RESOLUCION RECTORAL No. 1542
19 de noviembre de 2020

POR LA CUAL SE APRUEBA EL PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES DE LA CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS - UNIMINUTO

El Rector General de la Corporación Universitaria Minuto de Dios - UNIMINUTO, en uso de sus atribuciones estatutarias, y en especial la establecida en el literal m del artículo 40 de los Estatutos, y

CONSIDERANDO

Que para la Corporación Universitaria Minuto de Dios – UNIMINUTO es importante garantizar el uso eficaz, seguro y racional de la información, por lo que se hace necesario regular su empleo atendiendo las disposiciones legales y reglamentarias previstas para el efecto, en especial las contenidas en la Norma ISO/IEC 27000 *"Estándar de seguridad de la información; provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información"*, y la Norma ISO/IEC 31000 que *"Brinda principios y directrices para la gestión del riesgo"*.

Que para la Corporación Universitaria Minutos de Dios – UNIMINUTO, es fundamental la protección de la información, buscando la disminución del impacto generado por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la información, acorde con las necesidades internas, normatividad y los dispuestos por ley.

Que el artículo 2 de la Ley estatutaria No. 1581 del 17 de octubre de 2012, *"Por el cual se dictan disposiciones generales para la protección de Datos Personales"* en su ámbito de aplicación ordena *"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada"*.

Que el artículo 23 del Decreto 1377 de 2013, *"Medios para el ejercicio de los derechos"*, ordena que *"Todo responsable y encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto"*.

Que el artículo 26 del Decreto 1377 de 2013, *"Demostración"*, ordena que *"Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y este Decreto."*

Que el artículo 27 del Decreto 1377 de 2013, *"Políticas internas efectivas"* ordena que *"En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1.2.3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser*

consistentes con las impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar (1) la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la ley 1581/12 y este decreto. (2) La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación. (3) La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto de Tratamiento".

Que el uso adecuado y seguro de la información en la Institución, como de los datos personales recolectados y tratados por UNIMINUTO, demuestra la integridad, confidencialidad y disponibilidad de la información, generando un impacto positivo en el cumplimiento normativo, así como en la operación normal de la Institución.

Que la Corporación Universitaria Minuto de Dios – UNIMINUTO, entendiendo el compromiso de preservar la seguridad de la información, la recolección y tratamientos adecuado de los datos personales en el desarrollo de las actividades que apoyan la gestión académico - administrativa de la Institución, considera la importancia de reglamentar las principales directrices en relación con aspectos generales de la gestión y administración de los datos personales, mediante la implementación y adopción de un ***Programa Integral de Gestión de Datos Personales***, buscando establecer su apropiación, cumplimiento y concientización en concordancia con la misión y visión de UNIMINUTO, y el cumplimiento de las disposiciones legales para la protección de datos personales.

Que el presente Programa Integral de Gestión de Datos Personales fue presentado en el Comité de Tecnología de la Institución para su respectivo aval, quien consideró pertinente avanzar en su formalización e implementación, atendiendo la importancia y necesidad del mismo al interior de UNIMINUTO.

Que, en virtud de lo anterior, el Rector General de la Corporación Universitaria Minuto de Dios - UNIMINUTO,

RESUELVE

ARTÍCULO PRIMERO: Aprobar el Programa Integral de Gestión de Datos Personales – PIGD de la Corporación Universitaria Minuto de Dios – UNIMINUTO, el cual consta del siguiente contenido:

1. Introducción.

El presente Programa Integral de Gestión de Datos Personales - PIGD está orientado por los principios y la misión de UNIMINUTO. Tiene como objetivo definir los criterios, principios, procedimientos, controles y estructuras, con el fin de llevar a la práctica lineamientos y controles que deben ser adoptados e implementados para garantizar que los riesgos del tratamiento de los datos personales recolectados por UNIMINUTO, sean conocidos, tratados, gestionados y asumidos de una forma leal, lícita, adecuada, documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se

produzcan en los procesos, procedimientos, el entorno y las tecnologías de información de UNIMINUTO.

Se trata de un programa institucional estratégico y preventivo que permita adelantarse a cualquier situación, evento o incidente que atente contra la integridad, confidencialidad y disponibilidad de los datos personales, recolectados y tratados en sus diferentes Sedes, unidades de las Vicerrectorías Generales y Rectoría General, y en general, en el Sistema UNIMINUTO. Asimismo, desarrollar e implementar medidas para garantizar el cumplimiento del principio de responsabilidad demostrada, que le asiste a UNIMINUTO, en su calidad de responsable de la recolección y tratamiento de datos personales en el desarrollo de su función social.

