

POLÍTICA DE TRATAMIENTO DE INFORMACIÓN

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

OBJETIVO:

Establecer los criterios para la recolección, almacenamiento, uso, circulación, actualización y supresión de los datos personales tratados por El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI PO POLI - CISP

ALCANCE:

Esta política aplica para toda la información personal registrada en las bases de datos de El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI – CISP, quien actúa en calidad de responsable del tratamiento de los datos personales.

OBLIGACIONES:

Esta política es de obligatorio y estricto cumplimiento para El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI - CISP.

RESPONSABLE DEL TRATAMIENTO:

El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI - CISP, identificada con el NIT 800223957-2 con domicilio principal en la calle 49 -6813 piso 6 de la ciudad de Medellín (Antioquia), República de Colombia. portal www.cispalc.org Teléfono (604)604 3404 en la ciudad de Medellín (Antioquia).

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de los datos personales realizado por el COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI – CISP se regirá por los principios establecidos en la Ley 1581 de 2012, el Decreto 1377 de 2013, Decreto 886 de 2014, Decreto Único Reglamentario 1074 de 2015, y las demás normas que la modifiquen o complementen. Estos principios orientan la correcta gestión de la información y garantizan el respeto por los derechos de los titulares:

- Legalidad
- Finalidad
- Libertad
- Veracidad y calidad
- Transparencia
- Seguridad
- Confidencialidad

DEFINICIONES CLAVE

- Dato personal: información que permite identificar o hacer identifiable a una persona.
- Dato sensible: información que afecta la intimidad o cuyo uso indebido puede generar discriminación.
- Dato de menores de edad: información de niños, niñas o adolescentes cuya protección de los datos es prioritaria.
- Responsable del tratamiento: CISP.
- Encargado del tratamiento: proveedores, plataformas tecnológicas o aliados institucionales que procesan datos por encargo del CISP.
- Autorización: consentimiento previo, expreso e informado del titular para el tratamiento de sus datos.

MECANISMOS DE RECOLECCIÓN DE LA AUTORIZACIÓN

- EL COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI – CISP obtendrá la autorización previa, expresa e informada de los titulares a través de medios físicos, digitales o verbales verificables, tales como:
- Formularios o cartas físicas firmadas.
- Formularios electrónicos en plataformas de registro.
- Autorización mediante clic (“opt-in”) en plataformas educativas o aplicativos.
- Grabaciones de audio o video cuando aplique.
- Mensajería digital (correo electrónico, SMS o WhatsApp) siempre que quede evidencia de aceptación.

La autorización será conservada en los sistemas institucionales como evidencia de cumplimiento normativo.

TRATAMIENTO Y FINALIDAD:

El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI – CISP, en cumplimiento de la legislación colombiana y de los estándares internacionales de protección de datos, adopta esta política para garantizar que la información personal que recibe sea tratada con responsabilidad, seguridad, transparencia y respeto por los derechos de las personas y comunidades con las que trabaja.

El CISP solo recopila y utiliza datos personales para fines legítimos derivados de sus proyectos sociales, formativos, administrativos y de cooperación

internacional.

El tratamiento que realizará El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI – CISP con la información personal será el siguiente:

La recolección, almacenamiento, uso, circulación, actualización y supresión de datos enmarcados en la ejecución de proyectos son:

FINALIDAD
Realización de caracterizaciones, entrega de paquetes tecnológicos y asistencia técnica aplicable a la población objeto del contrato o convenio.
Recolección de evidencia tales como firmas, fotografías y videos para constatar la visita realizada de acompañamiento
Contactar el titular a través de medios telefónicos para realizar verificaciones de información, encuestas de percepción y/o confirmación de datos personales
Contactar al titular a través de medios electrónicos - SMS o Chat para el envío de noticias asociadas al proyecto que lo incluye
Poder contactarlo por medios digitales para la realización de talleres, ruedas de negocio y/o acompañamiento
Documentación requerida para la realización de los procesos de contratación de colaboradores para adelantar las ejecuciones respectivas de los proyectos o convenios
Documentos requeridos para adelantar los procesos de compra requeridos en la ejecución de los proyectos o convenios
Utilización de datos no sensibles de los titulares de la información para la elaboración de Cartillas, plegables u otros medios de divulgación escrita, audiovisual o telecomunicaciones.
Registro, identificación y participación en programas y proyectos.
Envío de comunicaciones, certificaciones, reportes e información relacionada con actividades del proyecto.
Administración de accesos, roles y perfiles en plataformas digitales y servidores NAS.

