Píldoras de Protección de Datos

apdcat

Autoritat Catalana de Protecció de Dades

ÍNDICE DE CONTENIDO

El derecho a la protección de datos

El derecho a la protección de datos es el derecho de toda persona a controlar sus datos personales. Esto permite que las personas puedan ver protegido este derecho y, también, el conjunto de derechos y libertades que pueden verse afectados por el tratamiento de datos personales. Aunque el individuo está en el centro de la protección de datos, ésta no es una cuestión únicamente personal, sino que da forma a la sociedad en la que vivimos. Por ejemplo, prohibiendo o requiriendo garantías adicionales para tratamientos concretos como la vigilancia sistemática de áreas públicas, el tratamiento de categorías especiales de datos o las decisiones automatizadas.

REGLAMENTO EUROPEO

El Reglamento general de protección de datos (RGPD) es la principal normativa europea sobre esta materia.

La normativa de protección de datos regula el uso de datos personales que realizan las organizaciones.

DATOS PERSONALES

Son datos personales cualquier información relacionada con una persona identificada o identificable.

Esta identificación puede ser directa (a través de un nombre, un teléfono, un número de identidad, etc.) o indirecta (con la combinación de diferentes factores físicos, psicológicos, económicos, culturales, sociales, etc.).

Cabe remarcar que los datos personales no son sólo los que se utilizan para identificar a una persona, sino todos los datos sobre esa persona.

DERECHOS

La normativa de protección de datos promueve la autodeterminación informativa. Es decir, quiere darle a las personas el derecho a decidir sobre el tratamiento de sus datos.

Derecho de acceso. Podemos solicitar información al responsable de tratamiento sobre si está tratando datos personales nuestros y, en caso afirmativo, recibir diversa información.

Derecho de rectificación. Podemos pedir que se corrijan nuestros datos, si son inexactos o incompletos.

Derecho de supresión. En determinados casos, podemos pedir que se supriman nuestros datos.

Derecho de portabilidad de los datos. Podemos solicitar nuestros datos personales, si el tratamiento se realiza por medios automatizados y se basa en el consentimiento o en el cumplimiento de un contrato.

Derecho de limitación. En determinados casos, podemos solicitar que se detenga el tratamiento de nuestros datos.

Derecho a no ser objeto de decisiones individuales automatizadas. Tenemos derecho a no ser objeto de decisiones basadas únicamente en un tratamiento automatizado, cuando esta decisión tiene efectos significativos.

DOCUMENTOS DE INTERÉS

- Reglamento general de protección de datos
- Ley orgánica de protección de datos personales y garantía de los derechos digitales
- Preguntas frecuentes

Hoy en día hacemos uso de todo tipo de servicios online, que tienen acceso a una gran cantidad de información: correo electrónico, tiendas en línea, redes sociales, aplicaciones bancarias, etc.

Perder el control de estas cuentas puede tener consecuencias graves: desde el acceso no autorizado o la pérdida de gran cantidad de información personal que almacenamos en la nube (correos, fotos, vídeos) hasta pérdidas económicas.

CONTRASEÑAS SEGURAS

Las contraseñas son la herramienta más utilizada para controlar el acceso a nuestras cuentas pero no sirve cualquier contraseña. De hecho, la dificultad que supone gestionar la gran cantidad de contraseñas que tenemos nos hace caer en prácticas de riesgo:

- ✗ Empleo de contraseñas cortas que, incluso, pueden ser palabras del diccionario. Éstas ofrecen muy poca protección. Un ataque basado en el diccionario es suficiente para romperlas.
- ✗ Reutilización de contraseñas. Cada vez que reutilicemos una contraseña, estamos diciendo a un servicio la contraseña que utilizamos en otros servicios. Aparte, la reutilización de contraseñas incrementa mucho el impacto en caso de que una contraseña se filtre. Piensa que existen servicios que utiliza una gran parte de la población; si se filtra una contraseña tuya, es fácil que un atacante pruebe con estos servicios.

Para que una contraseña sea útil, debe ser secreta y muy difícil de adivinar:

- ✓ Una buena contraseña debe ser compleja. Existen diferentes recomendaciones: largas con mayúsculas, minúsculas y caracteres especiales; o incluso frases.
- ✓ No compartas ni reutilices tus contraseñas.
- ✓ Ten precaución con las preguntas de seguridad. Si los hay, asegúrate de que sólo los conoces tú. Ten en cuenta que hay mucha información nuestra en internet y, además, estas preguntas se prestan a ataques de ingeniería social.
- ✓ Si guardas un recordatorio de la contraseña, hazlo de forma segura.

