistas, no existe una forma fácil ni clara de mitigar este tipo de ataques tan sofisticados, principalmente porque quienes han creado estas herramientas son expertos en vulnerabilidades de *software* y tienen a su alcance una enorme cantidad de recursos que les permiten investigar y descubrir muchos ataques de día cero que terminan garantizando la infección de nuevos dispositivos.

El efecto colateral de esto es que otros grupos también son potencialmente descubridores de estos problemas de seguridad y pueden estar explotándolos sin el conocimiento de sus víctimas.

En cualquier caso, a fin de minimizar el éxito de ataques como Pegasus, se recomienda mantener los dispositivos móviles actualizados y, como siempre, dudar de todos los mensajes recibidos de orígenes desconocidos.

Otros tipos de ataques

Ataques DoS y DDoS

Un ataque de denegación de servicio (DoS) está diseñado para sobrecargar los recursos de un sistema hasta el punto de que sea incapaz de responder a las legítimas solicitudes de servicio. Un ataque de denegación de servicio distribuido (DDoS) es similar, ya que también busca agotar los recursos de un sistema, pero en este caso es ejecutado por una gran cantidad de ordenadores infectados con *malware* que están controlados por el atacante. Estos ataques se llaman *ataques de denegación de servicio* porque el servidor víctima no puede proporcionar servicio a aquellos que quieren acceder a ellos. Es decir, en los ataques de red DoS y DDoS, el objetivo es simplemente interrumpir la efectividad del servicio del servidor atacado, mediante un alud de solicitudes ilegítimas. Dado que el sitio debe responder a cada solicitud, sus recursos se agotan con todas las respuestas. Esto imposibilita que el sitio sirva a los usuarios como lo hace normalmente y a menudo provoca un cierre completo.

Una forma habitual de prevenir los ataques DoS es utilizar un cortafuego que detecte si las solicitudes enviadas al servidor son legítimas. Las solicitudes atacantes pueden descartarse, lo que permite que el tráfico normal fluya sin interrupciones. Un ejemplo de un gran ataque a Internet de ese tipo se produjo en febrero de 2020 contra Amazon Web Services (AWS).

Ataques de contraseña

Las contraseñas son la herramienta de verificación de acceso preferida por la mayoría de la gente, por lo que descubrir la contraseña de una persona o servicio es una propuesta atractiva para un atacante. Esto puede conseguirse mediante varios métodos diferentes, algunos de ellos utilizando técnicas de ingeniería social.

Un atacante también puede utilizar un ataque de diccionario para averiguar la contraseña de un usuario. Un

16. Paso explosivo - CitizenLab

ataque de diccionario es una técnica que utiliza palabras y frases comunes, como las que se encuentran en un diccionario, para intentar adivinar la contraseña del objetivo. Un método eficaz para prevenir los ataques de fuerza bruta y diccionario contra contraseñas es configurar una política de bloqueo. Esto bloquea el acceso a dispositivos, sitios web o aplicaciones automáticamente después de un cierto número de intentos fallidos. Con una política de bloqueo, el atacante solo tiene algunos intentos antes de ser bloqueado y no poder acceder.

Otra posibilidad de ataque de contraseña se basa en el uso de los registradores de teclado (*keyloggers*). Se trata de un tipo de *software* malicioso diseñado para rastrear cada pulsación de tecla e informar de ello a un atacante. Normalmente, un usuario se descarga el *software* creyendo que es legítimo, pero este instala un registrador de teclado sin que el usuario sea consciente de ello. Para protegerse de estos ataques, es necesario ejecutar un escáner de virus. Las empresas de antivirus mantienen registros de los registradores de teclado más comunes y los marcarán como peligrosos.

Privacidad de la información

Aunque prácticamente todo el mundo tiene una idea más o menos clara de lo que es la privacidad, no existe una definición ampliamente aceptada por la comunidad académica. Un aspecto específico es la privacidad de la información, que aborda concretamente la información personal de un individuo y la divulgación de esa información personal. En otras palabras, la privacidad de la información es «el derecho de los individuos, grupos o instituciones a determinar por sí mismos cuándo, cómo y en qué medida se comunica a otros información sobre ellos».

La aparición y avances de las tecnologías de tratamiento de la información, el paso de un mundo analógico a otro digital centrado en los datos y la tendencia a recopilar y almacenar datos personales han llevado a entender la importancia, ahora más que nunca, de la preservación de la privacidad. Los dispositivos electrónicos actuales permiten a los seres humanos generar y grabar una cantidad extraordinaria de información en diferentes formas: fotos, audios, videoclips, documentos electrónicos. Además, cada vez se utilizan más las redes de telecomunicaciones para un gran abanico de actividades y servicios: leer el periódico, ir de compras, mantenerse en contacto con otras personas, operaciones bancarias, reservar vacaciones, redes sociales, agenda digital, etc. A todo esto, hay que añadir la presencia cada vez más frecuente de los dispositivos de la internet de las cosas (dispositivos IoT, *Internet of Things*), que generan una gran cantidad de datos para su aplicación en diferentes ámbitos. Los teléfonos móviles, los relojes inteligentes y otros dispositivos portátiles aumentan drásticamente la cobertura y rapidez con la que los datos biométricos y de comportamiento de las personas están disponibles para su procesamiento. En algunos casos, estos datos son compartidos con el conocimiento de las personas afectadas, por ejemplo, cuando los usuarios publican vídeos, fotos u opiniones sobre productos y temas de actualidad. Una cantidad mucho mayor se recopila de forma inadvertida cuando las personas navegan por páginas web, utilizan servicios de localización y aplicaciones similares o simplemente entran en espacios inteligentes enriquecidos con cualquier cosa, desde asistentes de voz a cámaras de circuito cerrado de televisión.

Los datos de comportamiento son muy descriptivos del individuo y ponen de manifiesto multitud de atributos. Contienen fuertes indicadores de rutinas, hábitos y también afecciones médicas y «tics». Las correlaciones conocidas entre rasgos fisiológicos y afecciones médicas incluyen la detección de depresión o consumo de antidepresivos en imágenes faciales, la detección de insuficiencias orgánicas debido a la coloración de los ojos (hepatitis) o de la piel (abuso de alcohol, estado físico general, y otros). Estos datos también pueden utilizarse para identificar a individuos de manera única; por ejemplo, la forma de andar se ha utilizado de forma muy relevante para identificar a individuos y revela atributos individuales como la edad, el género y condiciones fisiológicas.

Otra amenaza de privacidad puede provenir del uso de dispositivos portátiles para servicios basados en la ubicación (LBS) o monitorización de la salud. Los dispositivos que permiten monitorizar el cuerpo pueden recopilar información como es el ritmo cardíaco, su ubicación y trayectoria, y almacenarla en la nube del dispositivo o en el teléfono inteligente local. En consecuencia, la protección de la privacidad resulta cada vez más importante, ya que una gran cantidad de información privada puede ser utilizada indebidamente por terceros no deseados sin las correspondientes medidas de protección y el consentimiento de los usuarios.

