Protección de datos: Guía para particulares y familias

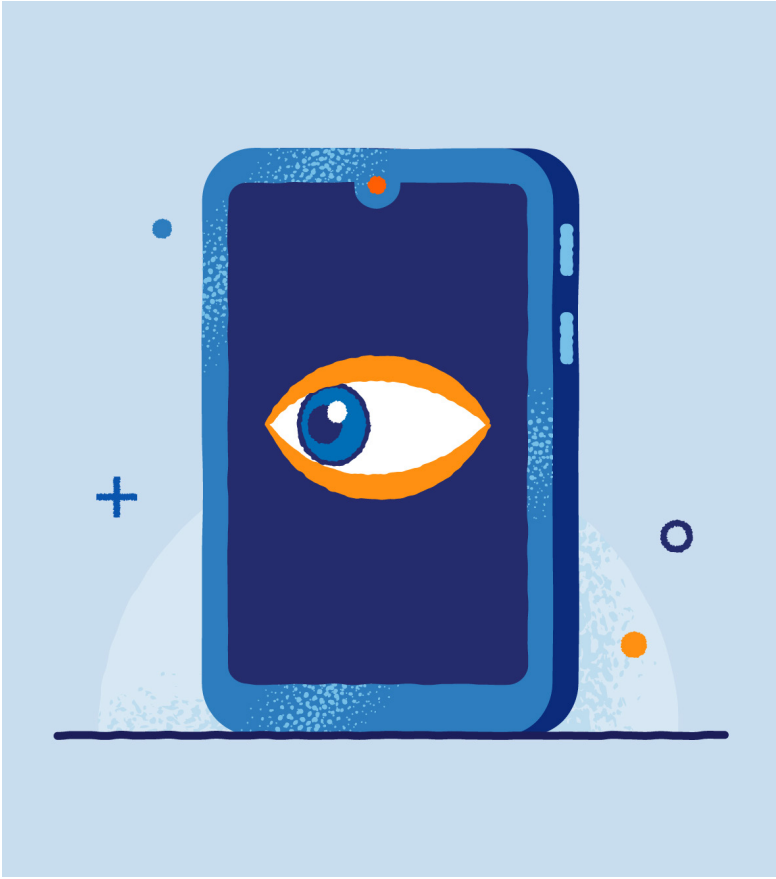
Protege tu información online y protege tu huella digital.

panda

Índice de contenidos

01.
Aspectos básicos de la privacidad de datos

En la era digital, la privacidad de datos se ha convertido en un protagonista anónimo. Es la figura misteriosa que acecha detrás de cada correo electrónico enviado, cada transacción realizada y cada sitio visitado. Sin embargo, para muchos, la privacidad de los datos es un concepto extraño que a menudo se pasa por alto hasta que es demasiado tarde.
La privacidad de los datos consiste en mantener segura tu información personal. Las empresas, gobiernos y ciberdelincuentes buscan esta información por diversas razones, por lo que es vital entender cómo mantener los datos protegidos.
Por suerte, este completo libro electrónico sobre la privacidad de los datos proporciona la información que necesitas para reclamar el control de tu huella digital.



¿Qué es la privacidad de datos?

Privacidad de datos es el control que un individuo u organización tiene sobre la información sensible almacenada o recopilada sobre ellos. Es la capacidad de determinar quién tiene acceso a estos datos, cómo se utilizan y las salvaguardias existentes para protegerlos de una exposición no autorizada..

Los datos personales asociados a la privacidad de datos incluyen información sensible como nombres, direcciones, números de la Seguridad Social así como datos financieros. También se extiende a datos menos abiertamente personales, como el historial de navegación, los datos de localización, las direcciones IP y las compras online. Además, puede abarcar datos biométricos, historiales médicos y datos laborales.

El concepto de privacidad de los datos se remonta a los primeros tiempos de la informática, cuando la información personal se almacenaba electrónicamente para diversos fines. A medida que se expandía el panorama digital, aumentó rápidamente la preocupación por el uso indebido de los datos y las violaciones de la privacidad.
La evolución de las redes sociales agravó aún más estas preocupaciones. Con usuarios que comparten libremente información personal en plataformas como Facebook y Twitter, la cantidad de datos que se generan ha alcanzado niveles sin precedentes.