GESTORES DE CONTRASEÑAS

Los gestores de contraseñas son una solución para guardar de forma segura la multitud de contraseñas que tenemos. De esta manera, basta con recordar la contraseña que da acceso al gestor.

Aparte, como no es necesario recordar las contraseñas, resulta más fácil utilizar contraseñas bastante complejas. Muchas veces es el propio gestor que ofrece la funcionalidad de generar contraseñas seguras.

Algunos de estos gestores tienen funcionalidades avanzadas, como alertar si descubre que una contraseña se ha filtrado e incluso cambiar las contraseñas de distintos servicios desde el propio gestor.

ATAQUES

Tus contraseñas se pueden filtrar aunque las gestiones correctamente. La causa puede ser una violación de seguridad del proveedor del servicio o un ataque contra un usuario, como:

Shoulder surfing (o mirar por encima del hombro). Observar la contraseña, cuando la introduces en un sitio público.

Software espía instalado en el dispositivo donde introduces tu contraseña (sea el dispositivo propio o uno ajeno).

Observar las comunicaciones de un dispositivo cuando se conecta a una red pública y las comunicaciones no son cifradas.

Phishing. Es el ataque más habitual, por la facilidad de implementarlo a gran escala de forma automatizada.

¿SE HAN FILTRADO?

RockYou2021.txt

En 2021 se publicó la mayor recopilación de contraseñas jamás hecha, con unos 8.000 millones de entradas.

Puedes utilizar la web https://haveibeenpwned.com para comprobar si se han publicado sus credenciales. Incluso puedes suscribirte para que te alerte si, en algún momento, las encuentra. Algunos administradores de contraseñas ya lo hacen automáticamente.

Servicios como el anterior no son infalibles: conviene cambiar las contraseñas periódicamente.

DOCUMENTOS DE INTERÉS

- Contraseñas seguras

Otras formas de autenticación

Aunque las contraseñas son el sistema más habitual de autenticación, no son una solución perfecta. Hemos visto que gestionarlas es complejo y que, incluso haciéndolo correctamente, existen riesgos. Pero las contraseñas no son el único sistema de autenticación. Otros, como el uso de múltiples factores o la identificación biométrica.

MÚLTIPLES FACTORES DE AUTENTICACIÓN

Las dificultades para gestionar contraseñas seguras y los múltiples ataques existentes ponen en duda la seguridad de este sistema.

Los sistemas de múltiple factor buscan mitigar estos riesgos, requiriendo diferentes elementos para autenticar a un usuario:

Algo que sé. Por ejemplo, una contraseña.

Algo que tengo. Por ejemplo, mi móvil o una tarjeta.

Algo que soy. Por ejemplo, mi huella digital.

Los sistemas de múltiple factor son una herramienta eficaz para mejorar la seguridad. Cada capa de autenticación añade una complejidad extra a los ataques.

La combinación de una contraseña con un código enviado al dispositivo móvil del usuario es una forma común de autenticación de doble factor.

Aunque pocos sitios web tienen esta funcionalidad activada por defecto, hay muchos que la ofrecen. Puedes consultar una lista (no exhaustiva) en https://2fa.directory/

IDENTIFICACIÓN BIOMÉTRICA

Las características fisiológicas de una persona son una forma de verificar su identidad. De hecho, cada vez es más común desbloquear el móvil con la impronta digital o la cara. Es un método cómodo para el usuario, pero ¿qué nivel de seguridad proporciona?

La precisión de los sistemas de identificación biométrica ha mejorado mucho en los últimos años. Por ejemplo, se estima que la probabilidad de que una persona aleatoria acceda a un dispositivo con Face ID es de una entre un millón. Ahora bien, un atacante no es una persona aleatoria. Por tanto, hay que valorar los riesgos:

- Los sistemas de identificación biométrica necesitan guardar nuestra firma (huella, cara, etc.). Por tanto, existe el riesgo de que nuestra firma biométrica se filtre. Por ejemplo, un ataque a la Oficina de Gestión de Personal de EE.UU. tuvo como resultado la filtración de más de 5 millones de huellas digitales de funcionarios.
- Como siempre en seguridad informática, hay una lucha entre quienes desarrollan los sistemas y quienes quieren romperlos. Por ejemplo, se han descrito ataques para engañar a sistemas basados en huellas y en la cara.
- Un problema físico del usuario puede acarrear la denegación del acceso. Por ejemplo, una herida en el dedo puede hacer fallar la autenticación con la huella digital.