Se considera que unos datos son sensibles si su divulgación, acceso o uso sin autorización puede causar daños, perjuicio, vergüenza o discriminación a una persona. Algunas normativas de privacidad, como el Reglamento general de protección de datos (RGPD) de la Unión Europea proporcionan definiciones específicas de información sensible y exigen que las organizaciones incorporen medidas adecuadas para proteger estos datos, como el cifrado, los controles de acceso y la minimización de datos.

El estudio de la privacidad puede dividirse en dos categorías: privacidad del contenido y privacidad de la interacción. En la primera clase, los atacantes pueden identificar a una persona a partir de un conjunto de datos

anonimizados o cifrados con cierto conocimiento sobre las personas afectadas. En el segundo caso, mientras se realiza una actividad digital, aunque la confidencialidad de la información que se transmite esté protegida mediante cifrado, el origen y el destino de la comunicación son fácilmente trazables. La información sobre quién se comunica con quién puede revelar información crítica que podría utilizarse. Por ejemplo, alguien que acceda a un sitio web con información sobre una enfermedad potencialmente mortal puede no obtener un seguro médico o perder su trabajo si esa información llega a la compañía de seguros o al empleador. La posibilidad de relacionar toda la información de tráfico generada por un usuario de Internet (por ejemplo, a través de la dirección IP, número de identificación nacional o número de la seguridad social) permite elaborar perfiles sofisticados de cada usuario.

Así pues, es necesario establecer un balance entre la necesidad de utilizar los datos personales y el derecho de las personas a la privacidad de los datos. La privacidad de los datos está estrechamente relacionada con la protección de los datos. La privacidad de los datos y la protección de los datos comparten el mismo objetivo: proteger los datos sensibles de las violaciones, los ciberataques y la pérdida accidental o intencionada de datos. Sin embargo, mientras que la privacidad de la información se centra en las normas sobre cómo las organizaciones pueden recopilar, almacenar y procesar información personal, la protección de los datos se centra en los controles de seguridad que garantizan la confidencialidad, la integridad y la disponibilidad de la información. Además, la protección de los datos implica a menudo proteger no solo la información personal, sino otros datos críticos para el negocio, como secretos comerciales de la empresa y datos financieros.

Tipo y sensibilidad de los datos

A fin de explorar los diferentes tipos de información sensible que definen y supervisan varias normativas, en primer lugar, hay que introducir los conceptos básicos de *información identificable de persona* (PII, *Personally Identifiable Information*) y de *información personal* (PI, *Personal Information*).

La PII o información identificable de persona se define como aquella información que, bien por sí sola o cuando se combina con otra información, puede utilizarse para identificar o rastrear la identidad de una persona. La PII constituye el tipo de datos disponible más habitual y de forma menos regulada. En términos más generales, el NIST (National Institute of Standards and Technology), en el documento *Guide to Protecting the Confidentiality of Personally Identifiable Information*, ofrece los siguientes ejemplos de información que pueden considerarse PII:

- Nombre: como puede ser el nombre completo o alias.
- Número de identificación personal: como el número del documento nacional de identidad, número de seguridad social (SSN), el número del pasaporte, el número del permiso de conducir, el número de identificación fiscal, el número de identificación del paciente o el número de la cuenta financiera o de la tarjeta de crédito.
- Datos de dirección: como la dirección postal o la dirección de correo electrónico.
- Características personales, incluidas imágenes fotográficas (especialmente de la cara u otra característica distintiva), radiografías, huellas dactilares u otras imágenes biométricas o datos de plantillas (por ejemplo, escáneres de retina, firma vocal, geometría facial).
- Información sobre una persona vinculada o vinculable a una de las anteriores (por ejemplo, fecha de nacimiento, lugar de nacimiento, raza, religión, peso, actividades, indicadores geográficos, información laboral, información médica, información educativa, información financiera).

La PI o información personal es una categoría más amplia. En otras palabras, toda la PII se considera PI, pero no toda la PI es PII. Así, la PI se define como aquella información que identifica, describe, se refiere, puede asociarse o podría razonablemente vincularse, directa o indirectamente, con una persona concreta. La PI, por tanto, puede incluir datos que están obviamente asociados a una identidad –como un nombre o una fecha de nacimiento, que a menudo también es PII– o interpretarse de forma legal extremadamente amplia. La PI puede y suele incluir aspectos como origen racial o étnico, afiliaciones u opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, orientación sexual, antecedentes penales, información médica o genética, datos biométricos, informes de localización, direcciones IP…

También es útil exponer qué tipos de datos no están sujetos a preocupaciones sobre la privacidad de los datos. Existen dos tipos principales:

- Datos de carácter personal no sensibles (PII): información que ya está en registros públicos, como una guía de teléfonos y un directorio *online*.
- Información no identificable personalmente (no-PII): datos que no pueden utilizarse para identificar a una persona. Los ejemplos incluyen identificadores de dispositivos o galletas (*cookies*). Sin embargo, algunas leyes de privacidad consideran que incluso las galletas pueden considerarse datos personales, ya que pueden dejar rastros que podrían ser utilizados en combinación con otros identificadores para establecer la identidad de una persona.

La definición de *información sensible*, también conocida como *datos sensibles*, es algo diferente dependiendo de las leyes de privacidad aplicables. Como definición global puede asumirse que la información sensible son aquellos

datos personales que la mayoría de jurisdicciones consideran que deberían ser tratados con un estándar de cuidado más elevado. Se considera que unos datos son sensibles si su divulgación, acceso o uso sin autorización puede causar daños, perjuicio, vergüenza o discriminación a una persona. Con frecuencia, la información sensible incluye datos de identificación personal, así como información financiera, médica, antecedentes penales y cualquier otro dato que pueda utilizarse para identificar o rastrear a una persona. La PII puede o no ser sensible o puede considerarse sensible solo en determinadas circunstancias. Por ejemplo, algunas PII como nombres, números de teléfono u otra información que puede ser de dominio público no suele considerarse sensible (aunque podría serlo en determinados contextos), mientras que otras PII como números de seguridad social, números de registro de extranjeros sí lo serían. Algunas normativas de privacidad, como el Reglamento general de protección de datos (RGPD) de la Unión Europea, proporcionan definiciones específicas de información sensible y exigen que las organizaciones incorporen medidas adecuadas para proteger estos datos, como el cifrado, los controles de acceso y la minimización de datos.

Por tanto, los datos sensibles requieren un mayor nivel de protección debido a su naturaleza delicada y personal, como la información médica, la orientación sexual, la religión, la raza, entre otros. Para protegerlos, es necesario aplicar medidas de seguridad más rigurosas. Y, dependiendo de la ley, es posible que se requieran diferentes tipos de consentimiento para recopilarla.

