

POLÍTICA DE  
**TRATAMIENTO DE DATOS  
PERSONALES DE LA  
UNIVERSIDAD CESMAG**



**"HOMBRES NUEVOS PARA TIEMPOS NUEVOS"**

Fray Guillermo de Castellana, OFM.Cap.



## TABLA DE CONTENIDO

<b>TÍTULO I.....</b>	<b>6</b>
<b>ASPECTOS GENERALES .....</b>	<b>6</b>
<b>CAPÍTULO I .....</b>	<b>6</b>
<b>OBJETIVOS, PROPÓSITOS, ALCANCES, MARCO NORMATIVO, DEFINICIONES, PRINCIPIOS .....</b>	<b>6</b>
ARTÍCULO 1. OBJETO Y PROPÓSITOS.....	6
ARTÍCULO 2. ALCANCE.....	7
ARTÍCULO 3. MARCO NORMATIVO.....	7
ARTÍCULO 4. DEFINICIONES.....	8
ARTÍCULO 5. PRINCIPIOS.....	10
<b>CAPÍTULO II .....</b>	<b>11</b>
<b>RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.....</b>	<b>11</b>
ARTÍCULO 6. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES Y DATOS DE CONTACTO.....	11
<b>TÍTULO II.....</b>	<b>12</b>
<b>DE LOS TITULARES DE LA INFORMACIÓN .....</b>	<b>12</b>
<b>CAPÍTULO I .....</b>	<b>12</b>
<b>DERECHOS DE LOS TITULARES DE LA INFORMACIÓN .....</b>	<b>12</b>
ARTÍCULO 7. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN.....	12
ARTÍCULO 8. DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES.....	12
<b>CAPÍTULO II .....</b>	<b>13</b>
<b>LEGITIMACIÓN PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR .....</b>	<b>13</b>
ARTÍCULO 9. EJERCICIO DE DERECHOS.....	13
<b>TÍTULO III.....</b>	<b>14</b>
<b>RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES.....</b>	<b>14</b>
ARTÍCULO 10. DEBERES COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.....	14
ARTÍCULO 11. DEBERES FRENTE AL TITULAR COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.....	14
ARTÍCULO 12. DEBERES COMO ENCARGADA DEL TRATAMIENTO.....	15
<b>TÍTULO IV .....</b>	<b>15</b>
<b>AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES .....</b>	<b>15</b>
ARTÍCULO 13. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES.....	15
ARTÍCULO 14. PRUEBA DE LA AUTORIZACIÓN.....	16
ARTÍCULO 15. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN.....	16
<b>TÍTULO V .....</b>	<b>16</b>
<b>PROCEDIMIENTOS PARA EL ADECUADO TRATAMIENTO DE DATOS PERSONALES.....</b>	<b>16</b>
ARTÍCULO 16. TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS.....	16
ARTÍCULO 17. RECOLECCIÓN.....	16
ARTÍCULO 18. ALMACENAMIENTO.....	17
ARTÍCULO 19. USO.....	17
ARTÍCULO 20. CIRCULACIÓN.....	17
ARTÍCULO 21. SUPRESIÓN.....	17
ARTÍCULO 22. TRATAMIENTO DE DATOS SENSIBLES.....	18
<b>TÍTULO VI.....</b>	<b>19</b>
<b>FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES .....</b>	<b>19</b>
<b>CAPÍTULO I .....</b>	<b>19</b>
<b>GENERALIDADES .....</b>	<b>19</b>
ARTÍCULO 23. FINALIDADES DEL TRATAMIENTO DE DATOS PERSONALES.....	19
ARTÍCULO 24. FINALIDADES GENERALES.....	19
<b>CAPÍTULO II .....</b>	<b>21</b>
<b>FINALIDADES ESPECÍFICAS .....</b>	<b>21</b>



ARTÍCULO 25. ASPIRANTES.....	24
ARTÍCULO 26. ESTUDIANTES.....	24
ARTÍCULO 27. EGRESADOS.....	24
ARTÍCULO 28. TRABAJADORES.....	26
ARTÍCULO 29. ASPIRANTES A PROCESOS DE SELECCIÓN DE PERSONAL.....	27
ARTÍCULO 30. ASPIRANTES Y APRENDICES.....	28
ARTÍCULO 31. PROVEEDORES, ALIADOS, CLIENTES, USUARIOS Y CIUDADANÍA EN GENERAL.....	29
ARTÍCULO 32. HIJOS, HERMANOS, CONYUGES DE ESTUDIANTES, TRABAJADORES.....	31
ARTÍCULO 33. FINALIDADES PARA EL TRATAMIENTO DE DATOS SENSIBLES.....	31
<b>TÍTULO VII.....</b>	<b>32</b>
<b>TRANSMISIÓN Y TRANSFERENCIA.....</b>	<b>32</b>
ARTÍCULO 34. TRANSMISIÓN.....	32
ARTÍCULO 35. TRANSFERENCIA.....	33
<b>TÍTULO VIII.....</b>	<b>33</b>
<b>CONSULTAS Y RECLAMOS.....</b>	<b>33</b>
ARTÍCULO 36. CONTENIDO Y PRESENTACIÓN DE CONSULTAS.....	33
ARTÍCULO 37. CONTENIDO Y PRESENTACIÓN DE RECLAMOS.....	34
ARTÍCULO 38. MEDIOS PARA PRESENTAR CONSULTAS O RECLAMOS.....	34
ARTÍCULO 39. PROCEDIMIENTO PARA CONSULTAS.....	35
ARTÍCULO 40. PLAZO DE RESPUESTA A CONSULTAS.....	36
ARTÍCULO 41. CONSULTAS INCOMPLETAS.....	36
ARTÍCULO 42. PROCEDIMIENTO PARA RECLAMOS.....	36
ARTÍCULO 43. PLAZO DE RESPUESTA A RECLAMOS.....	38
ARTÍCULO 44. RECLAMOS INCOMPLETOS.....	38
ARTÍCULO 45. REQUISITO DE PROCEDIBILIDAD.....	38
<b>TÍTULO IX.....</b>	<b>38</b>
<b>PROGRAMA INTEGRAL DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES.....</b>	<b>38</b>
<b>CAPÍTULO I.....</b>	<b>38</b>
<b>MEDIDAS DE SEGURIDAD.....</b>	<b>38</b>
ARTÍCULO 46. MEDIDAS DE SEGURIDAD.....	38
<b>CAPÍTULO II.....</b>	<b>39</b>
<b>POLÍTICAS INTERNAS.....</b>	<b>39</b>
ARTÍCULO 47. POLÍTICAS INTERNAS.....	39
ARTÍCULO 48. POLÍTICA GENERAL DE PRIVACIDAD DE LA INFORMACIÓN.....	39
ARTÍCULO 49. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.....	39
<b>CAPÍTULO III.....</b>	<b>40</b>
<b>SISTEMAS DE ADMINISTRACIÓN DE RIESGOS.....</b>	<b>40</b>
ARTÍCULO 50. SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES.....	40
ARTÍCULO 51. COMPONENTES DEL SISTEMA.....	40
ARTÍCULO 52. TIPOLOGÍA DE RIESGOS.....	40
ARTÍCULO 53. MEDIDAS DE PROTECCIÓN.....	41
<b>CAPÍTULO IV.....</b>	<b>41</b>
<b>PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES O INCIDENTES.....</b>	<b>41</b>
ARTÍCULO 54. PROTOCOLOS.....	41
<b>CAPÍTULO V.....</b>	<b>42</b>
<b>CAPACITACIÓN DE PROTECCIÓN DE DATOS PERSONALES.....</b>	<b>42</b>
ARTÍCULO 55. CAPACITACIONES.....	42
<b>CAPÍTULO VI.....</b>	<b>42</b>
<b>COMITÉ DE PROTECCIÓN DE DATOS PERSONALES.....</b>	<b>42</b>
ARTÍCULO 56. COMITÉ DE PROTECCIÓN DE DATOS PERSONALES.....	42
<b>CAPÍTULO VII.....</b>	<b>42</b>
<b>AUDITORÍAS.....</b>	<b>42</b>
ARTÍCULO 57. AUDITORÍAS.....	42
ARTÍCULO 58. OBJETIVOS DE LAS AUDITORÍAS.....	42



ARTÍCULO 59. METODOLOGÍA DE LAS AUDITORÍAS.....	43
ARTÍCULO 60. FRECUENCIA DE LAS AUDITORÍAS.....	43
ARTÍCULO 61. INFORME DE RESULTADOS.....	43
ARTÍCULO 62. COMPROMISO CON LA MEJORA CONTINUA.....	43
<b>CAPÍTULO VIII.....</b>	<b>43</b>
<b>SISTEMAS DE VIGILANCIA PARA PREVENIR Y DETECTAR RIESGOS.....</b>	<b>43</b>
ARTÍCULO 63. SISTEMAS DE VIDEOVIGILANCIA.....	43
ARTÍCULO 64. SISTEMAS DE VIDEOVIGILANCIA FRENTE A NIÑOS, NIÑAS Y ADOLESCENTES.....	44
ARTÍCULO 65. AVISOS O DISTINTIVOS EN ZONAS DE VIDEOVIGILANCIA.....	44
<b>CAPÍTULO IX.....</b>	<b>45</b>
<b>GESTIÓN DE COOKIES EN PLATAFORMAS DIGITALES INSTITUCIONALES.....</b>	<b>45</b>
ARTÍCULO 66. COOKIES.....	45
ARTÍCULO 67. ALMACENAMIENTO DE COOKIES.....	45
ARTÍCULO 68. ELIMINACIÓN DE COOKIES.....	45
<b>CAPÍTULO X.....</b>	<b>46</b>
<b>GESTIÓN DOCUMENTAL DEL CICLO DE VIDA DE DOCUMENTOS QUE CONTIENEN DATOS PERSONALES.....</b>	<b>46</b>
ARTÍCULO 69. GESTIÓN DE DOCUMENTOS.....	46
<b>CAPÍTULO XI.....</b>	<b>47</b>
<b>RELACIONES CONTRACTUALES.....</b>	<b>47</b>
ARTÍCULO 70. CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES EN CONTRATOS.....	47
<b>TÍTULO X.....</b>	<b>47</b>
<b>REGISTRO NACIONAL DE BASES DE DATOS Y PERIODO DE VIGENCIA DE BASES DE DATOS.....</b>	<b>47</b>
ARTÍCULO 71. REGISTRO NACIONAL DE BASES DE DATOS.....	47
ARTÍCULO 72. PERIODO DE VIGENCIAS DE BASES DE DATOS.....	48
<b>TÍTULO XI.....</b>	<b>48</b>
<b>DISPOSICIONES FINALES.....</b>	<b>48</b>
ARTÍCULO 73. CAMBIOS SUSTANCIALES.....	48
ARTÍCULO 74. INTERPRETACIÓN.....	48
ARTÍCULO 75. VIGENCIA.....	48
ARTÍCULO 76. DEROGATORIAS.....	48
ARTÍCULO 77. EJECUCIÓN DE LA POLÍTICA.....	48
ARTÍCULO 78. DIVULGACIÓN.....	48



## ACUERDO NUMERO 006 DE 2025

(FEBRERO 27)

Por el cual se adopta la nueva política de tratamiento de datos personales y el manual interno de políticas y procedimientos de la Universidad CESMAG.

### EL CONSEJO DIRECTIVO DE LA UNIVERSIDAD CESMAG,

En uso de sus atribuciones estatutarias, y

#### CONSIDERANDO:

Que el artículo 69 de la Constitución Política de Colombia garantiza la autonomía universitaria, consagrando que *“las universidades podrán darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley”*.

Que el artículo 28 de la Ley 30 de 1992 reafirma esta autonomía al reconocer el derecho de las universidades a definir y organizar sus labores formativas, académicas, docentes, científicas y culturales, y a establecer y modificar sus estatutos.

Que la Ley 1581 de 2012, mediante la cual se establece el régimen general de protección de datos personales, tiene como propósito garantizar el derecho de todas las personas a la protección de su información personal, permitiéndoles decidir sobre el uso de sus datos y asegurando su facultad de conocer, actualizar y rectificar la información recolectada en bases de datos gestionadas por entidades públicas o privadas, dentro de un marco de respeto a la dignidad humana, la privacidad y la autonomía.

Que el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015 dispone que los responsables del tratamiento de datos personales deben elaborar y divulgar sus políticas de tratamiento, las cuales deben ser puestas en conocimiento de los titulares y estar disponibles en un medio físico o electrónico, redactadas en un lenguaje claro y sencillo, y contener al menos la siguiente información: la identificación del responsable, el tratamiento al cual serán sometidos los datos y su finalidad cuando esta no haya sido informada mediante aviso de privacidad, los derechos de los titulares de los datos, la persona o área responsable de atender peticiones, consultas y reclamos, a la cual los titulares pueden dirigirse para ejercer sus derechos de acceso, actualización, rectificación, supresión de datos o revocación de la autorización, el procedimiento para el ejercicio de los derechos de los titulares, los periodos de vigencia de la base de datos, la fecha de entrada en vigencia de las políticas y la comunicación de cambios sustanciales en las políticas a los titulares.

Que, en virtud de las obligaciones derivadas del marco legal sobre protección de datos, el Consejo Directivo expidió el Acuerdo No. 074 del 2 de abril de 2014, que definió las políticas institucionales sobre el tratamiento de la información. Sin embargo, dado que el marco normativo ha evolucionado con el tiempo y considerando los cambios tecnológicos y organizacionales, se hace imperativa una actualización de esta política y el manual interno de políticas y procedimientos para garantizar su pertinencia y alineación con las disposiciones actuales.



Que, el Plan Estratégico de Desarrollo 2022 – 2029 “la meta es innovar”, se propone desarrollar en el objetivo estratégico 3, una arquitectura institucional bajo los principios de ética y buen gobierno que, a su vez, busca la transformación y apropiación de la gobernabilidad y gobernanza institucional, mediante un marco normativo, actualizado y pertinente. Esto implica la necesidad de un marco normativo actualizado, tal como establece el lineamiento estratégico 011, que promueve la transformación y fortalecimiento de la gobernabilidad institucional.

Que el Estatuto General de la Universidad, aprobado mediante Acuerdo 016 del 28 de septiembre de 2020, asigna al Rector, en el literal b del artículo 25, la función de “*proponer al Consejo Directivo las políticas institucionales de la Universidad CESMAG de acuerdo con la legislación vigente, el Estatuto General y los reglamentos, y fijar las políticas específicas*”.

Que el literal b del artículo 20 del Estatuto General de la Universidad establece que es función del Consejo Directivo “*aprobar, a propuesta del Rector y con la orientación del Consejo Máximo, las políticas de la Universidad CESMAG, en coherencia con su modelo de gestión y arquitectura institucional, de acuerdo con la legislación vigente, el Estatuto General y los reglamentos, y velar por su implementación y cumplimiento*”.

Que el Rector de la Universidad presenta al Consejo Directivo la propuesta de una nueva política de tratamiento de datos personales de la Universidad CESMAG.