Otras formas de autenticación

Vigila con quien compartes tus datos biométricos. Una contraseña es fácil de cambiar si se filtra, pero **nuestras características físicas no podemos cambiarlas.**

- Data leak exposes unchangeable biometric data of over 1 million people
- A security breach in India has left a billion people at risk of identity theft

DOCUMENTOS DE INTERÉS

- Guía de doble autenticación.

Phishing

La cantidad de ataques informáticos es muy grande; algunos requieren de grandes conocimientos técnicos, otros son una adaptación al entorno digital de la estafa de toda la vida. El phishing (o pesca) es precisamente esto último.

El hecho de ser un ataque relativamente sencillo no le quita impacto sino al contrario, pues se producen de forma masiva. Se calcula que a diario se envían sobre un 3.500 millones de correos electrónicos de phishing y que provoca el 90% de las filtraciones de datos.

¿QUÉ ES?

El phishing es una estafa hecha mediante comunicaciones electrónicas. Tiene 3 características destacadas:

- El correo electrónico es la herramienta más habitual. También es común el phishing telefónico (vishing), vía SMS (smishing) y vía WhatsApp u otra red social.
- El atacante emplea ingeniería social, haciéndose pasar por una persona u organización de confianza.
- El objetivo puede ser robar información personal (como credenciales), infectar el dispositivo o robar dinero.

EJEMPLOS

En general, el atacante quiere hacernos creer que debe realizarse una acción con cierta urgencia.

- Un correo que simula ser de nuestro banco y afirma que, por seguridad, se ha bloqueado nuestra cuenta. Este correo nos remite a una dirección maliciosa en la que introducir nuestras credenciales para desbloquearlo.
- SMS donde se afirma que no se ha podido entregar un paquete y que es necesario acceder a un enlace para reclamarlo.

RECOMENDACIONES

Herramientas como filtros de correo o software que bloquea contenido malicioso son útiles contra el phishing, pero no son infalibles. Para no picar, conviene ser prudente. Los siguientes consejos pueden ayudarnos:

- Sospecha de los mensajes no solicitados que transmiten la sensación de urgencia o que nos ofrecen cosas a cambio de nada.
- Si sospechas de un mensaje, busca parte del texto en un buscador para comprobar si está asociado a algún phishing conocido.
- Antes de seguir las indicaciones (descargar archivos, seguir enlaces, etc.) de mensajes poco habituales, confirma que es correcto por otra vía.
- Cuando un correo no solicitado te remite a una web, vigila. Podría redirigirte a una web maliciosa que aprovecha alguna vulnerabilidad del navegador para infectar a tu ordenador.
- Cuando un correo no solicitado te remite a una web de un servicio en el que tienes cuenta, revisa que la dirección del enlace sea correcta. A menudo se crean webs que simulan ser una auténtica para engañar a los usuarios. En caso de duda, es mejor acudir a la web del servicio directamente, sin seguir el enlace del correo.
- Cuando un correo no solicitado adjunte un archivo o el enlace para descargarlo, piensa que algunos archivos pueden incluir pedidos ejecutables. Es el caso de los documentos ofimáticos, pdf y html.

SMISHING

Has recibido un SMS que habla de algo urgente, de un premio, de un paquete que no se ha podido entregar, etc. Mantente alerta: las estafas también llegan por SMS.

El smishing es una variante del phishing realizado a través de SMS. El mensaje intenta que la víctima acceda a un enlace incluido en el mismo SMS, llame a un número de teléfono o responda al SMS.

Aparte del robo de datos personales, el smishing tiene como consecuencia muy común la utilización de servicios de telefonía premium (con coste adicional bastante elevado).

TELEFONÍA PREMIUM

Los números con tarificación adicional se han convertido en una forma habitual de estafar. Si recibes un SMS que intenta que llames o envíes un SMS a uno de estos números, vigila.

Son números con tarificación adicional:

- Los comenzados por 803, 806, 807 y 905
- Los SMS a números cortos que comienzan por 2, 3, 79 y 99.

Los SMS comenzados en 79 son especialmente peligrosos, puesto que son servicios de suscripción y nos cobrarán por cada mensaje que nos envíen.

Sólo necesitamos tus datos personales, envía un SMS desde tu móvil con la palabra OFERTA al 79… y le pediremos la dirección. En un plazo de 20 días te enviaremos el reloj.

Tiene un aviso importante. Llame al (…).