A continuación, se indican algunos de los tipos de información comúnmente considerados sensibles, tanto por el público en general como por los mandatos legales:

- **Información sanitaria personal** (PHI, *Personal Health Information*): historial médico, información sobre seguros y otros datos privados que recogen los proveedores de asistencia sanitaria y que podrían vincularse a una persona determinada.
- **Información financiera personal identificable** (PIFI, *Personally Identifiable Financial Information*): números de tarjetas de crédito, detalles de cuentas bancarias u otros datos relativos a las finanzas de una persona.
- **Expedientes académicos:** calificaciones, expedientes académicos, horario de clases, datos de facturación y otros registros relativos a la formación académica de una persona.

Los registros de una base de datos pueden contener información, que, según su naturaleza o tipología, pueden clasificarse en:

- **Atributos clave o identificadores:** son campos que identifican unívocamente a los sujetos de los datos (nombre, DNI, número de pasaporte, teléfono…). Este tipo de datos debe eliminarse de los registros anonimizados.
- **Casi identificadores:** son campos que, si bien por sí mismos y de forma aislada no identifican a un individuo (como edad, ocupación, código postal), agrupados con otros atributos casi-identificadores, pueden señalar de forma unívoca a un sujeto. Las técnicas de anonimización trabajan sobre estos datos, eliminando campos que no son necesarios para el tratamiento (en aplicación del principio de minimización), agregándolos o generalizándolos.
- **Atributos sensibles:** son los campos que contienen datos que podrían tener un mayor impacto en la privacidad de un individuo concreto, entre ellos las categorías especiales de datos, y que no deben ser vinculados con el sujeto de datos al que pertenecen (enfermedades, tratamientos médicos, nivel de renta…). Esta información puede ser de gran interés en el objeto del tratamiento de datos, pero, salvo que exista una legitimación para ello, debe mantenerse disociada de un sujeto concreto.
- **Otros:** la información que no pertenece a las tres categorías anteriores.

A continuación, se presentan algunas medidas para tratar los datos sensibles bajo un punto de vista de privacidad:

- **Minimización de datos:** se trata de recolectar solo los datos necesarios y relevantes para el propósito específico de la recolección. Es decir, deben recolectarse solo los datos necesarios para cumplir con un propósito específico y no más de lo necesario.
- **Consentimiento informado:** es importante obtener el consentimiento explícito y libre de la persona para recolectar y utilizar sus datos sensibles. El consentimiento debe ser informado, específico y otorgado de forma voluntaria.
- **Protección de datos:** los datos sensibles deben ser almacenados y protegidos adecuadamente para evitar el acceso no autorizado o el uso inadecuado. Pueden utilizarse medidas técnicas, como el cifrado, y medidas organizativas, como políticas de seguridad y acceso restringido a los datos.
- **Eliminación de datos:** es importante que los datos sensibles sean eliminados de forma segura una vez que ya no sean necesarios para el propósito para el que fueron recogidos.
- **Responsabilidad y transparencia:** las organizaciones que gestionan datos sensibles deben ser transparentes en cuanto a la recolección, uso y protección de los datos, y deben asumir la responsabilidad de garantizar la privacidad y seguridad de los datos.

En resumen, el tratamiento de los datos sensibles desde un punto de vista de privacidad requiere medidas de protección y seguridad específicas, así como transparencia y responsabilidad por parte de las organizaciones que manejan estos datos.

En los últimos años la preservación de la privacidad ha despertado un interés considerable entre toda la comunidad y, por tanto, también entre los académicos y los diseñadores. En consecuencia, se han desarrollado varios métodos para proteger la privacidad o se han establecido políticas con un amplio ámbito para la protección de datos sensibles. En la actualidad, no existen soluciones genéricas que puedan gestionar todos los problemas de privacidad relativos a la protección de la información sensible contra la divulgación no deseada mientras se conserva la utilidad de los datos. Las técnicas tradicionales se basaban únicamente en la anonimización, es decir, eliminando todos los identificadores –atributos que identifican sin ambigüedad a los participantes, como el número de seguridad social, el pasaporte, el nombre-apellido). Sin embargo, hay que tener en cuenta que las combinaciones únicas de valores de atributos pueden utilizarse para volver a identificar sin ambigüedad a un individuo en una base de datos sin identificadores explícitos, y al volver a identificar a un participante de una base de datos, se le pueden revelar los atributos confidenciales (sensibles) tales como el salario, las enfermedades, la ideología, etc.

Tecnologías de protección de la privacidad

Las tecnologías de protección de la privacidad (*Privacy-Enhancing Technologies*, PET) son un conjunto de herramientas técnicas diseñadas para proteger la privacidad de los datos personales en varias aplicaciones y sistemas de información. Estas tecnologías proporcionan un conjunto de mecanismos para minimizar la cantidad de información personal que se recopila, procesa y divulga, garantizando que se cumplan los principios fundamentales de privacidad. En la última década se han propuesto numerosas herramientas PET relacionadas con la anonimización del tráfico de red (por ejemplo, la red TOR), la gestión de identidades, el almacenamiento anónimo de datos, además de las técnicas criptográficas y de separación de la información.

Básicamente las técnicas de privacidad de datos pueden clasificarse en técnicas de perturbación de datos y técnicas de enmascaramiento o anonimización, tal y como se indica en la siguiente figura. A grandes rasgos se trata de eliminar o modificar determinados datos personales de una persona, de un conjunto de datos, de modo que la persona no pueda ser identificada directa o indirectamente a partir de estos datos. De esta forma se reduce el riesgo de que los datos sean utilizados de forma inapropiada o se divulguen sin autorización. Este proceso se realiza a través de diferentes técnicas, como la eliminación de ciertos campos de datos, la sustitución de los valores reales de los datos por valores ficticios o la agregación de los datos en categorías más generales.

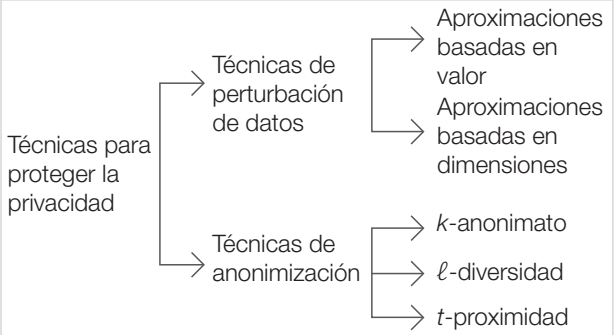

Figura 3: Técnicas para proteger la privacidad

Las técnicas de perturbación de datos son un conjunto de métodos consistentes en introducir cambios deliberados en los datos antes de su análisis o divulgación. Estas técnicas son especialmente relevantes en el contexto de la ciencia de datos, el aprendizaje automático y la minería de datos, en que se busca utilizar datos para obtener información valiosa sin revelar información sensible o identificable sobre las personas u organizaciones implicadas. El resultado es equivalente a añadir «ruido» en las bases de datos que permite la confidencialidad individual del registro. La perturbación de datos se aplica típicamente en los registros electrónicos de salud (EHR) para proteger la información sensible, aunque su uso no se limita a la industria sanitaria. Estas técnicas de perturbación pueden tener dos enfoques distintos: basados en valores y basados en dimensiones.