Por qué es importante la privacidad de datos

Con la tecnología avanzando a una velocidad vertiginosa, la importancia de la protección y privacidad de datos ya no es opcional: es un requisito. La privacidad de datos depende de que las personas puedan controlar su huella digital.

Cada vez que nos conectamos a Internet, generamos una gran cantidad de datos. Desde los simples "me gusta" en las redes sociales hasta nuestros hábitos de compra, estos datos aparentemente insignificantes dibujan una imagen vívida de quiénes somos. Cuando estos datos privados acaban en las manos equivocadas, las repercusiones pueden incluir:

Robo de identidad

Los datos personales pueden caer en las manos equivocadas, lo que puede conducir al fraude de identidad, en el que las personas pueden enfrentarse a transacciones no autorizadas o actividades delictivas realizadas en su nombre.

Fraude financiero

Con acceso a información financiera sensible, los ciberdelincuentes podrían llevar a cabo transacciones fraudulentas, provocando graves pérdidas monetarias.

Repercusiones legales

Sin la adherencia a las leyes y regulaciones de privacidad de datos, las empresas podrían enfrentarse a fuertes multas y acciones legales, dañando su reputación y sus finanzas.

Falta de confianza

Las empresas podrían perder la confianza de sus clientes, lo que afectaría a su fidelidad y provocaría pérdidas comerciales.

Aumento de la ciberdelincuencia

El riesgo de ciberataques podría aumentar a medida que los piratas informáticos puedan acceder fácilmente a datos más valiosos.

Pérdida de privacidad

Sin privacidad de datos, nuestra vida personal podría convertirse en un libro abierto accesible a cualquiera.

Manipulacion y explotación

Los datos podrían utilizarse para manipular comportamientos y decisiones, a menudo sin el conocimiento o consentimiento de la persona.

Protección de datos vs. Privcidad de datos vs. Seguridad de datos

Protección de datos, privacidad de datos y seguridad de datos son tres conceptos entrelazados pero distintos en el mundo de los datos digitales..

En resumen, la protección de datos, la privacidad de datos y la seguridad de datos funcionan en armonía. Cada una tiene una función distinta, pero juntas crean un entorno digital seguro.

02.
Información personal y sensible

En el extenso panorama de la privacidad de datos, entender la distinción entre información personal e información personal sensible es crucial para el cumplimiento legal, la gestión de riesgos y las consideraciones éticas. Esta distinción informa sobre las prácticas de tratamiento de datos, orienta las medidas de seguridad y ayuda a minimizar el daño potencial a las personas en caso de que los datos se vean comprometidos.

Esta sección explica en detalle la clasificación de los datos y cómo salvaguardar los detalles más íntimos de tu identidad digital.

¿Qué es la información personal?

La información personal, a menudo denominada datos personales, es cualquier información que pueda utilizarse para identificar a una persona concreta. Abarca una amplia gama de datos que pueden vincularse a una persona concreta. Dependiendo del contexto, puede contener nombres, direcciones, números de teléfono y mucho más.

Cómo controlar tu información personal

Para controlar eficazmente tu información personal, es esencial adoptar medidas proactivas que mejoren tu privacidad y seguridad en línea. Veamos algunos consejos importantes a tener en cuenta .

Limita la exposición en RRSS

Revisa y ajusta tu configuración de privacidad en tus redes sociales para controlar quién puede ver tus publicaciones e información personal.

Piensa antes de publicar

Antes de compartir datos personales en Internet, considera las posibles consecuencias y si es necesario revelar esa información.

lee las políticas de privacidad

Tómate tu tiempo para leer y comprender las políticas de privacidad de los sitios web y las aplicaciones que utilizas para saber cómo se recopilan, almacenan y comparten tus datos.

No aceptes la recopilación de datos

Siempre que sea posible, evita la recopilación de datos y elige servicios que sólo te pidan la información esencial.

¿Qué es la información personal sensible?

La información personal sensible es una categoría de información personal que se considera más crítica y requiere mayores niveles de protección. Incluye detalles que, de salir a la luz, podrían acarrear graves consecuencias como el robo de identidad, el ciberacoso o la discriminación.

Cómo controlar tu información personal sensible

Hoy en día, controlar la información personal confidencial es más importante que nunca. Con el aumento de las violaciones de datos y otras ciberamenazas, es esencial tomar medidas proactivas para salvaguardar estos valiosos datos.