DOCUMENTOS DE INTERÉS

- Undestanding phishing techniques

Seguimiento de las personas usuarias en internet

Internet está dominada por un reducido número de empresas que ofrecen sus servicios a miles de millones de personas, muchas veces sin contraprestación económica por parte de los usuarios. Esto es posible porque el principal beneficio de estas empresas tiene su origen en los datos que se recogen. Esto ha dado lugar a diversas tecnologías que permiten realizar un seguimiento bastante exhaustivo de las personas.

COOKIES

Las cookies son unos pequeños archivos de datos que guarda nuestro navegador cuando visitamos una web. La información que guarda este archivo la determina el propietario de la web y podrá recuperarla la próxima vez que visitemos su sitio.

Inicialmente, fueron pensadas para mejorar la experiencia del usuario, puesto que permiten guardar el estado actual de la web. Es decir, permiten las sesiones de usuario. Pronto se empezaron a utilizar para rastrear la actividad del usuario por parte de grandes empresas de internet que insertaban sus cookies (cookies de terceros) a gran cantidad de webs, lo que les permitía rastrear a todas las personas usuarias de estas webs.

Los navegadores permiten consultar las cookies que cada web almacena en nuestro equipo y gestionarlas. También podemos bloquearlas totalmente o de forma selectiva.

HUELLA DIGITAL

Aunque desactivamos las cookies, pueden rastrearnos utilizando las características de nuestro dispositivo. Cada dispositivo tiene unas características muy únicas (versión del sistema operativo, versión del navegador, resolución de la pantalla, zona horaria, lenguajes por defecto, etc.). Esta información es necesaria para presentar el contenido adecuadamente cuando navegamos por internet, pero a la vez puede utilizarse para rastrearnos.

IP Y DNS

La dirección IP es un conjunto de números que identifica nuestro dispositivo en internet. Cada comunicación que hacemos o recibimos en internet utiliza este identificador.

La IP de un dispositivo puede cambiar pero, por seguridad, los proveedores de servicios de internet (ISP) guardan la relación entre la IP y el usuario. De esta forma, en caso de necesidad se puede asociar una IP con una persona. En la medida en que todas nuestras comunicaciones pasan por nuestro ISP, éste puede ver la IP de los servicios con los que nos comunicamos.

La IP también revela otra información a terceras personas, como el proveedor de servicios de internet que utilizas y una localización aproximada (por ejemplo, a nivel de ciudad, aunque en ocasiones puede no ser correcta).

El servicio de nombres de dominio (DNS) traduce los nombres de las webs (por ejemplo, apdcat.gencat.cat) a la dirección IP que corresponde. De esta forma, podemos navegar por internet sin tener que recordar identificadores complejos.

Normalmente esta traducción la hace nuestro ISP, que de esta forma puede rastrear todas las webs que visitamos.

NAVEGACIÓN ANÓNIMA

Ser completamente anónimo en internet es muy difícil, pero existen algunas tecnologías sencillas que pueden ayudarnos a proteger nuestro anonimato.

- **La recomendación más básica sería evitar las cookies.** Así, evitamos que puedan rastrearnos de forma sencilla. Los navegadores incluyen opciones que nos permiten determinar las cookies que deseamos aceptar y que también permiten borrarlas.
- **VPN (red privada virtual)**. Uno de los usos de las VPN es evitar que rastreen nuestra actividad en internet. Establecemos una conexión cifrada con un servidor VPN, que será el encargado de realizar todas nuestras peticiones a internet; así, evitamos que esa actividad se pueda relacionar con nosotros. Ahora bien, la VPN tiene un punto débil: puesto que toda nuestra actividad pasa por el servidor VPN, no podemos escondernos de este servidor.
- **Red TOR**. La red TOR hace que nuestra actividad en internet pase por una red de diferentes nodos, donde cada nodo da un paso del descifrado de la comunicación antes de pasarla al siguiente nodo. El último nodo puede ver nuestra actividad (si no está cifrada extremo a extremo) pero, como ha pasado por nodos intermedios, no puede relacionarla con nosotros.

Cuando utilices estas técnicas para navegar anónimamente, piensa que no son infalibles. Por ejemplo, si mientras navegamos anónimamente entramos en nuestro correo electrónico, estamos revelando nuestra identidad al proveedor de este servicio que, a partir de ese momento, nos podrá rastrear. Tampoco podemos esconder en nuestro ISP que estamos utilizando estas tecnologías para navegar anónimamente.

