



# POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

## Centro Integral de Rehabilitación Colombia – CIREC

**Versión:** Documento integrado con observaciones y recomendaciones

**Estado:** Versión final para revisión institucional

**Entidad:** CIREC · NIT 860.066.767-4

### Propósito del documento

Establecer los lineamientos, principios, finalidades, responsabilidades y procedimientos para el tratamiento de los datos personales administrados por CIREC, incluidos los datos sensibles, garantizando el derecho fundamental al habeas data, la transparencia, la seguridad y el cumplimiento normativo.





## INTRODUCCIÓN

El Centro Integral de Rehabilitación Colombia – CIREC, identificado con NIT 860.066.767-4, en cumplimiento de la Ley 1581 de 2012, la Ley 1266 de 2008, el Decreto 1377 de 2013, el Decreto 886 de 2014 y demás normas vigentes en materia de protección de datos personales, adopta la presente Política de Tratamiento de Datos Personales.

CIREC reconoce que, en desarrollo de sus procesos administrativos, comerciales, asistenciales, laborales, tecnológicos y financieros, accede, recolecta, almacena, usa, circula, transmite, transfiere, actualiza, conserva y suprime datos personales, incluidos datos sensibles relacionados con la salud. Por ello, garantiza el derecho fundamental al habeas data mediante un tratamiento lícito, seguro, transparente, confidencial y responsable.

La presente política aplica a los tratamientos realizados por medios físicos y digitales, internos o gestionados por terceros, así como a la información obtenida a través de formularios, plataformas, canales telefónicos, sistemas de videovigilancia y demás herramientas tecnológicas e institucionales.

## 1. OBJETO

Establecer los lineamientos, principios, procedimientos, medidas de seguridad, finalidades y responsabilidades para el tratamiento de los datos personales administrados por CIREC, así como definir los derechos de los titulares y los mecanismos para su ejercicio.

## 2. ALCANCE

- Todas las bases de datos, archivos y sistemas de información, en formato físico o digital, administrados por CIREC.
- Funcionarios, trabajadores, contratistas, practicantes, proveedores, voluntarios y terceros que intervengan en el tratamiento de datos personales por cuenta de CIREC.
- Personas naturales que suministren información personal a CIREC en el marco de relaciones asistenciales, administrativas, comerciales, laborales, contractuales o de prestación de servicios.
- Visitantes y usuarios de la página web, en los casos en que CIREC recolecte o trate sus datos mediante formularios, plataformas virtuales, cookies, videovigilancia, sistemas de ingreso u otras herramientas tecnológicas.

## 3. RESPONSABLES INTERNOS

Se designan como responsables del cumplimiento de esta política las siguientes instancias internas:

- Oficial de Cumplimiento: supervisión integral del cumplimiento normativo.
- Dirección Comercial: tratamiento de datos comerciales y de relacionamiento con clientes y aliados.
- Área de Talento Humano: tratamiento de datos laborales, hojas de vida y seguridad social.
- Coordinación de Sistemas: implementación de controles técnicos y medidas de seguridad de la información.
- Todos los trabajadores, contratistas y terceros autorizados que traten datos personales en nombre de CIREC.

### 3.1. Oficial de Protección de Datos Personales

CIREC designará expresamente un Oficial de Protección de Datos Personales o la instancia que haga sus veces, responsable de coordinar la gestión operativa de esta política y servir de canal de atención especializado.

Funciones mínimas del Oficial de Protección de Datos Personales:

- Atender consultas, peticiones, quejas y reclamos relacionados con datos personales.
- Coordinar las respuestas dentro de los términos legales aplicables.
- Servir de enlace con la Superintendencia de Industria y Comercio.
- Gestionar y coordinar la respuesta frente a incidentes de seguridad que involucren datos personales.
- Supervisar el cumplimiento de plazos de conservación, deberes de información y controles internos.

Datos de contacto del Oficial de Protección de Datos Personales: correo electrónico [completar], extensión telefónica [completar] y horario de atención [completar].

## 4. DOCUMENTOS DE REFERENCIA

- Ley 1581 de 2012.
- Ley 1266 de 2008.
- Decreto 1377 de 2013.
- Decreto 886 de 2014.
- Guías y lineamientos de la Superintendencia de Industria y Comercio sobre protección de datos personales.