En mérito de lo expuesto,

### **ACUERDA:**

Adoptar una nueva política de tratamiento de datos personales y el manual interno de políticas y procedimientos de la Universidad CESMAG, contenidos en los siguientes artículos:

### **TÍTULO I**

### **ASPECTOS GENERALES**

### **CAPÍTULO I**

### **OBJETIVOS, PROPÓSITOS, ALCANCES, MARCO NORMATIVO, DEFINICIONES, PRINCIPIOS**

**ARTÍCULO 1. OBJETO Y PROPÓSITOS.** El objeto de esta política es establecer un marco integral para la gestión de datos personales en la Universidad CESMAG, en adelante llamada Universidad, garantizando el cumplimiento de la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normativas y directrices aplicables. En este sentido, la política tiene los siguientes propósitos:

1. Establecer los lineamientos para la recolección, almacenamiento, uso, circulación, supresión y disposición final de los datos personales tratados por la Universidad, en cumplimiento de la normativa vigente.



2. Comunicar de manera clara a las personas vinculadas a la Universidad los derechos que les otorga la Ley 1581 de 2012, así como las finalidades y el destino de sus datos personales en el ejercicio de las funciones institucionales.
3. Proporcionar información necesaria para que los titulares comprendan el tratamiento de sus datos y cómo pueden ejercer sus derechos en relación con la protección de su información personal.
4. Asegurar el cumplimiento efectivo de la normativa vigente sobre protección de datos personales, en consonancia con el principio de responsabilidad demostrada (Accountability), lo cual implica demostrar la implementación efectiva de las políticas de protección y el respeto por los derechos de los titulares.
5. Proteger los derechos de los titulares de datos personales, garantizando privacidad a través de un tratamiento seguro y conforme a la normativa vigente.
6. Establecer un procedimiento ágil y efectivo que permita a los titulares de los datos, sus causahabientes, representantes, apoderados u otras personas debidamente autorizadas realizar peticiones, consultas y reclamos relacionados con la información almacenada en las bases de datos de la Universidad, garantizando la protección de sus derechos y asegurando una atención y respuesta oportuna.
7. Velar porque los encargados del tratamiento de datos personales cumplan con la política de protección de datos de la Universidad.

**ARTÍCULO 2. ALCANCE.** Esta política es aplicable a toda la información personal recolectada, almacenada, utilizada, circulada y suprimida por la Universidad en todos sus campus, en su calidad de responsable o encargada del tratamiento de datos. La gestión de esta información será responsabilidad del personal de la institución y de los encargados del tratamiento de datos personales, quienes deberán observar los lineamientos establecidos en la presente política, a fin de garantizar la protección adecuada de los datos personales y el cumplimiento de la normativa vigente en materia de protección de datos.

**ARTÍCULO 3. MARCO NORMATIVO.** La presente política se implementa en concordancia con la normativa aplicable en materia de protección de datos personales, la cual incluye, pero no se limita a, las siguientes disposiciones:

1. Constitución Política de Colombia: artículos 15 y 20, que reconocen los derechos a la intimidad, el buen nombre y la libertad de expresión, y establecen la protección de datos personales y el derecho al habeas data.
2. Ley 1266 de 2008: por la cual se dictan disposiciones generales sobre el habeas data y se regula el manejo de la información contenida en bases de datos personales, especialmente lo relacionado con datos financieros, crediticios, comerciales, de servicios y provenientes de terceros países.
3. Ley 1581 de 2012: por la cual se establecen disposiciones generales para la protección de datos personales y se regulan los derechos de los titulares de los datos y las obligaciones de quienes realicen su tratamiento.
4. Decreto 1074 de 2015: decreto único reglamentario del sector comercio, industria y turismo, que compila y reglamenta las normas relacionadas con la protección de datos personales, incluyendo: (i) Decreto 1377 de 2013 que reglamenta parcialmente la Ley 1581 de 2012, estableciendo lineamientos sobre el tratamiento de datos personales y (ii) Decreto 886 de 2014 que reglamenta el artículo 25 de la Ley 1581 de 2012, sobre las medidas de seguridad de la protección de datos personales.



5. Circulares y guías de la Superintendencia de Industria y Comercio (SIC) que orientan la correcta implementación de la normativa sobre protección de datos personales, así como la atención de consultas y reclamos.

**ARTÍCULO 4. DEFINICIONES.** Para los efectos de esta política, se adoptan las definiciones establecidas en la Ley 1581 de 2012, el artículo 2.2.2.25.1.3 del capítulo 25, sección 1, del Decreto 1074 de 2015, y los lineamientos emitidos por la Superintendencia de Industria y Comercio. A continuación, se presentan las principales definiciones aplicables al tratamiento de datos personales:

1. **Acceso restringido:** el acceso a la información está limitado. La Universidad no pondrá a disposición los datos personales a través de medios de comunicación masiva, a menos que se implementen las medidas técnicas adecuadas que aseguren un control de acceso restringido únicamente a personas autorizadas.
2. **Autorización:** consentimiento previo, expreso e informado del titular para el tratamiento de sus datos personales.
3. **Aviso de privacidad:** comunicación verbal o escrita emitida por el responsable del tratamiento, dirigida al titular de los datos, para informarle sobre la existencia de las políticas de tratamiento, la forma de acceder a las mismas, lo cual incluye, el tratamiento al cual serán sometidos sus datos personales, la finalidad de los mismos, el carácter facultativo de la respuesta a las preguntas que les sean hechas cuando estas versen sobre datos sensibles o sobre los datos de los niños, niñas y adolescentes, los derechos que le asisten en virtud de la autorización, la identificación, dirección física o electrónica y teléfono de la Universidad y la posibilidad de revocar el consentimiento.
4. **Base de datos:** conjunto organizado de datos personales que es objeto de tratamiento.
5. **Circulación restringida:** los datos personales solo podrán ser tratados por el personal autorizado de la Universidad CESMAG o los encargados que, en el ejercicio de sus responsabilidades, esté habilitado para realizar estas actividades. No se compartirán datos con personas no autorizadas.
6. **Consulta:** es aquella petición que implica el acceso de información personal en las bases de datos de la Universidad, en virtud a las reglas del artículo 14 de la ley 1581 de 2012.
7. **Confidencialidad:** principio que garantiza que el acceso a los datos personales estará limitado a personas autorizadas. La Universidad CESMAG se compromete a proteger la confidencialidad de aquellos datos que no sean de carácter público, asegurando la privacidad del titular.
8. **Dato personal:** cualquier información vinculada o que pueda asociarse a una persona natural.
9. **Dato público:** información que no sea semiprivada, privada o sensible. Incluyen datos sobre el estado civil, profesión, calidad de comerciante o servidor público, y los que estén en registros públicos, documentos públicos, gacetas, boletines o sentencias judiciales ejecutoriadas que no estén sometidas a reserva.





10. **Dato privado:** información de naturaleza íntima o reservada, relevante únicamente para el titular de la misma.
11. **Dato semiprivado:** información que no es de carácter íntimo, reservado, ni público, y cuya divulgación puede ser de interés tanto para el titular como para ciertos sectores o grupos.
12. **Datos sensibles:** aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede causar discriminación, tales como origen racial o étnico, orientación política, convicciones religiosas, afiliaciones sindicales, datos sobre salud, vida sexual, o datos biométricos.
13. **Derechos de los niños, niñas y adolescentes:** en el tratamiento de datos personales, se garantizará la protección de los derechos de las personas menores de 18 años, asegurando la prevalencia del interés superior de los niños, niñas y adolescente, y respetando sus derechos fundamentales, de acuerdo con la normativa vigente en materia de protección de datos personales.
14. **Encargado del tratamiento:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
15. **Habeas data:** es el derecho fundamental que permite a las personas acceder, actualizar, rectificar y suprimir sus datos personales que estén en bases de datos, protegiendo su privacidad y control sobre la información que se recopila sobre ellas. Este derecho está regulado por el artículo 15 de la Constitución de 1991 y la Ley 1266 de 2008.
16. **Incidente de seguridad:** evento o acción que compromete la confidencialidad, integridad o disponibilidad de la información personal que reposa en la Universidad. Los incidentes pueden originarse por diversas causas, como errores humanos, fallas en sistemas, actos maliciosos o procedimientos inadecuados.
17. **Manual interno de políticas y procedimientos:** conjunto de directrices, normas y procedimientos establecidos por la Universidad para regular el tratamiento de datos personales que maneja, el cual contiene:
  - a. La identificación de la Universidad.
  - b. Políticas de protección de datos personales: lineamientos sobre cómo se debe recolectar, almacenar, procesar, circular y eliminar la información personal.
  - c. Procesos que se deben seguir para garantizar la seguridad y privacidad de los datos en todas las etapas de su manejo.
  - d. Mecanismos de seguridad: medidas de seguridad física, técnica y organizativa para proteger los datos de accesos no autorizados, alteraciones, pérdidas o divulgación indebida.
  - e. Procedimientos para que los titulares de los datos puedan ejercer sus derechos de acceso, rectificación, cancelación, oposición y revocación del consentimiento.
  - f. Responsables y encargados del tratamiento: personas o áreas dentro de la Universidad responsables de velar por el cumplimiento de las políticas y procedimientos establecidos.



- 18. Responsable del tratamiento:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el tratamiento de los datos personales.
- 19. Reclamo:** solicitud presentada por el titular de los datos personales o sus causahabientes ante el responsable o el encargado del tratamiento de los datos, cuando considere que la información contenida en una base de datos debe ser corregida, actualizada o suprimida, o cuando percibe que se ha producido un presunto incumplimiento de los deberes establecidos por la legislación en materia de protección de datos personales.
- 20. Titular:** persona natural cuyos datos personales son objeto de tratamiento. Incluye, sin limitarse a, aspirantes, estudiantes, egresados, trabajadores, aprendices, contratistas, clientes, proveedores, así como los niños y niñas del Centro de Educación Inicial María Goretti y cualquier otra persona relacionada con la Universidad.
- 21. Transferencia de datos:** envío de información o datos personales por parte del responsable o encargado del tratamiento ubicado en Colombia a un receptor, que también es responsable del tratamiento, ya sea dentro o fuera del país.
- 22. Transmisión de datos:** tratamiento de datos personales que implica su comunicación, dentro o fuera del territorio de Colombia, con el fin de que un encargado realice el tratamiento por cuenta del responsable.
- 23. Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión, realizadas por la Universidad o los encargados del tratamiento.

**ARTÍCULO 5. PRINCIPIOS.** Los principios que guían la aplicación de la política de tratamiento de datos personales de la Universidad están consagrados en el artículo 4 de la Ley 1581 de 2012 y se desarrollan conforme a los siguientes lineamientos:

- 1. Principio de legalidad:** el tratamiento de datos personales se realizará conforme a las disposiciones legales vigentes, aplicables en cada etapa del proceso, desde la recolección hasta la eliminación de los datos, garantizando el cumplimiento estricto de la normativa.
- 2. Principio de finalidad:** los datos personales recolectados serán utilizados únicamente para los fines específicos informados al titular al momento de otorgar su autorización. Estos fines serán claros y compatibles con la función de la Universidad.
- 3. Principio de libertad:** el tratamiento de datos personales solo podrá efectuarse con el consentimiento previo, expreso e informado del titular, o en los casos previstos por ley o por orden judicial.
- 4. Principio de veracidad, exactitud o calidad de la información:** los datos personales sometidos a tratamiento deben ser veraces, completos, exactos, actualizados, comprobables y comprensibles. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.



5. **Principio de transparencia:** el titular de los datos tiene derecho a conocer en cualquier momento y sin restricciones, la información sobre sus datos personales que repose en las bases de datos de la Universidad.
6. **Principio de acceso y circulación restringida:** el tratamiento y la circulación de los datos personales solo podrá realizarse con la autorización del titular o en cumplimiento de una obligación legal, asegurando que el acceso a dicha información esté restringido exclusivamente a las personas debidamente autorizadas.
7. **Principio de seguridad:** la Universidad implementará medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales y prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
8. **Principio de confidencialidad:** cualquier comunicación o divulgación de los datos personales solo debe ocurrir cuando esté legalmente autorizada, o cuando sea necesario para cumplir con las finalidades establecidas en la normativa vigente. Los datos personales que no tengan la naturaleza de públicos deben ser tratados de manera que se prevenga su divulgación, acceso no autorizado o uso indebido. La obligación de confidencialidad se mantiene incluso después de que la relación laboral, contractual o de servicios con la persona que gestiona los datos haya finalizado.
9. **Principio de permanencia de la información:** los datos personales serán conservados por el tiempo que sea necesario y razonable según las finalidades del tratamiento y conforme a las obligaciones legales o contractuales. Una vez cumplidos los fines, la Universidad procederá a la supresión de los datos, salvo que una norma disponga su conservación.
10. **Principio de responsabilidad demostrada (accountability):** la Universidad se obliga a demostrar, ante la Superintendencia de Industria y Comercio o cualquier autoridad competente, que ha implementado de manera efectiva las políticas y procedimientos necesarios para cumplir con la legislación sobre protección de datos personales. Esto incluye la creación de manuales, la identificación de riesgos y el mantenimiento de un inventario de bases de datos.

## CAPÍTULO II

### RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

**ARTÍCULO 6. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES Y DATOS DE CONTACTO.** El responsable del tratamiento de los datos personales es la Universidad CESMAG, institución privada de educación superior, sin ánimo de lucro y de utilidad común, con personería jurídica otorgada mediante Resolución N° 10735 de junio de 1982 del Ministerio de Educación Nacional, y modificada mediante Resolución N° 1853 de julio de 2002, que transformó su carácter académico de institución universitaria a universidad. Su NIT es 800.109.387-7, con domicilio en la ciudad de Pasto, departamento de Nariño, Colombia.

Dirección principal: Carrera 20A No. 14-53, Pasto.  
Correo electrónico: [correspondencia@unicesmag.edu.co](mailto:correspondencia@unicesmag.edu.co)  
Teléfono: 7244434



## TÍTULO II

### DE LOS TITULARES DE LA INFORMACIÓN

#### CAPÍTULO I

#### DERECHOS DE LOS TITULARES DE LA INFORMACIÓN

**ARTÍCULO 7. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN.** Dentro del marco de la política de tratamiento de datos personales de la Universidad, los titulares de la información tendrán los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales frente a la Universidad, en su calidad de responsable o encargada del tratamiento. Este derecho podrá ejercerse respecto a datos que sean parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.
2. Solicitar la prueba de la autorización otorgada a la Universidad, excepto en los casos donde la ley no requiera dicha autorización para el tratamiento de los datos personales.
3. Ser informado por la Universidad acerca del uso que se les ha dado a sus datos personales.
4. Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a lo dispuesto en la Ley 1581 de 2012 y demás normativas aplicables que la modifiquen, adicionen o complementen.
5. Revocar la autorización y/o solicitar la supresión de sus datos cuando el tratamiento de los mismos no respete los principios, derechos y garantías legales o constitucionales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio determine que la Universidad ha incurrido en conductas contrarias a la ley y la Constitución.
6. Acceder a sus datos personales que hayan sido objeto de tratamiento, en cualquier momento y sin costo alguno.
7. Recibir información clara y completa por parte de la Universidad sobre: (i) El tratamiento al que serán sometidos sus datos personales y la finalidad del mismo. (ii) El carácter facultativo de las respuestas a las preguntas que versen sobre datos sensibles o sobre los datos de niños, niñas o adolescentes. (iii) Los derechos que le asisten como titular de la información. (iv) Los datos de contacto del responsable del tratamiento en la Universidad, tanto físicos como electrónicos.

