



Socialización

Derechos y deberes de tratamiento de datos personales

Oficial de seguridad de la información / Bogotá D.E. / 14-12-2024





Tratamiento de datos personales

Conozca los derechos de pacientes y deberes de tratamiento en el INC

Ley 1581 de 2012

¿Qué es la protección de datos personales?



La protección de datos personales (habeas data) es un derecho fundamental (derecho humano) que otorga al ciudadano la facultad de controlar sus datos personales y la capacidad para decidir y disponer de éstos.

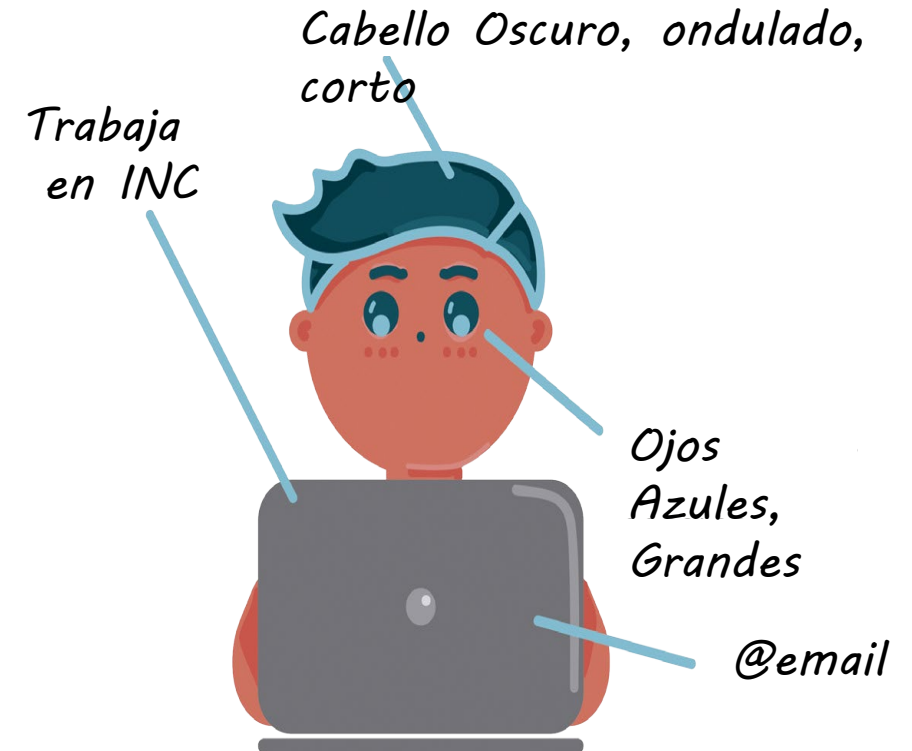
El tratamiento de datos hace referencia a cualquier operación o procedimiento técnico, sea o no automatizada que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. El tratamiento de datos esta regulado bajo los Art. 3, 4 y 6 de la **Ley 1581 de 2012**.

¿Qué es el dato personal?

Dato personal se refiere a cualquier tipo de información vinculada a una persona que puede utilizarse para identificar, directa o indirectamente a esa persona.

Es información muy valiosa para las empresas y el Estado: necesidad, valor económico.

La recogida y el tratamiento de datos personales es necesario para realizar cualquier actividad: buscar empleo, abrir una cuenta bancaria, pagar con tarjeta de crédito, comprar un vuelo, reservar un hotel, pedir una cita y recibir atención médica, etc.



¿Cómo identificar un dato personal?

Un **dato de carácter personal** es cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables y pueda ser relativa entre otras a:

❑ Su identidad

Nombre y apellidos, domicilio, filiación, una fotografía o video, etc.

❑ Sus ocupaciones

Estudios, trabajo, historial de actividades, etc.

❑ Su Patrimonio

Ingresos y egresos, cuentas bancarias, consumos, información fiscal, etc.

❑ Su Formación

Estudios, trayectoria, títulos, certificados etc.

