POLÍTICA DE TRATAMIENTO DE PROTECCIÓN DE DATOS PERSONALES DE LOS TITULARES

SYSDATEC
CENTRO DE DESARROLLO INTEGRAL S.A.S.

PRESENTACIÓN

En cumplimiento de lo establecido en la Constitución Política de Colombia, la Ley Estatutaria 1581 de 2012, el Decreto Único Reglamentario 1074 de 2015 y demás disposiciones que regulan la protección de datos personales, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., como Institución de Educación para el Trabajo y el Desarrollo Humano (ETDH), adopta la presente Política de Tratamiento de Datos Personales, con el propósito de garantizar el adecuado tratamiento de la información personal de todos los titulares con quienes mantiene relaciones académicas, laborales, contractuales, comerciales o institucionales.

Esta política establece los principios, criterios, responsabilidades y procedimientos que orientan la recolección, almacenamiento, uso, circulación, actualización, conservación, transferencia, transmisión y supresión de los datos personales, asegurando el respeto por los derechos fundamentales a la intimidad, el buen nombre, la privacidad y el hábeas data, así como el cumplimiento de las obligaciones legales aplicables.

La presente política es aplicable a todas las bases de datos administradas por la institución, independientemente de su medio de almacenamiento, incluyendo archivos físicos y digitales, plataformas académicas, sistemas de información, aplicaciones institucionales, sitios web, formularios electrónicos, plataformas virtuales de aprendizaje, servicios en la nube, correo institucional, sistemas administrativos y cualquier otro mecanismo autorizado para el tratamiento de datos personales.

De igual manera, constituye un instrumento de apoyo para el Sistema de Gestión de la Calidad de SYSDATEC, al fortalecer la gestión de la información documentada, la seguridad de la información, la gestión de riesgos asociados al tratamiento de datos personales y la mejora continua de los procesos institucionales, en concordancia con los lineamientos de la ISO 9001:2015, las NTC 5555:2011, NTC 5581:2011 y demás normas aplicables.

Todos los colaboradores, directivos, docentes, contratistas, proveedores y terceros que intervengan en el tratamiento de datos personales deberán conocer, aplicar y cumplir las disposiciones contenidas en esta política, garantizando que el tratamiento de la información se realice bajo los principios de legalidad, finalidad, libertad, transparencia, veracidad, acceso y circulación restringida, seguridad, confidencialidad y responsabilidad demostrada, promoviendo una cultura institucional orientada a la protección de los datos personales y al fortalecimiento de la confianza de la comunidad educativa y de los demás grupos de interés.

1. OBJETIVO

Establecer los lineamientos, principios, responsabilidades y procedimientos para el tratamiento de los datos personales recolectados, almacenados, utilizados, actualizados, compartidos, conservados y suprimidos por SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., garantizando la protección de los derechos de los titulares, el cumplimiento de la legislación colombiana vigente en materia de protección de datos personales y la implementación de medidas administrativas, técnicas y organizacionales que aseguren la confidencialidad, integridad, disponibilidad y seguridad de la información, en concordancia con el Sistema de Gestión de la Calidad y los principios de mejora continua.

2. ALCANCE

La presente Política de Tratamiento de Datos Personales aplica a todos los procesos, sedes, actividades, servicios y unidades organizacionales de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., así como a todas las personas naturales o jurídicas que, en calidad de responsables, encargados, colaboradores, docentes, contratistas, proveedores, aliados estratégicos o terceros autorizados, intervengan en el tratamiento de datos personales por cuenta de la institución.

Comprende el tratamiento de los datos personales contenidos en bases de datos físicas y digitales, sistemas de información, plataformas académicas y administrativas, plataformas virtuales de aprendizaje, sitios web institucionales, formularios físicos y electrónicos, aplicaciones informáticas, correo electrónico institucional, servicios en la nube, sistemas de videovigilancia, canales de atención presencial y virtual, redes sociales institucionales y cualquier otro medio autorizado para la recolección o tratamiento de información personal.

La política aplica al tratamiento de los datos personales de aspirantes, estudiantes, egresados, acudientes, padres de familia, docentes, colaboradores, contratistas, proveedores, aliados estratégicos, visitantes y demás titulares cuya información sea objeto de tratamiento por parte de la institución, durante todas las etapas del ciclo de vida de la información, desde su recolección hasta su disposición final, de conformidad con la Ley 1581 de 2012, el Decreto 1074 de 2015 y las demás disposiciones legales vigentes en materia de protección de datos personales.

Asimismo, esta política constituye un instrumento de apoyo para la gestión institucional, fortaleciendo la transparencia, la seguridad de la información, la gestión de riesgos asociados al tratamiento de datos personales y el cumplimiento de los requisitos del Sistema de Gestión de la Calidad implementado por la institución.

3. MARCO NORMATIVO

La presente Política de Tratamiento de Datos Personales se fundamenta en las disposiciones constitucionales, legales y reglamentarias vigentes en la República de Colombia, así como en los lineamientos emitidos por la Superintendencia de Industria y Comercio (SIC), autoridad nacional en materia de protección de datos personales. Estas disposiciones orientan la gestión responsable de la información personal por parte de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., garantizando el respeto por los derechos de los titulares y el cumplimiento de las obligaciones legales aplicables.

3.1. Constitución Política de Colombia

- **Artículo 15.** Reconoce el derecho fundamental al hábeas data, la intimidad personal y familiar, el buen nombre y la protección de los datos personales.
- **Artículo 20.** Garantiza el derecho a recibir y suministrar información veraz e imparcial.
- **Artículo 74.** Establece el derecho de acceso a los documentos públicos, salvo las excepciones previstas en la ley.

3.2. Ley Estatutaria 1581 de 2012: Por la cual se dictan las disposiciones generales para la protección de datos personales, estableciendo los principios, derechos, deberes y procedimientos para el tratamiento de datos personales por parte de responsables y encargados del tratamiento.

3.3. Decreto Único Reglamentario 1074 de 2015: Compila y reglamenta las disposiciones relacionadas con la protección de datos personales, definiendo las obligaciones de los responsables y encargados del tratamiento, así como los procedimientos para el ejercicio de los derechos de los titulares.

3.4. Ley 1266 de 2008: Por la cual se establecen las disposiciones generales del hábeas data financiero, crediticio, comercial y de servicios, aplicable cuando la institución trate información relacionada con obligaciones económicas o financieras.

3.5. Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, aplicable en lo relacionado con la administración, acceso y reserva de la información pública cuando corresponda.

3.6. Ley 2300 de 2023: Por medio de la cual se establecen medidas para proteger el derecho a la intimidad de los consumidores, regulando los canales, horarios y condiciones para la gestión de comunicaciones comerciales, de cobranza y atención a los titulares de datos personales.

3.7. Circular Única de la Superintendencia de Industria y Comercio: Contiene las instrucciones vigentes impartidas por la Superintendencia de Industria y Comercio respecto a la administración de bases de datos personales, el Registro Nacional de Bases de Datos (RNBD), las medidas de seguridad, la atención de consultas y reclamos y la implementación del principio de responsabilidad demostrada (*Accountability*).

3.8. Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability): Documento emitido por la Superintendencia de Industria y Comercio que establece las buenas prácticas para demostrar el cumplimiento de la legislación sobre protección de datos personales mediante políticas, procedimientos, controles, gestión del riesgo y mejora continua.

3.9. Ley 527 de 1999: Regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales, proporcionando el marco jurídico para la validez y conservación de documentos electrónicos.

3.10. Decreto 1377 de 2013: Aunque fue compilado en el Decreto 1074 de 2015, se cita como referente histórico por haber reglamentado inicialmente aspectos relacionados con la autorización del tratamiento de datos personales, los avisos de privacidad y los procedimientos para el ejercicio de los derechos de los titulares.

3.11. Ley 594 de 2000: Ley General de Archivos, que establece los principios para la administración, conservación, organización y disposición de la documentación producida y recibida por las organizaciones.

3.12. Sistema de Gestión de la Calidad: Como parte de su compromiso con la gestión responsable de la información, **SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S.** implementa y mantiene controles alineados con los siguientes referentes:

- **ISO 9001:2015** – Sistemas de Gestión de la Calidad. Requisitos.
- **NTC 5555:2011** – Sistemas de Gestión de la Calidad para Instituciones de Formación para el Trabajo.
- **NTC 5581:2011** – Programas de Formación para el Trabajo. Requisitos de calidad.
- **NTC 5580:2011** – Requisitos para el funcionamiento de Instituciones de Formación para el Trabajo y el Desarrollo Humano.

3.13. Normatividad Institucional: La presente política se articula con la documentación interna del Sistema de Gestión de la Calidad, especialmente con:

- Manual del Sistema de Gestión de la Calidad.
- Política de Seguridad de la Información (cuando aplique).
- Política de Gestión Documental.
- ACA-PD09 – Gestión de la Información Documentada.
- ACA-PD07 – Gestión de Riesgos y Oportunidades.
- ACA-PD06 – No Conformidades y Mejora.
- ACA-PD13 – Gestión y Planificación de los Cambios.

Procedimientos y lineamientos institucionales relacionados con el tratamiento, custodia y protección de la información.

4. DEFINICIONES

Para efectos de la presente Política de Tratamiento de Datos Personales, se adoptan las siguientes definiciones, conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás disposiciones aplicables:

4.1. Autorización: Consentimiento previo, expreso e informado otorgado por el titular para que SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. realice el tratamiento de sus datos personales, salvo las excepciones previstas en la ley.

4.2. Aviso de Privacidad: Comunicación verbal, escrita o electrónica mediante la cual el responsable del tratamiento informa al titular sobre la existencia de las políticas de tratamiento de datos personales, las finalidades del tratamiento, los derechos del titular y los mecanismos para ejercerlos.

4.3. Base de Datos: Conjunto organizado de datos personales, físicos o electrónicos, que son objeto de tratamiento por parte de la institución para el desarrollo de sus actividades académicas, administrativas, comerciales o de apoyo.

4.4. Dato Personal: Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable.

4.5. Dato Público: Dato calificado como tal por la ley o la Constitución Política y que no se considera de naturaleza reservada o semiprivada.

4.6. Dato Privado: Información que por su naturaleza íntima o reservada únicamente es relevante para su titular.

4.7. Dato Semiprivado: Información que no tiene naturaleza íntima, reservada ni pública, cuyo conocimiento puede interesar a determinados sectores o personas y cuyo tratamiento se encuentra sujeto a las condiciones establecidas por la ley.

4.8. Dato Sensible: Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación, como datos relacionados con origen étnico, orientación política, convicciones religiosas, datos biométricos, estado de salud, vida sexual o cualquier otra información protegida por la legislación vigente.

4.9. Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

4.10. Responsable del Tratamiento: Persona natural o jurídica que decide sobre la base de datos y el tratamiento de los datos personales. Para efectos de esta política, el responsable es SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S.

4.11. Titular: Persona natural cuyos datos personales son objeto de tratamiento.

4.12. Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como recolección, almacenamiento, organización, uso, circulación, actualización, consulta, conservación, transferencia, transmisión, bloqueo, supresión o eliminación.

4.13. Transferencia: Envío de datos personales a un responsable del tratamiento ubicado dentro o fuera del territorio colombiano, quien actuará como responsable de la información transferida.

4.14. Transmisión: Comunicación de datos personales a un encargado del tratamiento para que realice actividades por cuenta del responsable, dentro o fuera del territorio nacional.

4.15. Seguridad de la Información: Conjunto de políticas, controles, procesos y medidas destinadas a preservar la confidencialidad, integridad, disponibilidad y autenticidad de la información durante todo su ciclo de vida.

4.16. Incidente de Seguridad: vento real o potencial que compromete la confidencialidad, integridad, disponibilidad o uso adecuado de los datos personales y que puede ocasionar pérdida, alteración, destrucción, acceso no autorizado o divulgación indebida de la información.

4.17. Violación de Datos Personales: Incidente de seguridad que produce la destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos personales tratados por la institución.

4.18. Responsable Interno del Tratamiento: Servidor, colaborador o dependencia designada por la institución para coordinar la implementación, seguimiento y cumplimiento de la presente política.

4.19. Principio de Responsabilidad Demostrada (Accountability): Obligación del responsable del tratamiento de implementar medidas apropiadas para garantizar y demostrar el cumplimiento de la normatividad sobre protección de datos personales mediante políticas, procedimientos, controles, gestión de riesgos, auditorías y acciones de mejora.

4.20. Información Documentada: Información y el medio que la contiene, independientemente de su formato, que sirve como evidencia del tratamiento de datos personales y cuyo control se realiza conforme al Sistema de Gestión de la Calidad y al procedimiento institucional de gestión de la información documentada.

5. PRINCIPIOS

El tratamiento de los datos personales por parte de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. se realizará conforme a los principios establecidos en la legislación colombiana y en las buenas prácticas internacionales de protección de datos personales.

5.1. Principio de Legalidad: El tratamiento de los datos personales es una actividad reglada que deberá sujetarse a la Constitución Política, la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás disposiciones que regulen la materia.

5.2. Principio de Finalidad: Los datos personales serán tratados únicamente para las finalidades legítimas, específicas, explícitas e informadas al titular al momento de obtener su autorización o cuando la ley permita el tratamiento sin requerirla.

5.3. Principio de Libertad: El tratamiento solo podrá realizarse con el consentimiento previo, expreso e informado del titular, salvo las excepciones previstas en la legislación vigente.

5.4. Principio de Veracidad o Calidad: La información objeto de tratamiento deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible, evitando el tratamiento de datos parciales, incompletos o que puedan inducir a error.

5.5. Principio de Transparencia: La institución garantizará al titular el acceso a la información relacionada con sus datos personales y facilitará el ejercicio de sus derechos mediante los canales establecidos para tal fin.