Para UNIMINUTO, el desarrollo e implementación del presente Programa Integral de Gestión de Datos Personales, se define como un proceso que le permite a la comunidad educativa percibir un estado de confianza para el desarrollo de las actividades y cumplimiento normativo, dentro de las áreas y su entorno, mediante la materialización de las estrategias definidas en planes de acción y la adopción de una serie de lineamientos, procedimientos, controles y disposiciones para reconocer la existencia de riesgos asociados al tratamiento de datos personales, identificarlos, establecer el plan de tratamiento y determinar el nivel de aceptación que está dispuesto asumir UNIMINUTO.

2. Alcance

El presente Programa Integral de Gestión de Datos Personales – PIGD, aplica a nivel Sistema UNIMINUTO, y tiene los siguientes alcances:

a) Abarca toda la comunidad educativa que participa en el desarrollo de las diferentes funciones sustantivas de la Institución, tales como estudiantes, profesores, colaboradores, y egresados, de la Institución.
b) Involucra a contratistas, proveedores, consultores y demás colaboradores, que laboran en las instalaciones de UNIMINUTO y que utilicen tecnologías de información y de comunicaciones de la Institución, ya sean propias o arrendados.
c) Cobija todos los procedimientos, estrategias, programas, y acciones que involucre el tratamiento de datos personales de cualquier miembro de la comunidad educativa, de tal manera que en todo momento se lleve a la práctica la Política de Tratamiento de la Información definida por UNIMINUTO.
d) Incluye de manera especial, todo lo referente a los datos personales de los menores de edad, niños y adolescentes que por su labor misional trata UNIMINUTO, de tal manera que la Institución cumpla con todas las normas vigentes relacionadas con la protección de los datos sobre este sector de la población que es sujeto de especial protección.
e) Comprende el tratamiento de los datos sensibles de la comunidad educativa, los que solo se recolectarán y tratarán por razones del cumplimiento de la labor misional de UNIMINUTO y cumpliendo las directrices de la normatividad legal vigente.

3. Objetivos

Para UNIMINUTO es importante implementar una estrategia y procedimientos para salvaguardar el derecho a la intimidad y el buen nombre de los estudiantes, profesores, colaboradores, egresados y en general, de cualquier persona que entre en contacto con la Institución, a fin de dar cumplimiento a la normatividad sobre el tratamiento de los datos personales.

Se establecen los siguientes objetivos que permiten contribuir a cumplir y desarrollar el Programa Integral de Gestión de Datos Personales –PIGD de UNIMINUTO:

a) Adoptar y gestionar un Manual Interno de Protección de Datos Personales para generar un ambiente de correcto y cabal entendimiento de la normatividad de protección de datos personales por parte de las Sedes y Unidades de las Vicerrectorías Generales y Rectoría General, con el objetivo de atender los lineamientos y mejores prácticas, para que al momento de la recolección, creación, mantenimiento, transmisión, trasferencia y supresión de datos personales, cumplan la normatividad aplicable, al alcance de todos los colaboradores que hagan parte de UNIMINUTO y que actúen como responsables o encargados de la información administrada en las bases de datos.
a) Unificar criterios respecto del tratamiento de datos personales por parte de UNIMINUTO que servirá para elevar los estándares de transparencia institucional y respeto de los derechos de los titulares de los datos personales.
b) Orientar y dar lineamientos requeridos para el tratamiento de datos personales sobre los niños y adolescentes que hacen parte de la comunidad educativa, en virtud de la labor institucional de UNIMINUTO, acorde a las normas y procedimientos para proteger los derechos de esta población sujeta de especial protección.
c) Crear las condiciones de infraestructura tecnológica y procedimientos requeridos para llevar a la práctica la Política de Tratamiento de Información de UNIMINUTO, de tal manera que lo definido y consignado en ella se ejecute de manera cotidiana y efectiva.
d) Garantizar la protección del derecho de la intimidad y al buen nombre de todos los integrantes de la comunidad educativa y de quienes entren en contacto con ella, debido a su labor misional, a través de la protección y el tratamiento de sus datos personales y bajo lineamientos y disposiciones de la normatividad legal vigente.
e) Definir procedimientos, controles y estrategias necesarias para dar cumplimiento al principio de responsabilidad demostrada en el marco de la normatividad vigente sobre la protección de datos personales.
f) Gestionar los riesgos a los que están expuestos los datos personales, que permita identificarlos, evaluarlos, valorarlos y tratarlos de manera que se minimice su impacto en la operación de los procesos de la Institución.
g) Realizar seguimiento y control a los procesos y procedimientos del sistema UNIMINUTO, para identificar brechas de seguridad en el tratamiento de los datos personales, proponer opciones de mejora y apoyar el cumplimiento de la normatividad.
h) Definir y generar una cultura de adopción de la política de protección de datos personales.