**ARTÍCULO 8. DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES.** En cumplimiento del artículo 7 de la Ley 1581 de 2012 y del artículo 2.2.2.25.2.9, sección 2, del capítulo 25 del Decreto 1074 de 2015, la Universidad aplicará el tratamiento de datos personales de niños, niñas y adolescentes en cumplimiento de los siguientes parámetros y requisitos:



1. Interés superior: El tratamiento deberá responder y respetar el interés superior de los niños, niñas y adolescentes.
2. Derechos fundamentales: Se garantizará el respeto de sus derechos fundamentales.

Una vez cumplidos estos requisitos, la autorización debe ser previa, expresa e informada para el tratamiento y será otorgada por el representante legal de los niños, niñas o adolescentes, previo ejercicio del derecho de la persona menor de 18 años a ser escuchada y será exclusivamente para finalidades específicas que estén directamente relacionadas con el objeto y las funciones de la Universidad. La opinión de la persona menor de 18 años será valorada considerando su madurez, autonomía y capacidad para entender el asunto y se debe conservar prueba de la autorización en caso de ser requerida.

Es responsabilidad de la Universidad proporcionar información a los representantes legales y tutores sobre los riesgos potenciales a los que se enfrentan los niños, niñas y adolescentes en relación con el tratamiento indebido de sus datos personales.

La Universidad proveerá de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

## CAPÍTULO II

### LEGITIMACIÓN PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR

**ARTÍCULO 9. EJERCICIO DE DERECHOS.** Los derechos del titular de los datos personales podrán ser ejercidos por:

1. El titular: acreditando su identidad mediante la presentación de una fotocopia de su documento de identificación.
2. Los causahabientes: acreditando su condición mediante los siguientes documentos: copia del documento de identidad, registro civil de defunción del titular, documento que acredite su calidad como causahabiente y copia del documento de identidad del titular fallecido.
3. El representante y/o apoderado o terceros autorizados: previa acreditación de la representación, apoderamiento o autorización, mediante un poder o autorización debidamente otorgados, acompañando copia del documento de identidad tanto del titular como del apoderado o autorizado.
4. Representantes de niños, niñas o adolescentes: los derechos de los niños, niñas y adolescentes serán ejercidos por las personas facultadas para representarlos, quienes deberán presentar el registro civil de nacimiento de la persona menor de 18 años, copia de la cédula de ciudadanía del padre, madre o representante legal, y el documento que acredite la facultad de representación.



5. Entidades públicas en el ejercicio de sus funciones legales y/o administrativas o por orden judicial.

### TÍTULO III

#### RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

**ARTÍCULO 10. DEBERES COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.** La Universidad, en su calidad de responsable del tratamiento de datos personales, se compromete a cumplir los siguientes deberes:

1. Asegurar la seguridad de la información: conservar los datos personales bajo condiciones de seguridad adecuadas que prevengan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
2. Suministrar datos autorizados: proveer al encargado del tratamiento únicamente aquellos datos cuyo tratamiento cuente con la debida autorización, de conformidad con la establecido en la ley y en esta política.
3. Asegurar la calidad de la información: entregar al encargado del tratamiento datos veraces, completos, exactos, actualizados, comprobables y comprensibles.
4. Actualizar los datos: comunicar de manera inmediata al encargado del tratamiento cualquier novedad o actualización respecto de los datos previamente suministrados.
5. Rectificar la información: corregir los datos cuando sean incorrectos y comunicar al encargado del tratamiento sobre dicha rectificación.
6. Exigir el respeto por la seguridad y privacidad: velar porque el encargado del tratamiento cumpla con las condiciones de seguridad y privacidad de la información del titular.
7. Adoptar un manual interno de políticas internas y procedimientos para garantizar el adecuado cumplimiento de la ley.
8. Atender consultas y reclamos: gestionar las consultas y reclamos presentados por los titulares dentro de los términos establecidos por la ley y en esta política.
9. Comunicar información en discusión: informar al encargado del tratamiento cuando algún dato personal esté en discusión por parte del titular, tras la presentación de una reclamación que aún no haya sido resuelta.
10. Comunicar incidentes de seguridad: informar a la autoridad de protección de datos cuando se presenten violaciones de seguridad que represente riesgos en la administración de la información de los titulares.
11. Cumplir con las autoridades: atender las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio u otras autoridades competentes en materia de protección de datos personales.

**ARTÍCULO 11. DEBERES FRENTE AL TITULAR COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.** La Universidad, como responsable del tratamiento de datos personales, cumplirá los siguientes deberes frente al titular:

1. Garantizar el derecho de hábeas data: asegurar al titular, el ejercicio pleno de este derecho.



2. Solicitar y conservar la autorización: obtener y conservar, en las condiciones previstas en la ley, copia de la autorización otorgada por el titular para el tratamiento de sus datos personales.
3. Informar al titular: comunicar al titular de manera clara y previa lo siguiente: (i) el tratamiento al cual serán sometidos sus datos personales, (ii) la finalidad de los mismos, (iii) el carácter facultativo de la respuesta a las preguntas que les sean hechas cuando estas versen sobre datos sensibles o sobre los datos de los niños, niñas y adolescentes, (iv) los derechos que le asisten en virtud de la autorización y (v) la identificación, dirección física o electrónica y teléfono de la Universidad.
4. Responder solicitudes del titular: informar al titular, cuando lo solicite, acerca del uso y tratamiento que se ha dado a sus datos personales.

**ARTÍCULO 12. DEBERES COMO ENCARGADA DEL TRATAMIENTO.** En su calidad de encargada del tratamiento de datos personales la Universidad cumplirá los siguientes deberes, además de las disposiciones previstas en la ley y en otras normativas aplicables:

1. Garantizar el derecho de hábeas data: asegurar al titular, el ejercicio pleno de este derecho.
2. Protege la seguridad de la información: conservar los datos bajo condiciones que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
3. Actualizar, rectificar y suprimir datos: realizar estos procesos oportunamente en los términos establecidos en la ley.
4. Actualizar información reportada por los responsables: hacerlo dentro de los cinco (5) días hábiles contados a partir de su recepción.
5. Atender consultas y reclamos: tramitar las solicitudes de los titulares conforme a los plazos y términos legales.
6. Registrar “reclamo en trámite”: incluir esta leyenda en la base de datos en los términos establecidos en la ley y esta política.
7. Registrar “información en discusión judicial”: insertar ésta leyenda una vez se reciba notificación de una autoridad competente sobre procesos judiciales relacionados con datos.
8. Bloquear información controvertida: abstenerse de circular información cuestionada por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
9. Restringir el acceso a la información: permitir acceso únicamente a las personas autorizadas.
10. Informar incidentes de seguridad: comunicar a la Superintendencia de Industria y Comercio sobre violaciones a los códigos de seguridad que impliquen riesgos en la administración de los datos de los titulares.
11. Cumplir con instrucciones de la autoridad: acatar las instrucciones y requerimientos emitidos por la Superintendencia de Industria y Comercio.

## TÍTULO IV

### AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

**ARTÍCULO 13. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES.** La Universidad solicitará al titular de los datos personales su autorización para el tratamiento de estos de manera informada y previa a la recolección.



La autorización podrá obtenerse a través de los medios escritos, orales o mediante conductas inequívocas del titular que permitan concluir razonablemente que ha otorgado su consentimiento. En todos los casos, la Universidad deberá garantizar la conservación de una prueba verificable y comprobable de la autorización otorgada.

Esta autorización será requerida en cualquier escenario en el que se recolecten datos personales, incluidas imágenes, fotografías y videos del titular, independientemente del canal de comunicación utilizado. Esto aplica tanto para interacciones presenciales, telefónicas, correos electrónicos, formularios web u otros medios, asegurando siempre la posibilidad de consulta posterior y el registro correspondiente.

**ARTÍCULO 14. PRUEBA DE LA AUTORIZACIÓN.** Cada área, dependencia, departamento, facultad o programa de la Universidad deberá conservar la prueba de la autorización otorgada por los titulares de datos personales para su tratamiento, en cumplimiento de lo dispuesto en el artículo 2.2.2.25.2.5. sección 2 del capítulo 25 del Decreto 1074 de 2015.

Dicha conservación debe realizarse en formatos verificables y accesibles que permitan garantizar la trazabilidad de la autorización, asegurando su disponibilidad para eventuales consultas o requerimientos por parte de los titulares o autoridades competentes.

**ARTÍCULO 15. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN.** De conformidad con el artículo 10 de la Ley 1581 de 2012 no será necesario obtener la autorización explícita del titular cuando se trate de:

1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
2. Datos de naturaleza pública.
3. Casos de urgencia médica o sanitaria.
4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
5. Datos relacionados con el registro civil de la persona.

## TÍTULO V

### PROCEDIMIENTOS PARA EL ADECUADO TRATAMIENTO DE DATOS PERSONALES

**ARTÍCULO 16. TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS.** Los datos que se obtengan en el marco del cumplimiento de las funciones de la Universidad serán sujetos a la recolección, almacenamiento, uso, circulación o supresión.

**ARTÍCULO 17. RECOLECCIÓN.** Antes de recolectar datos personales, se presenta al titular un Aviso de Privacidad. Seguido de ello se debe obtener una autorización expresa para el tratamiento de los datos personales.

La recolección de datos personales se obtendrá a través de los siguientes medios, sin limitarse a ellos:

1. Aplicativos y documentos virtuales: cuando ingresa a los diferentes servicios soportados por sistemas de información y aplicaciones.
2. Formularios digitales disponibles en el portal oficial de la Universidad.





3. Medios virtuales: cuando se solicita información por chat, redes sociales.
4. Llamadas: se capturan datos personales para absolver una consulta, incluyendo grabación de esta.
5. Formatos físicos: diligenciados en atenciones presenciales.
6. Cámaras de videos o fotográficas: Cuando se capturan imágenes o videos en las instalaciones de la Universidad, o en eventos realizados por esta.

**PARÁGRAFO:** Si se recolectan datos sensibles, se solicitará autorización adicional, informando al titular que no está obligado a proporcionarlos.

**ARTÍCULO 18. ALMACENAMIENTO.** Los datos personales, bases de datos y archivos con información personal serán almacenados en archivos digitales o físicos propios o en custodia de terceros o en computadores institucionales, que cumplan con medidas de seguridad físicas y electrónicas, asegurando la confidencialidad, integridad y disponibilidad de la información. Solo el personal autorizado tendrá acceso a la información personal de acuerdo con su rol y funciones específicas, para lo cual deben firmar acuerdos de confidencialidad. Los datos serán almacenados únicamente durante el tiempo necesario para cumplir con sus finalidades, respetando los plazos legales aplicables.

**ARTÍCULO 19. USO.** La Universidad utilizará los datos personales del titular únicamente para las finalidades autorizadas, en estricto cumplimiento de las políticas de tratamiento de datos personales. Dicho uso se limitará a la ejecución de actividades relacionadas con sus funciones, obligaciones legales, objetivos institucionales o conforme al vínculo existente entre el titular y la Universidad.

**ARTÍCULO 20. CIRCULACIÓN.** Si los datos deben ser compartidos con terceros se celebrarán acuerdos que obliguen al cumplimiento de la normativa de protección de datos, para ello requerirá la autorización previa del titular. No obstante, en ciertos casos, y por mandato legal, o judicial la Universidad podrá suministrar datos personales a entidades que lo requieran. Se mantendrán registros de las transferencias realizadas, asegurando el uso responsable de los datos.

**ARTÍCULO 21. SUPRESIÓN.** La Universidad eliminará los datos personales que reposen en sus archivos digitales o físicos cuando:

1. Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
2. Se haya superado el periodo razonable para el cumplimiento de los fines para los que fueron previstos.
3. Así lo prevé la autorización de tratamiento de datos otorgado a la Universidad.
4. El titular solicite su eliminación y/o revoque la autorización otorgada para el tratamiento, cuando la autoridad competente haya determinado que, en el tratamiento de datos personales, la Universidad ha incurrido en conductas contrarias a la ley y a la Constitución.

En caso de que proceda la supresión de los datos personales del titular de la base de datos, la Universidad llevará a cabo la eliminación de manera que la información no pueda ser recuperada, mediante borrado lógico en plataformas digitales, destrucción física segura (trituration) de documentos. Sin embargo, el titular debe considerar que ciertos datos deberán mantenerse en registros históricos para el cumplimiento de obligaciones legales



de la Universidad. Así, la supresión se aplicará únicamente al tratamiento activo de dichos datos, conforme a la solicitud del titular.

**PARÁGRAFO:** La eliminación de los datos personales de los archivos digitales o físicos de la Universidad no se realizará cuando:

1. Exista un deber legal o contractual de permanecer en las bases de datos de la Universidad.
2. Con la eliminación de los datos personales se obstaculice actuaciones judiciales, administrativas, fiscales, investigación de delitos o actualización de sanciones administrativas.

**ARTÍCULO 22. TRATAMIENTO DE DATOS SENSIBLES.** El tratamiento de datos sensibles se realizará conforme a lo reglamentado en los artículos 5 y 6 de la Ley 1581 de 2012 y el artículo 2.2.2.25.2.3. del Decreto 1074 de 2015.

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

1. El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización. Para ello la Universidad como responsable del tratamiento de datos personales le informará el carácter sensible de los datos solicitados, así como el carácter facultativo de la autorización para tratar los datos.
2. El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
3. El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
4. El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

El tratamiento de datos sensibles se realizará en cumplimiento de las siguientes obligaciones:

1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su tratamiento.
2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles.



## TÍTULO VI

### FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES

#### CAPÍTULO I

#### GENERALIDADES

**ARTÍCULO 23. FINALIDADES DEL TRATAMIENTO DE DATOS PERSONALES.** En cumplimiento de la normatividad vigente, la Universidad realiza el tratamiento de datos personales almacenados en bases de datos con finalidades claramente definidas. Este tratamiento está destinado al desarrollo de las labores formativas, académicas, docentes, científicas, culturales y de extensión, administrativas, de servicio, financieras, así como a cualquier otra actividad que se relacione directa o indirectamente con la misión, objeto y funciones de la Universidad.

El manejo de los datos personales se realizará según el grupo de interés al que pertenezca el titular y en estricto cumplimiento de lo establecido en esta política.

Una vez sean recolectados los datos, estos, podrán ser consultados y transmitidos a las diferentes dependencias académicas, administrativas, y/o terceros aliados de la Universidad siempre que cuenten con las debidas garantías de protección, con el propósito de cumplir con sus funciones, objetivos y deberes como institución de educación superior.