— Las aproximaciones basadas en valor se refieren a métodos que modifican o perturban los valores de los datos, a la vez que preservan las propiedades estadísticas generales o las características del conjunto de datos. Estas técnicas dificultan la reidentificación de personas específicas en un conjunto de datos, pero todavía permiten obtener información y conocimientos significativos a partir de los datos perturbados. Básicamente, en vez de utilizar directamente los valores originales de los datos, las aproximaciones basadas en valores modifican estos valores de forma que conserva la utilidad de los datos para el análisis, pero reduce el riesgo de violaciones de la privacidad. Las aproximaciones basadas en valores se utilizan a menudo en escenarios donde es necesario analizar datos a nivel individual mientras se protege la privacidad. Algunos ejemplos pueden ser investigación médica, análisis de datos del censo y aplicaciones de aprendizaje automático. Estas técnicas ayudan a las organizaciones y los investigadores a adherirse a las regulaciones de privacidad y a los estándares éticos, a pesar de obtener conocimientos con valor de datos sensibles.

— Las aproximaciones basadas en dimensiones se refieren a métodos que se centran en perturbar o alterar los datos en dimensiones o atributos específicos del conjunto de datos, mientras se preserva su estructu-

ra global y propiedades estadísticas. Estas técnicas se utilizan para mejorar la protección de la privacidad añadiendo ruido o realizando modificaciones en determinadas características, reduciendo así el riesgo de reidentificación de las personas. Entre otras posibilidades, pueden utilizarse técnicas de aleatorización para introducir ruido controlado o alteraciones en las dimensiones seleccionadas, de modo que sea más difícil vincular puntos de datos específicos a personas mientras se permite el análisis significativo. Las aproximaciones basadas en dimensiones son especialmente útiles cuando se trabaja con conjuntos de datos en los que solo un subconjunto de atributos contiene información sensible, siendo esencial proteger estos atributos mientras se permite el análisis en dimensiones no sensibles. Estas técnicas encuentran el equilibrio entre la preservación de la privacidad y la utilidad de los datos, asegurando que todavía puedan obtenerse conocimientos significativos de los datos perturbados, mientras se reduce el riesgo de vulneraciones de la privacidad.

Las técnicas de anonimización para la privacidad se refieren a métodos y procesos utilizados para eliminar u ocultar la información personalmente identificable (PII) de conjuntos de datos, dificultando identificar o relacionar a personas específicas con los datos. Sin embargo, debe tenerse en cuenta que la eficacia de estas técnicas depende de varios factores, como la calidad del proceso de anonimización, los requisitos específicos de privacidad y el modelo de amenazas. En algunos casos, incluso los datos bien anonimizados pueden ser vulnerables a ataques de reidentificación si existen otras informaciones externas disponibles para los atacantes. A continuación, se indican algunos tipos de técnicas de anonimización.

— ***k*-anonimato:** el *k*-anonimato es una técnica de privacidad de datos que se utiliza para proteger la identidad de los individuos en conjuntos de datos que se comparten públicamente. La idea principal detrás del *k*-anonimato es que una entidad que publica un conjunto de datos debe garantizar que cada individuo en el conjunto de datos sea indistinguible de al menos *k*-1 otros individuos en el mismo conjunto de datos. En otras palabras, el *k*-anonimato asegura que no pueda identificarse a un individuo específico en un conjunto de datos compartido. Se dice que un individuo es *k*-anónimo dentro del conjunto de datos en el que está incluido si, y solo si, para cualquier combinación de los atributos casi-identificadores asociados, existen al menos otros *k*-1 individuos que comparten con él los mismos valores para esos mismos atributos. Hay que tener en cuenta que el *k*-anonimato no se centra en los atributos sensibles de los registros, sino en los atributos casi-identificadores que pueden permitir su vinculación.

Para aplicar la técnica del *k*-anonimato, se agrupan los datos por atributos que permiten identificar a una persona, como el nombre, la dirección, el número de identificación personal, etc. Después, se eliminan los atributos identificadores y se agrupan los datos en conjuntos que contienen al menos *k* individuos que comparten el mismo conjunto de valores de atributos. Para garantizar el *k*-anonimato, pueden utilizarse técnicas de generalización, agrupación o supresión de datos.

Por ejemplo, suponiendo que se posee un conjunto de datos de pacientes que incluye información sobre su edad, género, ciudad de residencia y resultado de una prueba médica. Para aplicar el *k*-anonimato, podrían agruparse los datos por edad, género y ciudad de residencia, y después eliminar los identificadores como nombres o números de identificación personal. Después, pueden generalizarse o suprimirse ciertos valores para garantizar que cada grupo contenga al menos *k* pacientes que comparten el mismo conjunto de valores de edad, género y ciudad de residencia.

Suponiendo que un hospital tiene una base de datos de pacientes que incluye su DNI, información sobre su edad, género, código postal y enfermedad:

DNI	Edad	Género	Código postal	Enfermedad
21057841	22	H	25036	Cardiovascular
74323432	23	H	25012	Respiratorio
23489343	18	H	25600	Cardiovascular
44648948	47	D	08870	Osteoporosis
78489455	42	D	08630	Respiratorio
61154615	50	D	08292	No enfermedad
54687897	23	H	17256	Páncreas
87879873	25	H	17800	Paget
91584168	19	D	17424	COVID
21548710	41	D	43008	Glaucoma
33728590	41	H	43001	Diabetes
09342859	41	D	43004	No enfermedad

Para aplicar la técnica de agregación mediante *k*-anonimato en esta tabla, podría procederse de la siguiente forma:

– **Definir el valor de *k***: *k* representa el nivel de anonimato que desea conseguirse, es decir, el número mínimo de individuos que deben estar presentes en cada grupo de atributos identificativos para que no sea posible identificar a ninguno de ellos. En este caso, se supone que se desea un nivel de anonimato de $k = 3$.
– **Eliminar los atributos identificadores** (en este caso el DNI) e identificar los atributos casi-identificadores: son aquellos atributos que combinados pueden permitir la identificación de un individuo en la tabla original. En este caso, son la edad, género y código postal.
– **Agrupar los datos:** deben organizarse los datos por cada combinación de atributos identificativos, de

forma que a partir de la enfermedad no pueda identificarse quién es el paciente y que al menos haya *k* posibilidades.