5.6. Principio de Acceso y Circulación Restringida: El acceso a los datos personales estará limitado exclusivamente a las personas autorizadas y se realizará conforme a las finalidades del tratamiento y a las restricciones previstas en la ley.

5.7. Principio de Seguridad: La institución implementará medidas administrativas, técnicas, físicas y organizacionales orientadas a proteger los datos personales frente a riesgos de pérdida, alteración, acceso no autorizado, uso indebido, destrucción o divulgación.

5.8. Principio de Confidencialidad: Todas las personas que intervengan en el tratamiento **de** datos personales deberán garantizar la reserva de la información, incluso después de finalizada su relación con la institución, salvo las excepciones previstas en la ley.

5.9. Principio de Responsabilidad Demostrada (Accountability): La institución adoptará mecanismos de gestión, seguimiento, evaluación y mejora continua que permitan demostrar el cumplimiento de las obligaciones legales relacionadas con la protección de datos personales y la eficacia de los controles implementados.

5.10. Principio de Minimización de Datos: La institución recolectará y tratará únicamente los datos personales que resulten adecuados, pertinentes y necesarios para el cumplimiento de las finalidades previamente definidas, evitando la obtención de información excesiva o innecesaria.

5.11. Principio de Privacidad desde el Diseño y por Defecto: Los procesos, sistemas de información, plataformas tecnológicas y nuevos servicios institucionales incorporarán medidas de protección de datos personales desde su diseño y configuración inicial, garantizando el tratamiento seguro de la información durante todo su ciclo de vida.

5.12. Principio de Mejora Continua: La institución revisará periódicamente la presente política, los procedimientos asociados y los controles implementados para fortalecer la gestión de los datos personales, adaptarse a los cambios normativos y tecnológicos y mejorar continuamente la eficacia del Sistema de Gestión de la Calidad y del programa institucional de protección de datos personales

6. ROLES Y RESPONSABILIDADES

Con el propósito de garantizar el cumplimiento de la legislación vigente en materia de protección de datos personales y fortalecer la gestión de la información institucional, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. establece los siguientes roles y responsabilidades para los responsables, encargados y demás personas que intervienen en el tratamiento de datos personales.

6.1. Dirección: La Dirección es la máxima autoridad responsable de garantizar la implementación, mantenimiento y mejora continua del Programa Institucional de Protección de Datos Personales. En consecuencia, le corresponde:

- Aprobar la Política de Tratamiento de Datos Personales y sus actualizaciones.
- Asignar los recursos humanos, tecnológicos, físicos y financieros necesarios para el cumplimiento de la normatividad aplicable.
- Promover una cultura institucional de protección de datos personales.
- Garantizar el cumplimiento de las obligaciones legales como Responsable del Tratamiento.
- Revisar periódicamente el desempeño del programa de protección de datos personales durante la Revisión por la Dirección.

6.2. Responsable del Tratamiento: SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en calidad de Responsable del Tratamiento, deberá:

- Garantizar el tratamiento lícito, transparente y seguro de los datos personales.
- Definir las finalidades para el tratamiento de la información.
- Implementar medidas administrativas, técnicas y organizacionales para proteger los datos personales.
- Garantizar el ejercicio de los derechos de los titulares.
- Mantener actualizada la presente política y los procedimientos asociados.
- Verificar el cumplimiento de las obligaciones por parte de los encargados del tratamiento.
- Atender los requerimientos de las autoridades competentes.

6.3. Líder del Proceso de Aseguramiento de la Calidad: El Líder del Proceso de Aseguramiento de la Calidad será responsable de coordinar la implementación y el seguimiento del Sistema de Gestión relacionado con la protección de datos personales. Sus responsabilidades incluyen:

- Coordinar la actualización de la Política de Tratamiento de Datos Personales.

- Verificar la aplicación de los procedimientos relacionados con el tratamiento de datos personales.
- Realizar seguimiento al cumplimiento de la normatividad vigente.
- Coordinar auditorías internas relacionadas con la protección de datos personales.
- Promover acciones de mejora derivadas de auditorías, incidentes, riesgos o cambios normativos.
- Mantener la trazabilidad documental conforme al procedimiento ACA-PD09 – Gestión de la Información Documentada.
- Presentar informes sobre el desempeño del sistema durante la Revisión por la Dirección.

6.4. Líderes de Proceso: Los líderes de proceso son responsables de garantizar que el tratamiento de los datos personales dentro de sus procesos se realice conforme a esta política. Para ello deberán:

- Identificar las bases de datos bajo su responsabilidad.
- Garantizar que los datos personales sean tratados únicamente para las finalidades autorizadas.
- Implementar los controles definidos para la protección de la información.
- Informar oportunamente cualquier incidente relacionado con datos personales.
- Verificar que los colaboradores del proceso conozcan y cumplan esta política.
- Gestionar la actualización de la información cuando sea necesario.

6.5. Coordinación y Secretaría: La Coordinación y la Secretaría serán responsables de:

- Administrar los registros documentales que contengan datos personales.
- Garantizar la adecuada custodia de los expedientes físicos y digitales.
- Controlar el acceso a la información conforme a los perfiles autorizados.
- Gestionar la conservación y disposición final de la documentación conforme a la legislación archivística y al Sistema de Gestión de la Calidad.
- Apoyar la atención de consultas y reclamos relacionados con datos personales.

6.6. Área de Tecnología o Responsable de Sistemas: El responsable de los servicios tecnológicos deberá:

- Implementar controles de seguridad informática para proteger la información institucional.
- Administrar los accesos a plataformas, sistemas de información y bases de datos.
- Gestionar copias de seguridad y mecanismos de recuperación de la

información.
- Monitorear los eventos de seguridad relacionados con los sistemas de información.
- Apoyar la investigación y tratamiento de incidentes de seguridad de la información.
- Implementar medidas para proteger la información almacenada en plataformas institucionales y servicios en la nube.

6.7. Talento Humano: El área responsable de la gestión del talento humano deberá:

- Garantizar el tratamiento adecuado de los datos personales de colaboradores, docentes y contratistas.
- Obtener las autorizaciones requeridas cuando corresponda.
- Custodiar la información laboral conforme a la legislación vigente.
- Promover actividades de capacitación y sensibilización sobre protección de datos personales.

6.8. Docentes, Funcionarios y Contratistas: Todos los docentes, funcionarios, contratistas y demás colaboradores deberán:

- Cumplir la presente política y los procedimientos institucionales relacionados.
- Utilizar los datos personales únicamente para el ejercicio de sus funciones.
- Mantener la confidencialidad de la información a la que tengan acceso.
- Proteger los documentos físicos y digitales bajo su responsabilidad.
- Reportar inmediatamente cualquier incidente, pérdida, acceso no autorizado o vulneración relacionada con datos personales.
- Participar en las actividades de formación y sensibilización programadas por la institución.

6.9. Encargados del Tratamiento: Los terceros que realicen tratamiento de datos personales por cuenta de la institución deberán:

- Cumplir las obligaciones legales aplicables y las condiciones contractuales establecidas por SYSDATEC.
- Implementar medidas de seguridad apropiadas para proteger la información.
- Tratar los datos únicamente conforme a las instrucciones impartidas por el Responsable del Tratamiento.
- Garantizar la confidencialidad de la información recibida.
- Informar oportunamente cualquier incidente de seguridad o incumplimiento relacionado con los datos personales.

6.10. Todos los Titulares de Acceso a Información: Toda persona que tenga acceso a datos personales administrados por la institución deberá actuar bajo los principios de legalidad, confidencialidad, integridad, disponibilidad, responsabilidad y seguridad de la información, utilizando los datos exclusivamente para las finalidades autorizadas y absteniéndose de divulgar, copiar, modificar o utilizar la información para fines diferentes a los permitidos por la ley o por la institución.

6.11. Responsable Institucional de Protección de Datos Personales: La Dirección designará un responsable institucional para coordinar el cumplimiento de la presente política y actuar como punto de contacto frente a consultas, reclamos y requerimientos relacionados con el tratamiento de datos personales. Entre sus funciones estarán:

- Coordinar la implementación y actualización del Programa Integral de Protección de Datos Personales.
- Asesorar a los procesos en el cumplimiento de la normatividad aplicable.
- Coordinar la atención de consultas, reclamos y solicitudes de los titulares.
- Hacer seguimiento al cumplimiento de los planes de acción derivados de auditorías, incidentes o cambios normativos.
- Promover la mejora continua de la gestión de datos personales y la cultura institucional de protección de la información.

7. CATEGORÍAS DE TITULARES

En desarrollo de sus actividades académicas, administrativas, comerciales e institucionales, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., como Institución de Educación para el Trabajo y el Desarrollo Humano (IETDH), realiza el tratamiento de datos personales pertenecientes a diferentes grupos de interés. Para efectos de la presente política, se establecen las siguientes categorías de titulares:

7.1. Aspirantes: Corresponde a las personas que manifiestan interés en ingresar a los programas de formación, cursos, diplomados o demás servicios ofrecidos por la institución.

Entre los datos tratados se encuentran, entre otros:

- Datos de identificación.
- Datos de contacto.
- Información académica.
- Información laboral (cuando aplique).
- Información suministrada mediante formularios físicos o digitales.
- Información obtenida a través de campañas institucionales, eventos o canales de atención.

El tratamiento de esta información tiene como finalidad gestionar procesos de inscripción, admisión, orientación, promoción institucional y seguimiento comercial.

7.2. Estudiantes: Comprende a las personas matriculadas en cualquiera de los programas académicos ofertados por la institución.

El tratamiento de sus datos personales podrá comprender:

- Información de identificación.
- Información académica.
- Historial de matrícula.
- Registros de evaluación.
- Asistencia.
- Información socioeconómica.
- Información financiera relacionada con obligaciones académicas.
- Registros de bienestar institucional.
- Evidencias académicas.
- Datos biométricos cuando exista autorización y sean necesarios para la prestación del servicio educativo.

La información será utilizada para garantizar la adecuada prestación del servicio educativo y el cumplimiento de las obligaciones legales e institucionales.

7.3. Padres de Familia, Acudientes y Responsables: Corresponde a los padres de familia, acudientes, representantes legales o responsables económicos de estudiantes menores de edad o cuando las condiciones académicas así lo requieran.

El tratamiento comprenderá la información necesaria para:

- Gestión académica.
- Contacto institucional.
- Procesos administrativos.
- Facturación.
- Seguimiento académico.
- Bienestar institucional.
- Atención de situaciones disciplinarias o administrativas.

7.4. Egresados: Incluye a quienes culminaron satisfactoriamente programas de formación ofrecidos por la institución.

La información podrá ser utilizada para:

- Expedición de certificados.
- Seguimiento a egresados.
- Estudios de impacto.
- Encuestas de satisfacción.
- Actualización de información.
- Promoción de educación continua.
- Bolsa de empleo.
- Actividades de relacionamiento institucional.

7.5. Docentes e Instructores: Comprende al personal docente vinculado mediante cualquier modalidad contractual.

El tratamiento de sus datos personales se realizará para:

- Procesos de selección y vinculación.
- Administración contractual.
- Gestión académica.
- Evaluación del desempeño.
- Formación y capacitación.
- Nómina y obligaciones laborales.
- Cumplimiento de obligaciones legales.

7.6. Colaboradores y Personal Administrativo: Corresponde al personal administrativo, directivo y demás colaboradores vinculados a la institución.

La información será tratada para:

- Administración del talento humano.
- Seguridad y salud en el trabajo.

- Nómina.
- Bienestar laboral.
- Evaluación del desempeño.
- Gestión contractual.
- Cumplimiento de obligaciones legales.

7.7. Contratistas y Prestadores de Servicios: Incluye personas naturales o jurídicas que prestan servicios a la institución.

El tratamiento de sus datos personales tendrá como finalidad:

- Gestión contractual.
- Verificación de requisitos.
- Supervisión contractual.
- Facturación y pagos.
- Cumplimiento de obligaciones tributarias y legales.
- Control de acceso a las instalaciones.

7.8. Proveedores: Comprende las personas naturales o jurídicas que suministran bienes o servicios a la institución.

Sus datos podrán ser utilizados para:

- Evaluación y selección.
- Contratación.
- Gestión de compras.
- Pagos.
- Seguimiento al desempeño.
- Cumplimiento de obligaciones contractuales y legales.

7.9. Aliados Estratégicos y Entidades Conveniadas: Incluye entidades públicas y privadas con las cuales la institución mantiene convenios académicos, administrativos, empresariales o de cooperación.

La información tratada estará orientada a:

- Administración de convenios.
- Desarrollo de proyectos.
- Prácticas empresariales.
- Actividades de extensión.
- Investigación.
- Cooperación institucional.

7.10. Visitantes: Comprende las personas que ingresan a las instalaciones de la institución por motivos académicos, administrativos, comerciales o institucionales.

Podrán tratarse datos relacionados con:

- Identificación.
- Registro de ingreso y salida.
- Imágenes captadas mediante sistemas de videovigilancia.
- Información de contacto cuando sea requerida.

7.11. Usuarios de Plataformas Digitales y Canales Electrónicos: Corresponde a las personas que interactúan con la institución mediante:

- Sitio web institucional.
- Plataforma académica Q10.
- Plataformas virtuales de aprendizaje.
- Formularios electrónicos.
- Correo institucional.
- WhatsApp Business.
- Redes sociales institucionales.
- Chat institucional.
- Campañas digitales.
- Otros servicios tecnológicos autorizados.

El tratamiento de esta información permitirá gestionar solicitudes, procesos académicos, atención al usuario, campañas institucionales, autenticación de usuarios, seguridad informática y mejora de los servicios digitales.

7.12. Participantes en Eventos, Cursos y Formación Continua: Incluye las personas que participan en seminarios, diplomados, cursos cortos, capacitaciones, eventos institucionales, actividades de extensión o educación continua.