Presentar un formulario de solicitud de acceso del interesado (DSAR)

- **Conoce tus derechos:** En virtud del Reglamento General de Protección de Datos (RGPD), tienes derecho a preguntar a una organización si está tratando o no tus datos..
- **Accede a la información:** Una solicitud de acceso del interesado (DSAR) te permite acceder a la información almacenada sobre ti y comprender su uso.
- **Exigir la rectificación:** Exige la rectificación de datos incorrectos o su supresión; las empresas están obligadas a cumplir en el plazo de un mes natural para el GDPR y de 45 días para la Ley de Privacidad del Consumidor de California (CCPA).

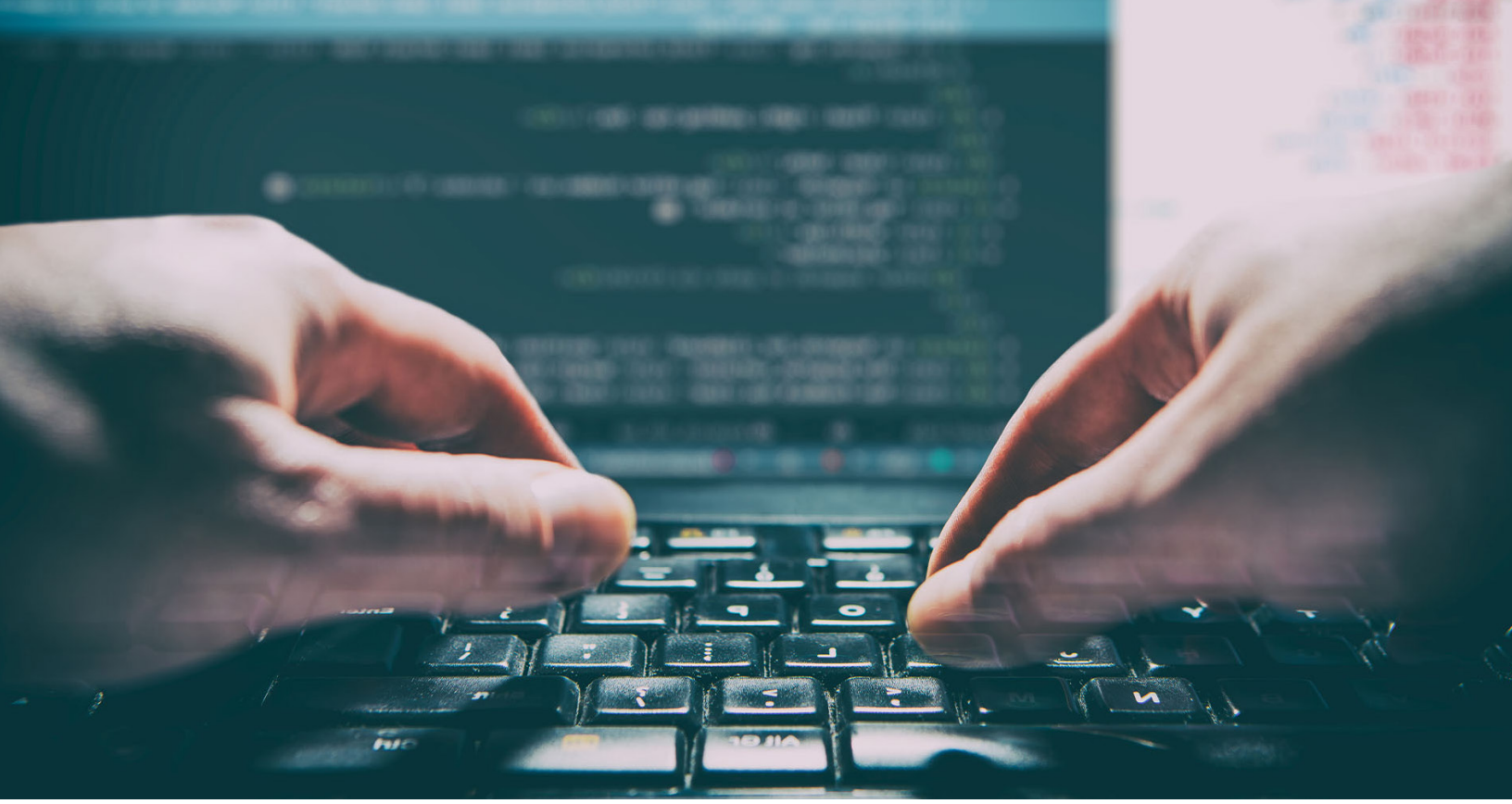
Utilizar los enlaces “No vender ni compartir mis datos personales