**ARTÍCULO 24. FINALIDADES GENERALES.** Las finalidades generales del tratamiento de datos personales por parte de la Universidad, sin limitarse exclusivamente a estas, incluyen:

1. Cumplimiento institucional: satisfacer obligaciones, deberes y objetivos de las labores formativas, académicas, docentes, científicas, culturales y de extensión.
2. Ofertas personalizadas: generar y enviar ofertas laborales, académicas y comerciales.
3. Organización de actividades: gestionar encuestas, cursos, boletines, calendarios, competencias, concursos, seminarios y congresos.
4. Campañas promocionales: divulgar campañas publicitarias, promocionales o de mercadeo.
5. Mejoramiento continuo: optimizar servicios, procesos y productos ofrecidos por la Universidad.
6. Autoevaluación y satisfacción: realizar seguimiento, medición del nivel de satisfacción y procesos de autoevaluación.
7. Bases de datos: crear bases de datos basadas en características y perfiles de los titulares, para caracterización de aspirantes, estadísticas y seguimiento a procesos relacionados con programas y eventos.
8. Gestión de solicitudes: tramitar y responder peticiones, quejas, reclamos, solicitudes y requerimientos judiciales o administrativos.
9. Fines de investigación: usar datos para fines históricos, científicos y estadísticos.
10. Gestión interna: ejecutar gestiones administrativas, operativas, financieras y técnicas.



11. Informes a entidades externas: presentar reportes a organismos como Fiscalía, Juzgados, Ministerio de Educación Nacional, DIAN, Superintendencias, cumplimiento de exigencias legales y estadísticas.
12. Contratación: celebrar contratos, convenios, acuerdos de voluntades y actas de intención.
13. Relaciones contractuales: gestionar relaciones contractuales con clientes, proveedores y trabajadores, incluyendo el pago de obligaciones.
14. Recursos humanos: desarrollar procesos de selección, vinculación y desvinculación laboral, evaluación, promoción, bienestar y demás aspectos relacionados con la administración del recurso humano.
15. Validación de información: verificar antecedentes, referencias y datos personales.
16. Seguridad social: cumplir con mandatos legales y administrativos en materia de seguridad social.
17. Control laboral: supervisar horarios de los trabajadores.
18. Identificación institucional: elaborar y emitir carnets de identificación.
19. Actualizaciones de políticas: enviar comunicaciones sobre cambios en la política de tratamiento de datos.
20. Auditorías: soportar procesos de auditoría interna o externa.
21. Transferencia de datos: compartir datos personales con terceros aliados para fines operativos de la Institución.
22. Promoción de servicios: ofrecer productos o servicios de la Universidad.
23. Captura de imágenes: registrar fotografías y videos con fines informativos, publicitarios, de seguridad y monitoreo, entre otros.
24. Monitoreo de seguridad: gestionar sistemas de vigilancia mediante cámaras de seguridad.
25. Grabación de actividades: registrar audios en reuniones, entrevistas y actividades educativas o administrativas.
26. Control de acceso: identificar y registrar entradas y salidas en las instalaciones universitarias.
27. Notificaciones y comunicaciones: enviar información relacionada con eventos académicos, educativos, culturales y procedimientos administrativos o judiciales.
28. Gestión de procesos: agilizar trámites institucionales y mejorar su organización.
29. Gestión integral: administrar procesos contractuales, fiscales, judiciales, financieros y contables de proveedores, estudiantes y colaboradores.
30. Medios de contacto: mantener comunicación a través de correo físico, electrónico, celular, mensajes de texto, redes sociales u otros medios digitales.
31. Información institucional: difundir información sobre productos, servicios, eventos y mensajes institucionales.
32. Cobro y recuperación: adelantar acciones de cobro y recuperación de cartera educativa e institucional.
33. Atención a solicitudes: responder peticiones, consultas y trámites administrativos o judiciales.
34. Diseño de programas: evaluar necesidades de formación para desarrollar cursos y talleres.
35. Interacción en plataformas institucionales: Facilitar el acceso y uso de los aplicativos destinados a la comunicación, gestión y desarrollo de actividades académicas y administrativas.
36. Otras actividades: ejecutar actividades relacionadas con las funciones propias de la Universidad, conforme a sus mandatos legales, estatutos y políticas.



## CAPÍTULO II

### FINALIDADES ESPECÍFICAS

**ARTÍCULO 25. ASPIRANTES.** En el marco del proceso de admisión, la Universidad trata los datos personales de aspirantes, incluyendo información como: nombre completo, número de identificación, correo electrónico, número de teléfono, historial académico, institución de procedencia, resultados de pruebas de estado, programa académico al que aplica, datos de representantes legales para personas menores de 18 años, datos sensibles biométricos de salud, orientación sexual, estrato, grupo poblacional, entre otros, para las siguientes finalidades:

1. Gestionar su proceso de inscripción y admisión.
2. Validar la identidad del aspirante y prevenir casos de suplantación o fraude.
3. Validar la información y documentación suministrada del aspirante
4. Establecer medios para enviar notificaciones y comunicaciones relacionadas con el proceso de admisión.
5. Proporcionar canales alternativos para contactar al aspirante en caso de requerir aclaraciones o gestionar requerimientos específicos.
6. Evaluar si el aspirante cumple con los requisitos mínimos para el ingreso al(los) programa(s) académico(s) solicitado(s).
7. Ofrecer medidas de accesibilidad o ajustes razonables durante el proceso de admisión en caso de ser necesario.
8. Permitir la interacción en las plataformas institucionales con el fin de gestionar el proceso de admisión, seguimiento de la postulación, presentación de evaluaciones, acceso a información académica y administrativa, comunicación de resultados y otros aspectos relacionados con el ingreso a la institución.
9. Caracterización de la población.
10. Cumplir con obligaciones legales.
11. Las demás actividades asociadas con las funciones y finalidades propias de la Universidad, y en todo caso de acuerdo con la ley.

**ARTÍCULO 26. ESTUDIANTES.** La Universidad trata los datos personales de estudiantes incluyendo información como: nombre completo, número de identificación, nacionalidad, lugar y fecha de nacimiento, correo electrónico, número de teléfono, datos de representantes legales para personas menores de 18 años, EPS, programa académico, semestre, grupo, jornada, institución de procedencia cuando aplique, espacios académicos matriculados, datos académicos, antecedentes disciplinarios, información financiera, datos biométricos, información médica, datos de personas de contacto, información de representantes legales para personas menores de 18 años, según corresponda, entre otros, para las siguientes finalidades:

1. Gestión académica y administrativa, registro y control académico: inscripción, admisión, matrícula, graduación, registro de calificaciones, evaluaciones, control de asistencia, control de horarios, sistemas de control de acceso al campus o eventos específicos, emisión de certificados y constancias, seguimiento del progreso académico, reservas de cupo, retiros, reingresos, homologaciones, movilidad académica, prácticas académicas, consultorios jurídicos, centro de conciliación, uso de cámara gesell, coterminalidad, monitorías, doble titulación, capacitaciones, formación



- continua, asesoramiento académico, acceso a servicios de salud, psicología, actividades extracurriculares, participación en eventos académicos, trabajo o tesis de grado, carnetización, uso de biblioteca, exámenes médicos, seguros, para organizar y coordinar viajes, incluyendo la reserva de tiquetes de transporte (aéreo, terrestre o marítimo) y la planificación de itinerarios, natación, centro de desarrollo y aprendizaje, formalizar la participación de los estudiantes en prácticas formativas y movilidad, gestión de la asignación a los escenarios de práctica y movilidad, facilitar el seguimiento y evaluación del desempeño de los estudiantes durante las prácticas formativas y movilidades, gestión y administración de riesgos laborales durante el desarrollo de prácticas académicas y judicaturas, cumplir obligaciones legales y reglamentarias relacionadas con la prevención de riesgos laborales y la protección de la salud y seguridad en escenarios de práctica cuando corresponda, servicios de certificación y procesos relacionados con grados y egresados de la Universidad, y, demás asociados al servicio educativo.
2. Gestión administrativa de la Universidad: planificación presupuestaria, gestión de recursos humanos, adquisición y acceso de materiales educativos, equipos y recursos, organización de clases, asignación de profesores, programación de actividades académicas curriculares y extracurriculares, desarrollos operativos, procedimientos, atención a estudiantes, entre otras.
  3. Gestión financiera y contable de la Universidad: gestión de facturación de matrículas y servicios asociados a la educación, gestión de pagos y financiación, envío de notificaciones importantes, labores de monitoreo, control y registro contable de las obligaciones contraídas con los estudiantes, gestión de becas, beneficios, incentivos y subsidios, gestión de cobros y acuerdos de pago de obligaciones dinerarias contraídas con la Universidad, ofrecimiento de servicios relacionados con la financiación de la matrícula a aliados financieros y comerciales.
  4. Gestión de archivo, historial académico de estudiantes, fines históricos, entrada y salida de documentos.
  5. Gestión de comunicación: envío de información relevante, circulares, comunicaciones institucionales, cambios de horarios, actividades, invitaciones a eventos o actividades académicas, científicas y culturales, información sobre programas de educación para el trabajo y desarrollo humano, contenidos por área de interés, promoción y difusión de los programas académicos, noticias, publicidad propia y de terceros vinculados directa o indirectamente a la Universidad, ofrecimientos de servicios de la Universidad, validación de la información suministrada a través de correos electrónicos, número de celular, dirección física y sistemas de mensajería instantánea, campañas de actualización de datos e información de cambio en el tratamiento de datos personales, publicaciones en redes sociales y página Web.
  6. Gestión de bienestar universitario, como, caracterización y desarrollo de estrategias de grupos poblacionales diversos existentes en la Universidad, para dar cumplimiento a las políticas de educación inclusiva y normativa conexas que le atañe, orientación, acompañamiento y asesoramiento académico y psicológico a los estudiantes para su bienestar y permanencia hacia la terminación exitosa de su formación, gestión de voluntariado y proyección social y demás actividades de bienestar.
  7. Medidas de control de acceso, monitoreo de instalaciones, gestión de riesgos, atención de situaciones de emergencia, seguimiento de casos de salud, atención de rutas por violencias basadas en género o acoso sexual.



8. Custodia y gestión de información de bases de datos y administración de sistemas de información, actualización de sistemas, protección y custodia de información y bases de datos.
9. Investigaciones académicas, administrativas y disciplinarias de estudiantes, sanciones impuestas.
10. Interactuar en plataformas institucionales: (i) gestionar el desarrollo académico durante su formación, (ii) llevar un control de asistencia, (iii) otorgar notas, (iv) realizar actividades grupales, (v) facilitar la comunicación con el docente, (vi) visualizar el avance de la actividad, (vii) conocer el tiempo de dedicación a la actividad, (viii) las demás actividades relacionadas con su proceso formativo.
11. Trámite y respuesta de solicitudes, quejas, reclamos, actuaciones judiciales.
12. Prestación de servicios de manera directa, en conjunto y/o a través de instituciones que tengan una relación directa o indirecta con la Universidad.
13. Generación de reportes, informes y estadísticas para gestión interna y externa.
14. Procesos de acreditación y autoevaluación de programas, evaluación del rendimiento académico de los estudiantes, análisis de tendencias educativas con el fin de mejorar la calidad y eficiencia del proceso educativo.
15. Aplicar encuestas para realizar perfilamiento de usuarios, investigaciones estadísticas o evaluar la calidad.
16. Investigaciones educativas o académicas, proyectos de innovación educativa, desarrollo de programas de estudio.
17. Gestión de tarjetas y matrículas profesionales de quienes obtengan el título cuando la Universidad suscriba convenios para tal fin.
18. Validación de la autenticidad y veracidad de la información suministrada a la Universidad o la reportada por la Universidad.
19. Controlar y prevenir el fraude en cualquiera de sus modalidades.
20. Verificación de datos y referencias.
21. Dar cumplimiento a obligaciones contraídas con estudiantes, egresados y aliados estratégicos.
22. Atención y seguimiento de requerimientos de autoridad judicial o administrativa
23. Prevenir y detectar posibles casos de fraude, robo de información confidencial, uso indebido de recursos de la Universidad y otras actividades delictivas.
24. Para monitorear áreas comunes, accesos, zonas de trabajo y otras áreas relevantes con el fin de prevenir vandalismo, intrusiones y otros incidentes de seguridad, que puedan ser utilizadas como evidencia de investigación.
25. Uso de cámaras de vigilancia por seguridad y para prevenir pérdidas y fraudes, tanto internos como externos, mediante la detección y el registro de actividades sospechosas o inusuales.
26. Cumplir con la normativa vigente en Colombia para las instituciones de educación superior con entidades administrativas y judiciales incluyendo auditorías y revisiones.
27. Mantener un canal de comunicación activo y recibir comunicaciones a través de los diferentes medios como correo electrónico, WhatsApp, llamada telefónica a celular o fijo, mensajes de texto (SMS) redes sociales, para ser informado sobre procesos y actividades académicas, administrativas, de investigación, de cultura, y del medio universitario.
28. Tomar imagen en video y fotografía en todas aquellas actividades que sean adelantadas por la Universidad en cumplimiento de la misión y objetivos institucionales,



para ser publicada en medios de comunicación, redes sociales institucionales, permanecer en el repositorio de imágenes y videos en las bases de datos de la Universidad, y ser empleadas en eventos académicos, administrativos, en investigación, requerimientos judiciales, y demás actividades relacionadas con el objeto de la universidad.

29. Realizar promoción, ejecución, desarrollo y evaluación de actividades académicas, administrativas, de bienestar universitario, de programas de responsabilidad social y apoyo a comunidades vulnerables, actividades culturales, recreativas, deportivas, y sociales, para lograr la consolidación de la comunidad educativa.
30. Crear bases de datos de acuerdo con las características, perfiles y caracterización de los titulares para desarrollo de los programas académicos y atender las necesidades de los estudiantes.
31. Compartir información académica del estudiante con padre, madre, acudiente o representante legal cuando acredite el vínculo que los relaciona y esté previamente autorizado.
32. Recolección de datos sensibles para brindar al estudiante servicios de bienestar universitario como lo son la salud, el acompañamiento psicológico, servicios de bienestar social, Eventualmente se podrán compartir datos sensibles asociados al estado de salud con terceros como padre, madre, acudiente, o representante legal, con aliados asociados con la Universidad como entidades prestadoras de salud, aseguradoras y prestadoras de servicios conexos.
33. Presentar informes a entidades externas como Fiscalía, Juzgados, Ministerio de Educación Nacional, Superintendencias, entre otras.
34. Análisis estadísticos.
35. Cumplimiento de las obligaciones legales.
36. Monitoreo y seguridad mediante cámaras de vigilancia.
37. Organizar y coordinar actividades extracurriculares.
38. Realizar investigaciones que aborden temas de diversidad, inclusión y bienestar social, asegurando el uso responsable y ético de los datos.
39. Grabación de audio de reuniones, entrevistas, comités y actividades educativas o administrativas en desarrollo del objeto y misión de la Universidad.
40. Llevar registros administrativos y operativos por participación en reuniones institucionales o relacionadas con la Universidad.
41. Gestionar información relacionada con programas de intercambio y movilidad académica.
42. Compartir imágenes en video en las que aparezca el titular, cuando sean solicitadas por otro titular en cumplimiento de requerimiento o actividad universitaria.
43. Recopilar y utilizar los datos de contacto de un familiar para ser utilizados exclusivamente en casos de emergencia o necesidad.
44. Facilitar la comunicación para notificaciones importantes relacionadas con los diferentes procesos de la Universidad.
45. Las demás actividades asociadas con las funciones y finalidades propias de la Universidad, y en todo caso de acuerdo con la ley.