4. Roles y responsabilidades para el tratamiento de los datos personales

Cada colaborador que tenga a su cargo un grupo o equipo de trabajo humano será el responsable, en UNIMINUTO, de velar por el estricto cumplimiento de las disposiciones legales e internas sobre el tratamiento de datos personales a los que tenga acceso. Por lo tanto, deberá obrar de manera profesional, ética y diligente, así como realizar todos los esfuerzos y gestiones necesarios para lograr dicho cometido. Al interior de cada Sede, y unidad de las Vicerrectorías Generales o de la Rectoría General , en todos los procesos que involucren la recolección y el tratamiento de datos personales, se deberán adoptar los lineamientos, controles y procedimientos para la aplicación y cumplimiento del presente programa, dada su condición de Responsables de la información de datos personales, que está contenida en los sistemas de información, sistemas de almacenamiento y respaldo, equipos de cómputos y documentación física de UNIMINUTO.

Cuando algún colaborador o área requiera claridad respecto del tratamiento legal de los datos personales en la Institución, consultará a la respectiva Secretaría de Sede a la que pertenece, o a quien realice la labor jurídica en la Sede; y para el caso del Sistema acudirán a la Dirección Jurídica, para solicitar el correspondiente concepto jurídico sobre el asunto en cuestión. En todo caso, se deberá coordinar la solicitud y respuesta a través del área de atención al usuario, como único punto de contacto entre el titular del dato, el área responsable de la base de datos y el Oficial de seguridad y cumplimiento, quien ejerce el rol de cumplimiento en la Protección de Datos Personales para UNIMINUTO.

A continuación, se relacionan las unidades responsables del adecuado tratamiento de Datos Personales a nivel Sistema en la Corporación Universitaria Minuto de Dios – UNIMINUTO:

4.1. Vicerrectoría General de Servicios Integrados

La Vicerrectoría General de Servicios Integrados, en coordinación con la Dirección Jurídica y la Dirección de Tecnología y Sistemas de Información, definirá, revisará y actualizará los procedimientos y documentación que, por su labor sustantiva, requieran la recolección y tratamiento de datos personales, para al desarrollo del presente programa y dar cumplimiento a la normatividad en protección de Datos Personales.

4.2. Vicerrectoría General Académica

La Vicerrectoría General Académica, en coordinación con la Dirección Jurídica y Dirección de Tecnología y Sistemas de Información, definirá, revisará y actualizará los procedimientos y documentación que, por su labor sustantiva de la gestión académica, requieran la recolección y tratamiento de datos personales, para al desarrollo del presente programa y dar cumplimiento a la normatividad de ley en protección de Datos Personales.

4.3. Dirección de Tecnología y Sistemas de Información

La Dirección de Tecnología y Sistemas de Información definirá e implementará los controles técnicos y herramientas informáticas, que permitan gestionar los accesos de los usuarios a las bases de datos de la Institución, a fin de que se preserve la confidencialidad, disponibilidad e integridad de la información contenida en ellas.

4.4. Dirección del Talento Humano

La Dirección del Talento Humano, en coordinación con la Dirección Jurídica y Dirección de Tecnología y Sistemas de Información, definirá, revisará y actualizará los procedimientos y documentación que requieran la recolección y tratamiento de datos personales, para al desarrollo del presente programa y dar cumplimiento a la normatividad en protección de datos personales. Asimismo, por su labor sustantiva de la gestión del Talento Humano deberá incluir en sus programas de inducción a los colaboradores, que ingresan y conforman la comunidad educativa de UNIMINUTO, un capítulo especial relacionado con la seguridad de la información y protección de datos personales, la cual deberá ser requisito de formación y la constancia debe anexarse a la hoja de vida del colaborador, la capacitación será definida en coordinación con la Dirección de Tecnología y Sistemas de Información y la Dirección Jurídica.