DOCUMENTOS DE INTERÉS

- A survey on web tracking

Seguridad física de los móviles

Nuestro móvil se ha convertido en una herramienta indispensable para realizar todo tipo de tareas: comunicación y gestiones personales, entretenimiento y trabajo. Evitar que se produzcan accesos no autorizados a nuestro dispositivo, ya que las consecuencias pueden ser importantes. Por su naturaleza, la protección física de los móviles es una tarea compleja pero imprescindible.

RECOMENDACIONES

- No dejes tu dispositivo desatendido. Aunque sólo sea un minuto, es tiempo más que suficiente para que un ladrón oportunista te lo robe.
- Configura un corto tiempo para el bloqueo de la pantalla. Un tiempo de bloqueo largo (o no tener bloqueo) podría permitir su uso en caso de pérdida o robo.
- Use contraseña, PIN, patrón u otro método para desbloquear el dispositivo. A la hora de entrar el código de desbloqueo, vigila que nadie pueda verlo, particularmente si utilizas un patrón.
- Realiza una copia de seguridad de los datos importantes.
- Activa la funcionalidad de localización, bloqueo remoto y borrado del dispositivo en caso de pérdida.
- Borra los datos de forma segura antes de dar, vender o reciclar su teléfono.

NO SABES DÓNDE ESTÁ TU MÓVIL

Tanto Android como iPhone implementan un servicio para localizar tu móvil y manejarlo remotamente. Puedes acceder a través de:

Android. Web "Encuentra mi dispositivo". https://www.google.com/android/find

iPhone. Web Find My. https://support.apple.com/find-my

Estas herramientas permiten:

- Mostrar la ubicación aproximada del dispositivo en el mapa.
- Hacer sonar el teléfono, aunque esté en silencio.
- Bloquear el teléfono remotamente y mostrar un mensaje que facilite el retorno del teléfono si alguien lo encuentra.
- Borrar el dispositivo de forma permanente. Una vez borrado el dispositivo, estas funcionalidades dejarán de estar disponibles.

Hay que tener en cuenta que estas funcionalidades sólo estarán disponibles si el dispositivo tiene conexión a Internet.

Seguridad física de los móviles

DOCUMENTOS DE INTERÉS

- Mobile Device security: tips for IT pros

Manipulación de las personas

Internet, datos masivos (big data) e inteligencia artificial han sido grandes avances tecnológicos pero tienen algunos aspectos oscuros. La gran cantidad de información sobre nosotros, junto con la capacidad de analizarla y tomar decisiones de forma automática, nos hace susceptibles de intentos de manipulación.

FAKE NEWS

Las noticias falsas siempre han existido, pero es con las redes sociales que han proliferado. Las redes sociales permiten que cualquier persona se convierta en creadora de contenido (ya no nos limitamos a los medios tradicionales) y facilitan su distribución.

Las noticias falsas son un reflejo de la posverdad, que hace referencia a la situación en la que los hechos objetivos son menos relevantes a la hora de modelar a la opinión pública que las creencias y las emociones.

La proliferación de noticias falsas tiene efectos muy negativos: las personas carecen de información veraz, la desinformación afecta a la credibilidad de los medios tradicionales, pueden generar hostilidad contra grupos de personas vulnerables, etc.

Algunas recomendaciones para evitar caer en la trampa de las noticias falsas:

- Consulta las plataformas de verificación de hechos (fact-checking).
- Verifica si la fuente de la noticia es creíble. Si la fuente es desconocida, una búsqueda en internet puede decirnos si otras fuentes más reconocidas se hacen eco.
- Comprueba los enlaces y citas. En muchas ocasiones se incluyen enlaces y citas falsas para reforzar la credibilidad de la noticia.
- Si hay contenido gráfico, haz una búsqueda con la imagen para ver si se trata de una imagen modificada o sacada de contexto.

PERFIL DE LAS PERSONAS USUARIAS

El perfil de un usuario es un conjunto de información que nos indica cómo es ese usuario. Entre otra información, puede incluir localización, formación académica, información laboral, intereses, opiniones.

Nuestras interacciones en internet generan gran cantidad de información sobre nosotros (noticias que leemos, objetos que compramos, búsquedas que hacemos, mensajes que publicamos, las amistades que tenemos, etc.). El análisis de toda esa información permite la creación de perfiles muy detallados. Puede decirse que nos conocen mejor que nosotros mismos.

El perfil de usuario permite la personalización de los servicios que recibimos. Esta tarea la realizan los sistemas de recomendación, basándose en nuestro perfil: pueden recomendar libros, modificar los resultados de nuestras búsquedas, recomendar noticias, etc.