Edad	Género	Código postal	Diagnóstico
<25	H	25***	Cardiovascular
<25	H	25***	Respiratorio
<25	H	25***	Cardiovascular
40-50	D	08***	Osteoporosis
40-50	D	08***	Respiratorio
40-50	D	08***	No enfermedad
<25	*	17***	Páncreas
<25	*	17***	Paget
<25	*	17***	COVID
41	*	4300*	Glaucoma
41	*	4300*	Diabetes
41	*	4300*	No enfermedad

Las columnas sensibles de interés no pueden revelar información que haya sido recortada en las columnas generalizadas. Por ejemplo, algunas enfermedades son únicas de hombres o mujeres, lo que podría revelar un atributo de género que había sido recortado y, por tanto, podría comprometer el anonimato.

Los valores en las columnas sensibles no son todos iguales para un grupo particular de *k*. Si los valores sensibles son iguales para un conjunto de *k* registros que comparten atributos casi-identificadores, entonces este conjunto de datos todavía es vulnerable a un ataque llamado *ataque de homogeneidad*. En un ataque de homogeneidad, el atacante utiliza el hecho de que es suficiente encontrar el grupo de registros al que pertenece la persona si todos tienen el mismo valor sensible. Por ejemplo, si todos los varones mayores de sesenta años del conjunto de datos tienen cáncer, si se sabe que Juan tiene más de sesenta años y está en el conjunto de datos, se tiene la certeza de que Juan tiene cáncer. Además, incluso si no todos los valores son iguales para un grupo de *k*, si no hay suficiente diversidad, todavía existe una alta probabilidad de que se aprenda algo más acerca de Juan. Si aproximadamente el 90 por ciento de los registros del grupo tienen el mismo valor sensible, un atacante puede inferir con gran certeza cuál es el atributo sensible de la persona. Medidas como la ℓ-diversidad y la *t*-proximidad (que serán explicadas posteriormente) pueden utilizarse para especificar que entre cualquier *k* registros coincidentes debe haber una cierta cantidad de diversidad en los valores sensibles. Para ilustrarlo, imaginando que las tres personas que forman parte del último bloque hubieran tenido la misma enfermedad, si se sabe que una de las personas que han formado parte de ese estudio vive en el código postal 43004, ya puede saberse qué enfermedad tiene y, por tanto, se habría comprometido su privacidad.

— **ℓ-diversidad:** este concepto se introdujo para evitar los ataques de homogeneidad indicados en el párrafo anterior. La ℓ-diversidad es una técnica que permite ampliar el *k*-anonimato asegurando que cada grupo de registros indistinguibles tenga como mínimo ℓ valores distintos para atributos sensibles. Esto añade una capa adicional de protección contra ataques basados en atributos. Se procede a ilustrar la ℓ-diversidad con un ejemplo. Suponiendo que se tiene un conjunto de datos que contiene los expedientes médicos de los pacientes, siendo uno de los atributos «diagnóstico», que indica la condición médica de cada paciente. Quiere publicarse una parte de este conjunto de datos con fines de investigación al tiempo que se preserva la privacidad de los pacientes.

Asumiendo que el conjunto de datos original es

Edad	Género	Código postal	Diagnóstico
29	H	90216	Diabetes
29	D	90219	Asma
31	H	90217	Asma
22	D	94105	Hipertensión
39	H	94117	Asma
24	D	94109	Asma
37	H	94126	Diabetes
26	D	90216	Diabetes
21	H	90213	Diabetes
36	H	94105	Hipertensión
27	H	90217	Hipertensión
28	D	90211	Hipertensión
22	H	90211	Hipertensión
34	H	90211	Hipertensión
23	D	94102	Diabetes
32	H	90213	Diabetes
24	H	90218	Asma
28	H	90214	Asma

una posible modificación de la base de datos, después de aplicar la ℓ-diversidad con $\ell = 3$, sería

Edad	Género	Código postal	Diagnóstico
30-34	H	9021*	Diabetes
30-34	H	9021*	Hipertensión
30-34	H	9021*	Asma
20-24	D	9410*	Hipertensión
20-24	D	9410*	Diabetes
20-24	D	9410*	Asma
25-29	D	9021*	Hipertensión
25-29	D	9021*	Diabetes
25-29	D	9021*	Asma
35-39	H	941**	Hipertensión
35-39	H	941**	Diabetes
35-39	H	941**	Asma

Edad	Género	Código postal	Diagnóstico
20-24	H	9021*	Hipertensión
20-24	H	9021*	Diabetes
20-24	H	9021*	Asma
25-29	H	9021*	Hipertensión
25-29	H	9021*	Diabetes
25-29	H	9021*	Asma

  - En este conjunto de datos modificado, se ha asegurado una 3-diversidad para el atributo «Diagnóstico». Para la categoría «Diabetes», hay cinco pacientes diferentes. Esto hace que sea más difícil para un adversario determinar la condición médica de un individuo específico basándose únicamente en el atributo «Diagnóstico» compartido.
  - La ℓ-diversidad es una forma de reforzar la protección de la privacidad de los atributos sensibles dentro de un conjunto de datos, particularmente cuando se entrega o se comparten datos para investigación o análisis, al tiempo que se reduce el riesgo de ataques de inferencia basados en atributos. El valor específico de ℓ en la ℓ-diversidad puede variar en función del nivel deseado de protección de la privacidad y la naturaleza del conjunto de datos.

— ***t*-proximidad:** La *t*-proximidad es una medida de privacidad que tiene como objetivo asegurar que la distribución de los atributos sensibles en un grupo de registros indistinguibles no sea significativamente distinta a la distribución general en el conjunto de datos.

Privacidad en las etapas de ciclo de vida de la información

Las técnicas y los mecanismos de privacidad varían en función de la fase del ciclo de vida de los datos. A continuación, se presentan las técnicas y los mecanismos de privacidad en las fases de recopilación, generación, almacenamiento y procesamiento de datos:

Etapa 1: recopilación de información personal

La primera etapa del ciclo de vida de la información es la recopilación de datos personales. Aquí, las entidades deben asegurarse obtener el consentimiento adecuado de los individuos antes de recopilar sus datos. Además, deben establecerse políticas claras y transparentes para informar a los usuarios sobre cómo se utilizará su información personal.

Etapa 2: almacenamiento y gestión de la información personal

Una vez que se recopila la información personal, es crucial garantizar su almacenamiento seguro y su correcta gestión. Esto implica implementar medidas técnicas y organizativas para proteger los datos contra accesos no autorizados, pérdidas o filtraciones. Además, es esencial establecer políticas y procedimientos claros sobre quién tiene acceso a la información personal y cómo se gestiona internamente. Entre otras técnicas se utilizan las siguientes:

— **Cifrado:** el cifrado de los datos implica transformarlos en una secuencia de caracteres incomprensible para cualquier persona que no tenga la clave de descifrado. Esto ayuda a proteger los datos almacenados en caso de que sean robados o se haya accedido a ellos de forma no autorizada.