**ARTÍCULO 27. EGRESADOS.** La Universidad trata los datos personales de egresados, incluyendo información como: nombre completo, número de identificación, correo electrónico, número de teléfono, dirección, datos biométricos, formación, experiencia, lugar de trabajo, según corresponda, entre otros, para las siguientes finalidades:





1. Mantener contacto con los egresados para informarles sobre eventos, actividades, noticias y novedades relacionadas con la institución.
2. Realizar estudios de seguimiento laboral y académico para evaluar el impacto de los programas educativos en la trayectoria profesional de los egresados.
3. Compartir ofertas laborales, pasantías o prácticas profesionales que sean gestionadas por la institución o sus aliados estratégicos.
4. Ofrecer información sobre programas de educación continua, posgrados, talleres, diplomados y otros servicios académicos diseñados para fortalecer las competencias de los egresados.
5. Fomentar la integración de los egresados en redes, asociaciones y grupos organizados de exalumnos, con el fin de fortalecer el vínculo con la institución.
6. Invitar a los egresados a participar como mentores, conferencistas o colaboradores en proyectos institucionales.
7. Realizar y participar en eventos y actividades de carácter académico, cultural, social, y deportivo.
8. Actualizar y mantener una base de datos precisa y actualizada de los egresados para la gestión de trámites administrativos, como solicitudes de certificaciones, duplicados de títulos o consultas institucionales.
9. Brindar acceso a beneficios exclusivos para egresados, como descuentos en programas académicos, acceso a bibliotecas, servicios recreativos o participación en eventos.
10. Facilitar procesos de postulación y conexión con empleadores que requieran perfiles profesionales relacionados con los programas académicos impartidos por la institución.
11. Emisión de carnets de identificación y registro de entrada y salida de egresados.
12. Controlar préstamo de libros e insumos de la biblioteca de la Universidad.
13. Realizar actividades de promoción, ejecución, desarrollo y evaluación de actividades propias de la Universidad.
14. Realizar difusión de convocatorias de emprendimiento, laborales y becas, entre otros, relacionados con el bienestar de los egresados.
15. Expedir certificaciones relacionadas con la Universidad.
16. Generación de reportes, informes y estadísticas para gestión interna y externa.
17. Facilitar la interacción en las plataformas institucionales con el fin de gestionar servicios y programas dirigidos a la comunidad de egresados.
18. Monitoreo y seguridad mediante cámaras de vigilancia.
19. Ofrecer servicios de orientación y apoyo a egresados.
20. Recopilar opiniones y encuestas para evaluar la satisfacción de egresados sobre servicios y actividades ofrecidas por la Universidad.
21. Recopilar información sobre preferencias y necesidades de futuros estudiantes para mejorar la oferta académica.
22. Recopilar y utilizar los datos de contacto de un familiar para ser utilizados exclusivamente en casos de emergencia o necesidad.
23. Procesos de renovación de registros calificados, acreditación y autoevaluación de programas.
24. Procedimientos de anulación de títulos.
25. Tomar imagen en video y fotografía en todas aquellas actividades que sean adelantadas por la Universidad en cumplimiento de la misión y objetivos institucionales, para ser publicada en medios de comunicación, redes sociales institucionales, permanecer en el repositorio de imágenes y videos en las bases de datos de la Universidad, y ser empleadas en eventos académicos, administrativos, en



investigación, requerimientos judiciales, y demás actividades relacionadas con el objeto de la universidad.

26. Garantizar el cumplimiento de las disposiciones legales aplicables relacionadas con la gestión de información personal de los egresados y su vínculo con la institución.
27. Las demás actividades asociadas con las funciones y finalidades propias de la Universidad, y en todo caso de acuerdo con la ley.

**ARTÍCULO 28. TRABAJADORES.** La Universidad trata los datos personales de sus trabajadores, incluyendo información como: nombre completo, número de identificación, lugar y fecha de nacimiento, nacionalidad, dirección, correo electrónico, número de teléfono, hoja de vida, experiencia laboral, antecedentes, formación académica, referencias, afiliaciones a EPS, ARL, fondo de pensiones, beneficiarios de seguridad social, información médica, datos biométricos, datos de acudientes y núcleo familiar, según corresponda, entre otros, para las siguientes finalidades:

1. Gestión laboral y contractual: (i) formalizar la relación laboral y cumplir con las obligaciones legales en materia laboral, tributaria y de seguridad social, (ii) efectuar gestiones relacionadas con el desarrollo del contrato laboral como permisos, licencias, vacaciones, entre otras, (iii) gestionar trámites de solicitudes, quejas, reclamaciones y conflictos laborales, (iv) realizar la gestión de archivo, hoja de vida y carpeta laboral, (v) gestionar el pago de salarios, prestaciones sociales y beneficios adicionales, (vi) verificar referencias laborales y antecedentes académicos, profesionales, judiciales disciplinarios, penales y fiscales, (vii) gestionar la entrega de dotaciones, (viii) llevar registros administrativos y operativos por participación en reuniones, grupos de trabajos o actividades institucionales o relacionadas con la Universidad. (ix) consultar el registro de inhabilidades por delitos sexuales contra personas menores de 18 años, de conformidad con la Ley 1918 de 2018 y su reglamentación.
2. Comunicación y administración interna: (i) facilitar la comunicación directa para comunicaciones y notificaciones laborales y entrega de documentación, (ii) emitir carnets de identificación y registrar entradas y salidas, (iii) contactar para enviar comprobantes de nómina, liquidaciones de prestaciones sociales y otros documentos, (iv) realizar comunicaciones internas y externas relacionadas con la relación laboral.
3. Bienestar y desarrollo: (i) implementar programas de bienestar laboral y actividades para trabajadores y sus beneficiarios, (ii) seguimiento, compromisos y evaluación de desempeño, (iii) planes de desarrollo profesional y capacitación, (iv) ofrecer cursos, talleres y programas de formación continua, (v) gestionar encuestas de satisfacción laboral, (vi) brindar apoyo psicológico para mejorar el ambiente laboral y abordar conflictos interpersonales, (v) procesos sobre la diversidad y la inclusión en el entorno laboral.
4. Salud y seguridad en el trabajo: (i) mantener registros de seguridad y salud en el trabajo, (ii) realizar exámenes médicos periódicos, evaluaciones de riesgos laborales y prevención de accidentes, (iii) atender situaciones de emergencia y rutas de violencia basada en género, (iv) realizar invitaciones y gestionar la integración y desarrollo de comités y brigadas de emergencia.
5. Seguridad y monitoreo: (i) monitorear mediante cámaras de vigilancia para garantizar la seguridad, (ii) grabar audio y video en reuniones, entrevistas y actividades administrativas, educativas y demás requeridas de acuerdo a los fines de la Universidad.



6. Apoyo en casos especiales: (i) salvaguardar el interés vital del trabajador en caso de emergencia o incapacidad, (ii) coordinar y organizar viajes relacionados con las actividades de la Universidad, (iii) recopilar datos de contacto de familiares para casos de emergencia, (iv) brindar asesoramiento y apoyo psicológico para la gestión del proceso de jubilación.
7. Relación con terceros: (i) suministrar información a terceros con los cuales la Universidad tenga relación, (ii) ofrecer acceso a beneficios institucionales para los trabajadores.
8. Promoción institucional y servicios: (i) Realizar estudios internos y compartir información de ofertas, (ii) contactar para invitar a eventos y ofrecer nuevos productos y servicios de la Universidad, (iii) utilizar imágenes en medios institucionales y redes sociales para actividades institucionales.
9. Innovación y desarrollo: (i) investigar y desarrollar nuevos servicios o procesos relacionados con las funciones de la Universidad, (ii) participar en proyectos de investigación e innovación educativa o académica, (iii) soportar procesos de renovación de registros calificados y acreditación.
10. Interacción en las plataformas institucionales: (i) gestionar los procesos académicos y administrativos, (ii) planificación y gestión de cursos, y actividades pedagógicas, (iii) evaluación del desempeño, (iv) reporte de notas, (v) comunicación con estudiantes y personal administrativo, (vi) participación en actividades relacionadas con su labor dentro de la institución.
11. Auditorías y cumplimiento normativo: (i) soportar auditorías internas y externas, (ii) validar información en listas regulatorias para prevenir riesgos de lavado de activos, financiación del terrorismo y cumplimiento normativo, (iii) presentar informes a entidades externas en cumplimiento de obligaciones legales, (iv) cumplir con las normativas legales e institucionales, (v) gestionar todas las actividades asociadas a las funciones propias del empleador, en concordancia con la ley.

**ARTÍCULO 29. ASPIRANTES A PROCESOS DE SELECCIÓN DE PERSONAL.** La Universidad trata los datos personales de aspirantes a los procesos de selección de personal, incluyendo información como: nombre completo, número de identificación, lugar y fecha de nacimiento, nacionalidad, dirección, correo electrónico, número de teléfono, hoja de vida, experiencia laboral, formación académica, referencias, datos biométricos, antecedentes, información médica, según corresponda, entre otros, para las siguientes finalidades:

1. Identificar los candidatos y vincularlos al proceso de selección.
2. Facilitar la comunicación con el candidato.
3. Verificar que el perfil cumple con los requisitos establecidos para el cargo.
4. Evaluar la idoneidad del candidato mediante entrevistas, pruebas psicotécnicas, evaluaciones técnicas o los medios que disponga la Universidad.
5. Cumplir con requisitos específicos del cargo, como aptitudes médicas o legales.
6. Cumplir con las normativas y leyes laborales relacionadas con el proceso de contratación.
7. Facilitar la toma de decisiones basada en información completa y verificada.
8. Mantener un registro adecuado de los datos de los candidatos para fines administrativos y de auditoría.
9. Verificar la información proporcionada por los candidatos.



10. Informar al aspirante sobre los resultados del proceso.
11. Considerar a los aspirantes para futuros puestos o programas dentro de la Universidad.
12. Analizar datos para mejorar los procesos de contratación y selección en la Universidad.
13. Generar reportes sobre la gestión institucional y el uso de recursos, promoviendo la rendición de cuentas.
14. Presentar informes a entidades externas como Fiscalía, Juzgados, Ministerio de Educación Nacional, Superintendencias, entre otras, que permitan dar cumplimiento a las exigencias legales y a análisis estadísticos requeridos a la Entidad.
15. Las demás actividades asociadas con las funciones y finalidades propias de la Universidad, y en todo caso de acuerdo con la ley.

**ARTÍCULO 30. ASPIRANTES Y APRENDICES.** La Universidad trata los datos personales de aspirantes a aprendices y aprendices, incluyendo información como: nombre completo, número de identificación, lugar y fecha de nacimiento, EPS, nacionalidad, edad, dirección, correo electrónico, número de teléfono, información académica, programa, semestre, institución educativa, historial académico relevante, disponibilidad horaria, información sobre habilidades o competencias específicas, información de representantes legales para personas menores de 18 años, registros de asistencia, evaluaciones, reportes de actividades, según corresponda, entre otros, para las siguientes finalidades:

1. Evaluar si el aspirante cumple con los requisitos mínimos de ingreso a la práctica.
2. Formalizar la participación de aprendices en las prácticas formativas o productivas.
3. Garantizar la compatibilidad con las actividades de las prácticas.
4. Gestionar y administrar la relación contractual derivada del contrato de aprendizaje.
5. Facilitar la comunicación entre las partes involucradas en el proceso.
6. Realizar seguimiento y evaluación del proceso de aprendizaje y el desempeño del aprendiz.
7. Comunicar al SENA las terminaciones, suspensiones y cualquier otro cambio relacionado con el contrato de aprendizaje, en cumplimiento de la normativa vigente.
8. Transferir datos personales a entidades públicas o autoridades judiciales en cumplimiento de sus funciones legales.
9. Cumplir con las obligaciones legales en materia de seguridad social, riesgos laborales y demás regulaciones aplicables.
10. Consultar el registro de inhabilidades por delitos sexuales contra personas menores de 18 años, de conformidad con la Ley 1918 de 2018 y su reglamentación.
11. Mantener registros de seguridad y salud en el trabajo, garantizando el bienestar del aprendiz.
12. Monitorear las instalaciones mediante sistemas de video vigilancia para garantizar la seguridad.
13. Gestionar la información relacionada con el expediente del aprendiz durante el desarrollo del contrato.
14. Brindar apoyo en la formación académica y práctica del aprendiz.
15. Validar y verificar la autenticidad de la información personal proporcionada.
16. Prevenir y detectar fraudes o actividades ilícitas.
17. Facilitar auditorías internas y externas relacionadas con la gestión del contrato de aprendizaje.
18. Atender consultas, quejas y reclamaciones en relación con el proceso de aprendizaje.



19. Utilizar la fotografía del aprendiz para su identificación en documentos institucionales, hojas de vida y carnet de uso permanente.
20. Difundir la fotografía y datos del aprendiz en la página web y redes sociales institucionales para la promoción de eventos académicos y comunicados oficiales.
21. Utilizar la imagen y/o voz del aprendiz en materiales audiovisuales para la difusión de actividades académicas y formativas.
22. Registrar la imagen y/o voz del aprendiz en sistemas de video vigilancia con fines de seguridad en las instalaciones de la Universidad.
23. Prevenir riesgos en actividades formativas y proteger la salud y seguridad del aprendiz.
24. Almacenar datos de salud obtenidos a partir de exámenes médicos requeridos para el cumplimiento del contrato de aprendizaje.
25. Gestionar incapacidades médicas y justificar ausencias durante el periodo de aprendizaje.
26. Archivar los datos del aprendiz en su hoja de vida institucional para la adecuada administración del contrato.
27. Recopilar y utilizar los datos de contacto de un familiar del aprendiz para ser utilizados en casos de emergencia o necesidad.
28. Procesar cuotas de sostenimiento de la práctica y otros beneficios, cuando aplique.
29. Las demás actividades asociadas con las funciones y finalidades propias de la Universidad, y en todo caso de acuerdo con la ley.

#### **ARTÍCULO 31. PROVEEDORES, ALIADOS, CLIENTES, USUARIOS Y CIUDADANÍA EN GENERAL.**

La Universidad trata los datos personales de proveedores, aliados, clientes, usuarios y ciudadanía en general, incluyendo información como: nombre completo, tipo y número de identificación, nacionalidad, fecha de nacimiento, dirección, correo electrónico, número de teléfono, nivel educativo, experiencia laboral, estrato socio económico, información de servicios, datos biométricos, información de representantes legales, entre otros para las siguientes finalidades:

1. Crear bases de datos de acuerdo con las características y perfiles de los titulares de datos personales, todo de acuerdo con lo dispuesto en la ley.
2. Verificar el cumplimiento de los acuerdos y compromisos asumidos en virtud de la relación o vínculo existente con los proveedores y clientes.
3. Mantener un canal de comunicación con la Universidad a través de correo electrónico, mensajería instantánea institucional, llamada telefónica al celular o teléfono fijo, mensajes de texto (SMS).
4. Presentar quejas, denuncias o reportes a las autoridades o entidades competentes en caso de incumplimiento de contratos u obligaciones.
5. Realizar la consulta de antecedentes y validaciones necesarias para efectuar convenios, contratos acuerdos u oferta de servicios por parte de la Universidad.
6. Controlar las solicitudes relacionadas con los servicios prestados por la Universidad.
7. Remitir las respuestas de las solicitudes, consultas y reclamos a los petitionarios o a autoridades que lo requieran.
8. Enviar comunicaciones, notificaciones, citaciones y demás documentos emitidos por la Universidad, vía correo electrónico, redes sociales, empresa de correo certificado o por cualquier medio de envío.
9. Adelantar los tramites, servicios y otros procedimientos administrativos que sean solicitados a la Universidad.