4.5. Oficial de Seguridad y Cumplimiento

Mediante la Resolución Rectoral No. 1468 de 2018, se asignaron funciones de cumplimiento de seguridad de la información y protección de datos personales, entre las cuales deberá cumplir las siguientes directrices para el desarrollo y cumplimiento del presente programa:

a) Coordinar con los Rectores, Vicerrectores Generales, y directores de unidades del Sistema, el establecimiento y cumplimiento de los controles en protección de datos personales que se definan en el presente programa.
a) Promover la cultura de apropiación y concientización del cumplimiento a la normatividad para el tratamiento de los datos personales en la Institución.

b) Realizar y actualizar el inventario de las Bases de Datos Personales y clasificarlas según áreas funcionales, tipo y/o finalidad.
c) Gestionar los riesgos asociados al tratamiento de datos personales existentes en la institución.
d) Gestionar el registro de las Bases de Datos Personales de la Institución ante la Superintendencia de Industria y Comercio - SIC, así mismo dar cumplimiento a la normativa y requerimientos que exige la SIC durante el registro y una vez registradas.
e) En coordinación con la Dirección Jurídica, revisar, analizar y evaluar, los procedimientos y documentación que hacen referencia al tratamiento de los datos personales, con el fin de determinar el cumplimiento a la normatividad de ley y presentar las recomendaciones y acciones de mejora.

4.6. Coordinación de Gestión de Experiencia al Cliente

La Coordinación de Gestión de Experiencia al Cliente es la encargada dentro del procedimiento como único canal en UNIMINUTO, para atender y gestionar las solicitudes de consultas y reclamos, generadas a partir del tratamiento de datos personales, a través de los diferentes canales de comunicación, así mismo unificar y responder las solicitudes o reclamos realizados por los titulares de los datos personales.

4.7. Colaboradores

Los colaboradores que, por su función sustantiva dentro de la Institución, participen en alguno de los diferentes ciclos del tratamiento de datos personales, deberán cumplir las siguientes directrices para el desarrollo y cumplimiento del presente programa:

a) Recolectar datos personales únicamente a través de las herramientas definidas por la Dirección de Tecnología y Sistemas de Información y formularios definidos en el Sistema de Gestión de Calidad.
b) Cumplir con todos los procedimientos, principios y criterios definidos en la Política de Seguridad de la Información y la Política de Tratamiento de Información de UNIMINUTO, las cuales se encuentran publicadas en la página web de UNIMINUTO en la sección de Documentos Institucionales.
c) No divulgar, ni compartir en ninguna circunstancia, los datos personales a los que tenga acceso y/o recolecte, a menos que sea bajo alguno de los procedimientos establecidos en la Política de Tratamiento de la Información de la Institución o por orden de autoridad judicial o administrativa.
d) Emplear los datos personales exclusivamente para los propósitos y finalidades para los cuales fueron recolectados y debidamente informados a los titulares de dichos datos.
e) Cumplir las medidas técnicas y administrativas que establezca UNIMINUTO, para garantizar la seguridad de los datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

f) Asumir todas las consecuencias frente del tratamiento inadecuado de los datos personales que recolecta y que da tratamiento, cuando alguno de los titulares denuncie una conducta impropia en el manejo de datos personales, que sea consecuencia de sus actuaciones negligentes y que conduzca a cualquier tipo de sanción.
g) Asumir las consecuencias a las que haya lugar y las establecidas en el Reglamento Interno de Trabajo y el contrato laboral, para faltas graves a las funciones contratadas, cuando se presente una conducta inapropiada en el manejo y tratamiento de los datos recolectados que estén bajo su custodia y responsabilidad.

5. Controles del Programa

5.1. Lineamientos de Políticas

5.1.1. Política de Seguridad de la Información

La Corporación Universitaria Minuto de Dios – UNIMINUTO, entendiendo el compromiso de preservar la seguridad de la información en el desarrollo de las actividades que apoyan la gestión académico - administrativa de la Institución, considera la importancia de reglamentar las principales políticas y directrices en relación con aspectos generales de la gestión y administración de la seguridad de la información y mediante la implementación de un Sistema de Gestión de Seguridad de la Información, buscando establecer su apropiación, y cumplimiento, en concordancia con la misión y visión de UNIMINUTO, en virtud de lo anterior, adoptó la Política de Seguridad de la Información mediante la expedición del Acuerdo No. 001 del 06 de Abril de 2018 proferido por el Consejo General de Tecnología, la cual es de obligatoria aplicación en todas las actividades y procedimientos que involucre el tratamiento de la información y datos personales.

5.1.2. Política de Tratamiento de Información

UNIMINUTO está comprometida con el respeto del derecho fundamental al Habeas Data en cabeza de todos sus estudiantes, profesores, colaboradores, egresados y cualquier persona en general que tenga un vínculo con UNIMINUTO. En virtud de lo anterior, adoptó la Política de Tratamiento de Información, mediante la expedición de la Resolución Rectoral No. 1484 del 7 de septiembre de 2018, la cual es de estricto cumplimiento por parte de todos los miembros de su comunidad educativa, y contratistas y terceros que obren en nombre de UNIMINUTO, en todas las actividades y procedimientos que involucre el tratamiento de datos personales.