La información será utilizada para:

- Inscripción.
- Control de asistencia.
- Certificación.
- Evaluación de satisfacción.
- Seguimiento académico.
- Promoción de nuevas actividades de formación.

7.13. Otras Categorías de Titulares: La institución podrá tratar datos personales pertenecientes a otras categorías de titulares cuando exista una finalidad legítima, autorización del titular o habilitación legal que lo permita, garantizando en todo momento el cumplimiento de los principios y obligaciones establecidos en la legislación vigente sobre protección de datos personales.

Parágrafo: Cada proceso institucional será responsable de identificar las categorías de titulares que administra, definir las finalidades específicas del tratamiento, implementar los controles de seguridad correspondientes y garantizar que el tratamiento de los datos personales se realice conforme a la presente política, la legislación vigente y los procedimientos del Sistema de Gestión de la Calidad, especialmente el ACA-PD09 – Gestión de la Información Documentada, el ACA-PD07 – Gestión de Riesgos y Oportunidades y el ACA-PD13 – Gestión y Planificación de los Cambios.

8. FINALIDADES DEL TRATAMIENTO DE LOS DATOS PERSONALES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en calidad de responsable del Tratamiento, realizará el tratamiento de los datos personales de los titulares de conformidad con la legislación vigente y exclusivamente para las finalidades legítimas, específicas, explícitas e informadas en la presente política o en la autorización otorgada por el titular, garantizando en todo momento el respeto por sus derechos fundamentales.

Las finalidades del tratamiento se desarrollan de acuerdo con la naturaleza de la relación que exista entre el titular y la institución.

8.1. Finalidades Generales: Los datos personales podrán ser tratados para:

- Identificar y autenticar a los titulares.
- Mantener actualizadas las bases de datos institucionales.
- Gestionar las relaciones académicas, administrativas, comerciales y contractuales.
- Dar cumplimiento a obligaciones legales, contractuales y reglamentarias.
- Atender solicitudes, consultas, peticiones, quejas, reclamos, sugerencias y felicitaciones.
- Garantizar la seguridad de las instalaciones, bienes, personas e información institucional.
- Gestionar la información documentada y los registros institucionales.
- Implementar acciones de seguimiento, evaluación y mejora continua.
- Elaborar estadísticas e indicadores institucionales con fines administrativos y de gestión.
- Gestionar auditorías internas y externas.
- Dar cumplimiento a requerimientos de autoridades competentes.
- Proteger los derechos e intereses legítimos de la institución y de los titulares.

8.2. Aspirantes: Los datos personales de los aspirantes podrán tratarse para:

- Gestionar procesos de inscripción y admisión.
- Brindar orientación académica.
- Validar requisitos de ingreso.
- Programar entrevistas o pruebas de ingreso.
- Enviar información sobre programas académicos, costos, promociones y convocatorias.
- Realizar seguimiento al proceso de matrícula.
- Elaborar estadísticas institucionales.
- Gestionar campañas de mercadeo educativo previamente autorizadas.

8.3. Estudiantes: La información de los estudiantes podrá tratarse para:

- Formalizar el proceso de matrícula.
- Administrar la historia académica.
- Gestionar el desarrollo de los programas de formación.
- Registrar asistencia, evaluaciones y resultados académicos.
- Expedir certificados, constancias y demás documentos académicos.
- Administrar plataformas académicas y virtuales.
- Gestionar prácticas empresariales.
- Realizar seguimiento académico y de permanencia.
- Gestionar procesos disciplinarios cuando corresponda.
- Administrar servicios de bienestar institucional.
- Gestionar procesos de certificación.
- Atender requerimientos de las autoridades educativas.
- Cumplir obligaciones legales derivadas de la prestación del servicio educativo.

8.4. Padres de Familia, Acudientes y Responsables: Los datos personales podrán tratarse para:

- Mantener comunicación permanente sobre el proceso académico del estudiante.
- Gestionar procesos administrativos y financieros.
- Informar novedades académicas y disciplinarias.
- Gestionar autorizaciones relacionadas con menores de edad.
- Atender solicitudes y requerimientos.
- Realizar procesos de facturación y recaudo.

8.5. Egresados: La institución podrá tratar la información de los egresados para:

- Mantener actualizado el directorio institucional.
- Expedir certificados.
- Realizar estudios de impacto.
- Gestionar procesos de seguimiento a egresados.
- Administrar la bolsa de empleo.
- Invitar a programas de formación continua.
- Promover actividades institucionales.
- Aplicar encuestas de satisfacción.

8.6. Docentes e Instructores: La información de los docentes podrá tratarse para:

- Procesos de selección y vinculación.
- Gestión contractual y administrativa.
- Administración de nómina.

- Evaluación del desempeño.
- Formación y capacitación.
- Gestión académica.
- Asignación de carga académica.
- Control de asistencia.
- Cumplimiento de obligaciones laborales y legales.

8.7. Colaboradores y Personal Administrativo: Los datos personales podrán utilizarse para:

- Administración del talento humano.
- Procesos de selección.
- Vinculación laboral.
- Gestión de nómina.
- Seguridad y Salud en el Trabajo.
- Evaluación del desempeño.
- Capacitación.
- Bienestar laboral.
- Gestión disciplinaria.
- Cumplimiento de obligaciones legales.

8.8. Contratistas y Proveedores: La institución podrá tratar los datos personales para:

- Selección y evaluación.
- Celebración y ejecución de contratos.
- Gestión documental contractual.
- Facturación y pagos.
- Cumplimiento de obligaciones tributarias.
- Evaluación del desempeño.
- Gestión de compras.
- Control de acceso a las instalaciones.
- Administración de convenios.

8.9. Aliados Estratégicos: La información podrá utilizarse para:

- Administración de convenios.
- Desarrollo de proyectos.
- Cooperación institucional.
- Investigación.
- Extensión.
- Prácticas empresariales.
- Gestión documental.
- Seguimiento de compromisos.

8.10. Participantes en Educación Continua: Los datos podrán tratarse para:

- Inscripciones.
- Registro de asistencia.
- Evaluaciones.
- Certificación.
- Encuestas de satisfacción.
- Gestión académica.
- Promoción de nuevos programas.

8.11. Visitantes: Los datos personales de visitantes podrán tratarse para:

- Control de ingreso y salida.
- Seguridad física.
- Videovigilancia.
- Atención de emergencias.
- Protección de bienes institucionales.
- Control de acceso.

8.12. Usuarios de Plataformas Tecnológicas: La información tratada mediante plataformas institucionales podrá utilizarse para:

- Administración de usuarios.
- Autenticación.
- Gestión académica.
- Prestación de servicios virtuales.
- Recuperación de credenciales.
- Soporte técnico.
- Seguridad informática.
- Gestión de incidencias.
- Auditoría de accesos.
- Conservación de registros electrónicos.

Incluye, entre otras:

- Plataforma Q10.
- Plataformas virtuales de aprendizaje.
- Sitio web institucional.
- Formularios electrónicos.
- Correo institucional.
- Google Workspace.
- Servicios en la nube.
- Aplicaciones móviles institucionales.
- Sistemas administrativos.

8.13. Mercadeo Institucional y Comunicaciones: Cuando exista autorización del titular, la institución podrá tratar los datos personales para:

- Informar sobre programas académicos.
- Promocionar cursos, diplomados y servicios.
- Enviar boletines informativos.
- Compartir invitaciones a eventos.
- Gestionar campañas institucionales.
- Realizar encuestas.
- Gestionar programas de fidelización.
- Difundir actividades académicas y culturales.

Las comunicaciones podrán realizarse mediante:

- Correo electrónico.
- Llamadas telefónicas.
- Mensajes SMS.
- WhatsApp Business.
- Redes sociales institucionales.
- Plataformas de mensajería autorizadas.
- Otros medios autorizados por el titular.

8.14. Videovigilancia: Las imágenes captadas por los sistemas de videovigilancia podrán utilizarse para:

- Protección de personas.
- Seguridad institucional.
- Protección de bienes.
- Prevención de incidentes.
- Atención de requerimientos de autoridades competentes.
- Investigación de incidentes de seguridad.

8.15. Cumplimiento Legal: Los datos personales podrán tratarse cuando sea necesario para:

- Cumplir obligaciones legales.
- Atender requerimientos judiciales.
- Responder solicitudes de autoridades administrativas.
- Cumplir obligaciones tributarias.
- Cumplir obligaciones laborales.
- Cumplir obligaciones contractuales.
- Atender auditorías y procesos de inspección, vigilancia y control.

8.16. Mejora Continua y Gestión Institucional: La institución podrá tratar información personal para:

- Evaluar la calidad de los servicios.
- Gestionar indicadores institucionales.
- Identificar oportunidades de mejora.
- Gestionar riesgos.
- Ejecutar auditorías internas y externas.
- Realizar revisiones por la dirección.
- Desarrollar proyectos de transformación digital.
- Fortalecer la seguridad de la información.
- Optimizar los procesos institucionales conforme al Sistema de Gestión de la Calidad.

Parágrafo Primero: Las finalidades descritas en el presente capítulo podrán desarrollarse mediante el uso de herramientas tecnológicas, sistemas de información, plataformas académicas, aplicaciones institucionales y servicios en la nube debidamente autorizados, garantizando en todo momento el cumplimiento de los principios de legalidad, finalidad, necesidad, proporcionalidad, seguridad y confidencialidad establecidos en la legislación vigente.

Parágrafo Segundo: Cuando el tratamiento de datos personales tenga una finalidad diferente a las aquí descritas o requiera una autorización adicional conforme a la legislación vigente, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. solicitará previamente la autorización correspondiente al titular o dará cumplimiento a las condiciones legales que habiliten dicho tratamiento.

9. DERECHOS DEL TITULAR

En cumplimiento de la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás disposiciones que regulan la protección de datos personales en Colombia, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. garantiza a los titulares de los datos personales el ejercicio pleno y efectivo de sus derechos, los cuales podrán ejercerse en cualquier momento a través de los canales institucionales establecidos para tal fin.

9.1. Derecho a Conocer: Conocer, acceder y consultar de manera gratuita los datos personales que sean objeto de tratamiento por parte de la institución, así como obtener información sobre las finalidades, categorías de datos tratados, responsables y terceros autorizados para su tratamiento, de conformidad con las condiciones establecidas en la legislación vigente.

9.2. Derecho a Actualizar: Solicitar la actualización de sus datos personales cuando estos hayan sufrido modificaciones o cambios que afecten su vigencia, exactitud o utilidad para las finalidades del tratamiento.

9.3. Derecho a Rectificar: Solicitar la corrección de los datos personales cuando sean inexactos, incompletos, fraccionados, induzcan a error o no correspondan con la realidad del titular, aportando los documentos que soporten la solicitud cuando sea necesario.

9.4. Derecho a Solicitar Prueba de la Autorización: Solicitar evidencia de la autorización otorgada para el tratamiento de sus datos personales, salvo cuando la ley establezca que dicha autorización no sea requerida.

9.5. Derecho a Ser Informado: Ser informado, previa solicitud, respecto del uso que la institución ha dado a sus datos personales, las finalidades del tratamiento, las categorías de información administradas y los terceros con quienes, cuando sea procedente, se haya compartido la información.

9.6. Derecho a Revocar la Autorización: Revocar en cualquier momento la autorización otorgada para el tratamiento de sus datos personales cuando no exista un deber legal o contractual que obligue a la institución a conservar la información, de conformidad con la normatividad vigente.

9.7. Derecho a Solicitar la Supresión de los Datos: Solicitar la eliminación de sus datos personales cuando considere que no están siendo tratados conforme a los principios, derechos y garantías constitucionales y legales, siempre que no exista una obligación legal, contractual, académica, administrativa o judicial que obligue a la institución a conservarlos.

9.8. Derecho a Presentar Consultas y Reclamos: Presentar consultas, peticiones, quejas o **reclamos** relacionados con el tratamiento de sus datos personales ante **SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S.**, de conformidad con los procedimientos establecidos en la presente política.

9.9. Derecho a Presentar Quejas ante la Superintendencia de Industria y Comercio: Presentar quejas ante la **Superintendencia de Industria y Comercio (SIC)** cuando considere que se ha presentado una presunta infracción a las normas sobre protección de datos personales, una vez haya agotado el trámite de consulta o reclamo ante la institución, salvo las excepciones previstas por la legislación vigente.

9.10. Derecho a la Confidencialidad: Exigir que las personas autorizadas para el tratamiento de los datos personales mantengan la reserva y confidencialidad de la información, incluso después de finalizada la relación con la institución, salvo las excepciones previstas en la ley.

9.11. Derecho a la Seguridad de la Información: Recibir garantías respecto de la implementación de medidas administrativas, técnicas, físicas y organizacionales orientadas a proteger los datos personales contra pérdida, alteración, acceso no autorizado, uso indebido, destrucción o divulgación no autorizada.

9.12. Derecho a la Atención Oportuna: Obtener respuesta a las consultas, solicitudes y reclamos dentro de los términos establecidos en la legislación vigente sobre protección de datos personales.

9.13. Derecho a la No Discriminación: No ser objeto de discriminación por ejercer los derechos relacionados con la protección de sus datos personales o por solicitar información sobre el tratamiento realizado por la institución.

9.14. Derecho a Ejercer sus Derechos por Medio de Representante: Los derechos previstos en la presente política podrán ser ejercidos directamente por el titular o por su representante legal, apoderado, causahabientes o por las personas autorizadas conforme a la legislación vigente, acreditando la calidad en la que actúan.

Parágrafo Primero: El ejercicio de los derechos previstos en la presente política será gratuito y podrá realizarse mediante los canales de atención definidos por la institución. Cuando las solicitudes sean manifiestamente infundadas, excesivas o repetitivas, la institución podrá actuar conforme a lo permitido por la legislación vigente.