## 5. DEFINICIONES

**Autorización:** Consentimiento previo, expreso e informado otorgado por el titular para realizar el tratamiento de sus datos personales.

**Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento, en soporte físico o digital.

**Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

**Dato Sensible:** Dato que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación; incluye, entre otros, datos de salud, biométricos, origen racial o étnico, convicciones religiosas o filosóficas, afiliación sindical y vida sexual.

**Encargado del Tratamiento:** Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable, siguiendo sus instrucciones.

**Responsable del Tratamiento:** Persona natural o jurídica que decide sobre la recolección y las finalidades del tratamiento de los datos personales. Para efectos de esta política, el responsable es CIREC.

**Titular:** Persona natural cuyos datos personales son objeto de tratamiento por parte de CIREC.

**Transferencia de Datos Personales:** Envío de datos personales a otro responsable del tratamiento, nacional o internacional, para que decida sobre su uso de manera autónoma.

**Transmisión de Datos Personales:** Comunicación o entrega temporal de datos personales a un encargado del tratamiento, dentro o fuera del país, para que realice el tratamiento por cuenta del responsable.

**Tratamiento:** Toda operación o conjunto de operaciones realizadas sobre datos personales, tales como recolección, almacenamiento, uso, circulación, actualización, transmisión, transferencia, supresión o anonimización.

## 6. DISPOSICIONES GENERALES

### 6.1. Identificación del Responsable del Tratamiento

Centro Integral de Rehabilitación Colombia – CIREC

- NIT: 860.066.767-4.
- Dirección sede asistencial: Carrera 54 No. 65-25, Barrio Modelo Norte – Bogotá.

- Dirección sede administrativa: Calle 70B 57 09, Barrio San Fernando – Bogotá.
- Correo institucional general: [completar].
- Correo de protección de datos personales: protecciondedatos@cirec.org.co.
- Teléfono: (+571) 7953600.
- Indicar si la línea corresponde a atención local o gratuita nacional: [completar].
- Horario de atención para consultas y reclamos: [completar].
- Página web institucional y enlace directo de publicación de la política: [completar].

### 6.2. Marco Legal

El tratamiento de los datos personales realizado por CIREC se enmarca en el cumplimiento estricto de la normativa vigente en materia de protección de datos en Colombia. Este marco establece reglas, principios y obligaciones para garantizar el adecuado uso, almacenamiento, circulación, transmisión, transferencia y supresión de la información personal, incluyendo los datos sensibles relacionados con la salud.

### 6.3. Principios del Tratamiento

El tratamiento de la información por parte de CIREC se rige por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad, necesidad y responsabilidad demostrada.

### 6.4. Finalidades del Tratamiento

Los datos personales tratados por CIREC podrán ser utilizados para las siguientes finalidades institucionales, de acuerdo con la naturaleza de la relación con cada titular:

#### A. Finalidades comerciales

- Gestionar cotizaciones, solicitudes y requerimientos de usuarios, clientes, aliados o empresas.
- Registrar y actualizar información de clientes y contactos.
- Realizar seguimiento comercial, fidelización y procesos de posventa.

#### B. Finalidades administrativas y financieras

- Cumplir obligaciones legales, contractuales, contables, tributarias y regulatorias.
- Ejecutar procesos administrativos internos.
- Realizar actividades de facturación, pagos, cartera, contratación y certificaciones.
- Gestionar información de proveedores y contratistas.



### C. Finalidades asistenciales

- Registrar y actualizar datos de usuarios en plataformas institucionales.
- Gestionar autorizaciones, órdenes de servicio y procesos asistenciales.
- Administrar información de historias clínicas y demás documentos requeridos para la atención.
- Garantizar la prestación integral y continua de los servicios.

### D. Finalidades de seguridad

- Implementar y gestionar sistemas de vigilancia mediante CCTV.
- Controlar el acceso físico a instalaciones y áreas restringidas.
- Prevenir riesgos, incidentes o actividades ilícitas.
- Proteger bienes, infraestructura, personal y usuarios.

### E. Finalidades laborales y de talento humano

- Gestionar hojas de vida, procesos de selección y contratación.
- Administrar historias laborales, nómina, seguridad social y demás obligaciones legales.
- Realizar evaluaciones, reportes, verificaciones y auditorías relacionadas con talento humano.