5.2. Procedimientos

La implementación y/o actualización de los siguientes procedimientos y documentación, entre otros, harán parte del desarrollo e implementación del presente programa:

a) Procedimientos Operacionales

Se deben desarrollar, implementar y mejorar los procedimientos académicos – administrativos, para que los titulares de los datos puedan ejercer sus derechos a conocer, actualizar, rectificar y suprimir información o revocar la autorización, de manera tal que se encuentren acordes tanto con las políticas generales de protección de datos personales, así como con la normatividad colombiana. De esta manera, se podrán gestionar adecuadamente los riesgos inherentes al tratamiento de información personal dentro de las actividades de operación de UNIMINUTO.

b) **Inventario y Registro de Bases de Datos Personales:**

La Ley 1581 de 2012 o Régimen General de Protección de Datos Personales, es la norma aplicable al tratamiento de la información personal contenida en cualquier base de datos de la Institución. Esta norma, igualmente, designó a la Superintendencia de Industria y Comercio- SIC como Autoridad de Protección de Datos para garantizar que, en su tratamiento, se respeten los principios, derechos, garantías y procedimientos dispuestos en la ley y le atribuyó la administración del Registro Nacional de Bases de Datos – RNBD, disposición a la cual debe dar cumplimiento la Institución ante la SIC.

c) Autorización del titular para el tratamiento de sus datos personales

En toda actividad que, por su función sustantiva o transversal, se requiera recolectar datos personales, deberá garantizarse que se solicite y obtenga la autorización previa, expresa e informada por parte del titular de los datos personales. Este procedimiento debe estar integrado en todas las actividades de UNIMINUTO, que realizan esta labor y debe dar cumplimiento a la normatividad definida en la ley 1581 de 2012, el decreto 1377 de 2013 y las demás disposiciones que profiera la Superintendencia de Industria y Comercio - SIC.

d) **Gestión de Incidentes de la Seguridad de la Información.**

Para la Corporación Universitaria Minuto de Dios – UNIMINUTO, un incidente de seguridad de la información se define como un único o una serie de eventos de seguridad de la información en tratamiento de datos personales indeseados o inesperados, que tienen una probabilidad significativa de comprometer la

operación y de amenazar la protección de los datos personales de los cuales es responsable UNIMINUTO. Asimismo, aquellos eventos que puede involucrar un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas de información o recursos informáticos; o una violación a la Política de Seguridad de la Información. En razón a lo anterior, la Dirección de Tecnología y Sistemas de Información garantizará que se defina y se establezca el procedimiento para el reporte, evaluación y tratamiento adecuado de los incidentes de seguridad.

e) <u>Gestión de Consultas y Reclamos de los titulares</u>

El Oficial de Seguridad y Cumplimiento, en coordinación con la Dirección Jurídica, deben diseñar, implementar y actualizar los procedimientos formales que den cumplimiento a la atención de las consultas y reclamos que eleven los titulares de los datos personales, para que los titulares de los datos puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información o revocar la autorización.

El objetivo de las consultas es informar o suministrar al titular del dato o a los sujetos legitimados sobre la información que UNIMINUTO tiene sobre dicha persona. UNIMINUTO está obligado a proporcionar toda la información contenida en sus bases de datos o archivos sobre el solicitante, en los términos señalados en la Ley. Los reclamos tienen por objeto corregir, actualizar, o suprimir datos o elevar una queja por el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012.

Teniendo en cuenta que se trata de garantizar el derecho fundamental habeas data, estos procedimientos deben ser revisados en coordinación con la Dirección Jurídica y el Oficial de Seguridad y Cumplimiento, con acompañamiento de la Dirección de Planeación y Calidad, con el fin de garantizar que estén acordes con la normatividad y la misión institucional de UNIMINUTO.

f) <u>Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales.</u>

UNIMINUTO debe incorporar en sus procedimientos las medidas necesarias y controles para asegurar la protección de datos personales, cuyo tratamiento sea realizado por encargados de tratamientos internacionales de datos personales. Se deben contemplar los siguientes aspectos entre otros:

1. Disposiciones que incluyan requisitos para que los encargados cumplan con las normas colombianas de protección de datos personales.
2. Formación y educación en temas de protección de datos personales para los empleados del responsable que tienen acceso a la información personal.
3. Cláusula de adherencia a las políticas de tratamiento de la información si utilizan subcontratistas.
4. Realización de auditorías internas y/o externas.
5. Acuerdos con los encargados y sus empleados aceptando el cumplimiento de las políticas y protocolos para el tratamiento de la información de UNIMINUTO.
6. Cuando UNIMINUTO desee enviar o transmitir datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, deberá establecer mediante cláusulas contractuales o a través de un contrato de transmisión de datos personales, entre otros, lo siguiente:

    a) Los alcances del tratamiento;
    b) Las actividades que el Encargado realizará en nombre de UNIMINUTO.
    c) Las obligaciones que debe cumplir el Encargado respecto del Titular del dato y UNIMINUTO.
    d) La obligación del Encargado de dar cumplimiento a las obligaciones del Responsable observando la política de tratamiento de datos.
    e) El deber del Encargado de tratar los datos de acuerdo con la finalidad autorizada para el mismo y observando los principios establecidos en la ley colombiana y la política de tratamiento de datos.
    f) La obligación del Encargado de proteger adecuadamente los datos personales y las bases de datos, así como de guardar confidencialidad respecto del tratamiento de los datos transmitidos.

5.3. Gestión de riesgos asociados al tratamiento de los datos personales

La Dirección de Planeación y Calidad, en coordinación con la Direccion de Tecnología y Sistemas de Información, debe gestionar los riesgos a los que están expuestos los datos personales, acorde con la estructura organizacional, los procesos y procedimientos internos asociados al tratamiento de la información, que permita identificarlos, medirlos, controlarlos, monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo, en desarrollo del cumplimiento en las normas de protección de datos personales.

5.4. Formación y educación

La ley colombiana exige a UNIMINUTO lo siguiente: (i) Adoptar medidas apropiadas para cumplir sus obligaciones legales sobre tratamiento de datos personales, y (ii) Estar en capacidad de evidenciar el correcto cumplimiento de sus deberes. Para el efecto, deben contar con herramientas idóneas que les permitan probar lo anterior ante las autoridades y los titulares de los datos.

La responsabilidad demostrada requiere que los directivos y demás colaboradores que hacen parte de UNIMINUTO generen una cultura de debido tratamiento de datos personales, lo cual implica no sólo conocer la regulación y políticas sobre el tema, sino implementar esas normas en todas las gestiones que sean pertinentes.

De allí, que se deba impartir una formación de carácter general sobre las medidas y la importancia de dar cumplimiento a la normatividad en protección de datos personales para todos los colaboradores que traten directamente datos personales; asimismo, deberá completarse una capacitación complementaria, adaptada específicamente a sus funciones. Esta formación debe ser permanente, como actualización y reforzamiento de la responsabilidad que le asisten al tratar los datos personales.

En coordinación con la Dirección Jurídica y el Oficial de Seguridad y Cumplimiento, los colaboradores que deleguen las Sedes y Unidades de las Vicerrectorías Generales y de la Rectoría General, como líderes de la protección de datos personales para sus respectivas áreas, deben reforzar con una capacitación más especializada, con el fin de facilitar el monitoreo y mejora continua de los procesos y procedimientos.

5.5. Comunicación externa

UNIMINUTO propenderá por informar a los titulares de los datos personales sus derechos, de acuerdo con lo establecido en el artículo 11 de la Ley 1581 de 2012, así como los programas de control que se han implementado. Las comunicaciones dirigidas a los titulares serán claras y comprensibles y no limitarse a una simple reiteración de la ley.

Así mismo, todas las normas que se profieran al interior de la Institución, tendientes a garantizar el cumplimiento de la normatividad en Habeas Data, serán publicadas en la página de Documentos Institucionales de UNIMINUTO. Los procedimientos para la atención de consultas y reclamos relacionados con habeas data, se encuentran publicados en la Política de Tratamiento de Información, el Manual Interno de Protección de Datos Personales, Programa de Gestión de Datos (PGD) y Responsabilidad Demostrada de UNIMINUTO, y en el Sistema de Gestión de Calidad dispuesto por la Institución.

5.6. Cronograma de desarrollo del Programa Integral de Gestión de Datos Personales – PIGD

Con el fin de llevar una gestión controlada del Programa Integral de Gestión de Datos Personales – PIGD se incorpora el siguiente cronograma de actividades anual, el cual debe ser evaluado y mejorado por el Oficial de seguridad y cumplimiento, en coordinación con la Dirección Juridica, de acuerdo con la normatividad colombiana y la dinámica de UNIMINUTO que incorpore el tratamiento de datos personales.