— **Acceso restringido:** pueden establecerse medidas para limitar el acceso a los datos almacenados solo a las personas que tienen permiso. Esto incluye la implementación de sistemas de autenticación y autorización para garantizar que solo las personas autorizadas tengan acceso a los datos.

Etapa 3: uso y procesamiento de la información personal

Durante esta etapa, las organizaciones utilizan la información personal recopilada para los fines previstos. Sin embargo, es importante garantizar que el uso y el procesamiento de los datos se realicen de forma compatible con las leyes y regulaciones de privacidad aplicables. Las organizaciones deben establecer restricciones y controles adecuados para asegurarse de que la información personal solo se utilice de acuerdo con los consentimientos otorgados por los individuos. Entre otras técnicas se utilizan las siguientes:

— **Anonimización o perturbación:** se modifican los conjuntos de datos recopilados para publicarlos garantizando la privacidad. De esta forma se permite el procesamiento de los datos para fines específicos sin revelar la identidad del individuo.

— **Minimización de datos:** como se ha mencionado anteriormente, la minimización de datos implica publicar solo la información necesaria para el propósito específico de su uso.

Etapa 4: retención y eliminación de la información personal

La retención y la eliminación de la información personal es una etapa crítica en el ciclo de vida de la información. Las entidades deben definir períodos de retención claros y cumplir las obligaciones legales y reguladoras. Además, deben implementar procedimientos adecuados para eliminar de forma segura y permanente los datos personales cuando ya no sean necesarios para los fines para los que se recopilaron.

En resumen, las técnicas y mecanismos de privacidad en las fases de generación, almacenamiento y procesamiento de datos incluyen la anonimización, perturbación, minimización, encriptación, acceso restringido, consentimiento informado. Es importante implementar estas me-

didas para garantizar la privacidad y la seguridad de los datos en cada fase del ciclo de vida de los datos.

Aspectos de la privacidad

Distinguimos tres tipos de privacidad: la privacidad de los datos, la privacidad del usuario y la privacidad de la localización. La privacidad de datos, la privacidad de usuarios y la privacidad de localización son conceptos diferentes, pero relacionados en el contexto de la privacidad *online*. La privacidad de datos se refiere a la protección de los datos personales, la privacidad de usuarios se refiere a la protección de la identidad *online* de un individuo, y la privacidad de localización se refiere a la protección de la información de localización de un individuo.

A modo de resumen podría decirse:

— La privacidad de datos hace referencia al derecho de una persona a controlar la información personal que comparte con los demás. Esta información puede incluir su nombre, dirección, número de teléfono, dirección de correo electrónico, historial de navegación, historial de compras, etc.
— La privacidad de usuarios hace referencia al derecho de una persona a controlar su identidad *online*. Esta identidad puede incluir su nombre de usuario, contraseña, perfiles de redes sociales, etc.
— La privacidad de localización hace referencia al derecho de una persona a controlar su información de localización. Esta información puede ser recopilada por agencias gubernamentales, empresas tecnológicas u otros terceros.

Privacidad de los datos

Se refiere a la protección de los datos personales de un individuo, como su nombre, dirección, número de identificación, información financiera, historial médico, entre otros. La privacidad de datos implica que estos datos solo sean recopilados, almacenados y utilizados de forma legal y ética, y que se implementen medidas adecuadas para garantizar su seguridad. La privacidad de datos se enfoca en la protección de los datos como entidad en sí misma.

Algunos ejemplos prácticos de privacidad de los datos:

— Una empresa de comercio electrónico debe obtener el consentimiento informado de un cliente antes de recopilar sus datos personales, como su nombre, dirección de correo electrónico y detalles de pago.
— Una empresa de análisis de datos debe utilizar técnicas de anonimización de datos para eliminar cualquier información que pueda identificar a un individuo de los datos recopilados antes de utilizarlos para el análisis.
— Una empresa de servicios financieros debe limitar el acceso a los datos personales a solo aquellos empleados que necesitan tener acceso para realizar sus funciones laborales.
— Un servicio de correo electrónico debe utilizar técnicas de cifrado para proteger los datos mientras se transmiten de un servidor a otro.

Privacidad de usuario

Se refiere a la protección de la identidad *online* de un individuo, incluyendo su nombre de usuario, contraseña, direcciones de correo electrónico y otra información personal que pueda identificarle. La privacidad de usuario implica que esta información solo se comparta con terceros con el consentimiento del usuario y que se implementen medidas de seguridad para protegerla de la exposición no autorizada. La privacidad de usuario se enfoca en la protección de la identidad del usuario y de la forma en que se utiliza en línea.

Algunos ejemplos prácticos de la privacidad del usuario:

— Un sitio web de redes sociales debe permitir a los usuarios configurar sus preferencias de privacidad, tales como quién puede ver su perfil y quién puede ver sus publicaciones.
— Una aplicación de mensajería debe permitir a los usuarios controlar quién puede ver su información de contacto, como el número de teléfono o la dirección de correo electrónico.
— Un servicio de correo electrónico debe permitir a los usuarios controlar quién puede enviarles correos electrónicos y quién puede ver la bandeja de entrada.
— Un servicio de transmisión de vídeo debe permitir a los usuarios controlar quién puede ver su historial de visualización y qué recomendaciones de contenido se les muestran.

Privacidad de localización

La privacidad de localización es el derecho de una persona a controlar la información sobre su ubicación geográfica, histórico de localizaciones y patrones de desplazamiento. Esta información puede ser recopilada por varios dispositivos y aplicaciones, como teléfonos móviles, ordenadores, sistemas de navegación GPS y aplicaciones de seguimiento de actividad.

La privacidad de localización es importante por varias razones. En primer lugar, puede ser utilizada para rastrear los movimientos de una persona y, en segundo lugar, la información de localización puede ser utilizada para crear perfiles de comportamiento y, en consecuencia, ser utilizada con objetivos de *marketing* o fines de espionaje.

Muchas de las acciones que se realizan a través de Internet, como llamar a alguien por teléfono móvil, hacer un *post* sobre un evento, utilizar el sistema de navegación de un coche o pagar con tarjeta de crédito, van dejando un

rastro ininterrumpido de nuestras actividades cotidianas. Estas acciones se registran fácilmente y se almacenan de forma persistente en bases de datos. La privacidad de la ubicación requiere que esta información solo se recopile y comparta de forma transparente y legal, y que los usuarios tengan control sobre cómo se utiliza y se comparte.

La práctica común adoptada por los recopiladores y propietarios de datos para proteger la privacidad de los individuos que monitorizan es la pseudonimización, también conocida como *despersonalización*. Este sencillo enfoque consiste en eliminar todos los identificadores personales (por ejemplo, información que esté directamente relacionada con la identidad de la persona, como el nombre, el número de teléfono, la dirección precisa, el número de matrícula, etc.) y sustituirlos por algún pseudoidentificador. Desgraciadamente, la pseudonimización solo proporciona un nivel muy bajo de protección, por ejemplo, la correlación cruzada naif de los datos pseudonimizados con información adicional (obtenida, por ejemplo, de datos de redes sociales de acceso público) puede permitir la reidentificación, es decir, la revelación de las identidades de los usuarios con una alta probabilidad. Así pues, la primera medida a adoptar para proteger la privacidad de localización es desactivar la ubicación del teléfono móvil cuando no sea necesaria.