FINALIDAD
Gestión de logs, auditorías internas, trazabilidad y control de operaciones.
Respaldo, custodia, conservación y recuperación de información.
Generación de estadísticas, indicadores, análisis de avance y seguimiento.
Evaluación de impacto, informes técnicos y sistematización de experiencias.
Cumplimiento de obligaciones derivadas de acuerdos, convenios, auditorías y cooperación internacional.
Atención de requerimientos de autoridades administrativas, judiciales o de control.

TRATAMIENTO DE DATOS SENSIBLES:

Los datos sensibles recolectados serán tratados con las siguientes finalidades:

FINALIDAD
Realización de la caracterización, entrega de paquetes tecnológicos y asistencia técnica aplicable a la población objeto del contrato o convenio.
Recolección de evidencia tales como firmas, fotografías y videos para constatar la visita realizada de acompañamiento.

El tratamiento de datos sensibles o de menores se realizará únicamente cuando:

FINALIDAD
Sea necesario para cumplir los objetivos del proyecto.
Exista autorización expresa del titular o representante legal.
Se garantice protección reforzada,

FINALIDAD

confidencialidad y proporcionalidad.

Responda al interés superior del niño, niña o adolescente.

TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES

El CISP podrá transmitir o transferir datos personales a aliados, proveedores tecnológicos o cooperantes internacionales ubicados dentro o fuera del país, exclusivamente para el cumplimiento de proyectos, actividades misionales o finalidades autorizadas.

Toda transferencia internacional se realizará conforme a:

Contratos de transmisión con cláusulas de confidencialidad y seguridad.

Reglas establecidas por la SIC sobre países con niveles adecuados de protección.

El CISP garantizará que los terceros cumplan estándares de protección equivalentes o superiores a los exigidos en Colombia.

Cuando no sea posible poner a disposición la presente política completa, el CISP publicará un aviso de privacidad que incluirá:

- Identificación del responsable.
- Finalidades del tratamiento.
- Derechos del titular.
- Mecanismos de contacto.
- Enlace a la política completa.

CONSERVACIÓN Y ELIMINACIÓN SEGURA DE LA INFORMACIÓN

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir las finalidades autorizadas o por obligaciones legales o contractuales. Una vez cumplidas las finalidades, el CISP:

- Eliminará los datos de manera segura e irreversible.
- Implementará mecanismos como borrado seguro, destrucción física

anonimización.

TRATAMIENTO DE INFORMACIÓN EN PLATAFORMAS DIGITALES

El CISP recolecta datos derivados del uso de plataformas como Moodle, aulas virtuales, ERP, NAS, sistemas de trazabilidad y registro de logs, exclusivamente para:

- Gestión de accesos, roles y perfiles.
- Auditoría interna y trazabilidad de actividades.
- Seguridad informática y continuidad operativa.
- Seguimiento académico y acompañamiento técnico.

El tratamiento se realizará bajo medidas de seguridad avanzadas y protocolos de acceso autorizado.

DERECHOS DE LOS TITULARES:

Como titular de sus datos personales Usted tiene derecho a:

- (i) Acceder de forma gratuita a los datos proporcionados que hayan sido objeto de tratamiento.
- (ii) Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.
- (iii) Solicitar prueba de la autorización otorgada.
- (iv) Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la normatividad vigente.
- (v) Revocar la autorización y/o solicitar la supresión del dato, siempre que no exista un deber legal o contractual que impida eliminarlos.
- (vi) Abstenerse de responder las preguntas sobre datos sensibles.

Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS

El área de Administración es la dependencia que tiene a cargo dar trámite a las solicitudes de los titulares para hacer efectivos sus derechos.

Responsable Katalina Santos Zuluaga Correo electrónico:
contactenos@cispcolombia.org

Facebook:<https://www.facebook.com/CISPalc/>

Dirección: Calle 49 # 68 - 13, piso 6, Barrio Suramericana Medellín

Teléfono 604 604 3404

PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA

En cumplimiento de las normas sobre protección de datos personales, El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI - CISP presenta el procedimiento y requisitos mínimos para el ejercicio de sus derechos:

Para la radicación y atención de su solicitud le solicitamos suministrar la siguiente información:

- Nombre completo y apellidos
- Datos de contacto (Dirección física y/o electrónica y teléfonos de contacto), Medios para recibir respuesta a su solicitud,
- Motivo(s)/hecho(s) que dan lugar al reclamo con una breve descripción del derecho que desea ejercer (conocer, actualizar, rectificar, solicitar prueba de la autorización otorgada, revocarla, suprimir, acceder a la información)
- Firma (si aplica) y número de identificación.