### F. Finalidades tecnológicas y de plataformas digitales

- Administrar usuarios y accesos a sistemas informáticos, aplicativos y plataformas.

- Realizar mantenimiento, soporte técnico y gestión de infraestructura tecnológica.
- Implementar controles de seguridad digital y ciberseguridad.
- Mejorar la experiencia de usuarios en canales electrónicos.

### G. Finalidades institucionales y generales

- Gestionar comunicaciones institucionales, campañas informativas y notificaciones.
- Tramitar consultas, peticiones, quejas, reclamos o solicitudes de los titulares.
- Realizar auditorías internas y externas, revisiones y verificaciones de cumplimiento.
- Ejecutar acciones de mejora continua en procesos, servicios y sistemas de gestión.

### 6.5. Principio de temporalidad o conservación

Los datos personales serán conservados únicamente por el tiempo necesario para cumplir las finalidades para las cuales fueron recolectados, las obligaciones legales, contractuales o regulatorias aplicables y los plazos previstos en las normas de archivo y retención documental. Una vez cumplidas las finalidades y vencidos los plazos aplicables, los datos serán eliminados, anonimizados o archivados según corresponda.

Categoría de datos	Plazo de conservación	Fundamento / criterio	Tratamiento posterior
Historias clínicas	Mínimo 20 años desde la última atención	Resolución 1995 de 1999 y normas aplicables del sector salud	Archivo definitivo o transferencia al archivo histórico, según proceda
Datos contables y tributarios	10 años	Estatuto Tributario, art. 632 y soportes contables	Eliminación segura certificada o conservación legal
Información laboral	Hasta 20 años después de la terminación	Normativa laboral, seguridad social y gestión documental	Eliminación segura o archivo histórico
Datos contractuales de proveedores	5 años posteriores a la finalización del contrato	Normativa civil, comercial y contractual	Eliminación segura
Grabaciones CCTV	30 días calendario	Principio de necesidad, seguridad física y trazabilidad	Eliminación automática salvo incidente, investigación o requerimiento de autoridad
Registros de acceso físico	6 meses	Seguridad corporativa y control de acceso	Eliminación automática



Categoría de datos	Plazo de conservación	Fundamento / criterio	Tratamiento posterior
Cookies analíticas	Hasta 24 meses	Consentimiento y configuración del sitio web	Eliminación automática o anonimización
Hojas de vida no seleccionadas	6 meses desde el cierre del proceso	Gestión documental y minimización del dato	Eliminación segura o devolución, cuando aplique

**Nota:** Los plazos iniciarán desde el último tratamiento, la finalización de la relación o el cumplimiento de la finalidad. En caso de litigio, investigación o requerimiento de autoridad, la conservación se extenderá hasta la decisión definitiva.

## 6.6. Derechos de los titulares

Los titulares de datos personales tratados por CIREC tienen los siguientes derechos:

- a) Conocer, actualizar y rectificar sus datos personales frente a CIREC, especialmente cuando resulten parciales, inexactos, incompletos, fraccionados, induzcan a error o su tratamiento esté expresamente prohibido o no haya sido autorizado.
- b) Solicitar prueba de la autorización otorgada a CIREC, salvo cuando expresamente la ley exceptúe este requisito.
- c) Ser informado por CIREC, previa solicitud, respecto del uso que se ha dado a sus datos personales.
- d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la normatividad vigente en materia de protección de datos personales.
- e) Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- f) Acceder en forma gratuita a sus datos personales objeto de tratamiento.
- g) Ser informado de manera clara y previa cuando se soliciten datos sensibles, indicando que se trata de datos sensibles, la finalidad específica, el carácter facultativo de su entrega y que no está obligado a autorizar su tratamiento.
- h) En caso de datos de menores, que sus representantes legales ejerzan los derechos que correspondan en su nombre.

Canales para el ejercicio de derechos: correo electrónico [protecciondatos@cirec.org.co](mailto:protecciondatos@cirec.org.co); dirección física de las sedes institucionales; teléfono [completar]; horario de atención [completar].

Autoridad de control: Superintendencia de Industria y Comercio – SIC, línea gratuita nacional 018000 910165, sitio web [www.sic.gov.co](http://www.sic.gov.co) y canales virtuales de trámites vigentes.