❑ Su Salud

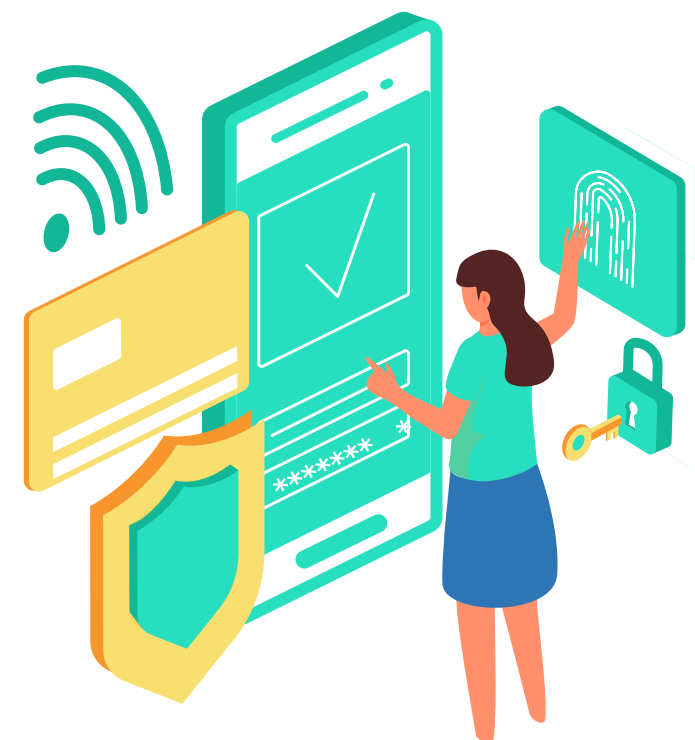
Estado de salud, historia clínica, enfermedades físicas o psicológicas, etc.

❑ Sus Características

Tipo de sangre, ADN, discapacidades, raza, peso, etc.

❑ Su vida y Hábitos

Sexuales, políticos, ideológicos, creencias, etc.



Ámbito de Aplicación de tratamiento de datos



Tratamiento efectuado en **territorio colombiano** o cuando al responsable o encargado del tratamiento no establecido en territorio colombiano le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Excepciones de aplicación:

- ☐ Ámbito exclusivamente **personal o doméstico**.
- ☐ Bases de datos y archivos que tengan por finalidad la **seguridad y defensa nacional**, así como la prevención, detección, **monitoreo y control del lavado de activos y el financiamiento del terrorismo**.
- ☐ Bases de datos que tengan como fin y contengan información de **inteligencia y contrainteligencia**.
- ☐ Bases de datos y archivos de **información periodística** y otros contenidos editoriales.
- ☐ Bases de datos y archivos regulados por la Ley 79 de 1993 (**Censos de Población y Vivienda**).
- ☐ Bases de datos y archivos regulados por la Ley 1266 de 2008 (**Habeas Data Financiero**).

Categorías de datos personales



Dato público: El dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión oficio o calidad de servidor público.

Dato privado: El dato que por su naturaleza íntima o reservada sólo es relevante para el titular del dato

Dato semiprivado: El dato que no tenga naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación pueda interesar no sólo al titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero o crediticio de actividad comercial o de servicios (Ley 1266 de 2008).

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Ejemplos de Categorías de datos personales



Público

Entre otros, los que están en los registros públicos, documentos públicos, gacetas, boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.



Semiprivado

Bases de datos que contengan información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.



Privado

Datos telefónicos, electrónicos, laborales, sobre infracciones administrativas o penales, información de entidades financieras, gestoras y servicios comunes de la seguridad social. Bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, base de datos de operadores de servicios de comunicación electrónica.



Sensibles

Datos de salud, historia clínica, ideología, afiliación sindical, creencias, religión, origen racial o étnico, vida sexual, datos biométricos, datos derivados de la violencia de género y en general cualquier tipo de dato que pueda ser causal de discriminación.

Derechos de tratamiento de datos personales

1. Conocer

El titular de la información puede solicitar y acceder a sus datos personales recopilados en el instituto y recibir información respecto del su uso y finalidades a través de los responsables o encargados de tratamiento en el INC.

2. Verificar

El titular de la información tiene derecho de solicitar la actualización y rectificación de información frente a los datos inexactos, incompletos o fraccionados, como aquellos que induzcan a error, con excepción de las condiciones clínicas del paciente, diagnósticos y opiniones de la historia clínica

3. Revocar y/o suprimir

El titular de la información puede revocar la autorización y/o solicitar la supresión de sus datos personales para que dejen de ser tratados, sin que con su ejercicio se haga imposible la prestación de la atención, o se repudien deberes legales o contractuales del titular con el INC.

4. Tratamiento

El Titular de la información o familiares pueden solicitar tratamiento de datos personales mediante la presentación de una solicitud por medio del envío de un correo electrónico a la dirección pqrs@cancer.gov.co, o radicando una comunicación escrita en la ventanilla de correspondencia .

5. Respuesta: A partir de la recepción de la solicitud de tratamiento de datos personales, el Instituto tiene 10 días hábiles para dar respuesta, prorrogable por un término máximo de (5) días hábiles. Si vencido el término, el Instituto no elimina los datos, el Titular podrá solicitar una reclamación ante la SIC.



Deberes de tratamiento de datos personales



1. Conservar

Solicitar y conservar, en las condiciones previstas por la ley, copia de la respectiva autorización otorgada por el Titular de los datos personales.

2. Informar

Informar debidamente al titular de la información sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada y publicada en la presente política para garantizar la protección de datos personales.