Parágrafo Segundo: El ejercicio de los derechos del titular no afectará el tratamiento de la información cuando este sea necesario para el cumplimiento de obligaciones legales, contractuales, académicas, administrativas, tributarias, laborales, judiciales o regulatorias, ni cuando exista un deber de conservación documental establecido por la legislación colombiana o por el **Sistema de Gestión de la Calidad** de la institución.

Parágrafo Tercero: SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. dispondrá de canales presenciales y electrónicos para facilitar el ejercicio de los derechos de los titulares, garantizando la trazabilidad de las solicitudes, la protección de la información suministrada y el cumplimiento de los términos legales de respuesta, en concordancia con los principios de transparencia, seguridad, confidencialidad y mejora continua.

10. DEBERES DEL RESPONSABLE DEL TRATAMIENTO

En cumplimiento de lo establecido en la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás disposiciones aplicables, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en su calidad de Responsable del Tratamiento de Datos Personales, se compromete a garantizar el cumplimiento de los principios, derechos y obligaciones relacionados con la protección de los datos personales, implementando las medidas administrativas, técnicas, jurídicas y organizacionales necesarias para asegurar un tratamiento adecuado de la información.

Para tal efecto, la institución deberá cumplir con los siguientes deberes:

10.1. Garantizar el Ejercicio del Derecho al Hábeas Data: Garantizar al titular el pleno y efectivo ejercicio de los derechos de acceso, consulta, actualización, rectificación, supresión de datos personales, revocatoria de la autorización y demás derechos establecidos en la legislación vigente.

10.2. Solicitar y Conservar la Autorización: Solicitar la autorización previa, expresa e informada del titular cuando sea requerida por la ley y conservar evidencia de dicha autorización, garantizando su disponibilidad cuando sea solicitada por el titular o por la autoridad competente.

10.3. Informar la Finalidad del Tratamiento: Informar al titular, de manera clara, suficiente y previa a la recolección de los datos personales, las finalidades específicas para las cuales será utilizada su información, así como los derechos que le asisten y los mecanismos para ejercerlos.

10.4. Garantizar la Veracidad y Actualización de la Información: Adoptar medidas razonables para que la información personal sea veraz, completa, exacta, actualizada, comprobable y comprensible, realizando las actualizaciones, rectificaciones o supresiones que resulten procedentes.

10.5. Conservar la Seguridad de los Datos Personales: Implementar y mantener medidas administrativas, físicas, técnicas y tecnológicas orientadas a proteger los datos personales contra pérdida, alteración, acceso no autorizado, uso indebido, destrucción, divulgación o cualquier otra forma de tratamiento no autorizada.

10.6. Garantizar la Confidencialidad: Exigir a todos los colaboradores, contratistas, proveedores y terceros autorizados el cumplimiento del deber de confidencialidad respecto de los datos personales tratados, incluso después de finalizada la relación laboral, contractual o institucional.

10.7. Atender Consultas y Reclamos: Recibir, tramitar y responder oportunamente las consultas, peticiones, quejas y reclamos relacionados con el tratamiento de datos personales, garantizando el cumplimiento de los términos y procedimientos establecidos en la legislación vigente y en la presente política.

10.8. Informar Incidentes de Seguridad: Adoptar las acciones necesarias para gestionar los incidentes que comprometan la seguridad de los datos personales y, cuando corresponda, informar oportunamente a los titulares y a las autoridades competentes, de conformidad con la normatividad vigente.

10.9. Garantizar el Cumplimiento por Parte de los Encargados: Verificar que los encargados del tratamiento de datos personales cumplan las obligaciones legales, contractuales y de seguridad establecidas por la institución, formalizando las responsabilidades mediante los instrumentos jurídicos correspondientes.

10.10. Conservar la Información Conforme a la Ley: Conservar los datos personales únicamente durante el tiempo necesario para cumplir las finalidades del tratamiento, las obligaciones legales, contractuales, académicas, tributarias, laborales o regulatorias, aplicando posteriormente los criterios institucionales para su archivo, conservación o eliminación segura.

10.11. Implementar el Principio de Responsabilidad Demostrada: Implementar políticas, procedimientos, controles, indicadores, actividades de seguimiento y mecanismos de mejora continua que permitan demostrar el cumplimiento de las obligaciones establecidas en la legislación sobre protección de datos personales y la eficacia de las medidas implementadas.

10.12. Capacitar y Sensibilizar al Personal: Promover programas permanentes de formación y sensibilización dirigidos a colaboradores, docentes, contratistas y demás personas que intervengan en el tratamiento de datos personales, fortaleciendo la cultura institucional de protección de la información.

10.13. 10.13 Gestionar los Riesgos Asociados al Tratamiento de Datos Personales: Identificar, evaluar, controlar y realizar seguimiento a los riesgos relacionados con el tratamiento de datos personales, implementando acciones preventivas y correctivas orientadas a minimizar su impacto y fortalecer la seguridad de la información.

10.14. Mantener Actualizada la Información Documentada: Actualizar la presente política, los procedimientos, formatos, registros y demás información documentada relacionada con la protección de datos personales cuando se presenten cambios normativos, organizacionales, tecnológicos o de otra naturaleza que afecten su aplicación.

10.15. Cooperar con las Autoridades Competentes: Atender oportunamente los requerimientos formulados por la Superintendencia de Industria y Comercio y demás autoridades competentes, suministrando la información y colaboración necesarias para el ejercicio de sus funciones de inspección, vigilancia y control.

Parágrafo Primero: Los deberes establecidos en el presente capítulo deberán ser observados por todas las dependencias, colaboradores, docentes, contratistas, proveedores y terceros que intervengan en el tratamiento de datos personales por cuenta de **SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S.**, dentro del ámbito de sus responsabilidades y competencias.

Parágrafo Segundo: El cumplimiento de estos deberes será objeto de seguimiento mediante auditorías internas, revisión de indicadores, evaluación de riesgos, gestión de incidentes, revisiones por la Dirección y demás mecanismos definidos por el **Sistema de Gestión de la Calidad**, con el propósito de garantizar la mejora continua del Programa Institucional de Protección de Datos Personales.

Parágrafo Tercero: El incumplimiento de las obligaciones establecidas en la presente política podrá dar lugar a la adopción de las medidas administrativas, disciplinarias, contractuales o legales que correspondan, sin perjuicio de las acciones que puedan ejercer los titulares de los datos personales o las autoridades competentes conforme a la legislación vigente.

11. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en calidad de responsable del Tratamiento de Datos Personales, solicitará la autorización previa, expresa e informada del titular antes de realizar el tratamiento de sus datos personales, salvo en los casos expresamente exceptuados por la legislación colombiana.

La autorización constituye el consentimiento otorgado por el titular para que la institución recolecte, almacene, use, consulte, actualice, circule, transfiera, transmita, conserve y suprima sus datos personales conforme a las finalidades establecidas en la presente política y en la normatividad vigente.

La institución garantizará que la autorización sea obtenida mediante mecanismos que permitan demostrar su otorgamiento y conservar la evidencia correspondiente durante el tiempo que sea necesario para atender las finalidades del tratamiento y las obligaciones legales aplicables.

11.1. Características de la Autorización: La autorización deberá cumplir, como mínimo, las siguientes condiciones:

- Ser previa al tratamiento de los datos personales, salvo las excepciones legales.
- Ser expresa, manifestando de forma clara la voluntad del titular.
- Ser informada, indicando las finalidades del tratamiento, los derechos del titular, la identificación del responsable y los canales para ejercer dichos derechos.
- Ser verificable, permitiendo demostrar que fue otorgada por el titular mediante los mecanismos definidos por la institución.

11.2. Medios para Obtener la Autorización: La autorización podrá obtenerse mediante cualquiera de los siguientes mecanismos, siempre que permitan conservar evidencia de su otorgamiento:

- Formularios físicos de inscripción o matrícula.
- Formularios electrónicos.
- Plataformas académicas o administrativas.
- Sitio web institucional.
- Firma manuscrita.
- Firma electrónica o digital.
- Correo electrónico.
- Grabaciones de voz cuando la legislación lo permita.
- Sistemas biométricos debidamente autorizados.
- Aplicaciones institucionales.
- Otros mecanismos tecnológicos legalmente válidos.

11.3. Contenido de la Autorización: La autorización deberá informar al titular, como mínimo:

- La identidad y datos de contacto del Responsable del Tratamiento.
- Las finalidades específicas para las cuales serán tratados los datos personales.
- Los derechos que le asisten como titular.
- Los canales habilitados para presentar consultas, solicitudes o reclamos.
- La posibilidad de conocer la presente Política de Tratamiento de Datos Personales.

11.4. Conservación de la Autorización: La institución conservará la evidencia de la autorización otorgada por el titular durante el tiempo que resulte necesario para demostrar el cumplimiento de la legislación vigente, garantizar el ejercicio de los derechos del titular y atender requerimientos de las autoridades competentes.

La conservación podrá realizarse en medios físicos, electrónicos o digitales que garanticen la autenticidad, integridad, disponibilidad, confidencialidad y trazabilidad de la información.

11.5. Revocatoria de la Autorización: El titular podrá revocar en cualquier momento la autorización otorgada para el tratamiento de sus datos personales, siempre que no exista un deber legal, contractual, académico, administrativo o judicial que obligue a la institución a continuar con el tratamiento o conservar la información.

La solicitud de revocatoria será atendida conforme al procedimiento establecido en la presente política y en los términos definidos por la legislación vigente.

11.6. Casos en los que no se Requiere Autorización: De conformidad con la Ley 1581 de 2012, no será necesaria la autorización del titular cuando el tratamiento de los datos personales corresponda, entre otros, a los siguientes casos:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos, siempre que se adopten las medidas de protección correspondientes.
- Datos relacionados con el Registro Civil de las personas.
- Las demás situaciones previstas por la legislación vigente.

11.7. Actualización de la Autorización: Cuando se modifiquen de manera sustancial las finalidades del tratamiento, cambien las condiciones bajo las cuales se obtuvo la autorización o exista una obligación legal que así lo exija, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. solicitará una nueva autorización al titular o informará oportunamente los cambios, según corresponda.

Parágrafo Primero: La autorización para el tratamiento de datos personales podrá obtenerse de manera independiente o incorporarse dentro de contratos, formularios de inscripción, procesos de matrícula, convenios, registros electrónicos, plataformas institucionales u otros documentos utilizados por la institución, siempre que su contenido sea claro, específico, verificable y cumpla los requisitos establecidos en la legislación vigente.

Parágrafo Segundo: Cuando el tratamiento involucre datos personales sensibles o datos personales de niños, niñas y adolescentes, la institución obtendrá la autorización conforme a los requisitos especiales previstos en la legislación colombiana, garantizando el respeto por los derechos fundamentales de sus titulares y la aplicación del principio del interés superior del menor.

Parágrafo Tercero: Las evidencias relacionadas con las autorizaciones para el tratamiento de datos personales constituyen información documentada del Sistema de Gestión de la Calidad y deberán administrarse conforme al ACA-PD09 – Gestión de la Información Documentada, garantizando su adecuada identificación, conservación, protección, disponibilidad y trazabilidad durante el tiempo de retención definido por la institución y la legislación vigente.

12. TRATAMIENTO DE DATOS PERSONALES SENSIBLES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en cumplimiento de la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás disposiciones aplicables, reconoce que los datos personales sensibles requieren un nivel especial de protección debido a que su tratamiento indebido puede afectar la intimidad del titular o generar actos de discriminación.

En consecuencia, la institución implementará medidas jurídicas, administrativas, técnicas y organizacionales para garantizar el tratamiento seguro, confidencial y restringido de este tipo de información.

12.1. Definición de Datos Sensibles: Se consideran datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, entre ellos:

- Origen racial o étnico.
- Orientación política.
- Convicciones religiosas o filosóficas.
- Pertenencia a sindicatos u organizaciones sociales.
- Datos relativos a la salud física o mental.
- Información biométrica.
- Datos genéticos.
- Vida sexual.
- Cualquier otra información que la legislación vigente clasifique como dato sensible.

12.2. Principios para el Tratamiento de Datos Sensibles: La institución realizará el tratamiento de datos sensibles observando los siguientes criterios:

- Se efectuará únicamente cuando exista una finalidad legítima y necesaria.
- Se limitará al mínimo indispensable para el cumplimiento de la finalidad autorizada.
- Se garantizará la confidencialidad y el acceso restringido.
- Se implementarán controles de seguridad reforzados.
- Se respetarán en todo momento los derechos fundamentales del titular.

12.3. Autorización para el Tratamiento: El tratamiento de datos sensibles requerirá la autorización previa, expresa e informada del titular, salvo las excepciones previstas por la legislación colombiana.

Al momento de solicitar la autorización, la institución informará claramente:

- Que el suministro de los datos sensibles es facultativo.
- La finalidad específica del tratamiento.
- Los derechos que asisten al titular.
- Los mecanismos para ejercer dichos derechos.

La negativa del titular a suministrar datos sensibles no podrá ser utilizada como criterio de discriminación cuando dichos datos no sean indispensables para la prestación del servicio o el cumplimiento de una obligación legal.

12.4. Finalidades del Tratamiento de Datos Sensibles: Cuando resulte estrictamente necesario y exista autorización o habilitación legal, la institución podrá tratar datos sensibles para las siguientes finalidades:

- Gestionar procesos de bienestar institucional.
- Atender situaciones relacionadas con la salud de estudiantes, docentes, colaboradores o visitantes en casos de emergencia.
- Implementar programas de Seguridad y Salud en el Trabajo.
- Gestionar procesos de inclusión, permanencia y atención diferencial.
- Cumplir obligaciones legales o requerimientos de autoridades competentes.
- Administrar sistemas de control de acceso mediante mecanismos biométricos, cuando estos sean implementados y exista autorización del titular.
- Atender requerimientos derivados de procesos disciplinarios, judiciales o administrativos cuando la ley lo autorice.