## 6.7. Obtención de la autorización

CIREC obtiene la autorización del titular mediante formatos físicos de consentimiento, formularios de registro, plataformas digitales institucionales, mensajes de datos, grabaciones o mensajes informativos en comunicaciones telefónicas y demás medios idóneos permitidos por la ley.

La autorización para el tratamiento de datos sensibles deberá ser previa, expresa e informada. En todos los casos se informará al titular que no está obligado a suministrar datos sensibles y que no se generará perjuicio por no hacerlo, salvo cuando la información sea indispensable para la prestación del servicio asistencial o para el cumplimiento de un deber legal.

## 6.8. Excepciones a la obtención de autorización

Conforme al artículo 10 de la Ley 1581 de 2012, CIREC podrá realizar tratamiento de datos personales sin necesidad de obtener autorización previa del titular en los siguientes casos:

- Información requerida por autoridad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública conforme a la Constitución y la ley.
- Casos de urgencia médica o sanitaria cuando sea necesario proteger el interés vital del titular o de otra persona y no sea posible obtener la autorización.
- Tratamiento autorizado por la ley para fines históricos, estadísticos o científicos, siempre que se garantice la anonimización o disociación irreversible de los datos.
- Datos relacionados con el registro civil de las personas.
- Tratamiento necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o administrativo.
- Datos necesarios para la ejecución de un contrato en el que el titular sea parte, o para la aplicación de medidas precontractuales cuando el titular lo haya solicitado.



- Cumplimiento de obligaciones legales a las que esté sujeto CIREC.

Aun en los casos de excepción, CIREC garantizará el cumplimiento de los principios de tratamiento y la protección de los derechos de los titulares.

## 6.9. Procedimiento para el ejercicio de derechos

### Consultas

El titular podrá consultar sus datos personales a través de correo electrónico, solicitud escrita o formularios institucionales. CIREC dará respuesta en un término máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la consulta. Cuando no fuere posible atenderla dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá, la cual no podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

### Reclamos

El titular o sus causahabientes podrán presentar reclamo cuando consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización, supresión, revocatoria de la autorización o cuando adviertan el presunto incumplimiento de los deberes de CIREC.

El reclamo deberá contener, como mínimo: identificación del titular; descripción clara y precisa de los hechos y de la solicitud; dirección física y/o correo electrónico para recibir la respuesta; y documentos que se pretendan hacer valer.

- Si el reclamo se presenta incompleto, CIREC requerirá al interesado dentro de los cinco (5) días hábiles siguientes para que subsane las fallas. Si transcurren dos (2) meses desde el requerimiento sin que el solicitante aporte la información requerida, se entenderá que ha desistido del reclamo.
- Si CIREC no es competente para resolver el reclamo, dará traslado al responsable o encargado competente dentro de los dos (2) días hábiles siguientes e informará de ello al titular.
- Una vez recibido el reclamo completo, se incluirá en la base de datos correspondiente una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles.
- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo completo. Si no fuere posible atenderlo en dicho término, se informará al titular los motivos de la demora y la fecha en que se resolverá, la

Política de Tratamiento de Datos Personales · CIREC

cual no podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Proceso general de atención: radicación por correo, escrito o formulario; verificación de identidad del titular o apoderado; registro interno del caso; análisis y trámite; y respuesta dentro del plazo legal.

## 6.10. Medidas de seguridad

### A. Medidas técnicas

- Políticas de contraseñas seguras con requisitos mínimos y periodicidad de cambio.
- Cifrado o encriptación de información sensible y datos personales almacenados o transmitidos por medios electrónicos.
- Copias de seguridad periódicas y planes de recuperación ante desastres y contingencias tecnológicas.
- Control de acceso lógico a aplicaciones, sistemas de información y bases de datos.
- Monitoreo de sistemas y uso de herramientas de seguridad informática, incluyendo antivirus, firewall y detección de intrusiones.

### B. Medidas administrativas

- Diseño, adopción y actualización periódica de políticas internas de protección de datos.
- Gestión de permisos y roles según el principio de acceso mínimo necesario.
- Supervisión del cumplimiento normativo por parte del Oficial de Cumplimiento, el Oficial de Protección de Datos y las áreas responsables.

### C. Medidas humanas

- Capacitación continua al personal sobre protección de datos, seguridad de la información y prevención de incidentes.
- Firma de acuerdos de confidencialidad por parte de funcionarios, contratistas y terceros que accedan a la información.