El término máximo previsto por la ley para resolver su reclamación es de quince (15) días hábiles, contado a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI - CISP informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez cumplidos los términos señalados por la Ley 1581 de 2012 y las demás normas que la reglamenten o complementen, el Titular al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, actualización, rectificación, supresión y revocación podrá poner su caso en conocimiento de la Superintendencia de Industria y Comercio –Delegatura para la Protección de Datos Personales.

DEBERES DEL CISP COMO RESPONSABLE DEL TRATAMIENTO

El CISP se compromete a:

- Obtener autorización previa e informada cuando sea necesario..
- Garantizar seguridad, integridad y confidencialidad de la información.
- Velar porque los encargados cumplan las mismas reglas de protección.
- Informar oportunamente cualquier cambio en la política o incidente de seguridad que comprometa los datos.

MEDIDAS DE SEGURIDAD Y ADMINISTRACIÓN DE LA INFORMACIÓN

El CISP implementa medidas de protección acordes con las capacidades técnicas de la organización y con las exigencias actuales:

- Controles administrativos
- Sistema de Gestión del CISP
- Restricción de acceso según roles y perfiles.
- Acuerdos de confidencialidad con empleados y contratistas.
- Controles tecnológicos
- Servidores NAS con autenticación, permisos diferenciados y registros de actividad.
- Cifrado de información según criticidad.
- Plataformas de formación y seguimiento con perfiles, autenticación y control de accesos.
- Copias de seguridad periódicas y planes de continuidad operativa.
- Eliminación segura y definitiva de información cuando ya no sea necesaria.

Controles físicos

Custodia de documentos con acceso limitado.

Protocolos de archivo físico y digital.

GESTIÓN DE INCIDENTES DE SEGURIDAD

El COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI – CISP implementa un instructivo para la identificación, análisis, contención, notificación y cierre de incidentes de seguridad que puedan de alguna manera comprometer la confidencialidad, integridad o disponibilidad de los datos personales bajo su custodia.

Se considerará incidente de seguridad cualquier evento que afecte o pueda afectar el tratamiento adecuado de la información, tales como accesos no autorizados, pérdida de información, fallas técnicas, divulgación indebida o vulneraciones a los sistemas que almacenan datos personales.

Cuando ocurra un incidente de seguridad, el CISP actuará conforme a las siguientes directrices:

- Detección y reporte inmediato: Todo empleado y/o contratista deberá reportar de manera inmediata cualquier evento sospechoso o incidente confirmado al área responsable de seguridad de la información.
- Análisis y contención del incidente: El equipo de innovación evaluará el alcance del incidente, identificará los datos afectados, aplicará medidas de contención y establecerá acciones de mitigación para evitar daños adicionales.
- Notificación interna y documentación: Todos los incidentes serán notificados al representante país, donde se documentarán los hechos, tiempos, causas, medidas adoptadas y estado del caso hasta su cierre.
- Notificación al titular cuando sea aplicable: En los casos en que el incidente pueda afectar de manera significativa los derechos de los titulares, el CISP

comunicará de forma clara y oportuna la situación, indicando las medidas adoptadas y los canales de contacto disponibles.

- Notificación a la Superintendencia de Industria y Comercio (SIC): Cuando el incidente implique un riesgo alto para los titulares o afecte significativamente la seguridad de la información, el CISP reportará la situación ante la SIC, conforme a los plazos y lineamientos establecidos por dicha entidad.
- Acciones correctivas y de mejora continua: Finalizado el incidente generado, se implementarán medidas correctivas y de mejora para evitar su repetición, incluyendo ajustes a los protocolos, refuerzos de seguridad, capacitación al personal o mejoras tecnológicas.

ACTUALIZACIONES

Esta política entra en vigor desde su publicación y podrá actualizarse para incorporar nuevas disposiciones legales, estándares internacionales, lineamientos de cooperación o ajustes internos de seguridad de la información.

VIGENCIA:

La presente Política para el Tratamiento de Datos Personales rige a partir del 01 de enero de 2020.

Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar su información, sus datos serán eliminados de nuestras bases de datos.

Los períodos de permanencia de los datos en la base son los siguientes:

Los datos personales proporcionados se conservarán mientras se mantenga la relación contractual con el titular de la información o con el proyecto o convenio firmado para la Administración de la información.

Los datos personales proporcionados se conservarán mientras no se solicite su supresión por el interesado y siempre que no exista un deber legal de conservarlos.

Las bases de datos administradas por el CISP tendrán una vigencia igual al tiempo necesario para cumplir las finalidades autorizadas. Una vez dichas finalidades se hayan cumplido y no exista obligación legal o contractual de conservar la información, los datos serán eliminados o anonimizados de manera segura.