12.5. Medidas de Protección: Para garantizar la protección de los datos sensibles, la institución implementará, entre otras, las siguientes medidas:

- Restricción de acceso únicamente al personal autorizado.
- Control de perfiles y permisos de acceso.
- Protección física y lógica de los archivos.
- Uso de contraseñas seguras y mecanismos de autenticación.
- Copias de seguridad y planes de recuperación de la información.
- Registro y trazabilidad de los accesos cuando técnicamente sea posible.
- Capacitación permanente del personal autorizado.
- Suscripción de compromisos de confidencialidad por parte de quienes tengan acceso a este tipo de información.

12.6. Prohibiciones: La institución se abstendrá de:

- Utilizar datos sensibles para finalidades diferentes a las autorizadas o permitidas por la ley.
- Divulgar información sensible a terceros no autorizados.
- Solicitar datos sensibles cuando no sean necesarios para el cumplimiento de la finalidad del tratamiento.
- Realizar tratamientos que puedan generar discriminación o vulneración de los derechos fundamentales del titular.

12.7. Conservación de los Datos Sensibles: Los datos sensibles serán conservados únicamente durante el tiempo necesario para cumplir la finalidad que justificó su tratamiento o mientras exista una obligación legal o contractual que exija su conservación.

Una vez desaparecida dicha necesidad, la institución procederá a su archivo, anonimización, bloqueo o eliminación segura, conforme a la legislación vigente y a los procedimientos institucionales de gestión de la información documentada.

Parágrafo Primero: El acceso a los datos sensibles estará restringido exclusivamente a las personas que, por razón de sus funciones, requieran conocer dicha información para el cumplimiento de sus responsabilidades, quienes deberán observar estrictamente el deber de confidencialidad y las políticas de seguridad de la información de la institución.

Parágrafo Segundo: Cuando la institución implemente nuevos procesos, plataformas tecnológicas o servicios que impliquen el tratamiento de datos sensibles, deberá realizar previamente una evaluación de riesgos, establecer las medidas de control correspondientes y actualizar, cuando sea necesario, la presente política y los procedimientos asociados, en concordancia con el ACA-PD07 – Gestión de Riesgos y Oportunidades, el ACA-PD09 – Gestión de la Información Documentada y el ACA-PD13 – Gestión y Planificación de los Cambios.

Parágrafo Tercero: El tratamiento de datos personales sensibles será objeto de seguimiento mediante auditorías internas, revisión de controles de seguridad, análisis de incidentes y evaluación periódica de riesgos, con el fin de garantizar el cumplimiento de la legislación vigente, fortalecer la seguridad de la información y promover la mejora continua del Sistema de Gestión de la Calidad.

13. TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en cumplimiento de la Constitución Política de Colombia, la Ley 1581 de 2012, el Decreto 1074 de 2015, el Código de la Infancia y la Adolescencia (Ley 1098 de 2006) y demás disposiciones aplicables, reconoce que los datos personales de los niños, niñas y adolescentes (NNA) gozan de especial protección y, por tanto, su tratamiento se realizará bajo criterios de responsabilidad, confidencialidad, seguridad y respeto por el interés superior del menor.

La institución únicamente realizará el tratamiento de datos personales de menores de edad cuando dicho tratamiento sea necesario para el desarrollo de sus actividades académicas, administrativas o de bienestar, garantizando en todo momento la protección de sus derechos fundamentales.

13.1. Principios para el Tratamiento de Datos de Menores: El tratamiento de datos personales de niños, niñas y adolescentes se realizará conforme a los siguientes principios:

- Prevalencia del interés superior del niño, niña o adolescente.
- Respeto por sus derechos fundamentales.
- Protección integral de su información personal.
- Necesidad y proporcionalidad del tratamiento.
- Confidencialidad y acceso restringido.
- Seguridad de la información.
- Finalidad legítima y previamente informada.
- Responsabilidad demostrada por parte de la institución.

13.2. Autorización para el Tratamiento: El tratamiento de datos personales de menores de edad requerirá la autorización previa, expresa e informada del padre, madre o representante legal, salvo las excepciones previstas en la legislación vigente.

Cuando la naturaleza del tratamiento y el nivel de madurez del menor lo permitan, la institución procurará escuchar su opinión y tener en cuenta su voluntad, conforme al principio de autonomía progresiva y a las disposiciones del Código de la Infancia y la Adolescencia.

13.3. Finalidades del Tratamiento: La institución podrá tratar los datos personales de niños, niñas y adolescentes para las siguientes finalidades:

- Gestionar procesos de inscripción, admisión y matrícula.
- Administrar el proceso académico.

- Registrar asistencia, evaluaciones y desempeño académico.
- Gestionar procesos de certificación.
- Administrar plataformas académicas y virtuales.
- Desarrollar actividades pedagógicas, culturales, deportivas y de bienestar.
- Gestionar procesos de orientación y acompañamiento académico.
- Atender situaciones de emergencia que puedan afectar la integridad del menor.
- Cumplir obligaciones legales y requerimientos de las autoridades competentes.
- Mantener comunicación con los padres, acudientes o representantes legales.
- Gestionar procesos administrativos y financieros relacionados con la prestación del servicio educativo.
- Realizar seguimiento a la permanencia y trayectoria educativa.
- Administrar las prácticas de seguridad institucional y control de acceso.

13.4. Datos que Podrán ser Tratados: Dependiendo de la finalidad autorizada, la institución podrá tratar, entre otros:

- Datos de identificación.
- Información de contacto.
- Información académica.
- Información de matrícula.
- Registros de asistencia.
- Registros de evaluación.
- Información socioeconómica cuando sea necesaria.
- Información de salud únicamente cuando resulte indispensable para garantizar la atención, seguridad o bienestar del menor y exista autorización o habilitación legal.
- Imágenes captadas mediante sistemas de videovigilancia institucional.
- Fotografías, videos o material audiovisual, únicamente cuando exista autorización expresa para su uso con fines institucionales, académicos o de divulgación.

13.5. Medidas Especiales de Protección: La institución implementará medidas reforzadas para proteger la información de los menores, entre ellas:

- Acceso restringido únicamente al personal autorizado.
- Custodia segura de la información física y digital.
- Control de acceso a plataformas académicas.
- Protección mediante credenciales institucionales.
- Copias de seguridad de la información.
- Capacitación permanente del personal sobre protección de datos personales.
- Aplicación de controles de seguridad informática.
- Seguimiento periódico al cumplimiento de esta política.

13.6. Uso de Imágenes y Material Audiovisual: Las fotografías, videos, grabaciones de voz o cualquier otro material audiovisual en el que aparezcan niños, niñas o adolescentes únicamente serán utilizados para fines académicos, institucionales, pedagógicos, culturales o de divulgación autorizados por la institución, siempre que exista la autorización previa, expresa e informada del padre, madre o representante legal, salvo los casos permitidos por la legislación vigente.

La institución adoptará medidas para evitar el uso indebido, la reproducción no autorizada o la difusión que pueda afectar la dignidad, seguridad o privacidad del menor.

13.7. Restricciones del Tratamiento: La institución se abstendrá de:

- Tratar datos personales de menores para finalidades diferentes a las autorizadas.
- Divulgar información personal a terceros no autorizados.
- Solicitar información excesiva o innecesaria.
- Utilizar la información con fines discriminatorios.
- Publicar información personal en medios físicos o digitales sin la autorización correspondiente.
- Realizar cualquier tratamiento que pueda poner en riesgo los derechos fundamentales del menor.

13.8. Conservación de la Información: Los datos personales de los menores serán conservados únicamente durante el tiempo necesario para cumplir las finalidades del tratamiento o mientras exista una obligación legal, académica o administrativa que justifique su conservación.

Finalizado dicho término, la información será archivada, anonimizada o eliminada de manera segura conforme a la legislación vigente y a los procedimientos institucionales de gestión documental.

Parágrafo Primero: Los padres, madres, acudientes o representantes legales podrán ejercer en cualquier momento los derechos de acceso, consulta, actualización, rectificación, supresión y revocatoria de la autorización respecto de los datos personales del menor, de conformidad con los procedimientos establecidos en la presente política y la legislación vigente.

Parágrafo Segundo: Cuando el tratamiento de datos personales de niños, niñas y adolescentes implique el uso de nuevas tecnologías, plataformas digitales, herramientas de inteligencia artificial, servicios en la nube o aplicaciones institucionales, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S.

realizará previamente la evaluación de los riesgos asociados, implementará las medidas de seguridad correspondientes y garantizará el cumplimiento de los principios de protección de datos personales, en concordancia con el Sistema de Gestión de la Calidad y los procedimientos institucionales aplicables.

Parágrafo Tercero: El tratamiento de datos personales de niños, niñas y adolescentes será objeto de seguimiento periódico mediante auditorías internas, evaluación de riesgos, revisión de controles de seguridad y acciones de mejora continua, con el fin de garantizar el cumplimiento de la legislación vigente, proteger los derechos de los menores y fortalecer la confianza de la comunidad educativa en la gestión responsable de la información por parte de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S..

14. CANALES PARA CONSULTAS, PETICIONES, QUEJAS Y RECLAMOS

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en cumplimiento de la Ley 1581 de 2012 y el Decreto 1074 de 2015, pone a disposición de los titulares de los datos personales diferentes canales de atención para el ejercicio de sus derechos de acceso, consulta, actualización, rectificación, supresión, revocatoria de la autorización y presentación de peticiones, quejas o reclamos relacionados con el tratamiento de sus datos personales.

Las solicitudes podrán presentarse a través de cualquiera de los siguientes canales institucionales:

14.1. Atención Presencial: Los titulares podrán presentar sus solicitudes personalmente en las instalaciones de la institución durante los horarios de atención establecidos. **Dirección:** *Calle 4 No. 14-29, Líbano, Tolima*

14.2. Correo Electrónico: Las consultas, solicitudes, peticiones, quejas o reclamos relacionados con la protección de datos personales podrán remitirse al siguiente correo institucional:

Correo electrónico para Protección de Datos Personales: direccion@sysdatec.edu.co

Correo institucional de PQRSF: pqrsf@sysdatec.edu.co

14.3. Sitio Web Institucional: Los titulares podrán consultar la presente Política de Tratamiento de Datos Personales y presentar solicitudes mediante los formularios electrónicos o canales de contacto habilitados en el sitio web institucional.

Página web institucional: https://www.sysdatec.edu.co

14.4. Línea Telefónica y WhatsApp Institucional: La institución podrá atender consultas relacionadas con la protección de datos personales mediante los canales telefónicos y de mensajería institucional autorizados.

Los canales oficiales publicados por la institución serán utilizados únicamente para orientación, recepción de solicitudes y seguimiento de los trámites correspondientes.

14.5. Canales Electrónicos Institucionales: Cuando la naturaleza de la solicitud lo permita, la institución podrá recibir y responder consultas mediante:

- Correo electrónico institucional.

- Formularios web.
- Plataforma académica.
- Sistemas de atención institucional.
- Otros medios electrónicos oficialmente autorizados.

14.6. Atención a Personas con Discapacidad o Condiciones Especiales: La institución procurará brindar los apoyos razonables necesarios para garantizar que las personas con discapacidad, adultos mayores o quienes presenten condiciones especiales puedan ejercer efectivamente sus derechos relacionados con la protección de datos personales.

14.7. Horario de Atención: Las consultas y reclamos serán recibidos durante los horarios oficiales de atención establecidos por la institución y publicados en sus canales oficiales.

Cuando las solicitudes sean presentadas por medios electrónicos fuera del horario laboral, se entenderán radicadas el siguiente día hábil.

14.8. Radicación de Solicitudes: Toda consulta, petición, queja o reclamo deberá contener, como mínimo:

- Nombre completo del titular o de su representante.
- Tipo y número del documento de identificación.
- Información de contacto (correo electrónico, dirección o teléfono).
- Descripción clara y precisa de la solicitud.
- Documentos que soporten la solicitud, cuando sea necesario.
- En caso de actuar mediante representante, el documento que acredite dicha representación.

La institución podrá solicitar información adicional cuando resulte necesaria para verificar la identidad del solicitante o atender adecuadamente la solicitud.

14.9. Seguimiento a las Solicitudes: Todas las consultas y reclamos recibidos serán registrados y gestionados conforme al procedimiento institucional de atención de PQRSF y al procedimiento para el ejercicio de los derechos de los titulares establecido en la presente política.

La institución garantizará la trazabilidad de cada solicitud hasta su cierre, conservando la evidencia correspondiente como parte de la información documentada del Sistema de Gestión de la Calidad.

Parágrafo Primero: La presentación de consultas, peticiones, quejas o reclamos relacionados con el tratamiento de datos personales será gratuita y no requerirá formalidades diferentes a las establecidas por la legislación vigente y la presente

política.

Parágrafo Segundo: Cuando la solicitud sea presentada por una persona distinta al titular, esta deberá acreditar su legitimación para actuar mediante poder, representación legal, calidad de causahabiente o cualquier otro mecanismo previsto por la legislación colombiana.

Parágrafo Tercero: Los registros generados durante la atención de consultas y reclamos relacionados con la protección de datos personales constituyen información documentada del Sistema de Gestión de la Calidad y serán administrados conforme al ACA-PD09 – Gestión de la Información Documentada, garantizando su adecuada conservación, confidencialidad, disponibilidad y trazabilidad durante el tiempo de retención establecido por la institución y la legislación vigente.

15. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DE LOS TITULARES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. garantizará a los titulares de los datos personales el ejercicio efectivo de los derechos de acceso, consulta, actualización, rectificación, supresión, revocatoria de la autorización y demás derechos previstos en la legislación vigente, mediante un procedimiento transparente, oportuno, trazable y conforme a los principios de legalidad, confidencialidad, seguridad y debido proceso.

Todas las solicitudes serán gestionadas conforme a los términos establecidos en la Ley 1581 de 2012, el Decreto 1074 de 2015 y la presente política.

15.1. Presentación de la Solicitud: El titular, su representante legal, apoderado o causahabiente podrá presentar consultas, solicitudes, peticiones, quejas o reclamos relacionados con el tratamiento de datos personales a través de los canales oficiales definidos por la institución.

La solicitud deberá contener, como mínimo:

- Nombre completo del titular.
- Tipo y número del documento de identificación.
- Datos de contacto.
- Descripción clara y precisa de la solicitud.
- Documentos que soporten la solicitud, cuando corresponda.
- Acreditación de la representación, cuando aplique.

Responsable: Titular o representante autorizado.

15.2. Recepción y Radicación: Una vez recibida la solicitud, la institución verificará que contenga la información mínima requerida y procederá a asignar un número de radicado para garantizar la trazabilidad del trámite.

Cuando la solicitud se encuentre incompleta, se requerirá al solicitante para que subsane la información faltante dentro de los términos establecidos por la legislación vigente.

Responsable: Secretaría o dependencia encargada de la atención de PQRSF.

15.3. Validación de Identidad: Antes de suministrar información personal o ejecutar cualquier actuación sobre los datos personales, la institución verificará la identidad del titular o de quien actúe en su representación, con el fin de proteger la confidencialidad de la información y prevenir accesos no autorizados.

Cuando existan dudas razonables sobre la identidad del solicitante, podrá requerirse información adicional para efectuar la validación correspondiente.

Responsable: Dependencia encargada de la atención de la solicitud.

15.4. Análisis de la Solicitud: La dependencia competente analizará el contenido de la solicitud, verificará la información existente en las bases de datos institucionales y determinará la procedencia de la consulta, actualización, rectificación, supresión, revocatoria o cualquier otro derecho solicitado.

Cuando la solicitud involucre diferentes procesos institucionales, se coordinará la participación de las dependencias correspondientes para garantizar una respuesta integral.

Responsable: Líder del proceso responsable de la información.

15.5. Elaboración de la Respuesta: Con base en el análisis realizado, la institución elaborará la respuesta correspondiente, indicando de manera clara:

- La decisión adoptada.
- Las actuaciones realizadas.
- La información solicitada, cuando proceda.
- Los fundamentos legales o institucionales que sustentan la decisión.
- Los recursos o mecanismos disponibles para el titular cuando no esté conforme con la respuesta.

Las respuestas serán emitidas dentro de los términos establecidos en la legislación vigente.

Responsable: Líder del proceso responsable de la información.

15.6. Comunicación al Titular: La respuesta será comunicada al titular mediante el canal utilizado para presentar la solicitud o por el medio autorizado por este, garantizando la confidencialidad y seguridad de la información suministrada.

Cuando la información contenga datos personales sensibles o información

reservada, la institución adoptará las medidas necesarias para asegurar que únicamente el titular o su representante autorizado tenga acceso a ella.

Responsable: Secretaría o dependencia encargada de la atención.

15.7. Ejecución de las Acciones: Cuando la solicitud sea procedente, la institución realizará las acciones necesarias para:

- Actualizar la información.
- Rectificar los datos personales.
- Suprimir la información cuando corresponda.
- Revocar la autorización.
- Incorporar observaciones o restricciones en las bases de datos.
- Implementar las medidas derivadas de la decisión adoptada.

Las actuaciones deberán quedar registradas como evidencia del cumplimiento del procedimiento.

Responsable: Líder del proceso

15.8. Cierre y Conservación del Registro: Una vez ejecutadas las acciones correspondientes y comunicada la respuesta al titular, se procederá al cierre del trámite, conservando la totalidad de los registros y evidencias generadas durante el procedimiento conforme a los tiempos de retención establecidos por la institución y la legislación vigente.

Los registros serán administrados como información documentada del Sistema de Gestión de la Calidad.

Responsable: Secretaría y Líder del Proceso de Aseguramiento de la Calidad.

Términos de Respuesta: La institución dará trámite a las consultas y reclamos dentro de los plazos establecidos por la legislación colombiana sobre protección de datos personales.

- **Consultas:** serán atendidas dentro de los diez (10) días hábiles siguientes a su recepción. Cuando no sea posible atenderlas dentro de este término, se informará al interesado antes de su vencimiento, indicando los motivos de la demora y la nueva fecha de respuesta, la cual no podrá superar los cinco (5) días hábiles siguientes.

- **Reclamos:** serán atendidos dentro de los quince (15) días hábiles siguientes al día de su recepción. Cuando no sea posible atender el reclamo dentro de este término, la institución informará al interesado los motivos de la demora y

señalará la nueva fecha de respuesta, la cual no podrá superar los ocho (8) días hábiles siguientes.

Parágrafo Primero: Cuando la solicitud no sea competencia de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., la institución orientará al solicitante, cuando sea posible, sobre la entidad competente para atender su requerimiento.

Parágrafo Segundo: Toda actuación derivada del ejercicio de los derechos de los titulares deberá garantizar los principios de confidencialidad, seguridad, integridad, disponibilidad, legalidad, transparencia y responsabilidad demostrada, manteniendo la trazabilidad de las actividades realizadas y la protección de los datos personales durante todo el procedimiento.

Parágrafo Tercero: El presente documento se integrará con el Procedimiento Institucional de PQRSF, el ACA-PD09 – Gestión de la Información Documentada, el ACA-PD07 – Gestión de Riesgos y Oportunidades, el ACA-PD06 – No Conformidades y Mejora y el ACA-PD13 – Gestión y Planificación de los Cambios, con el fin de asegurar el tratamiento adecuado de las solicitudes, la conservación de las evidencias, la mejora continua y el cumplimiento de los requisitos legales y del Sistema de Gestión de la Calidad.

16. SEGURIDAD DE LA INFORMACIÓN

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. implementará medidas administrativas, técnicas, físicas y organizacionales orientadas a proteger los datos personales y demás activos de información contra riesgos que puedan afectar su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, garantizando el cumplimiento de la Ley 1581 de 2012, el Decreto 1074 de 2015 y los lineamientos del Sistema de Gestión de la Calidad.

La seguridad de la información constituye un compromiso institucional y será responsabilidad de todos los colaboradores, docentes, contratistas, proveedores y terceros autorizados que intervengan en el tratamiento de datos personales.

16.1. Objetivo de la Seguridad de la Información: Garantizar que la información administrada por la institución sea protegida durante todo su ciclo de vida mediante la implementación de controles que prevengan la pérdida, alteración, destrucción, acceso no autorizado, divulgación indebida o cualquier otra situación que pueda afectar la protección de los datos personales y la continuidad de los procesos institucionales.

16.2. Principios de Seguridad: La gestión de la seguridad de la información se desarrollará conforme a los siguientes principios:

- **Confidencialidad:** garantizar que la información únicamente sea accesible para las personas debidamente autorizadas.
- **Integridad:** proteger la información contra modificaciones no autorizadas, pérdida o alteración.
- **Disponibilidad:** asegurar que la información esté disponible cuando sea requerida para el cumplimiento de las funciones institucionales.
- **Autenticidad:** verificar la identidad de las personas que acceden o administran la información.
- **Trazabilidad:** mantener evidencia de las actividades realizadas sobre la información cuando la naturaleza del sistema lo permita.

16.3. Controles Administrativos: La institución implementará controles administrativos orientados a fortalecer la protección de los datos personales, entre ellos:

- Definición de roles y responsabilidades para el tratamiento de la información.
- Clasificación de la información conforme a su nivel de sensibilidad.
- Gestión de autorizaciones y perfiles de acceso.
- Suscripción de compromisos de confidencialidad por parte del personal autorizado.
- Capacitación periódica en protección de datos personales y seguridad de la

información.
- Gestión documental conforme al Sistema de Gestión de la Calidad.
- Evaluación periódica del cumplimiento de esta política.

16.4. Controles Técnicos: La institución implementará mecanismos tecnológicos adecuados para proteger la información digital, incluyendo, entre otros:

- Gestión segura de usuarios y contraseñas.
- Control de accesos a sistemas de información y plataformas institucionales.
- Copias de seguridad periódicas de la información crítica.
- Protección mediante antivirus y herramientas de seguridad informática.
- Actualización periódica de software y sistemas operativos.
- Protección de redes y dispositivos institucionales.
- Monitoreo de eventos de seguridad cuando sea técnicamente viable.
- Uso de mecanismos de autenticación para plataformas institucionales.
- Protección de los servicios en la nube utilizados por la institución.

16.5. Controles Físicos: Con el fin de proteger la información física y los equipos institucionales, la institución implementará medidas tales como:

- Control de acceso a las instalaciones.
- Protección de archivos físicos y expedientes.
- Custodia de documentos confidenciales.
- Control del préstamo y devolución de documentos.
- Protección de equipos de cómputo y dispositivos de almacenamiento.
- Restricción de acceso a áreas críticas.
- Medidas para la prevención de pérdida, hurto o deterioro de la información.

16.6. Gestión de Accesos: El acceso a la información institucional se otorgará conforme al principio de necesidad de conocer y de acuerdo con las funciones asignadas a cada colaborador.

La institución garantizará que:

- Cada usuario disponga únicamente de los permisos necesarios para el desempeño de sus funciones.
- Los accesos sean revisados periódicamente.
- Los permisos sean modificados o eliminados cuando cambien las funciones del usuario o finalice su vínculo con la institución.
- Se mantenga el control sobre las cuentas institucionales y credenciales de acceso.

16.7. Seguridad en Plataformas Tecnológicas: La información administrada mediante plataformas académicas, administrativas y tecnológicas será protegida mediante controles orientados a garantizar su disponibilidad y seguridad.

Estos controles aplicarán, entre otros, a:

- Plataforma académica Q10.
- Plataformas virtuales de aprendizaje.
- Sitios web institucionales.
- Correo electrónico institucional.
- Google Workspace.
- Servicios de almacenamiento en la nube.
- Sistemas administrativos y financieros.
- Plataformas de atención al usuario.
- Herramientas institucionales autorizadas para la gestión de la información.

16.8. Copias de Seguridad y Recuperación: La institución implementará mecanismos para realizar copias de seguridad de la información crítica, garantizando su disponibilidad y recuperación en caso de incidentes que afecten la continuidad de los procesos institucionales.

Las copias de seguridad serán protegidas conforme a los controles definidos por la institución y estarán sujetas a procesos periódicos de verificación.

16.9. Gestión de Riesgos de Seguridad de la Información: Los riesgos relacionados con la protección de datos personales serán identificados, evaluados, tratados y monitoreados conforme al procedimiento institucional de Gestión de Riesgos y Oportunidades, implementando los controles necesarios para reducir la probabilidad de ocurrencia y el impacto de eventos que puedan comprometer la seguridad de la información.

16.10. Auditoría y Seguimiento: La institución realizará seguimiento periódico a la eficacia de los controles de seguridad mediante:

- Auditorías internas.
- Revisión de incidentes.
- Seguimiento a planes de acción.
- Evaluación de riesgos.
- Revisión por la Dirección.
- Verificación del cumplimiento de la presente política.
- Evaluación de la eficacia de las acciones de mejora implementadas.

16.11. Responsabilidad de los Usuarios: Toda persona que tenga acceso a información institucional deberá:

- Proteger las credenciales de acceso asignadas.
- Utilizar los recursos tecnológicos únicamente para fines autorizados.
- Mantener la confidencialidad de la información.
- Reportar inmediatamente cualquier incidente de seguridad.
- Cumplir las políticas institucionales relacionadas con la protección de datos personales.
- Evitar el acceso, divulgación, modificación o eliminación no autorizada de información.

Parágrafo Primero: La institución revisará periódicamente los controles de seguridad implementados, considerando cambios tecnológicos, organizacionales, normativos, nuevos riesgos identificados, resultados de auditorías, incidentes de seguridad y oportunidades de mejora, con el fin de fortalecer continuamente la protección de la información institucional.

Parágrafo Segundo: Cuando la institución contrate proveedores externos para el almacenamiento, procesamiento, transmisión o administración de datos personales, verificará que estos implementen medidas de seguridad acordes con la legislación vigente y las obligaciones contractuales establecidas, garantizando la protección de la información durante todo el ciclo del tratamiento.

Parágrafo Tercero: Las actividades relacionadas con la seguridad de la información estarán articuladas con el Sistema de Gestión de la Calidad, especialmente con el ACA-PD07 – Gestión de Riesgos y Oportunidades, el ACA-PD09 – Gestión de la Información Documentada, el ACA-PD06 – No Conformidades y Mejora y el ACA-PD13 – Gestión y Planificación de los Cambios, promoviendo la mejora continua de los controles implementados y el cumplimiento de los requisitos legales e institucionales.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. implementará un proceso para la identificación, reporte, evaluación, tratamiento, seguimiento y cierre de los incidentes de seguridad que puedan comprometer la confidencialidad, integridad, disponibilidad o autenticidad de los datos personales y demás activos de información administrados por la institución.

La gestión de incidentes tiene como propósito minimizar los impactos sobre los titulares de los datos personales, garantizar la continuidad de los procesos institucionales, prevenir la recurrencia de los eventos y fortalecer la mejora continua del Sistema de Gestión de la Calidad.

17.1. Objetivo de la Gestión de Incidentes: Establecer el procedimiento para gestionar oportunamente los incidentes de seguridad de la información, mediante la identificación de sus causas, la implementación de acciones de contención, corrección y mejora, así como el cumplimiento de las obligaciones legales de reporte cuando estas sean aplicables.