La regulación normativa de la protección de datos

Debido a las crecientes preocupaciones públicas, los gobiernos están ocupados creando y adaptando leyes de protección de datos y privacidad. De hecho, la necesidad de abordar los problemas actuales de privacidad y proteger los derechos de privacidad de los datos es una tendencia global. El Reglamento general de protección de datos de la UE (RGPD) es la ley más conocida, pero muchos países, incluidos Brasil, India y Nueva Zelanda, han promulgado nuevas regulaciones de privacidad o han reforzado las leyes existentes para regular cómo pueden recopilarse, almacenarse, utilizarse, divulgarse y transmitirse datos personales.

En España, la regulación de la protección de datos está compuesta por dos documentos principales:

— El Reglamento general de protección de datos (RGPD), que es una normativa europea que se aplica a todos los estados miembros de la Unión Europea, incluida España.
— La Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), que es una ley española que desarrolla el RGPD.

El RGPD es una norma europea que establece un marco de protección de datos personales en toda la Unión Europea. Esta normativa se aplica a todas las empresas que procesan datos personales de ciudadanos de la Unión Europea, independientemente de la ubicación de la empresa. El RGPD define sus datos personales como «toda información sobre una persona física identificada o identificable». Esto incluye información como el nombre, la dirección, el número de teléfono, la dirección de correo electrónico, el historial de navegación y el historial de compras. El RGPD establece una serie de principios que deben ser respetados por las personas que tratan datos personales. Estos principios incluyen:

— Lealtad y transparencia: las personas deben ser informadas sobre cómo se tratan sus datos personales, y estos solo pueden tratarse con un propósito determinado y lícito.
— Minimización de datos: solo pueden recopilarse aquellos datos personales que son necesarios para la finalidad prevista.
— Limitación de la conservación: los datos personales solo pueden conservarse durante el tiempo necesario para la finalidad prevista.
— Integridad y confidencialidad: los datos personales deben ser protegidos contra el acceso, la modificación, la divulgación o la destrucción no autorizada.
— Responsabilidad: las personas que tratan datos personales deben ser responsables de cumplir los principios del RGPD.

La LOPDGDD complementa el RGPD y establece una serie de medidas específicas para la protección de los datos personales en España. Estas medidas incluyen:

— La creación de la Agencia Española de Protección de Datos (AEPD), que es el organismo encargado de velar por el cumplimiento de la normativa de protección de datos en España.
— El derecho de los ciudadanos a solicitar el acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos y oposición al tratamiento de sus datos personales.
— El deber de las empresas de notificar a la AEPD cualquier incidencia de seguridad que pueda afectar a los datos personales de sus clientes.

Adicionalmente, en Cataluña existe una autoridad de control específica, la Autoridad Catalana de Protección de Datos (APDCAT), que es la entidad encargada fundamentalmente de supervisar y garantizar la aplicación de las dos normativas mencionadas. También tiene otras funciones como promover la sensibilización y la comprensión del público respecto de los riesgos, las normas, las garantías y los derechos relacionados con el tratamiento, y asesorar, de conformidad con el derecho de los estados miembros, el parlamento nacional, el gobierno y otras instituciones y organismos, sobre las medidas legislativas y administrativas relativas a la

protección de los derechos y libertades de las personas físicas en cuanto al tratamiento de la normativa de protección de datos en Cataluña. La APDCAT trabaja de forma coordinada con la Agencia Española de Protección de Datos (AEPD) para garantizar una protección efectiva de los derechos de los ciudadanos en relación con sus datos personales.

Guía de buenas prácticas

Durante todo el documento se han dado recomendaciones; este capítulo proporciona una recopilación de las expuestas y añade alguna más, combinando tanto la parte de ciberataques como la parte de la privacidad de la información.

Recomendaciones generales

Se ha visto que la ciberseguridad es un tema complejo; cada día se sufren más ataques. Aunque no existe un sistema totalmente seguro, aplicar el sentido común y hacer caso de unas directrices muy claras puede ayudar a minimizar el impacto de posibles ataques. Por tanto, se recomienda seguir estos puntos generales de seguridad:

- **Concienciación y formación:** es importante que las personas que manejan datos personales sean conscientes de la importancia de la privacidad y sepan cómo protegerla. Es necesario formar a los empleados y usuarios en buenas prácticas de privacidad.
- **Verificación de la fuente:** es necesario verificar la fuente antes de proporcionar información personal o financiera, y evitar responder a correos electrónicos, llamadas telefónicas o mensajes sospechosos.
- **Privacidad en redes sociales:** es necesario revisar la configuración de privacidad en las cuentas de redes sociales y ajustar las opciones para proteger la información personal, permitiendo compartir solo la estrictamente necesaria.
- **Navegación segura:** es necesario utilizar un navegador web seguro y configurarlo para bloquear galletas de terceros y evitar su seguimiento. Garantizar también que las páginas web que se visiten sean seguras y utilicen el protocolo HTTPS.
- **Correo electrónico seguro:** es necesario utilizar un servicio de correo electrónico seguro y cifrado, y evitar enviar información confidencial a través del correo electrónico.
- **Compra *online* segura:** es necesario verificar que el sitio web sea seguro antes de efectuar una compra *online*, y utilizar una tarjeta de crédito virtual o un servicio de pago seguro.
- **Protección de la identidad:** es necesario mantener la información personal segura y proteger la identidad *online* mediante la utilización de herramientas como el bloqueo de crédito y la monitorización de la identidad.

Cómo guardar la información personal

Como ya se ha visto, los datos y la información en general son tanto el objetivo de los atacantes de los sistemas como una preocupación para los servicios *online* que suelen utilizarse. Por tanto, tanto cuando se tienen datos de terceros como cuando se está ofreciendo un servicio, deben tenerse en cuenta los siguientes puntos:

- **Utilización de cifrado:** tanto a nivel de los datos que se transmiten hacia un destinatario como los datos que se guardan en cualquier dispositivo de almacenamiento.
- **Minimización de datos:** es necesario recopilar y almacenar solo la información necesaria para cumplir el propósito específico de la recopilación de datos. No es necesario recopilar datos innecesarios.
- **Consentimiento informado:** es necesario obtener el consentimiento explícito e informado de las personas antes de recopilar los datos. El consentimiento debe ser libremente dado y las personas deben saber exactamente qué se está haciendo con sus datos.
- **Seguridad de los datos:** es importante garantizar la seguridad de los datos personales mediante la implementación de medidas de seguridad técnicas y organizativas adecuadas, como el cifrado, la autenticación de usuarios, el control de acceso y la monitorización de la actividad.
- **Transparencia:** es necesario informar a las personas sobre el uso de sus datos personales, incluyendo quiénes son los responsables del tratamiento de los datos, el propósito de la recopilación de datos y cómo se utilizarán los datos.
- **Derechos de los usuarios:** las personas tienen derechos en relación con los datos personales, como el derecho de acceso, rectificación, supresión, limitación del tratamiento y portabilidad de datos. Es importante garantizar que se respeten estos derechos.
- **Evaluaciones de impacto:** es necesario llevar a cabo evaluaciones de impacto de la privacidad para identificar y minimizar los riesgos para la privacidad en la recopilación y el tratamiento de datos personales.
- **Revisión y actualización:** es necesario revisar y actualizar las políticas y prácticas de privacidad de forma regular para asegurarse de que se siguen las mejores prácticas y se adaptan a los cambios en la normativa y la tecnología.