- **Compruebe los sitios web de las empresas:** Busca opciones ampliadas como “No vender ni compartir mi información” en virtud de la Ley de Derechos de Privacidad de California (CPRA) en las páginas de inicio y las páginas de política de privacidad de los sitios web de las empresass.
- **No participar:** Rechaza que tu información personal o sensible se venda o comparta con terceros; las empresas están legalmente obligadas a cumplir esta obligación.

Exclusión de la recopilación en sitios web o navegadores

- **Realiza una búsqueda online:** Realice una búsqueda online de tu nombre para encontrar sitios web de intermediarios de datos como Radaris, Pipl, Spokeo y Whitepages que incluyan tu información.
- **Solicita la eliminación de tus datos:** Visita las páginas de exclusión voluntaria de estas plataformas o envía una solicitud por correo electrónico para que eliminen tus datos.
- **Utiliza recursos:** Utiliza recursos como Privacy Rights Clearinghouse para obtener un directorio completo de sitios web y sus opciones de exclusión.
- **Revisa las políticas de privacidad:** Revisa las políticas de privacidad de tus instituciones financieras para excluirte del intercambio de datos con intermediarios.

03.
¿Qué es una filtración de datos?



Probablemente hayas oído hablar de empresas que han sufrido filtraciones masivas de datos y hayas pensado: “¿Cómo ha ocurrido?” o “¿Y si yo me hubiera visto afectado?”. Una filtración de datos puede asustar, y también puede tener consecuencias graves como el fraude con tarjetas de pago o incluso el robo de identidad.
A continuación te explicamos cómo pueden afectarte las filtraciones de datos, cómo se producen y cómo prevenirlas

¿Qué es una fuga de datos?

Una filtración de datos es un incidente de seguridad en el que alguien expone o roba información privada, confidencial o sensible sin autorización. Ocurren por varias razones, desde errores humanos a ataques maliciosos, y las consecuencias pueden ser importantes. Cualquiera corre el riesgo de sufrir una violación de datos, especialmente si sus cuentas no están protegidas.

Las filtraciones de datos pueden dar lugar a:

- **Robo de credenciales**
  Ejemplo: Los hackers accedieron sin autorización a una base de datos que contenía los nombres de usuario y las contraseñas de los usuarios de una plataforma de redes sociales, lo que condujo a la toma generalizada de cuentas y al uso indebido de información personal.

- **Robo de identidad**
  Ejemplo: Un ciberdelincuente utilizó información personal robada, como números de la Seguridad Social y direcciones, para solicitar fraudulentamente préstamos y tarjetas de crédito a nombre de las víctimas, causando daños financieros y problemas relacionados con la identidad.

- **Activos compormetidos**
  Ejemplo: Un malware infectó la red de una empresa, permitiendo a los atacantes controlar sistemas críticos y datos sensibles, interrumpiendo las operaciones y causando importantes pérdidas financieras.

- **Fraude con tarjetas de pago**
  Ejemplo: Un ciberataque atacó el sistema de procesamiento de pagos de un minorista en línea, lo que provocó el robo de la información de las tarjetas de crédito de los clientes, que luego se utilizó para realizar compras no autorizadas.

- **Acceso de terceros a cuentas**
  Ejemplo: Un proveedor de servicios en la nube sufrió una filtración de datos, lo que permitió a terceros no autorizados acceder a archivos e información confidenciales almacenados por sus clientes, lo que dio lugar a posibles fugas de datos y violaciones de la privacidad.

¿Cómo se producen?

Las filtraciones de datos pueden ser un tipo de ciberdelincuencia si se hacen de forma malintencionada, pero también pueden ser un error involuntario de alguien con acceso autorizado a los datos. Las causas de las violaciones de datos incluyen:

Personas internas con malas intenciones

Las personas con acceso a la base de datos abusan intencionadamente de sus privilegios de acceso para robar o filtrar información sensible.