#	Actividad	Responsables	Periodicidad	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov
1	Inducción seguridad de la información y protección de datos personales	* Dirección de Talento Humano * Oficial de seguridad y cumplimiento * Áreas responsables de las Bases de Datos Personales * Sedes	Permanente	X	X	X	X	X	X	X	X	X	X	X
2	Revisión y actualización curso capacitación colaboradores	* Oficial de seguridad y cumplimiento * Dirección Juridica * Áreas Responsables colaboradores * Dirección de Talento Humano	Anual							X				
3	Identificación y actualización de BDP	* Oficial de seguridad y cumplimiento *Áreas Responsables de las Bases de Datos Personales * Sedes	Anual				X							
4	Gestión de Riesgos BDP	* Oficial de seguridad y cumplimiento * Áreas Responsables de las Bases de Datos Personales * Dirección de Planeación y Calidad	Semestral			X					X			
5	Registro y actualización BDP - SIC	* Oficial de seguridad y cumplimiento	Permanente	X	X	X	X	X	X	X	X	X	X	X
6	Evaluación de procedimientos	* Áreas Responsables * Oficial de seguridad y cumplimiento * Dirección Jurídica * Dirección de Planeación y Calidad * Sedes	Anual							X				
7	Planes de acción y tratamiento	* Áreas Responsables * Oficial de seguridad y cumplimiento * Dirección Jurídica * Sedes	Permanente	X	X	X	X	X	X	X	X	X	X	X
8	Cultura de Seguridad de la Información y protección de datos personales	* Oficial de seguridad y cumplimiento *Áreas Responsables de las Bases de Datos Personales * Sedes	Permanente	X	X	X	X	X	X	X	X	X	X	X
9	Auditoría externa	* Oficial de seguridad y cumplimiento * Dirección Jurídica * Dirección de Planeación y Calidad * Auditoría General	Anual				X							
10	Cumplimiento y control	* Auditoría General * Oficial de seguridad y cumplimiento * Dirección de Planeación y Calidad	Bimestral			X			X			X		

6. EVALUACIÓN Y REVISIÓN CONTINUA

Para UNIMINUTO es importante la revisión continua y periódica del Programa Integral de Gestión de Datos Personales – PIGD; con el fin de garantizar su eficacia permanente, el cumplimiento y adherencia de los estándares de Responsabilidad Demostrada; de allí que el Oficial de Seguridad y Cumplimiento supervisará, evaluará y revisará el presente programa para asegurar que continúe siendo pertinente y eficaz, así mismo gestionará

los recursos necesarios para el desarrollo del mismo, contemplando los siguientes aspectos:

a) En coordinación con la Auditoría General, definir un plan de auditorías de cumplimiento y supervisión al Programa.
b) Realizar las auditorías para evaluar y revisar los controles del programa, asimismo el cumplimiento de la normatividad que regula la materia y lineamientos definidos por UNIMINUTO en cumplimiento de la protección de datos personales.

Para el control y seguimiento se incorporan las siguientes listas de verificación que se deben contemplar como mínimo en el desarrollo del seguimiento y cumplimiento del presente programa:

LISTA VERIFICACIÓN RESPONSABILIDAD DEMOSTRADA EN PROTECCIÓN DE DATOS PERSONALES	
1. Compromiso de la Institución	
1.1 Desde la alta Dirección	1. Designar a una persona o al área que asumirá la función de protección de datos dentro de la Institución.
	2. Aprobar y monitorear el Programa Integral de Gestión de Datos Personales.
	3. Informar de manera periódica al Rector General sobre su ejecución.
	4. Definir responsabilidades específicas para otras áreas de la Institución respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposiciones final de los datos personales que se tratan.
1.2 Oficial de Seguridad y Cumplimiento	5. Cumplir la función de ***Oficial de Seguridad y Cumplimiento.***
	6. Dar trámite a las solicitudes de los titulares de los datos personales, para el ejercicio de los derechos de protección de datos personales y la normatividad que la regula.
	7. Gestionar el Programa Integral de Gestión de datos personales.
	8. Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
	9. Gestionar la implementación efectiva de las políticas y procedimientos adoptados para cumplir las normas, así como la implementación de buenas prácticas y controles para la gestión de la información y datos personales definidos en la Institución.
	10. Gestionar los incidentes de seguridad y/o el monitoreo continuo de las acciones correctivas.
	11. Gestionar la implementación del programa de concientización en seguridad de la información y datos personales para el Sistema UNIMINUTO.
	12. Mantener actualizados los lineamientos, estándares, procedimientos y toda la documentación necesaria para el cumplimiento de la política de seguridad de la información y la Política de tratamiento de la Información.
	13. Registrar las bases de datos personales de la Institución en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio - SIC.