3. Respetar

Exigir a los operadores, proveedores y a terceros, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

4. Reportar

Reportar inmediatamente a los responsables o encargados de tratamiento de datos personales, cuando se observe tratamiento indebido o no autorizado de datos personales, o se presente una fuga o pérdida de información.

5. Comunicar

Comunicar a los operadores del tratamiento a su cargo o bajo su responsabilidad, cuando determinada información se encuentra en discusión o controversia, o se presente una reclamación.

6. Operar seguro

Garantizar efectivamente los derechos de los titulares de la información. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella, y tomar las medidas necesarias para darles cumplimiento. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado.

7. Transferir

Cuando las bases de datos o archivos vayan a ser suministrados a terceros deberá, de manera previa, informar al titular y solicitar su autorización conforme lo establece la política de manejo de datos personales.

Procedimiento de acceso a consulta de datos del titular

El Titular de los datos personales puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido al INSTITUTO NACIONAL DE CANCEROLOGÍA, enviado, mediante correo electrónico a pqrs@cancer.gov.co, indicando en el asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a CALLE 1 # 9 - 85 Bogotá, Distrito Capital - Colombia.

Una vez recibida la solicitud, INSTITUTO NACIONAL DE CANCEROLOGÍA resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.



Adopción de LEPD en el INC

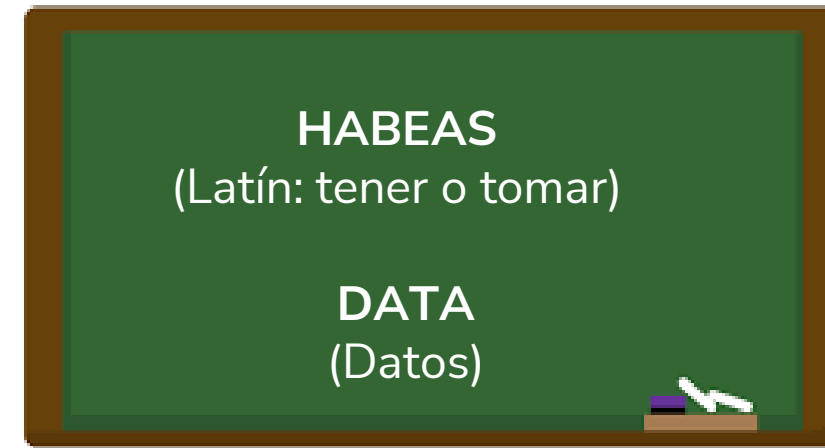
La adaptación a la LEPD consiste en ajustar en el instituto las disposiciones de dicha Ley y de las normas que la desarrollan en la operación del INC

Tiene 3 pilares:

Jurídico: cumplimiento de las disposiciones legales y aportación de toda la documentación jurídica necesaria.

Administrativo: procedimientos, capacitación de usuarios, nombramiento de encargado de la recepción de peticiones y solicitudes, nombramiento de responsable de seguridad.

Técnico: implementación y cumplimiento de las medidas y controles de seguridad, Mantenimiento mensual y Anual.



Pilar Jurídico de protección de datos



Ley estatutaria 1581 de 2012 –Ley de protección de datos (**LEPD**) mediante la cual se regula el derecho fundamental de habeas data con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y privada, y establece las excepciones de tratamiento de datos .

- **Decreto reglamentario 1377 de 2013** por el cual se reglamenta parcialmente la ley 1581 de 2012, establece los lineamientos para: la política de tratamiento de información , avisos de privacidad, reglas de transferencia y transmisiones de datos personales, la autorización para el tratamiento de datos , y solicita proveer una descripción de los procedimientos usados para el tratamiento, y descripción de las finalidades para las cual la información es recolectada .Finalmente establece que las entidades deben poder demostrar su responsabilidad de cumplimiento de la ley 1581.
- **Decreto 090 de 2018 -SIC.** Modifica El decreto único 1074 de 2015, para incluir la obligación de inscripción en el registro nacional de bases de datos (RNBD) a las personas jurídicas de naturaleza publica
- **Circular externa 003 de 1 de agosto de 2018,** instructivo para el diligenciamiento del RNBD
- **Circular externa conjunta 04 de 2019 –Procuraduría y SIC.** Aclara que que la interoperabilidad se rige por la ley 1581 de 2012, y que las entidades publicas o administrativas no requieren la autorización de la persona para tratar datos personales cuando la información se necesita para el ejercicio de sus funciones.
- **Resolución 1409 de 2002 – Minsalud** Establece lineamientos para el Tratamiento de datos personales para segundo uso o distintos de aquellos para los que los datos fueron recopilados originalmente, y la utilización de datos de sistema integrado de información de la protección Social SISPRO, con fines históricos, estadísticos y científicos.