10. Realizar campañas, actividades de divulgación, capacitaciones, cursos, oferta de servicios, laboral, y educativa.
11. Elaborar estudios, estadísticas, encuestas, análisis de tendencias, relacionados con los servicios que presta la Universidad.
12. Presentar informes a entidades externas como Fiscalía, Juzgados, Ministerio de Educación Nacional, Superintendencias, entre otras, que permitan dar cumplimiento a las exigencias legales y a análisis estadísticos requeridos a la Entidad.
13. Gestionar la información necesaria para el cumplimiento de las obligaciones tributarias, contractuales, comerciales, corporativas y contables.
14. Suministrar información de los servicios relacionados con el vínculo con el titular a través de los diferentes medios de contacto como correo electrónico, mensajería institucional, redes sociales, mensajes, llamadas, correo certificado.
15. Evaluar la calidad de los servicios prestados.
16. Capturar imágenes en video y fotografía para su publicación en medios de comunicación, redes sociales y plataformas institucionales. Estas imágenes se almacenarán en el repositorio de la Universidad y estarán disponibles para su uso en eventos académicos, administrativos, de investigación.
17. Tomar la imagen fotografía y en video de reuniones virtuales y presenciales de tipo académico, administrativo, comercial, o de oferta de servicios.
18. Llevar un control de ingreso y salida a las diferentes sedes de la Universidad.
19. Evaluar las condiciones socioeconómicas con el fin de acceder a los programas ofrecidos por la Universidad.
20. Supervisar el uso de las instalaciones de la Universidad por parte de los usuarios.
21. Enviar información a proveedores, clientes, usuarios sobre actividades, eventos y servicios ofrecidos.
22. Recopilar datos para analizar y mejorar la calidad de los programas académicos y servicios.
23. Asegurar el cumplimiento de normatividad nacional, regional e institucional.
24. Gestionar la información necesaria para la contratación de servicios y productos.
25. Proveer información y asistencia a la ciudadanía sobre programas y servicios de la Universidad.
26. Monitoreo y seguridad mediante cámaras de vigilancia.
27. Controlar el acceso a plataformas y recursos digitales utilizados por proveedores, clientes, y usuarios.
28. Monitorear y analizar datos para prevenir y detectar conductas fraudulentas.
29. Administrar datos para facilitar alianzas y colaboraciones con otras instituciones y organizaciones.
30. Administrar información de donantes
31. Gestionar programas de financiamiento a través de donaciones.
32. Generar reportes sobre la gestión institucional y el uso de recursos, promoviendo la rendición de cuentas.
33. Recopilar y utilizar los datos de contacto de un familiar para ser utilizados exclusivamente en casos de emergencia o necesidad.
34. Las demás actividades asociadas con las funciones y finalidades propias de la Universidad, y en todo caso de acuerdo con la ley.



**ARTÍCULO 32. HIJOS, HERMANOS, CONYUGES DE ESTUDIANTES TRABAJADORES Y COLABORADORES.** La Universidad trata los datos personales de los hijos, hermanos, cónyuges de estudiantes, trabajadores y colaboradores, incluyendo información como: nombre completo, documento de identificación personal, lugar y fecha de nacimiento, edad, dirección, vacunas, afiliación a EPS, datos biométricos, información de condiciones de salud, nombres de padres representante legal o acudiente, número de teléfono, correo de padre o acudiente, registros civiles, declaraciones maritales de convivencia, recibos de pagos de matrícula, según corresponda, entre otros, para las siguientes finalidades:

1. Prestar el servicio de educación inicial, ocasional en el Centro de Desarrollo y Aprendizaje María Goretti, lo cual incluye, pero no se limita, a: (i) el proceso de inscripción, (ii) aplicar las rutas y protocolos de atención de personas menores de 18 años, (iii) actualizar los registros y documentos que hacen parte de la información de personas menores de 18 años para el desarrollo de las diferentes actividades, (iv) desarrollar procesos de evaluación relacionados con la prestación del servicio, (v) preparar y presentar informes sobre actividades desarrolladas, (vi) facilitar la comunicación con padres o acudiente en caso de emergencias o temas relacionados con el servicio, (vii) confirmar que cumplen los requisitos para acceder al servicio, (viii) asegurar que las personas menores de 18 años cuenten con las condiciones de salud necesarias para participar en las actividades. (ix) capturar imágenes en video y fotografía para su publicación en medios de comunicación, redes sociales y plataformas institucionales. Estas imágenes se almacenarán en el repositorio de la Universidad y estarán disponibles para su uso en eventos académicos, administrativos, de investigación, (x) verificar la identidad de la persona a quien se entrega a la persona menor de 18 años, (xi) establecer comunicación con padres de familia, representantes o acudientes, (xii) solicitar elementos que se requiera para la persona menor de 18 años, (xiii) enviar información oportuna y adecuada sobre la atención y cuidado de las personas menores de 18 años, (xiv) participar en eventos y organizaciones que sean establecidas para los padres, representantes o acudientes, (xv) programar reuniones horarios y demás compromisos, (xvi) requerir elementos de cuidado personal.
2. Gestionar los beneficios para los estudiantes que acrediten parentesco con hermanos, hijos, padres, cónyuges o compañeros permanentes, conforme a lo establecido en el Reglamento de Becas, Incentivos, Beneficios y Subsidios a estudiantes de la Universidad.

**PARÁGRAFO:** Las finalidades mencionadas anteriormente frente a datos de personas menores de 18 años están sujetas a los lineamientos previstos en el artículo 8 de la presente política.

**ARTÍCULO 33. FINALIDADES PARA EL TRATAMIENTO DE DATOS SENSIBLES.** Los datos sensibles como salud, orientación sexual, estrato, grupo poblacional, orientación religiosa, orientación política, origen racial, étnico, orientación filosófica, pertenencia a sindicatos, entre otros, serán tratados de acuerdo con las finalidades específicas establecidas en la autorización de tratamiento de datos personales, así como con las siguientes:



1. Brindar servicios de orientación e intervención psicológica individual y grupal a la comunidad universitaria.
2. Identificar los grupos poblacionales con los que interactúa la Universidad y promover programas para población con similares características.
3. Diseñar programas y actividades que promuevan la inclusión y la equidad en la Universidad.
4. Recopilar y analizar datos sensibles para evaluar la efectividad de programas de apoyo psicológico, salud o bienestar social.
5. Identificar y prevenir situaciones de discriminación dentro de la comunidad universitaria.
6. Capacitar el personal sobre manejo de diversidad, inclusión y atención a la salud mental.
7. Proporcionar servicios específicos, como asesoramiento psicológico o programas de salud.
8. Planificar las actividades para estudiantes con discapacidades o necesidades especiales.
9. Proporcionar acompañamiento académico adaptado a las circunstancias personales del titular.
10. Asegurar el cumplimiento de leyes y regulaciones que promueven la igualdad y la no discriminación en el entorno académico.
11. Participar en investigaciones o proyectos colaborativos que aborden temas de salud, políticos, religiosos, étnicos.
12. Medir la efectividad de programas diseñados para fomentar la inclusión de grupos específicos dentro de la Universidad.

**PARÁGRAFO:** Las finalidades mencionadas anteriormente están sujetas a la autorización facultativa del titular de los datos, dado que se trata de información sensible.

## TÍTULO VII

### TRANSMISIÓN Y TRANSFERENCIA

**ARTÍCULO 34. TRANSMISIÓN.** De conformidad con lo establecido en el artículo 2.2.2.25.5.2 del Decreto 1074 de 2015, para la transmisión de datos personales la Universidad deberá suscribir un contrato de transmisión de datos con el encargado del tratamiento de datos personales. El contrato señalará:

1. Los alcances del tratamiento.
2. Las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales.
3. Las obligaciones del encargado para con el titular y el responsable.

Mediante dicho contrato el encargado se comprometerá a realizar el tratamiento de datos de acuerdo con las finalidades que los titulares hayan autorizado, conforme a la normatividad vigente, y de conformidad con las obligaciones de la Universidad relacionadas en esta política e incluirse las siguientes:

1. Dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.





2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
3. Guardar confidencialidad respecto del tratamiento de los datos personales.

**ARTÍCULO 35. TRANSFERENCIA.** Para la transferencia de datos se dará cumplimiento a lo establecido en el artículo 26 de la Ley 1581 de 2012 y demás normativa vigente.

En acatamiento de la ley, la Universidad prohíbe a sus trabajadores la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que exige la ley.

Esta prohibición no regirá cuando se trate de:

1. Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia.
2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública.
3. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
4. Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
5. Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

## TÍTULO VIII

### CONSULTAS Y RECLAMOS

**ARTÍCULO 36. CONTENIDO Y PRESENTACIÓN DE CONSULTAS.** Las consultas dirigidas a la Universidad deberán contener como mínimo lo siguiente:

1. Motivo, referencia o asunto: solicitud de acceso o consulta de datos.
2. Nombre completo del titular, del representante, y/o del causahabiente (cuando aplique) y número de identificación.
3. Manifestación clara de que información desea acceder o consultar.
4. Información para notificaciones, número de celular, dirección física y electrónica del titular, representante o causahabientes cuando aplique.
5. Copia legible del documento de identificación que permita la validación de identidad del titular, representante o causahabiente.
6. Firma del titular.
7. Soportes que acrediten la representación o la calidad de causahabientes (cuando aplique).



De conformidad con el artículo 2.2.2.25.4.2, sección 4, capítulo 25 del Decreto 1074 de 2015, la Universidad permitirá que el titular consulte de forma gratuita sus datos personales en los siguientes casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.

A partir de la segunda consulta por mes, la Universidad podrá cobrar al titular los gastos de envío cuando sea por correo certificado, conservando el comprobante de dichos gastos para presentarlo a la Superintendencia de Industria y Comercio si es necesario.

**ARTÍCULO 37. CONTENIDO Y PRESENTACIÓN DE RECLAMOS.** Los reclamos se formularán mediante solicitud dirigida a la Universidad y deberán contener como mínimo lo siguiente:

1. Motivo, referencia o asunto: solicitud de reclamo.
2. Nombre completo del titular, del representante, y/o del causahabiente (cuando aplique) y número de identificación.
3. La descripción de los hechos que dan lugar al reclamo.
4. Manifestación clara de lo que se pretende: actualizar, corregir, suprimir, revocar.
5. Información para notificaciones, número de celular, dirección física y electrónica del titular, representante o causahabientes cuando aplique.
6. Copia legible del documento de identificación que permita la validación de identidad del titular representante o causahabiente.
7. Soportes que acrediten la representación o la calidad de causahabientes (cuando aplique).
8. Documentos que se quiera hacer valer como pruebas.

**ARTÍCULO 38. MEDIOS PARA PRESENTAR CONSULTAS O RECLAMOS.** El titular del dato personal o su representante podrá presentar su consulta o reclamo a través de los siguientes canales:

1. Correo electrónico: [correspondencia@unicesmag.edu.co](mailto:correspondencia@unicesmag.edu.co)
2. La página web: <https://www.unicesmag.edu.co/> para ello es necesario completar el formato de recepción de reclamos o consultas disponible en el portal web, incluyendo todos los datos requeridos, y adjuntado los soportes correspondientes, concluida la radicación el sistema generará un número de radicación que permitirá al solicitante hacer seguimiento.
3. Oficina ubicada en la Carrera 20 A No. 14 – 53, Pasto, en la Secretaría General de la Universidad. En este caso, el personal autorizado registrará el reclamo o consulta en el sistema y proporcionará al solicitante un número de radicación para seguimiento posterior.

Las consultas o reclamos radicadas en Secretaría General podrán realizarse dentro de los horarios de atención de lunes a viernes de 07:00 a.m. a 12:00 m y de 2:00 p.m. a 06:00 p.m. dentro de los días hábiles establecidos por la Universidad, con excepción de los períodos de receso como Semana Santa, mitad de año y vacaciones colectivas de fin de año, según los calendarios académicos autorizados por la Universidad.



**PARÁGRAFO PRIMERO:** El titular podrá ejercer sus derechos mediante el mismo medio por el cual se recolectó su información, o por el canal que considere oportuno, para lo cual se seguirá el procedimiento establecido en la presente política.

**PARÁGRAFO SEGUNDO:** En los casos en que el tratamiento de datos personales sea realizado por un encargado del tratamiento, el responsable del tratamiento de datos registrará la información de contacto del encargado para que el titular pueda adelantar ante este el ejercicio de sus derechos, sin perjuicio de la posibilidad que tiene de acudir directamente al responsable del tratamiento.

**ARTÍCULO 39. PROCEDIMIENTO PARA CONSULTAS.** La Universidad, como responsable del tratamiento de los datos personales, establece este procedimiento para la atención y respuesta a las consultas:

No.	PASO	RESPONSABLE	ACCIÓN
1	Recepción de solicitudes y remisión	Secretaría General	Recibe, identifica la solicitud de consulta presentada por medio físico, por la página o por correo electrónico, y la radica a través de Orfeo, asignando un número de radicación para que el solicitante pueda consultar el estado de la solicitud, y de forma inmediata se remite a la dependencia encargada del tratamiento de datos con copia al Oficial de protección de datos personales.
2	Elaboración y respuesta	Dependencia responsable del dato	Una vez recibida la solicitud, cuenta con cinco (5) días hábiles contados a partir de la fecha de recibo de la solicitud para elaborar, proyectar y enviar la respuesta para aprobación y firma del Oficial de protección de datos personales.
3	Aprobación de respuesta	Oficial de Protección Datos	Evento 1: En un término máximo de dos (2) días, revisará y aprobará la respuesta proyectada.  Evento 2: En un plazo máximo de dos (2) días, revisará la respuesta. Si se requieren ajustes, la respuesta se devolverá a la dependencia responsable del dato, quien tendrá un (1) día para realizar las adecuaciones necesarias y reenviarla para su aprobación. Una vez enviada la respuesta ajustada, el Oficial de protección de Datos personales tendrá dos (2) días para aprobarla, firmarla y remitirla a Secretaría General.



No.	PASO	RESPONSABLE	ACCIÓN
4	Remisión de respuesta	Secretaría General	Al término máximo de diez (10) días contados a partir de la fecha de radicación, se debe remitir la respuesta final al interesado.

**ARTÍCULO 40. PLAZO DE RESPUESTA A CONSULTAS.** Una vez radicada la solicitud, la consulta será atendida en un término máximo de diez (10) días hábiles a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho lapso, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término, de conformidad con el artículo 14 de la Ley 1581 de 2012.

**ARTÍCULO 41. CONSULTAS INCOMPLETAS.** Si la consulta no cumple con los requisitos previamente establecidos, el Secretario General, dentro de los dos (2) días hábiles siguientes al recibo de la petición, mediante comunicación solicitará al peticionario la complementación de la información de su solicitud o de los documentos requeridos. En tal evento el plazo se contará a partir del momento en el cual el peticionario complete la información o documentación. Si el peticionario no allega la información solicitada en el término máximo de un mes, la consulta será archivada de conformidad con lo establecido en el artículo 17 de la Ley 1755 de 2015.