### D. Medidas para información física

- Custodia adecuada y archivo seguro de documentos físicos que contengan datos personales.
- Implementación de mecanismos de eliminación segura cuando la información haya cumplido su periodo de conservación.
- Control de acceso a áreas restringidas donde se almacena documentación sensible o historias clínicas.



## 6.11. Transferencias y transmisiones de datos personales

### A. Transmisión de datos a encargados del tratamiento

CIREC podrá transmitir datos personales a encargados del tratamiento, nacionales o internacionales, únicamente cuando exista un contrato de transmisión que establezca el alcance, la finalidad y la duración del tratamiento, así como obligaciones de seguridad, confidencialidad y protección de los datos.

- El encargado no podrá utilizar los datos para finalidades distintas a las instruidas por CIREC.
- No podrá subcontratar el tratamiento sin autorización previa y escrita de CIREC.
- Deberá eliminar o devolver los datos al finalizar el servicio, según corresponda.
- CIREC podrá auditar el cumplimiento de las obligaciones asumidas por el encargado.
- El encargado deberá notificar incidentes de seguridad en un plazo máximo de veinticuatro (24) horas desde su detección.

CIREC mantendrá un registro actualizado de encargados, indicando nombre, país cuando aplique y tipo de tratamiento realizado.

### Fases del protocolo

- Fase 1 – Detección y contención (0 a 24 horas): cualquier colaborador que detecte o sospeche un incidente deberá reportarlo de inmediato al canal interno designado; el Oficial de Protección de Datos y la Coordinación de Sistemas evaluarán la naturaleza del incidente, los datos afectados y las medidas inmediatas de contención.
- Fase 2 – Investigación y evaluación (24 a 72 horas): se documentará la cronología del incidente, la causa raíz, los sistemas comprometidos, las categorías de datos afectadas y el número estimado de titulares involucrados.
- Fase 3 – Notificación: cuando corresponda, CIREC notificará a la Superintendencia de Industria y Comercio y a los titulares afectados en los plazos definidos por la normativa y según el nivel de riesgo identificado.
- Fase 4 – Remediación y mejora continua (30 a 90 días): se implementarán medidas correctivas, actualización de controles, capacitación y cierre formal con lecciones aprendidas.

Nivel	Criterios orientadores	Acción de gestión
Crítico	Datos sensibles de salud a gran escala, datos financieros o acceso externo no autorizado confirmado.	Notificación prioritaria a SIC y a titulares afectados, con activación inmediata de contingencias.
Alto	Datos personales de múltiples titulares, con potencial riesgo de fraude, suplantación o afectación relevante.	Notificación a SIC dentro del plazo aplicable y evaluación de notificación a titulares.
Medio	Afectación limitada, sin exposición externa confirmada, pero con necesidad de corrección.	Registro interno, análisis, remediación y fortalecimiento de controles.

## B. Transferencia internacional de datos a nuevos responsables

Las transferencias internacionales de datos personales solo procederán cuando se cuente con autorización previa, expresa e informada del titular o cuando aplique una excepción legal, y además se garantice un nivel adecuado de protección conforme a la normativa colombiana.

- La autorización informará, cuando aplique, el país de destino, la finalidad y la identidad del nuevo responsable.
- El país de destino deberá contar con nivel adecuado de protección, o deberán suscribirse mecanismos contractuales válidos o contarse con autorización de la SIC cuando resulte exigible.
- El titular conservará la posibilidad de ejercer sus derechos ante CIREC como responsable original.

## 6.12. Gestión de incidentes de seguridad de datos personales

CIREC adoptará y mantendrá un protocolo interno para la detección, análisis, contención, documentación, notificación y remediación de incidentes de seguridad que puedan comprometer datos personales.



Nivel	Criterios orientadores	Acción de gestión
Bajo	Incidente menor o evento sin compromiso real de datos.	Registro interno y lección aprendida.

**Registro interno de incidentes:** CIREC mantendrá un registro actualizado de todos los incidentes, incluyendo fecha y hora de detección, descripción, datos afectados, acciones tomadas y responsables de la gestión.