17.2. Definición de Incidente de Seguridad: Se considera incidente de seguridad cualquier evento real o potencial que comprometa la confidencialidad, integridad, disponibilidad o autenticidad de los datos personales o de la información institucional, tales como:

- Acceso no autorizado a la información.
- Pérdida o extravío de documentos físicos.
- Robo o pérdida de equipos que contengan información institucional.
- Alteración o modificación no autorizada de datos.
- Eliminación accidental de información.
- Divulgación indebida de datos personales.
- Ataques informáticos o ciberataques.
- Infección por software malicioso.
- Suplantación de identidad o uso indebido de credenciales.
- Fugas de información.
- Fallas en los sistemas de información que comprometan la disponibilidad de los datos.
- Cualquier otro evento que afecte la seguridad de la información.

17.3. Identificación y Reporte del Incidente: Todo colaborador, docente, contratista, proveedor o tercero que detecte un incidente o una posible vulneración de la seguridad de la información deberá reportarlo inmediatamente al Líder del Proceso correspondiente y al Responsable Institucional de Protección de Datos Personales, utilizando los canales institucionales definidos para tal fin.

El reporte deberá contener, como mínimo:

- Fecha y hora del incidente.
- Lugar o sistema afectado.
- Descripción del evento.
- Información posiblemente comprometida.
- Persona que reporta.
- Evidencias disponibles.

17.4. Contención del Incidente: Una vez recibido el reporte, la institución adoptará las medidas inmediatas necesarias para contener el incidente y evitar su propagación o el incremento de sus efectos.

Entre las acciones de contención podrán implementarse:

- Suspensión temporal de accesos.
- Aislamiento de equipos o sistemas afectados.
- Recuperación de respaldos.
- Cambio de credenciales.
- Protección de documentos físicos.
- Restricción de accesos.
- Otras medidas que permitan controlar el evento.

17.5. Evaluación del Incidente: El Responsable Institucional de Protección de Datos Personales, en coordinación con el Líder del Proceso involucrado y el responsable de tecnología cuando corresponda, evaluará:

- La naturaleza del incidente.
- Las causas que lo originaron.
- La información comprometida.
- El número de titulares afectados.
- El nivel de impacto.
- Los riesgos derivados del incidente.
- Las posibles consecuencias legales, académicas, administrativas o reputacionales.

Cuando sea necesario, se documentarán los hallazgos como evidencia para la adopción de acciones posteriores.

17.6. Tratamiento del Incidente: Con base en los resultados de la evaluación, la institución implementará las acciones necesarias para:

- Restablecer la disponibilidad de la información.
- Corregir las causas identificadas.
- Recuperar la información cuando sea posible.
- Reducir el impacto sobre los titulares.
- Evitar la repetición del incidente.
- Fortalecer los controles de seguridad existentes.

Cuando el incidente constituya una no conformidad del Sistema de Gestión de la Calidad, se gestionará conforme al **ACA-PD06 – No Conformidades y Mejora**.

17.7. Comunicación y Notificación: Cuando la legislación vigente o la naturaleza del incidente lo requiera, la institución comunicará oportunamente el evento a:

- Los titulares de los datos personales afectados.
- La Superintendencia de Industria y Comercio u otras autoridades competentes, cuando corresponda.
- Las partes interesadas que deban conocer la situación para la protección de sus derechos o el cumplimiento de obligaciones legales.

Las comunicaciones deberán realizarse preservando la confidencialidad de la información y evitando una divulgación innecesaria de datos personales.

17.8. Seguimiento y Verificación de la Eficacia: Una vez implementadas las acciones correctivas y preventivas, el Líder del Proceso de Aseguramiento de la Calidad realizará seguimiento para verificar:

- La eficacia de las acciones implementadas.
- La eliminación o control de las causas del incidente.
- La actualización de los controles de seguridad.
- La reducción del riesgo asociado.
- El cumplimiento de los requisitos legales y de la presente política.

Los resultados servirán como información de entrada para la mejora continua y la Revisión por la Dirección.

17.9. Registro y Conservación de la Información: Todos los incidentes de seguridad deberán documentarse y conservarse como evidencia del tratamiento realizado.

Los registros deberán incluir, como mínimo:

- Número consecutivo del incidente.
- Fecha de ocurrencia.
- Fecha de reporte.
- Descripción del incidente.
- Clasificación del incidente.
- Nivel de impacto.
- Acciones implementadas.
- Responsable del tratamiento.
- Estado del incidente.
- Fecha de cierre.

La información será administrada conforme al ACA-PD09 – Gestión de la Información Documentada y a las Tablas de Retención Documental vigentes.

17.10. Mejora Continua: Los incidentes de seguridad serán analizados periódicamente con el fin de identificar tendencias, causas recurrentes y oportunidades de mejora.

Los resultados podrán generar:

- Actualización de procedimientos.
- Modificación de controles.
- Programas de capacitación.
- Actualización de matrices de riesgos.
- Cambios tecnológicos.
- Acciones correctivas y preventivas.
- Revisión de políticas institucionales.

Parágrafo Primero: Todo colaborador, docente, contratista, proveedor o tercero autorizado tiene la obligación de reportar inmediatamente cualquier incidente o sospecha de vulneración de la seguridad de la información del que tenga conocimiento. La omisión del reporte podrá dar lugar a las acciones administrativas, disciplinarias o contractuales que correspondan.

Parágrafo Segundo: La gestión de los incidentes de seguridad deberá desarrollarse bajo los principios de oportunidad, confidencialidad, proporcionalidad, trazabilidad y mejora continua, procurando minimizar los efectos sobre los titulares de los datos personales y la operación institucional.

Parágrafo Tercero: La gestión de incidentes de seguridad se articulará con el Sistema de Gestión de la Calidad, especialmente con los procedimientos:

- ACA-PD06 – No Conformidades y Mejora.
- ACA-PD07 – Gestión de Riesgos y Oportunidades.
- ACA-PD09 – Gestión de la Información Documentada.
- ACA-PD13 – Gestión y Planificación de los Cambios.

Cuando un incidente evidencie fallas en los controles institucionales, genere riesgos significativos o implique cambios en procesos, tecnologías o requisitos legales, se deberán activar los procedimientos correspondientes para asegurar la implementación de acciones correctivas, la actualización de la gestión del riesgo y la mejora continua del Sistema de Gestión de la Calidad.

18. TRANSFERENCIA Y TRANSMISIÓN NACIONAL E INTERNACIONAL DE DATOS PERSONALES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en desarrollo de sus actividades académicas, administrativas, comerciales e institucionales, podrá realizar la transferencia o transmisión de datos personales a terceros ubicados dentro o fuera del territorio colombiano, siempre que dichas operaciones sean necesarias para el cumplimiento de las finalidades autorizadas por el titular o se encuentren permitidas por la legislación vigente.

En todos los casos, la institución garantizará que dichas operaciones se desarrollen conforme a los principios de legalidad, finalidad, seguridad, confidencialidad, responsabilidad demostrada y protección de los derechos de los titulares.

18.1. Transferencia Nacional de Datos Personales: La institución podrá transferir datos personales a otras personas naturales o jurídicas ubicadas en Colombia cuando:

- Exista autorización previa del titular, cuando esta sea exigible.
- Sea necesario para el cumplimiento de obligaciones legales o contractuales.
- Se requiera para el desarrollo de convenios académicos, administrativos o institucionales.
- Sea necesario para la prestación de servicios educativos.
- Exista un requerimiento de autoridad competente.
- La transferencia esté autorizada por la legislación vigente.

Las entidades receptoras deberán garantizar niveles adecuados de protección de los datos personales y cumplir las obligaciones establecidas en la normativa colombiana.

18.2. Transmisión Nacional de Datos Personales: La institución podrá transmitir datos personales a terceros que actúen como Encargados del Tratamiento para el desarrollo de actividades necesarias para la operación institucional, tales como:

- Servicios tecnológicos.
- Plataformas académicas.
- Servicios de alojamiento de información.
- Gestión documental.
- Facturación electrónica.
- Servicios de mensajería.
- Soporte tecnológico.
- Procesamiento de información.
- Servicios administrativos.

En estos casos se formalizarán los acuerdos o contratos correspondientes, estableciendo las obligaciones del encargado respecto a la protección de los datos personales, la confidencialidad de la información y las medidas de seguridad aplicables.

18.3. Transferencia Internacional de Datos Personales: La institución podrá realizar transferencias internacionales de datos personales únicamente cuando:

- Exista autorización del titular, cuando sea requerida.
- El país receptor ofrezca niveles adecuados de protección conforme a la legislación colombiana.
- La transferencia se encuentre permitida por la Ley 1581 de 2012 y las demás normas aplicables.
- Sea necesaria para el cumplimiento de obligaciones contractuales, académicas o legales.

Cuando el país receptor no cuente con un nivel adecuado de protección, la institución verificará la existencia de las excepciones legales que permitan realizar la transferencia y adoptará las garantías adicionales necesarias para proteger los derechos de los titulares.

18.4. Transmisión Internacional de Datos Personales: La institución podrá utilizar proveedores de servicios ubicados fuera del territorio nacional para el almacenamiento, procesamiento, respaldo, soporte o administración de información institucional, siempre que dichos proveedores implementen medidas de seguridad acordes con la legislación vigente y las buenas prácticas internacionales de protección de datos.

Estas transmisiones podrán involucrar servicios tecnológicos tales como:

- Plataformas de correo electrónico institucional.
- Servicios de almacenamiento en la nube.
- Plataformas académicas y educativas.
- Sistemas de videoconferencia.
- Plataformas de colaboración institucional.
- Herramientas de productividad.
- Plataformas de automatización institucional.
- Servicios de inteligencia artificial autorizados por la institución.
- Otros servicios tecnológicos que apoyen la operación institucional.

18.5. Garantías para la Transferencia y Transmisión: Antes de realizar cualquier transferencia o transmisión de datos personales, la institución verificará, según corresponda:

- La existencia de una finalidad legítima.
- La necesidad del tratamiento.
- La autorización del titular cuando sea exigible.

- La existencia de contratos o acuerdos de tratamiento de datos personales.
- La implementación de medidas de seguridad apropiadas.
- El cumplimiento de la legislación colombiana.
- La confidencialidad de la información.
- La capacidad del tercero para proteger adecuadamente los datos personales.

18.6. Obligaciones de los Receptores de la Información: Los terceros que reciban datos personales deberán:

- Utilizar la información únicamente para las finalidades autorizadas.
- Implementar medidas de seguridad apropiadas.
- Garantizar la confidencialidad de la información.
- No divulgar los datos a terceros sin autorización o habilitación legal.
- Informar oportunamente cualquier incidente de seguridad que comprometa la información recibida.
- Cumplir las obligaciones establecidas en los contratos y en la legislación vigente sobre protección de datos personales.

18.7. Servicios Tecnológicos Utilizados por la Institución: Para el desarrollo de sus actividades, la institución podrá utilizar plataformas tecnológicas nacionales o internacionales que impliquen transmisión de datos personales, entre ellas:

- Plataforma académica Q10.
- Google Workspace.
- Servicios de almacenamiento en la nube autorizados.
- Plataformas institucionales de aprendizaje virtual.
- Sitios web institucionales.
- Plataformas de videoconferencia.
- Plataformas de correo electrónico.
- Herramientas de automatización de procesos.
- Sistemas contables y administrativos.
- Plataformas de mensajería institucional.
- Servicios de inteligencia artificial previamente autorizados por la institución para apoyar procesos académicos, administrativos o de gestión.

La utilización de estos servicios estará sujeta a la evaluación de riesgos, la implementación de controles de seguridad y la suscripción de los acuerdos contractuales que resulten aplicables.

18.8. Restricciones: La institución no realizará transferencias o transmisiones de datos personales cuando:

- Se encuentren prohibidas por la legislación vigente.
- No existan las garantías mínimas de protección de la información.
- El tratamiento exceda las finalidades autorizadas.
- Se vulneren los derechos fundamentales de los titulares.

Parágrafo Primero: Toda transferencia o transmisión nacional o internacional de datos personales deberá estar respaldada por mecanismos jurídicos que regulen las responsabilidades de las partes, incluyendo acuerdos de confidencialidad, contratos de transmisión de datos personales, cláusulas de protección de datos o cualquier otro instrumento legal que garantice el cumplimiento de la legislación vigente.

Parágrafo Segundo: La incorporación de nuevos proveedores tecnológicos, plataformas digitales, servicios en la nube o herramientas de inteligencia artificial que impliquen transferencia o transmisión de datos personales deberá ser previamente evaluada por la institución, considerando los riesgos para la privacidad, la seguridad de la información, el cumplimiento normativo y las medidas de protección requeridas, conforme al ACA-PD07 – Gestión de Riesgos y Oportunidades y al ACA-PD13 – Gestión y Planificación de los Cambios.

Parágrafo Tercero: Las actividades de transferencia y transmisión de datos personales serán objeto de seguimiento mediante auditorías internas, evaluación de proveedores, revisión de contratos, monitoreo de incidentes y acciones de mejora continua, garantizando su articulación con el Sistema de Gestión de la Calidad, especialmente con el ACA-PD09 – Gestión de la Información Documentada, el ACA-PD06 – No Conformidades y Mejora, el ACA-PD07 – Gestión de Riesgos y Oportunidades y el ACA-PD13 – Gestión y Planificación de los Cambios, con el propósito de preservar la seguridad de la información y proteger los derechos de los titulares.

19. CONSERVACIÓN Y DISPOSICIÓN FINAL DE LOS DATOS PERSONALES

SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. conservará los datos personales únicamente durante el tiempo necesario para cumplir las finalidades para las cuales fueron recolectados, atender las obligaciones legales, contractuales, académicas, administrativas, tributarias, laborales y regulatorias, así como garantizar el ejercicio de los derechos de los titulares y la adecuada gestión de la información institucional.