Personas externas con mala intención

Alguien ajeno a la organización ataca una base de datos mediante phishing, malware, ataques a vulnerabilidades o ataques de denegación de servicio (DoS).

Personas internas accidentalmente

Personas con acceso autorizado exponen accidentalmente datos debido a errores o falta de medidas de seguridad. Esto se clasifica técnicamente como una fuga de datos, ya que es un error interno; sin embargo, sigue teniendo las mismas consecuencias para los afectados, y la empresa todavía puede enfrentarse a ramificaciones legales..

Fases de una filtración de datos

A diferencia de lo que pueda suponer tu imaginación, una violación de datos malintencionada no se parece tanto a alguien vestido de negro que se cuela en un edificio con una memoria USB como a personas en una ubicación remota maquinando cómo piratear una base de datos.

Sin embargo, no todas las violaciones de datos son malintencionadas. Algunas son el resultado de un error humano o de una negligencia, pero eso lo veremos más adelante. He aquí las tres etapas de una violación de datos intencionada.

1. Investigación

Al principio de una operación de filtración de datos, el atacante elige un objetivo -normalmente una empresa u organización con acceso a datos personales- e investiga cómo puede infiltrarse en la base de datos de su objetivo.

El atacante recopila detalles como información sobre los empleados, registros financieros y presupuestos de seguridad. También busca vulnerabilidades como contraseñas débiles, software obsoleto o conexiones de red desprotegidas.

2. Ataque

Tomando lo que ha aprendido de su investigación, el hacker puede ahora atacar el sistema de datos. Estas son algunas de las formas más comunes en que los atacantes acceden a los sistemas o redes de la empresa:

- **Robo de credenciales:**
  Pueden recopilar nombres de usuario y contraseñas comprometidos a través de la Dark Web, phishing, ataques de fuerza bruta o incluso el robo físico de dispositivos para hacerse pasar por usuarios legítimos y obtener acceso a los sistemas.

- **Correos electrónicos de phishing**
  Los atacantes también utilizan información personal de sus investigaciones, como puestos de trabajo o nombres de compañeros de trabajo, para engañar a sus objetivos para que proporcionen credenciales o hagan clic en un enlace malicioso que descarga malware en su ordenador.

- **Malware**
  Los hackers utilizan software malicioso para infectar secretamente y tomar el control del ordenador o la red de la víctima para robar datos.

- **Explotación de vulnerabilidades**
  El atacante utiliza vulnerabilidades como contraseñas débiles, configuraciones erróneas o sistemas sin parches encontrados en el sistema informático de una empresa para obtener acceso.

- **Ataques de denegación de servicio (DoS)**
  Este ataque abruma un sitio web con excesivo tráfico falso hasta que queda inaccesible para los usuarios reales. Es una distracción de otras debilidades de seguridad para que los atacantes puedan llevar a cabo violaciones de datos.

3. Extraer datos

Una vez que los atacantes han obtenido acceso al sistema o red del objetivo, pueden localizar y extraer datos valiosos o sensibles, incluyendo información personal, registros financieros o cualquier otro dato que puedan vender en la Dark Web.

A continuación, los datos extraídos se copian o transfieren a los propios servidores del atacante, donde pueden controlarlos y explotarlos. A menudo, una empresa no sabrá que sus datos han sido robados hasta que un tercero, como las fuerzas de seguridad, los proveedores de servicios o los clientes, denuncie la filtración.

04.
Cómo protegerte a ti mismo y tu información

Panda Dome dispone de un plan de protección para cualquier estilo de vida, para que puedas navegar sin preocupaciones.

Seguridad en la red

La seguridad en la red implica la implementación de medidas para proteger los equipos informáticos de accesos no autorizados, ciberataques y violaciones de datos. Esto incluye asegurar la infraestructura de red, monitorizar el tráfico e implementar protocolos de encriptación robustos.

Utiliza con seguridad las redes Wi-Fi públicas

Ten cuidado al conectarte a redes Wi-Fi públicas para evitar el acceso no autorizado a datos confidenciales.

Utiliza una VPN

Mejora la privacidad y la seguridad online cifrando el tráfico de Internet cuando accedas a redes públicas.

Instala un cortafuegos

Implementa una barrera contra el acceso no autorizado a tu red, proporcionando una capa adicional de defensa contra las ciberamenazas.