### 6.13. Inscripción y actualización en el RNBD

CIREC registrará y mantendrá actualizadas sus bases de datos ante el Registro Nacional de Bases de Datos – RNBD, conforme al Decreto 886 de 2014 y las disposiciones que lo modifiquen o sustituyan, cuando resulte aplicable.

### 6.14. Tratamiento de datos de menores

CIREC tratará datos personales de niños, niñas y adolescentes únicamente cuando ello responda y respete el interés superior del menor, asegure el respeto de sus derechos fundamentales y exista autorización otorgada por su representante legal, salvo las excepciones legales aplicables.

### 6.15. Tratamiento de datos sensibles

CIREC realiza tratamiento de datos personales sensibles, especialmente aquellos relacionados con la salud de los usuarios, así como datos biométricos y demás categorías definidas por la ley. En estos casos se observarán reglas especiales de información, autorización, acceso restringido y mayor nivel de protección.

- Antes de recolectar datos sensibles, CIREC informará al titular que se trata de datos sensibles, la finalidad concreta del tratamiento y que la respuesta a las preguntas que versen sobre dichos datos es facultativa.
- El tratamiento de datos sensibles requerirá autorización previa, expresa e informada del titular, salvo en los casos de excepción previstos en la ley.
- Ninguna actuación, trámite o servicio será condicionado a la entrega de datos sensibles, excepto cuando estos sean indispensables para la prestación del servicio asistencial o el cumplimiento de obligaciones legales, circunstancia que será informada claramente.
- Los datos sensibles estarán sujetos a mayores medidas de seguridad, acceso restringido y controles internos.

### 6.16. Tratamiento de datos personales mediante sistemas de videovigilancia

CIREC cuenta con sistemas de videovigilancia (CCTV) en sus instalaciones físicas con fines de seguridad de las personas, bienes e infraestructura.

- Finalidad: prevenir y atender incidentes de seguridad, proteger la integridad de usuarios, colaboradores, visitantes y bienes de CIREC, y apoyar investigaciones internas o requerimientos de autoridades competentes.
- Avisos informativos: en las áreas vigiladas se ubicarán avisos visibles que informen la existencia de videovigilancia, la identificación de CIREC como responsable, la finalidad del tratamiento y el canal donde puede consultarse esta política.
- Conservación y acceso: las imágenes serán conservadas por el tiempo estrictamente necesario para cumplir las finalidades señaladas o el que determinen las normas aplicables. Solo tendrán acceso las personas autorizadas y, cuando corresponda, las autoridades competentes.
- Ejercicio de derechos: los titulares podrán ejercer sus derechos respecto de las imágenes captadas conforme al procedimiento de consultas y reclamos previsto en esta política.

### 6.17. Tratamiento de datos mediante cookies y tecnologías similares

CIREC podrá utilizar cookies y tecnologías similares en su sitio web institucional para garantizar el funcionamiento del portal, mejorar la experiencia del usuario, analizar la navegación y, cuando aplique, personalizar contenidos o campañas.

- Cookies necesarias: permiten el funcionamiento básico del sitio, la seguridad, la sesión y la accesibilidad.
- Cookies analíticas: permiten medir tráfico, estadísticas de uso y patrones de navegación.
- Cookies de funcionalidad: recuerdan preferencias del usuario, como idioma, región o tamaño de fuente.



- Cookies de marketing: solo se utilizarán si resultan aplicables y con consentimiento explícito, para personalizar publicidad y medir la efectividad de campañas.

Al ingresar por primera vez al sitio web, el usuario deberá visualizar un banner o mecanismo equivalente de gestión del consentimiento, con opciones para aceptar todas las cookies, rechazar las no esenciales o configurar sus preferencias. El usuario podrá modificar dichas preferencias en cualquier momento a través de la configuración del sitio o de su navegador.

La desactivación de cookies necesarias puede afectar la funcionalidad del sitio web. CIREC aplicará a otras tecnologías similares, como píxeles de seguimiento o web beacons, los mismos criterios de transparencia, necesidad y consentimiento descritos en esta sección.

## 7. VIGENCIA

La presente política rige a partir de su publicación y tendrá vigencia indefinida, sin perjuicio de las actualizaciones que CIREC deba adoptar por cambios normativos, operativos o institucionales. Las bases de datos se conservarán mientras exista finalidad legítima, obligación legal o contractual, o consentimiento válido que justifique el tratamiento.