**ARTÍCULO 42. PROCEDIMIENTO PARA RECLAMOS.** La Universidad, como responsable del tratamiento de los datos personales, establece este procedimiento para la atención y respuesta a reclamos:

No.	PASO	RESPONSABLE	ACCIÓN
1	Recepción, identificación y radicación del reclamo	Secretaría General	Recibe, identifica y radica la solicitud de reclamo presentada por medio físico, por la página o por correo electrónico, y la radica a través de Orfeo, para que el solicitante pueda consultar el estado de atención del reclamo; y de forma inmediata remite la solicitud a la dependencia responsable del dato con copia al correo electrónico del Oficial de Protección de datos Personales.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.



No.	PASO	RESPONSABLE	ACCIÓN
2	Elaboración de respuesta	Dependencia responsable del dato	<p>Realizará el proyecto de respuesta en un término de ocho (8) días siguientes a la recepción del reclamo. En caso de requerirse, podrá consultar a la Oficina Jurídica a la mayor brevedad posible, para que esta pueda apoyar la respuesta dentro de este término.</p> <p>Una vez proyectada la respuesta, la remitirá al Oficial de protección de datos personales para su aprobación.</p>
3	Aprobación respuesta	Oficial protección datos	<p>de de</p> <p>Evento 1: en un término máximo de dos (2) días, revisará y aprobará la respuesta proyectada.</p> <p>Evento 2: en un plazo máximo de dos (2) días, revisará la respuesta. Si se requieren ajustes, la respuesta se devolverá a la dependencia responsable del dato, quien tendrá un (1) día para realizar las adecuaciones necesarias y reenviarla para su aprobación. Una vez enviada la respuesta ajustada, el Oficial de protección de Datos Personales tendrá dos (2) días para aprobarla, y enviará la respuesta aprobada a Secretaría General.</p> <p>Si la situación presentada lo requiere, debe realizar un análisis de las causas que generaron el reclamo y establecer un Plan de Acción para evitar que vuelva a ocurrir, enviando copia al Comité de Protección de Datos (numeral 6 del presente procedimiento)</p>
4	Envío respuesta	de Secretaría General	Al término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de recibo del reclamo, remitirá la respuesta final al interesado.
5	Cierre reclamo	del Secretaría General	Con el envío de la respuesta al interesado, se actualizará la base de datos cambiando la leyenda “reclamo en trámite” por “reclamo



No.	PASO	RESPONSABLE	ACCIÓN
			decidido”, la actualización se realizará una vez se envíe la respuesta al interesado.
6	Seguimiento	Comité de Protección de Datos	En caso de existir Plan de Acción, se realiza seguimiento y se verifica o ajusta las acciones propuestas.

**ARTÍCULO 43. PLAZO DE RESPUESTA A RECLAMOS.** El término máximo para atender reclamos será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado, por intermedio de la Secretaría General, los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

**ARTÍCULO 44. RECLAMOS INCOMPLETOS.** Una vez radicado el reclamo, si este resulta incompleto, el Secretario General, requerirá al reclamante dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En tal evento el plazo se contará a partir del momento en el cual el peticionario complete la información o documentación. En caso de que quien lo reciba no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

**ARTÍCULO 45. REQUISITO DE PROCEDIBILIDAD.** El titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante la Universidad.

## TÍTULO IX

### PROGRAMA INTEGRAL DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

#### CAPÍTULO I

#### MEDIDAS DE SEGURIDAD

**ARTÍCULO 46. MEDIDAS DE SEGURIDAD.** La Universidad adoptará las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros de datos personales, previniendo su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Para desarrollar medidas de seguridad efectivas, la Universidad CESMAG desarrollará el Programa Integral de Gestión de Protección de Datos Personales (PIGPD), que contemplará los siguientes componentes:

1. Políticas internas
2. Sistema de administración de riesgos asociados al tratamiento de datos personales
3. Protocolos de respuesta en el manejo de violaciones e incidentes
4. Capacitación en protección de datos



5. Comité de protección de datos personales
6. Auditorías para verificar el cumplimiento de las políticas y normativas internas
7. Sistemas de vigilancia para prevenir y detectar riesgos.
8. Gestión de Cookies en plataformas digitales institucionales
9. Gestión documental: adecuado control del ciclo de vida de los documentos que contienen datos personales
10. Relaciones contractuales a través de cláusulas específicas en los contratos para garantizar el cumplimiento de la normativa de protección de datos por partes de terceros vinculados con la Universidad.

## CAPÍTULO II

### POLÍTICAS INTERNAS

**ARTÍCULO 47. POLÍTICAS INTERNAS.** En cumplimiento al artículo 2.2.2.25.6.2. la Universidad adopta las siguientes políticas para garantizar la gestión responsable y segura de la información: (i) Política general de privacidad de la información. (ii) Política general de seguridad de la información.

**ARTÍCULO 48. POLÍTICA GENERAL DE PRIVACIDAD DE LA INFORMACIÓN.** La Universidad reconoce la importancia de garantizar un tratamiento transparente, seguro y adecuado de la información personal contenida en sus bases de datos. Por ello se compromete a salvaguardar el derecho a la autodeterminación informática mediante los siguientes lineamientos:

- a. **Participación voluntaria y autorización informada:** La Universidad asegura la participación voluntaria de los titulares en los procesos de suministro, captación y actualización de datos personales, obteniendo siempre su autorización previa, expresa e informada.
- b. **Prohibición de transferencia sin autorización:** No se cederán, venderán ni compartirán datos personales sin el consentimiento expreso del titular, salvo en los casos previstos por la ley.
- c. **Tratamiento por terceros:** Las actividades de tratamiento de datos podrán ser realizadas por aliados, contratistas y/o proveedores de servicios autorizados, quienes estarán obligados, tanto contractual como legalmente, a garantizar la confidencialidad y el uso exclusivo de la información para los fines establecidos en los acuerdos o contratos con la Universidad.

**ARTÍCULO 49. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.** La Universidad, consciente de la importancia de proteger la confidencialidad, integridad y disponibilidad de la información, ha dispuesto el desarrollo del siguiente marco estratégico para la seguridad de sus datos y procesos:

1. **Protección integral:** la Institución ha dispuesto recursos humanos y tecnológicos para garantizar la seguridad de su información y bases de datos.
2. **Manual de seguridad de la información:** establece directrices específicas para proteger los datos almacenados, promover la continuidad de los procesos



administrativos y académicos, y fomentar una cultura de responsabilidad entre los colaboradores.

**PARÁGRAFO.** La Universidad no se hace responsable por las consecuencias derivadas de:

- a. El acceso indebido o fraudulento por parte de terceros a sus sistemas de almacenamiento de información.
- b. Fallas técnicas ajenas a su control que afecten la integridad o conservación de los datos.

### CAPÍTULO III

#### SISTEMAS DE ADMINISTRACIÓN DE RIESGOS

**ARTÍCULO 50. SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES.** La Universidad adoptará un Sistema de Gestión de Riesgos orientado a identificar, evaluar y mitigar los riesgos relacionados con el tratamiento de datos personales en sus actividades. Este sistema incluirá herramientas, indicadores y recursos necesarios para garantizar una gestión adecuada y efectiva de dichos riesgos. El diseño del sistema tendrá en cuenta la estructura organizacional, los procesos internos, la cantidad y naturaleza de las bases de datos, así como los tipos de datos personales tratados. Prestará especial atención a escenarios que representen riesgos frecuentes o de alto impacto, los cuales puedan comprometer la calidad del servicio o la seguridad de la información de los titulares.

**ARTÍCULO 51. COMPONENTES DEL SISTEMA.** El sistema de administración de riesgos asociados al tratamiento de datos personales deberá contener:

1. **Identificación de riesgos:** se identificarán los riesgos potenciales, incluyendo el riesgo residual e incidentes previos relacionados con el tratamiento de datos personales.
2. **Evaluación de probabilidad e impacto:** se determinará la probabilidad de ocurrencia de los riesgos y su impacto en caso de materializarse.
3. **Acciones de mitigación y control:** se definirán y ejecutarán acciones concretas para mitigar los riesgos identificados y se evaluará la efectividad, suficiencia y oportunidad de dichas medidas.
4. **Clasificación de controles:** se especificará el tipo de control implementado, clasificándolo como automático, discrecional, obligatorio, preventivo o correctivo.
5. **Seguimiento y monitoreo:** se realizarán evaluaciones periódicas para verificar la eficacia de las medidas implementadas y realizar los ajustes necesarios.

**ARTÍCULO 52. TIPOLOGÍA DE RIESGOS.** El sistema considerará los siguientes eventos o acciones de riesgo, entre otros:

1. **Delitos y Fraudes:** Incluye accesos no autorizados, suplantación de identidad, hurto de información confidencial, falsificación de documentos o uso indebido de datos. Estos actos pueden vulnerar la privacidad de los titulares y generar pérdidas económicas para la Universidad.
2. **Eventos naturales y fallos técnicos:** desastres naturales (terremotos, inundaciones) y fallos técnicos (cortes de energía, fallas en sistemas informáticos) que pueden derivar





en pérdida de datos, interrupción de servicios y afectación a la accesibilidad de información crítica.

3. **Errores humanos y decisiones administrativas:** divulgación accidental de datos sensibles, manejo inadecuado de información o incumplimiento de protocolos de seguridad que comprometan la integridad de los datos personales. Estos errores pueden provocar brechas de seguridad y comprometer la integridad de la información.
4. **Condiciones de seguridad inadecuadas:** deficiencias en medidas de seguridad física, como controles de acceso insuficientes en instalaciones que almacenan datos, lo cual facilita accesos no autorizados y robo de información.
5. **Ciberataques y pérdida de información:** hackeos, malware, robo de contraseñas o accesos indebidos que comprometen la integridad, disponibilidad y confidencialidad de los datos almacenados.
6. **Accesos no autorizados:** brechas en protocolos de seguridad que permitan el acceso de personas no autorizadas a sistemas, bases de datos o instalaciones, exponiendo información sensible y poniendo en riesgo la seguridad de los titulares y la reputación institucional.

**ARTÍCULO 53. MEDIDAS DE PROTECCIÓN.** A través del sistema de protección, la Universidad implementará medidas preventivas, correctivas y de mitigación para evitar o reducir los daños derivados de la materialización de amenazas. Dichas medidas estarán orientadas a:

1. Proteger la integridad, disponibilidad y confidencialidad de los datos personales.
2. Garantizar el cumplimiento de las normativas legales vigentes en materia de protección de datos personales.
3. Fortalecer la confianza de los titulares en el manejo de su información por parte de la Institución.

## CAPÍTULO IV

### PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES O INCIDENTES

**ARTÍCULO 54. PROTOCOLOS.** Con el propósito de fortalecer la seguridad y protección de los datos personales, la Universidad implementará protocolos de respuesta específicos para gestionar incidentes y vulneraciones relacionadas con su sistema de información. Estos protocolos contemplarán lo siguiente:

1. Procedimiento de manejo de incidentes o vulneraciones a sistemas de información.
2. Área o persona responsable de manejar los incidentes o vulneraciones a sistemas de información.
3. Mecanismos para rendir informes internos y reportar los incidentes a la Superintendencia, informando el tipo de incidentes, la fecha que ocurrió y que tuvo conocimiento del mismo, la causal, el tipo de datos personales comprometido, la cantidad de titulares afectados.
4. Mecanismos que permitan reportar incidentes y comunicarse de manera eficiente con los titulares afectados: notificar a los titulares sobre el incidente de seguridad relacionado con sus datos personales y las posibles consecuencias, proporcionar herramientas a los afectados para minimizar el daño potencial causado.



## CAPÍTULO V

### CAPACITACIÓN DE PROTECCIÓN DE DATOS PERSONALES

**ARTÍCULO 55. CAPACITACIONES.** Para la Universidad es fundamental mantener a los trabajadores administrativos, docentes, estudiantes, aprendices y público en general, informados sobre las disposiciones y normativas relacionadas con la protección de datos personales. Con este fin, la Universidad ha incorporado capacitaciones sobre el tratamiento adecuado de los datos personales.

Esta formación garantizará que todos los miembros de la comunidad universitaria estén al tanto de las mejores prácticas y de los requisitos legales en materia de protección de datos.

A lo largo del periodo formativo, se llevarán a cabo capacitaciones específicas por grupos de trabajo. Estas sesiones estarán diseñadas para facilitar la comprensión y aplicación de las directrices sobre manejo de información y medidas de seguridad, ajustándose a las particularidades y operaciones de cada área de la Universidad.

Se buscará crear una cultura de protección de datos que involucre a todos los miembros de la comunidad, promoviendo así un enfoque proactivo en la gestión de la información personal.

En consecuencia, la Universidad se compromete a garantizar que su personal esté debidamente preparado y consciente de la importancia de la protección de datos personales, promoviendo así el cumplimiento de la normativa y la salvaguarda de la privacidad de todos los titulares de datos.

## CAPÍTULO VI

### COMITÉ DE PROTECCIÓN DE DATOS PERSONALES

**ARTÍCULO 56. COMITÉ DE PROTECCIÓN DE DATOS PERSONALES.** Se creará un Comité de Protección de Datos Personales. Este Comité será responsable de supervisar el programa de protección de datos personales en la Universidad. Servirá como un espacio de control donde se revisarán, discutirán, validarán y aprobarán directrices orientadas a implementar, consolidar y mejorar continuamente las actividades relacionadas con el tratamiento de datos.

## CAPÍTULO VII

### AUDITORÍAS

**ARTÍCULO 57. AUDITORÍAS.** La Universidad llevará a cabo auditorías con el objeto de evaluar la efectividad de las políticas y procedimientos implementados en el ámbito de la protección de datos personales en pro de garantizar que se cumplan los estándares establecidos y para identificar posibles incumplimientos que puedan comprometer la seguridad y la privacidad de la información.

**ARTÍCULO 58. OBJETIVOS DE LAS AUDITORÍAS.** Las auditorías tendrán varios objetivos a saber:



1. Evaluación de la eficacia: medir la efectividad de las políticas y procedimientos existentes en la gestión de datos personales, asegurando que se apliquen de manera consistente y efectiva en toda la Universidad.
2. Detección de incumplimientos: identificar cualquier incumplimiento de la normativa de protección de datos, así como desviaciones de los procedimientos internos establecidos, que puedan poner en riesgo la seguridad de la información.
3. Recomendaciones de mejora: proporcionar recomendaciones concretas para mejorar las prácticas de gestión de datos y ajustar las políticas existentes, promoviendo un enfoque de mejora continua.

**ARTÍCULO 59. METODOLOGÍA DE LAS AUDITORÍAS.** Las auditorías se llevarán a cabo utilizando una metodología estructurada que podrá incluir:

1. Revisión documental: análisis de la documentación existente relacionada con las políticas de protección de datos, registros de incidentes y procedimientos de manejo de información.
2. Entrevistas y encuestas: realización de entrevistas y encuestas a trabajadores y grupos de trabajo para obtener información sobre la implementación de las políticas y su comprensión por parte del personal.
3. Pruebas de cumplimiento: ejecución de pruebas prácticas para verificar la correcta aplicación de las normas, políticas y procedimientos en situaciones reales.