Pilar Administrativo de protección de datos



Pecados de las Plataformas web
al solicitar la autorización
**para el tratamiento de datos
sin los requisitos de ley**

Solicitar la autorización para el tratamiento de datos personales sin los llenos de los requisitos, puede generar sanciones por parte de la SIC.

La autorización debe contar por lo mínimo, con los siguientes elementos:

- Finalidad del uso de sus datos.
- El tratamiento de los datos.
- El responsable de la información.
- Los derechos que le asisten al titular al momento de suministrar sus datos.
- Donde consultar la política de tratamiento de información.

Autorización de los Titulares de datos personales

Conforme a lo señalado en la circular conjunta 04 de 2019 de la Superintendencia de industria y Comercio (SIC) y la Agencia Nacional de Defensa Jurídica del Estado, el INSTITUTO NACIONAL DE CANCEROLOGIA realiza el tratamiento de datos personales en ejercicio propio de sus funciones y para el efecto **no requiere la autorización previa, expresa e informada del Titular.**

Sin embargo, cuando no corresponda a sus funciones la entidad deberá obtener la autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos o físicos. Así mismo se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus datos personales.

Pilar Técnico de protección de datos

Autenticación fuerte: Para proteger los sistemas del instituto contra el acceso no autorizado, el instituto utiliza una combinación de autenticación multifactorial, autorización basada en roles, integración con servicios de autenticación de dominio, y sistemas de autenticación fuerte

Acceso a la red de cero confianza (ZTNA): El Instituto utiliza un enfoque ZTNA para autenticar, autorizar y perfilar a los usuarios y dispositivos de manera granular antes de permitirles acceder a recursos de red que sean necesarios para desempeñar sus funciones.

Menor Privilegio: Los usuarios y dispositivos en el instituto solo tienen acceso a los recursos y datos necesarios para llevar a cabo sus funciones, evitando privilegios innecesarios.

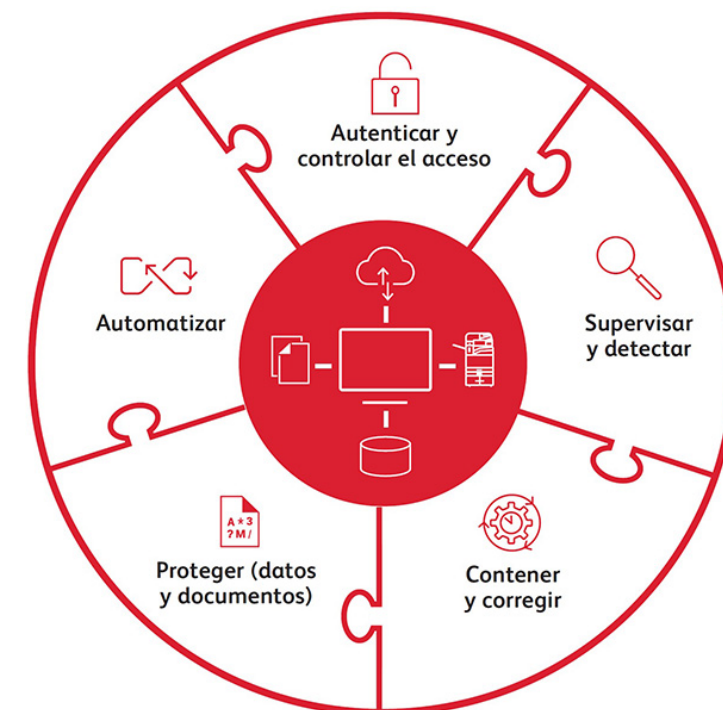
Segmentación de redes: El Instituto segmenta su red en zonas de seguridad para limitar el acceso a los sistemas y datos confidenciales, y limitar el impacto de posibles ataques cibernéticos. Los recursos críticos se aíslan y protegen, minimizando la exposición a amenazas potenciales, y el desplazamiento lateral de amenazas.

Protección de Datos: Los datos sensibles en reposo o en tránsito del instituto se cifran para protegerlos contra accesos no autorizados

Telemetría continua: El instituto analiza múltiples fuentes de datos de telemetría, salud y capacidad, para identificar patrones y relaciones que podrían indicar una amenaza, fallo, o un riesgo potencial.

Inteligencia de amenazas automatizada: El instituto utiliza técnicas y herramientas basadas aprendizaje automático, inteligencia artificial y correlación de riesgo para identificar, detectar y analizar, proteger y automatizar la respuesta ante amenazas cibernéticas, y desplegar capacidades de recuperación efectiva ante ciber-incidentes.

Estrategia de Ciberseguridad Confianza Cero



Glosario LEPD

Base de Datos: Conjunto organizado de datos personales en físico o digital.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Usuario: Cualquier persona que acceda o haga uso de las bases de datos.



Gracias por su atención



@incancerologia



Instituto Nacional de Cancerología

www.cancer.gov.co