Cómo utilizar los dispositivos

Si bien aprender a guardar los datos de forma correcta es importante, también lo es cómo se controlan y se utilizan los dispositivos personales, que, al fin y al cabo, proporcionan el acceso a los datos que se desea proteger. De esta forma pueden darse las siguientes recomendaciones:

- **Contraseñas seguras:** es necesario utilizar contraseñas fuertes y diferentes para cada dispositivo y cuenta de servicios *online*. Es necesario cambiar las contraseñas periódicamente.
- **Autenticación de dos factores:** es muy conveniente habilitar la autenticación de dos factores siempre que sea posible. Esto añade una capa adicional de seguridad para proteger dispositivos y cuentas.
- **Actualizaciones de *software:*** es necesario mantener los dispositivos y aplicaciones actualizados con las últimas versiones de *software* y actualizaciones de seguridad para evitar vulnerabilidades.
- **Antivirus y cortafuegos:** es necesario utilizar programas de antivirus y cortafuegos para proteger los dispositivos de virus, *software* malicioso y otros ataques informáticos.
- **Redes seguras:** debe evitarse en la medida de lo posible la conexión a redes wifi abiertas, ya que pueden ser vulnerables a ataques informáticos.
- **Privacidad de la cámara y el micrófono:** es necesario tomar medidas para proteger la privacidad de la cámara y el micrófono de los dispositivos, como tapar la cámara o desactivar el micrófono cuando no estén en uso.
- **Copias de seguridad:** es necesario realizar copias de seguridad periódicas de los datos importantes almacenados en los dispositivos, para protegerlos en caso de pérdida, robo o fallo del dispositivo.
- **Configuración de privacidad:** es necesario revisar y ajustar la configuración de privacidad de los dispositivos y aplicaciones para garantizar que la información personal se protege adecuadamente y se evita el acceso no autorizado.
- **Limitación de la información personal:** es necesario limitar la información personal que se comparte en los dispositivos personales, especialmente en redes sociales y aplicaciones de mensajería.
- **Revisión de permisos de aplicaciones:** es necesario revisar regularmente los permisos que se han concedido a las aplicaciones y revocar los que no necesiten acceder a la información personal.
- **Uso de VPN o de infraestructura confianza cero (*Zero Trust*):** es necesario utilizar una red privada virtual (VPN) para cifrar la conexión a Internet y proteger la privacidad *online*, especialmente cuando la conexión sea desde fuera de la red corporativa.

Conclusiones

Este documento ha mostrado grandes problemas de forma resumida, los grandes puntos a tener en cuenta tanto desde el punto de vista de ciberataques como desde el punto de vista de privacidad de los datos que se utilizan en el día a día.

En cuanto a los ciberataques, lo que se observa es que, de forma más o menos activa, un mal actor busca hacer un uso ilegítimo de un sistema o robar cierta información para recibir algún beneficio. Se ha visto que la gran mayoría de los ataques se centran en la ingeniería social o bien se aprovechan de vulnerabilidades en el *software* existente para apropiarse de la información o sistemas con los errores. Como consecuencia de estos ataques, se ha visto que existen grupos de cibercrimen organizado, conocidos como APT, que por motivos económicos o políticos realizan ataques dirigidos a víctimas cuidadosamente seleccionadas. Estos ataques, hoy en día, en una proporción muy elevada son con *software* de secuestro, donde el atacante tiene por objetivo extorsionar a la víctima cifrando los datos existentes en sus sistemas y amenazando con publicarlos en la web oscura.

En relación con ciberataques, se ha mostrado también, si bien no puede considerarse un ataque por sí mismo, el sistema Pegasus, un *software* de ciberespionaje que se utiliza para observar grupos terroristas, pero que ha sido noticia en los últimos tiempos por el mal uso que han hecho del mismo ciertos gobiernos.

En cuanto a la privacidad de los datos, ha podido observarse el impacto y las implicaciones que tiene compartir datos privados (sean o no personales) en Internet. Se ha podido ver qué tipos de datos existen según su sensibilidad, y qué hacer para poder almacenarlos y tratarlos con el nivel de privacidad que corresponda. Para ello se han visto también las tecnologías existentes actualmente para poder proteger los datos personales.

Complementando esto, se ha estudiado también el impacto de la privacidad en las etapas del ciclo de vida de la información, donde se ha podido ver cómo la privacidad es importante en todos los niveles de almacenamiento de la información. El último punto importante de la privacidad que se ha estudiado han sido los diferentes aspectos de privacidad que afectan a la información. Así, se ha podido observar la privacidad desde el punto de vista de los propios datos, pero también considerando los usuarios y la localización de los datos.

Por último, a modo de sumario, se han presentado una serie de buenas prácticas para tratar de mitigar al máximo posible la presencia de ciberataques en los sistemas, así como el procedimiento a seguir para garantizar que los datos publicados en la red cumplen con las garantías de privacidad necesarias.

Consell Assessor del Parlament sobre Ciència i Tecnologia

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Informe de ciberseguridad y privacidad para el Parlament de Catalunya

Autores: Miquel Soriano, René Serral-Gracià
Universitat Politècnica de Catalunya

El Consejo Asesor del Parlamento sobre Ciencia y Tecnología (CAPCIT) es un órgano del Parlamento creado en 2008 con el objetivo de coordinar la información y el asesoramiento en materia científica y tecnológica que necesiten los diputados y los órganos del Parlamento. El CAPCIT es un órgano de composición mixta, formado por los diputados que son miembros del mismo y por representantes de las principales instituciones científicas y tecnológicas de Cataluña: el Instituto de Estudios Catalanes (IEC), la Fundación Catalana para la Investigación y la Innovación (FCRI), el Consejo Catalán de la Comunicación Científica (C4), la Real Academia de Ciencias y Artes de Barcelona (RACAB), la Asociación Catalana de Entidades de Investigación (ACER) y una representación de las universidades públicas y privadas. Para más información: http://www.parlament.cat/capcit.