**ARTÍCULO 60. FRECUENCIA DE LAS AUDITORÍAS.** Las auditorías se llevarán a cabo de forma regular, con una frecuencia determinada por el Comité de Protección de Datos. Esta frecuencia puede ser anual, semestral o trimestral, dependiendo del nivel de riesgo asociado y de los cambios en la normativa o en las operaciones de la Universidad.

**ARTÍCULO 61. INFORME DE RESULTADOS.** Al finalizar cada auditoría, se elaborará un informe detallado que podrá incluir:

1. Hallazgos significativos: un resumen de los hallazgos más significativos, incluyendo incumplimientos detectados y áreas de mejora.
2. Recomendaciones: sugerencias específicas para abordar las deficiencias identificadas y mejorar la protección de datos.
3. Plan de Acción: un plan de acción con plazos y responsables para la implementación de las recomendaciones, asegurando así el seguimiento adecuado.

**ARTÍCULO 62. COMPROMISO CON LA MEJORA CONTINUA.** La Universidad se compromete a utilizar los resultados de las auditorías como una herramienta para fomentar la mejora continua en la gestión de datos personales. Las lecciones aprendidas se integrarán en la capacitación del personal y en la actualización de políticas, asegurando un enfoque proactivo y adaptativo ante los desafíos en el ámbito de la protección de datos.

## CAPÍTULO VIII

### SISTEMAS DE VIGILANCIA PARA PREVENIR Y DETECTAR RIESGOS

**ARTÍCULO 63. SISTEMAS DE VIDEOVIGILANCIA.** La Universidad implementa un Sistema de Vigilancia, mediante cámaras de video vigilancia con el objetivo de garantizar



la seguridad de sus bienes materiales y de las personas que acceden a sus instalaciones.  
El ejercicio de este sistema estará sujeto a:

1. Las imágenes recolectadas serán conservadas únicamente por el tiempo necesario para cumplir con la finalidad del Sistema de Vigilancia, y no permanecerán en las bases de datos por un período superior a 30 días. Una vez alcanzado este objetivo, las imágenes serán eliminadas. Sin embargo, si las imágenes son objeto de consulta, reclamo, o están involucradas en algún procedimiento administrativo o judicial, se conservarán hasta que se resuelva dicha situación.
2. La base de datos que almacena las imágenes será inscrita en el Registro Nacional de Bases de Datos, salvo en casos donde el tratamiento consista únicamente en la reproducción o emisión en tiempo real.
3. Se suscribirá cláusulas de confidencialidad con el personal que tenga acceso a las imágenes.
4. Las cámaras no se instalarán en lugares donde la recolección pueda afectar la vida privada de las personas.
5. La visualización de imágenes grabadas se restringirá a áreas de acceso controlado.
6. El proceso para el ejercicio de los derechos de consulta y reclamo del titular se regirá por el procedimiento contemplado en esta política, y bajo los requisitos en ella establecidos, adicionalmente se requerirán datos específicos para localizar las imágenes como fecha y horas específicas, en caso de que aparezcan terceros, será necesaria la autorización de estos para la divulgación, si no se cuenta con la autorización de los terceros, se garantizará el anonimato de sus datos mediante técnicas que preserven su privacidad, como el desenfoque o la fragmentación de las imágenes.

**ARTÍCULO 64. SISTEMAS DE VIDEOVIGILANCIA FRENTE A NIÑOS, NIÑAS Y ADOLESCENTES.** El tratamiento de imágenes de niños, niñas y adolescentes a través de la video vigilancia tiene como finalidad garantizar la seguridad durante las actividades realizadas dentro de la Institución, generando un entorno seguro que favorezca el desarrollo de las actividades realizadas por la persona menor de 18 años y respetando sus derechos fundamentales.

Para ello se aplicarán las siguientes reglas:

1. Contar con la autorización de los padres o representantes legales de las personas menores de 18 años y con la aquiescencia de estos, teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto.
2. Informar a los padres o representantes legales acerca de la finalidad y el tratamiento al cual serán sometidos los datos personales de las personas menores de 18 años, así como los derechos que les asisten.
3. Limitar la recolección y demás tratamiento de las imágenes, de acuerdo con lo que resulte proporcional y adecuado en consideración a la finalidad previamente informada.
4. Garantizar la seguridad y reserva de los datos personales de las personas menores de 18 años.
5. Restringir el acceso y la circulación de las imágenes, conforme a lo establecido en la ley.

**ARTÍCULO 65. AVISOS O DISTINTIVOS EN ZONAS DE VIDEOVIGILANCIA.** La Universidad informará a los titulares de los datos personales que se encuentran en áreas de



video vigilancia mediante avisos distintivos en las zonas de video vigilancia, especialmente en los puntos de ingreso a los lugares que están siendo vigilados, así como en el interior de estos espacios.

Dichos avisos contendrán:

1. Información del responsable del tratamiento y sus datos de contacto.
2. Indicación del tratamiento que se dará a los datos y la finalidad del mismo.
3. Los derechos de los titulares.
4. Indicación de dónde está publicada la Política de Tratamiento de la Información.

## CAPÍTULO IX

### GESTIÓN DE COOKIES EN PLATAFORMAS DIGITALES INSTITUCIONALES

**ARTÍCULO 66. COOKIES.** La Universidad utiliza cookies para mejorar la experiencia de navegación, siendo estos pequeños archivos de texto que se almacenan en el dispositivo del usuario al visitar nuestras páginas, que permiten personalizar el contenido y recordar preferencias, así como analizar el tráfico del sitio para optimizar su funcionamiento.

La Universidad puede utilizar diferentes categorías de cookies, que permiten que nuestras plataformas funcionen de manera más eficiente y personalizada al ingresar a nuestra página institucional o cualquiera de nuestros sitios web y al dar clic en "ACEPTAR" en el aviso emergente de cookies, permite ofrecerle contenido relevante y a analizar el tráfico del sitio, lo que a su vez nos implica optimizar nuestras aplicaciones y servicios.

Este consentimiento implica que ha tomado conocimiento acepta los términos y condiciones, así como nuestras políticas relacionadas con el tratamiento y protección de datos personales de acuerdo con la normativa vigente y directrices de la Superintendencia de Industria y Comercio (SIC).

En la Universidad, hemos desarrollado un Manual de Seguridad de la Información. Este manual proporciona pautas y lineamientos específicos que serán esenciales para todos los trabajadores, promoviendo una cultura de responsabilidad y vigilancia en la gestión de la información.

La Universidad no se responsabiliza por cualquier consecuencia derivada del ingreso indebido o fraudulento por parte de terceros a la base de datos y/o por alguna falla técnica en el funcionamiento y/o conservación de datos en el sistema de almacenamiento de la información, por causas que no le sean imputables.

**ARTÍCULO 67. ALMACENAMIENTO DE COOKIES.** Las cookies quedan almacenadas en el dispositivo que ingresó a la página web de la Universidad, dependiendo del tipo de dispositivo que se tenga.

**ARTÍCULO 68. ELIMINACIÓN DE COOKIES.** Para eliminar las cookies, debe tener en cuenta el navegador que utiliza. A continuación, relacionamos y enlazamos los navegadores para que conozca el procedimiento para eliminar las Cookies:

1. [Google Chrome](#)



2. Safari
3. FireFox
4. Opera
5. Internet Explorer
6. Android
7. Windows Phone
8. Blackberry

También, se puede navegar de manera incógnito para que el navegador no guarde este tipo de información.

## CAPÍTULO X

### GESTIÓN DOCUMENTAL DEL CICLO DE VIDA DE DOCUMENTOS QUE CONTIENEN DATOS PERSONALES

**ARTÍCULO 69. GESTIÓN DE DOCUMENTOS.** La Universidad, comprometida con la protección de los datos personales, establece lineamientos claros para la gestión de documentos que contienen dicha información. Estas directrices incluyen su adecuada conservación, el lugar de almacenamiento, las condiciones bajo las cuales serán resguardados, y el tiempo de conservación, definido según la normatividad legal aplicable o por disposición interna de la Institución. Asimismo, se contemplan las acciones relacionadas con la disposición final de los documentos, las cuales se especifican a continuación:

1. **Transporte a archivos históricos:** El traslado de documentos con datos personales se realizará bajo adecuadas medidas de seguridad. Los documentos físicos serán transportados en empaques sellados que eviten accesos no autorizados, mientras que los documentos digitales se enviarán por canales encriptados y seguros. Cada movimiento será registrado detalladamente, especificando el lugar de origen, el destino, el tipo de documento y el responsable del proceso.
2. **Reciclaje:** Los documentos físicos podrán ser transformados en materia prima reutilizable, siempre y cuando se garantice que los datos personales no puedan ser recuperados ni expongan la privacidad de los titulares.
3. **Reutilización:** La información contenida en los documentos podrá ser utilizada para fines diferentes, siempre que exista autorización expresa del titular en el marco de esta política. Este proceso se llevará a cabo bajo medidas estrictas de seguridad que aseguren la privacidad.
4. **Conservación:** Los documentos serán resguardados en su estado original, bajo condiciones de seguridad que prevengan cualquier acceso no autorizado o deterioro, garantizando su integridad durante el período definido.
5. **Digitalización:** Los documentos físicos podrán ser convertidos a formatos digitales para garantizar su preservación y un acceso más eficiente. Este proceso se realizará de manera confidencial, asegurando la protección de los datos personales.
6. **Destrucción:** Cuando corresponda la supresión de los datos personales, los documentos serán eliminados de manera irreversible. Esto incluirá el borrado seguro de plataformas digitales y la destrucción física de los documentos. Sin embargo, ciertos datos podrán mantenerse en registros históricos cuando sea necesario para cumplir



obligaciones legales de la Universidad. La eliminación se aplicará únicamente al tratamiento activo de los datos, conforme a las solicitudes de los titulares y la normativa vigente.

## CAPÍTULO XI

### RELACIONES CONTRACTUALES

**ARTÍCULO 70. CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES EN CONTRATOS.** En todos los contratos celebrados por la Universidad se incluirá una cláusula de confidencialidad y manejo de la información, mediante la cual las partes contratantes se comprometen a garantizar la reserva de los datos personales que puedan llegar a conocerse o tratarse en el marco de la relación contractual.

Esta cláusula establecerá que los datos personales recolectados serán tratados conforme a lo dispuesto en esta política, la cual será puesta a disposición del contratante previo a la suscripción del contrato. Al firmar el contrato, las partes manifiestan su aceptación expresa de las disposiciones contenidas en la política.

De igual manera, se informará a los contratantes sobre las finalidades específicas del tratamiento de sus datos y los derechos que les asisten como titulares, en cumplimiento de la normatividad vigente en materia de protección de datos personales.

## TÍTULO X

### REGISTRO NACIONAL DE BASES DE DATOS Y PERIODO DE VIGENCIA DE BASES DE DATOS

**ARTÍCULO 71. REGISTRO NACIONAL DE BASES DE DATOS.** La Universidad en cumplimiento del artículo 25 de la Ley 1581 y el capítulo 26 sección 1 del Decreto 1074 de 2015 y sus normas modificatorias, registrará sus bases de datos en el Registro Nacional de Bases de Datos (RNBD) administrado por la Superintendencia de Industria y Comercio. Este registro incluirá la presente política de tratamiento de datos personales y se llevará a cabo de acuerdo con el procedimiento y de conformidad a los lineamientos y las fechas previstas por la Superintendencia de Industria y Comercio. Las bases de datos que se creen con posterioridad a ese plazo, se inscribirán dentro de los dos (2) meses siguientes, contados a partir de su creación.

La Universidad se reserva el derecho de clasificar y conservar como confidencial cierta información contenida en sus bases de datos, conforme a lo establecido por la ley, sus estatutos y reglamentos internos. Esta decisión está en línea con el derecho fundamental a la educación, la libertad de cátedra y la autonomía universitaria.

En cumplimiento de lo anterior, la Universidad ha implementado un inventario de bases de datos que será actualizado según las necesidades y circunstancias que puedan surgir. Este inventario constituye una herramienta esencial para garantizar la transparencia y el adecuado manejo de la información, y se ajusta a las funciones institucionales de la Universidad y a las finalidades establecidas en el Título VI de la presente política.



Las bases de datos de la Universidad están disponibles para consulta, y pueden ser accedidas a través del siguiente enlace: <https://rnbd.sic.gov.co/sisi/consultatitulares/consultas#>, diligenciando como nombre o razón social "Universidad CESMAG" e ingresando el código que suministra la página.

**ARTÍCULO 72. PERIODO DE VIGENCIAS DE BASES DE DATOS.** Los datos personales se conservarán en las bases de datos de responsabilidad de la Universidad y serán objeto de tratamiento durante el tiempo establecido en la normatividad que regula esta materia o por un tiempo que sea razonable y necesario para el cumplimiento de la finalidad para la cual son obtenidos los datos y de conformidad con la autorización otorgada por los titulares de los datos personales.

## TÍTULO XI

### DISPOSICIONES FINALES

**ARTÍCULO 73. CAMBIOS SUSTANCIALES.** Los cambios sustanciales de esta política, referidos a la identificación del responsable y a la finalidad del tratamiento de los datos personales y que afecten el contenido de la autorización, se podrán consultar en el siguiente link: <https://www.unicesmag.edu.co/wp-content/uploads/2022/11/politicas-tratamiento-datos-UNICESMAG.pdf>

**ARTÍCULO 74. INTERPRETACIÓN.** El Consejo Directivo será el intérprete del presente Acuerdo y resolverá las ambigüedades y conflictos que se puedan presentar para su aplicación.

**ARTÍCULO 75. VIGENCIA.** La presente política entrará en vigor desde la fecha de su aprobación.

**ARTÍCULO 76. DEROGATORIAS.** La presente política deja sin efecto las disposiciones que le sean contrarias y en particular el Acuerdo No. 074 de 2014.

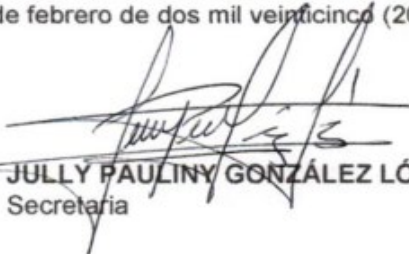
**ARTÍCULO 77. EJECUCIÓN DE LA POLÍTICA.** Es responsabilidad de todos los miembros de la Universidad, de acuerdo con sus competencias, velar por el cumplimiento de esta política.

**ARTÍCULO 78. DIVULGACIÓN.** Esta política se divulgará en los términos de lo establecido en el Acuerdo 038 del 26 de noviembre de 2021 del Consejo Directivo y estará disponible para su consulta en el repositorio de la página Web de la Universidad.

### PUBLÍQUESE Y CÚMPLASE

Dado en Pasto, a los veintisiete (27) días del mes de febrero de dos mil veinticinco (2025).

  
CHRISTIAN CAMILO CASTAÑO RAMÍREZ  
Presidente

  
JULY PAULINY GONZÁLEZ LÓPEZ  
Secretaria