La conservación y disposición final de los datos personales se realizará conforme a la legislación vigente, las Tablas de Retención Documental (TRD), la Política de Gestión Documental y los procedimientos del Sistema de Gestión de la Calidad.

19.1. Criterios para la Conservación de los Datos: Los datos personales serán conservados considerando, entre otros, los siguientes criterios:

- La finalidad para la cual fueron recolectados.
- Los tiempos de retención establecidos en la legislación vigente.
- Las obligaciones contractuales asumidas por la institución.
- Los requisitos académicos y administrativos aplicables.
- Los términos de prescripción de acciones legales.
- Los lineamientos establecidos en las Tablas de Retención Documental.
- Los requerimientos de las autoridades competentes.
- Las necesidades de auditoría, control y mejora continua.

19.2. Conservación de la Información Física: Los documentos físicos que contengan datos personales serán administrados conforme a las políticas institucionales de gestión documental, garantizando:

- Identificación adecuada de los expedientes.
- Organización y clasificación documental.
- Custodia en lugares seguros.
- Control de acceso al archivo.
- Protección contra pérdida, deterioro o acceso no autorizado.
- Conservación durante el tiempo de retención establecido.

19.3. Conservación de la Información Digital: La información almacenada en medios electrónicos será administrada mediante controles orientados a garantizar:

- Disponibilidad.
- Integridad.
- Confidencialidad.
- Recuperación de la información.
- Copias de seguridad.
- Control de accesos.
- Protección frente a incidentes de seguridad.
- Conservación conforme a los tiempos definidos por la institución.

Estos controles aplicarán a las plataformas académicas, administrativas, sistemas de información, correo institucional, servicios en la nube y demás medios tecnológicos utilizados por la institución.

19.4. Archivo de la Información: Una vez finalizada la utilización activa de los datos personales, la información podrá permanecer en archivo de gestión, archivo central o archivo histórico, según corresponda, respetando los tiempos de retención definidos por la normatividad archivística y las necesidades institucionales.

Durante el período de archivo, la información continuará protegida mediante los controles de seguridad establecidos por la institución.

19.5. Disposición Final de los Datos Personales: Cumplidos los tiempos de conservación y siempre que no exista obligación legal, contractual o administrativa para mantener la información, la institución procederá a definir su disposición final, la cual podrá consistir en:

- Conservación permanente cuando exista obligación legal o valor histórico.
- Archivo histórico.
- Anonimización de la información.
- Eliminación segura.
- Destrucción física de documentos.
- Borrado seguro de archivos electrónicos.
- Otra disposición autorizada por la legislación vigente.

La disposición final deberá garantizar que la información no pueda ser recuperada, utilizada o divulgada de manera no autorizada.

19.6. Eliminación Segura: La eliminación de datos personales deberá realizarse mediante procedimientos que garanticen la destrucción segura de la información, evitando su reconstrucción o recuperación posterior.

Dependiendo del medio de almacenamiento, podrán utilizarse mecanismos tales como:

- Trituración de documentos físicos.
- Destrucción certificada.
- Eliminación permanente de archivos electrónicos.
- Sobrescritura segura de medios digitales.
- Destrucción de dispositivos de almacenamiento cuando corresponda.
- Otros mecanismos técnicamente apropiados.

19.7. Conservación por Obligación Legal: Cuando exista una disposición legal, judicial, administrativa o contractual que obligue a conservar determinada información, la institución mantendrá los datos personales durante el tiempo exigido por la normatividad aplicable, aun cuando hayan desaparecido las finalidades iniciales del tratamiento.

En estos casos, la información únicamente podrá utilizarse para atender dichas obligaciones.

19.8. Suspensión del Tratamiento: Cuando proceda la supresión de los datos personales, pero exista una obligación de conservación, la institución restringirá el tratamiento de la información exclusivamente a las finalidades que justifiquen su permanencia, limitando el acceso únicamente al personal autorizado.

19.9. Seguimiento y Control: El Líder del Proceso de Aseguramiento de la Calidad, en coordinación con los líderes de proceso y las dependencias responsables de la gestión documental, realizará seguimiento periódico al cumplimiento de los tiempos de conservación y de las actividades de disposición final, verificando:

- Cumplimiento de las Tablas de Retención Documental.
- Conservación adecuada de la información.
- Aplicación de controles de seguridad.
- Eliminación segura cuando corresponda.
- Conservación de las evidencias del proceso.
- Cumplimiento de la legislación vigente.

Parágrafo Primero: La conservación y disposición final de los datos personales deberá realizarse en armonía con la Ley General de Archivos (Ley 594 de 2000), las Tablas de Retención Documental (TRD), las políticas institucionales de gestión documental y el ACA-PD09 – Gestión de la Información Documentada, garantizando la integridad, autenticidad, disponibilidad y confidencialidad de la información durante todo su ciclo de vida.

Parágrafo Segundo: Cuando los datos personales se encuentren almacenados por terceros en calidad de encargados del tratamiento o proveedores de servicios tecnológicos, SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. verificará que la conservación, devolución o eliminación de la información se realice conforme a las obligaciones contractuales, las medidas de seguridad acordadas y la legislación vigente sobre protección de datos personales.

Los resultados de estas actividades constituirán información de entrada para la Revisión por la Dirección, contribuyendo al fortalecimiento de la gestión documental, la protección de los datos personales y la mejora continua de los procesos institucionales.

20. ACTUALIZACIÓN DE LA POLÍTICA

La presente Política de Tratamiento de Datos Personales será revisada y actualizada por SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. cuando se presenten cambios en la legislación aplicable, en la estructura organizacional, en los procesos institucionales, en las tecnologías utilizadas para el tratamiento de datos personales o cuando se identifiquen oportunidades de mejora derivadas del Sistema de Gestión de la Calidad.

La actualización de la política tendrá como finalidad garantizar su vigencia, pertinencia y eficacia, asegurando el cumplimiento de los requisitos legales, la protección de los derechos de los titulares y la adecuada gestión de los riesgos asociados al tratamiento de datos personales.

20.1. Causales de Actualización: La presente política será objeto de revisión y actualización cuando ocurra cualquiera de las siguientes situaciones:

- Modificaciones en la legislación sobre protección de datos personales.
- Nuevos lineamientos emitidos por la Superintendencia de Industria y Comercio.
- Cambios en la estructura organizacional o en las responsabilidades institucionales.
- Creación, modificación o eliminación de procesos institucionales.
- Implementación de nuevas plataformas tecnológicas, sistemas de información o servicios digitales.
- Incorporación de nuevas finalidades para el tratamiento de datos personales.
- Cambios en las categorías de titulares o en las bases de datos administradas por la institución.
- Resultados de auditorías internas o externas.
- Materialización de incidentes de seguridad de la información.
- Cambios en la evaluación de riesgos relacionados con la protección de datos personales.
- Acciones correctivas, preventivas o de mejora derivadas del Sistema de Gestión de la Calidad.
- Requerimientos de autoridades competentes.
- Cualquier otra situación que haga necesaria la actualización del documento.

20.2. Responsables de la Actualización: La actualización de la presente política será coordinada por el Líder del Proceso de Aseguramiento de la Calidad, en conjunto con el Responsable Institucional de Protección de Datos Personales y los líderes de los procesos involucrados.

La aprobación de las modificaciones corresponderá a la Dirección, conforme a la estructura documental del Sistema de Gestión de la Calidad.

20.3. Control de Cambios: Toda modificación realizada a la presente política deberá:

- Ser documentada mediante el control de cambios institucional.
- Contar con la justificación técnica, legal o institucional correspondiente.
- Identificar la versión, fecha de aprobación y descripción de los cambios realizados.
- Conservar la trazabilidad de las versiones anteriores conforme al procedimiento de gestión de la información documentada.

20.4. Comunicación de las Actualizaciones: Una vez aprobada una nueva versión, la institución garantizará su divulgación mediante los canales institucionales que correspondan, con el fin de que los titulares, colaboradores, docentes, contratistas, proveedores y demás partes interesadas conozcan las modificaciones realizadas.

Cuando los cambios afecten de manera significativa las finalidades del tratamiento o los derechos de los titulares, la institución adoptará las medidas necesarias para informar oportunamente dichas modificaciones y, cuando la legislación lo exija, obtener una nueva autorización para el tratamiento de los datos personales.

20.5. Seguimiento a la Implementación: El Líder del Proceso de Aseguramiento de la Calidad realizará seguimiento a la implementación de las modificaciones aprobadas, verificando:

- La actualización de la información documentada relacionada.
- La aplicación de los nuevos lineamientos por parte de los procesos.
- La actualización de formatos, registros y procedimientos asociados.
- La ejecución de las actividades de socialización y capacitación cuando sean necesarias.
- La eficacia de las acciones implementadas.

Los resultados del seguimiento constituirán información de entrada para la Revisión por la Dirección y para los procesos de mejora continua.

Parágrafo Primero: La presente política será revisada como mínimo una vez al año, aun cuando no se presenten cambios normativos o institucionales, con el fin de verificar su vigencia, eficacia y alineación con la legislación aplicable, el contexto institucional y los objetivos del Sistema de Gestión de la Calidad.

Parágrafo Segundo: Toda actualización de la política deberá gestionarse conforme al ACA-PD09 – Gestión de la Información Documentada y, cuando implique modificaciones en procesos, tecnologías, responsabilidades o requisitos legales, se aplicará igualmente el ACA-PD13 – Gestión y Planificación de los Cambios,

garantizando la evaluación de impactos, la trazabilidad documental y la implementación controlada de los cambios.

Parágrafo Tercero: La actualización de esta política forma parte del proceso de mejora continua de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S. y será apoyada por los resultados de auditorías internas y externas, el análisis de indicadores, la gestión de riesgos, la atención de incidentes de seguridad, las consultas y reclamos de los titulares, los requerimientos de las autoridades competentes y la Revisión por la Dirección, con el propósito de fortalecer permanentemente la protección de los datos personales y la eficacia del Sistema de Gestión de la Calidad.

21. VIGENCIA

La presente Política de Tratamiento de Datos Personales rige a partir de la fecha de su aprobación por la Dirección de SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., deroga todas las disposiciones internas que le sean contrarias y será de obligatorio cumplimiento para directivos, colaboradores, docentes, contratistas, proveedores, aliados estratégicos, encargados del tratamiento y demás personas que, en ejercicio de sus funciones o por razón de su relación con la institución, realicen tratamiento de datos personales.

La política permanecerá vigente mientras la institución realice tratamiento de datos personales y conservará plena validez hasta que sea modificada, sustituida o derogada mediante un acto administrativo interno expedido por la Dirección.

Las bases de datos administradas por la institución tendrán una vigencia acorde con las finalidades para las cuales fueron creadas y con los tiempos de conservación establecidos en la legislación colombiana, las Tablas de Retención Documental, las obligaciones legales, contractuales, académicas y administrativas, así como en los procedimientos del Sistema de Gestión de la Calidad.

La institución podrá actualizar la presente política en cualquier momento cuando se presenten cambios en la legislación vigente, en la estructura organizacional, en los procesos institucionales, en las tecnologías utilizadas para el tratamiento de datos personales o cuando se identifiquen oportunidades de mejora derivadas de auditorías, gestión de riesgos, incidentes de seguridad, revisión por la dirección o demás mecanismos de mejora continua.

Toda actualización será aprobada por la Dirección, controlada conforme al ACA-PD09 – Gestión de la Información Documentada, comunicada a las partes interesadas a través de los canales institucionales y publicada en los medios que la institución determine para garantizar su consulta permanente.

Parágrafo Primero: La presente política será revisada como mínimo una (1) vez por año para verificar su vigencia, pertinencia, eficacia y conformidad con la legislación aplicable, el contexto institucional y los requisitos del Sistema de Gestión de la Calidad, aun cuando no se presenten modificaciones normativas.

Parágrafo Segundo: Las versiones anteriores de esta política serán conservadas conforme a los lineamientos del ACA-PD09 – Gestión de la Información Documentada, garantizando la trazabilidad documental, el control de versiones y la conservación de la información histórica cuando exista obligación legal, administrativa o institucional para ello.

Parágrafo Tercero: La presente Política de Tratamiento de Datos Personales será

publicada y estará permanentemente disponible para consulta de los titulares a través del sitio web institucional y de los demás medios oficiales definidos por SYSDATEC CENTRO DE DESARROLLO INTEGRAL S.A.S., en cumplimiento de los principios de transparencia, acceso a la información y responsabilidad demostrada establecidos en la legislación colombiana sobre protección de datos personales.

CESAR AUGUSTO CASTELBLANCO CELIS
Director

CONTROL DE REVISIÓN Y APROBACIÓN

Elaboró	Revisó	Aprobó
Cesar A. Castelblanco C.	Mercedes Duque Chacón	Cesar A. Castelblanco C.
Cargo	**Cargo**	**Cargo**
Director	Talento Humano	Director
Fecha	**Fecha**	**Fecha**
13 de enero de 2026	28 de enero de 2026	12 de febrero de 2026

CONTROL DE CAMBIOS DE DOCUMENTOS

Fecha	Versión	Descripción del cambio
17/01/2019	V02	Se ajusta el documento al nuevo formato elaboración de documentos.
12/02/2026	V03	Actualización integral de la Política de Tratamiento de Datos Personales, incorporando la normatividad vigente, fortaleciendo los lineamientos para la protección de datos personales, la seguridad de la información, la gestión de incidentes, la transferencia y transmisión de datos, la conservación de la información, los derechos de los titulares y las responsabilidades institucionales. Se ajustó la estructura documental conforme al Sistema de Gestión de la Calidad y a los procedimientos institucionales vigentes.