Mientras que muchas aplicaciones son beneficiosas para las personas usuarias, los malos usos de estos perfiles conllevan riesgos importantes. Por ejemplo, estos perfiles se pueden vender o se pueden utilizar en un contexto electoral para hacer publicidad personalizada (diciendo a cada potencial elector lo que quiere oír).

Manipulación de las personas

FILTRO BURBUJA

El conocido filtro burbuja resulta de una aplicación demasiado estricta de la personalización. El algoritmo restringe demasiado la información que se presenta al usuario según su perfil y da una visión muy limitada de la realidad.
En algunos casos, el filtro burbuja puede tener efectos muy perniciosos. Por ejemplo, si sólo nos muestran las noticias que son afines a nuestra forma de pensar, podemos acabar creyendo que la realidad es así.

DEEP FAKES

El desarrollo de la IA permite cosas que hace unos años habrían sido impensables. Permite, por ejemplo, que una máquina lea un texto con la voz de una persona concreta. Pero no sólo eso: también permite modificar los rasgos faciales de una persona, para simular que está diciendo algo concreto. De esta forma tenemos los hipertrucajes (deep fakes).

DOCUMENTOS DE INTERÉS

- ¿Qué son las fake news?
- ¿Burbujas de filtro? Hacia una fenomenología algorítmica
- What are deep fakes and how are they created?

Compra por internet

En sus inicios, el comercio online provocaba una fuerte desconfianza, sobre todo a la hora de realizar los pagos. Esto se ha superado en la última década y con la pandemia las compras online han marcado un hito. Ahora bien, ¿cuál es la seguridad real que ofrece el comercio en línea?

TIENDA DE CONFIANZA

- Compra en tiendas de confianza. Éste es un punto realmente importante, sobre todo porque en tiendas foráneas reclamar puede ser bastante más complicado.
- Si no conoces la tienda, la evaluación realizada por otros clientes o los sellos de confianza pueden ayudarte a decidir.
- Vigila si la oferta es demasiado buena. En especial, si te ha llegado a través de un correo electrónico no solicitado.
- En la URL phishing se crea una web falsa que simula una auténtica. La forma de acceder a esta web suele ser un enlace en un correo no solicitado. Muchas veces, la dirección de la tienda falsa se asemeja a la auténtica, pero tiene alguna diferencia.

SEGURIDAD DE LOS DATOS

- Si creas una cuenta, asegúrate de que está bien protegida. Si un atacante consigue entrar, el impacto puede ser elevado, incluso económicamente, si tu cuenta guarda los datos de pago. Use una contraseña fuerte y no la reutilices.

- La tarjeta es el sistema más habitual de pago online. La seguridad depende del sistema utilizado:
    - Las pasarelas de pago son más seguras, porque la tienda te redirige a la web de un banco a la hora de realizar el pago. Así, evita gestionar datos bancarios.
    - Si no se utiliza pasarela de pago, la seguridad de tus datos es responsabilidad de la tienda.

SEGURIDAD DE EQUIPOS Y COMUNICACIONES

Una vez tenemos localizado un sitio de confianza, es necesario que la compra se haga con las mejores garantías de seguridad, tanto para el dispositivo utilizado como para las comunicaciones.

- Mantén el equipo en buen estado de seguridad: ten el sistema operativo y las aplicaciones actualizadas, protege tu cuenta con algún sistema de autenticación, utiliza software antivirus, evita descargar aplicaciones de sitios no confiables, etc.
- No hagas compras desde dispositivos ajenos, ya que no conoces su estado de seguridad.
- Realiza tus compras desde una conexión a internet confiable. Precaución con las wifi públicas, porque tus datos podrían ser interceptados. En casa, la wifi cifrada y con contraseña fuerte.
- Verifica que la tienda utiliza el protocolo https. El navegador lo indica con un icono de un candado cerrado.

EN CASO DE DUDA

En caso de duda, es mejor posponer la compra.

Compra por internet

HECHA LA COMPRA

- Los productos comprados en línea tienen las mismas garantías que los comprados presencialmente.
- Salvo algunos productos, tienes 14 días para desistir de la compra.
- Recuerda que tienes derechos sobre sus datos personales: acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de datos y no ser objeto de decisiones automatizadas.

DOCUMENTOS DE INTERÉS

- Compras y contratos por internet


apdcat
Autoritat Catalana de Protecció de Dades