Autenticación y control de acceso

La autenticación y el control de acceso son componentes esenciales de la privacidad de datos, ya que garantizan que sólo las personas o sistemas autorizados pueden acceder a datos o recursos sensibles. Estas medidas verifican la identidad de los usuarios y aplican restricciones a sus acciones dentro de una red o sistema.

- **Elige contraseñas seguras y únicas**
  Refuerza la seguridad de las cuentas creando contraseñas complejas que sean únicas para cada cuenta para mitigar el riesgo de acceso no autorizado.

- **Establece un doble factor de autenticación**
  Añade una capa adicional de seguridad exigiendo una forma secundaria de verificación, como un código enviado a un dispositivo de confianza, además de una contraseña.

- **Supervisa la información de la cuenta**
  Revisa regularmente la actividad de la cuenta para detectar comportamientos sospechosos o intentos de acceso no autorizados. Informa inmediatamente de cualquier actividad sospechosa o intento de acceso no autorizado a las autoridades o proveedores de servicios pertinentes.

- **No compartas nunca los códigos que recibas por mensaje de texto o email**
  Evita compartir los códigos de verificación recibidos a través de texto o correo electrónico, ya que podrían ser interceptados por atacantes que intenten un acceso no autorizado.

Protección y recuperación de datos

La protección y recuperación de datos se refiere a las estrategias y tecnologías utilizadas para salvaguardar y restaurar los datos en caso de borrado accidental, corrupción o ciberataques. Implica implantar soluciones de copia de seguridad, cifrado y planes de recuperación en caso de catástrofe para garantizar la integridad y disponibilidad de los datos.

Haz copias de seguridad de tus datos

Protégete contra la pérdida de datos debida a ciberataques o fallos de hardware haciendo copias de seguridad periódicas de los archivos y documentos importantes.

Instala software antivirus

Protégete contra el malware y otras ciberamenazas instalando software antivirus de confianza para detectar y eliminar software malicioso de tus dispositivos.

Conocimientos generales sobre ciberseguridad

Es importante conocer los principales y comunes signos de piratería informática para poder actuar lo antes posible y recuperar tus cuentas.

Estas son algunas señales de advertencia de que es posible que te hayan hackeado:

- El uso de Internet del dispositivo aumenta drásticamente
- La velocidad de funcionamiento del dispositivo disminuye
- La batería se agota rápidamente sin explicación
- Recibes solicitudes no autorizadas para cambiar contraseñas
- Se descargan automáticamente nuevos programas o aplicaciones

05.
Preguntas frecuentas sobre la privacidad de datos

En esta sección respondemos algunas de las preguntas más frecuentes sobre la privacidad de datos

¿Cuál es la finalidad de la Ley de privacidad de datos?

La finalidad de la Ley de Protección de Datos es salvaguardar la información personal de las personas regulando su recogida, tratamiento y almacenamiento, fomentando así la transparencia y la protección de datos.

¿Cuáles son los 4 tipos de privacidad de datos?

Los cuatro tipos de privacidad de datos corresponden a distintos niveles de acceso y sensibilidad:

Privacidad de datos pública

Pertenece a la información destinada al consumo público, como la información general de contacto de la empresa, y generalmente no requiere una protección estricta de la privacidad.

Privacidad de datos interna

Se refiere a datos accesibles sólo dentro de la empresa y suele requerir medidas de protección para evitar el acceso no autorizado por parte de terceros.

Privacidad de datos confidenciales

Se refiere a información sensible que requiere medidas de privacidad reforzadas para restringir el acceso a personas autorizadas dentro de la organizaciónindividuals within the organization.

Privacidad de datos restringida

Se refiere a datos altamente sensibles sujetos a estrictos controles de privacidad, que a menudo requieren permisos especiales de acceso y manejo para minimizar el riesgo de exposición no autorizada o uso indebido.

¿Qué se consideran datos de privacidad?

Los datos de privacidad, también conocidos como información de identificación personal (IIP), abarcan cualquier información que pueda identificar directa o indirectamente a una persona. Esto incluye detalles básicos de identidad como el nombre y la fecha de nacimiento, información de contacto como direcciones de correo electrónico y números de teléfono, datos financieros como números de tarjetas de crédito e información sensible como historiales médicos.