LISTA VERIFICACIÓN RESPONSABILIDAD DEMOSTRADA EN PROTECCIÓN DE DATOS PERSONALES	
	14. Acompañar y asistir a la Institución en la atención de visitas y los requerimientos que realice la SIC y obtener las declaraciones de conformidad de la SIC cuando sea requerido.
	15. Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las políticas de seguridad de la información y tratamiento de la información personal.
	16. Dar a conocer las políticas de Seguridad de la Información y el Manual de Seguridad de la Información a los diferentes usuarios de la Institución.
1.3 Presentación de informes	17. Definir de manera clara la estructura de generación de reportes. Esto implica saber qué tipo de reporte, para asignar responsabilidades claras en el evento de una queja o de una violación a los códigos de seguridad.
	18. Documentar el proceso de generación de reportes como parte del Programa.
	19. Generar reportes a las autoridades de Dirección y Gobierno de la Institución e informar en estos el estado del programa de protección de datos personales.
2. Controles del programa	
2.1 Procedimientos operacionales	20. Implementar Procedimientos administrativos acordes con la Política de Tratamiento de Información y la Política de Seguridad de la Información, de forma tal que se pueda manejar adecuadamente los riesgos inherentes al tratamiento de la información personal, dentro de las actividades de gestión operacional.
2.2 Inventario de las bases de datos con información personal	21. Conocer los datos que almacenan, cómo se utilizan y si realmente son necesarios, teniendo en cuenta la finalidad para la cual se recolectan.
	22. Identificar en qué parte del procedimiento o actividad se obtienen los datos, si deben solicitar la autorización del titular y, de ser así, si están conservando prueba de la misma para su posterior consulta.
	23. En caso de manejo de datos de niños, niñas y adolescentes, implementar medidas adecuadas para garantizar la protección reforzada de dicha información.
	24. Asegurarse de que se esté informando al titular o a quien corresponda (datos de menores) que no existe obligación de suministrar tales datos. La clasificación de la información recopilada por la Institución.
2.3 Políticas Institucionales	25. Los lineamientos deben implementar los principios que rigen el Tratamiento de Datos Personales, estar acordes con la normatividad interna de UNIMINUTO, y estar debidamente documentadas y publicadas.
	26. La recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal, incluyendo requisitos para obtener la autorización.
	27. Lineamientos a lo ordenado por la ley en el acceso y corrección de los datos personales.
	28. Lineamientos en la conservación y eliminación de la información personal.
	29. Lineamientos en el uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos.
	30. Inclusión en todos los medios contractuales de la Institución una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce a suficiencia la política institucional se acepta, y

LISTA VERIFICACIÓN RESPONSABILIDAD DEMOSTRADA EN PROTECCIÓN DE DATOS PERSONALES	
	se permite a la compañía utilizar dicha información de forma responsable.
	31. Gestionar las solicitudes y reclamos en datos personales.
	32. Si hay otras políticas de la Institución (en talento humano, contratos, transparencia) elementos que permitan cumplir con las normas de protección de datos personales.
2.4 Sistema de administración de riesgos asociados al tratamiento de datos personales	33. Definir un sistema de administración de riesgos asociados a las bases de datos personales, acorde con la estructura organizacional, los procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y tipos de datos personales tratados por la Institución. Este sistema debe permitir identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.
	34. Identificar los riesgos a que se ven expuestos los datos personales en desarrollo de su tratamiento.
	35. Documentar los procesos y procedimientos que se implementen dentro del ciclo de vida de los datos personales.
	36. Definir la metodología de identificación de riesgos asociados al tratamiento de la información personal.
	37. Identificar los riesgos e incidentes ocurridos, respecto de este tipo de información, en los casos que aplique.
	38. Determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de datos personales y su impacto en el caso de materializarse.
	39. Realizar acciones que se deben tomar para controlar y/o mitigar los riesgos a que se ven expuestos los datos personales, con el fin de disminuir la posibilidad y /o las consecuencias de su materialización de los mismos. Para analizar los controles es preciso establecer, al menos, si son suficientes, efectivos y oportunos, como también identificar el tipo de control, esto es, si son manuales, automáticos, discrecionales, obligatorios, preventivos, o correctivos.
	40. Realizar un seguimiento constante para velar por las medidas que se hayan establecido sean efectivas.
	41. Llevar una registro de incidentes que contemple: base de datos y datos comprometidos, titulares, fecha del incidente, y de descubrimiento, acciones correctivas realizadas y responsables.
	42. Evaluar los riesgos periódicamente e implementar estas evaluaciones en toda la organización dentro de cada nuevo proyecto que involucre datos personales.
2.5 Requisitos de formación y educación	43. Impartir una formación de carácter general y particular al personal que maneje datos personales, la formación debe ser permanente.
2.6 Protocolos de respuesta en el manejo de violaciones e incidentes	44. Rendir informes internos y reportar los incidentes a los titulares y a la Superintendencia de Industria y Comercio – SIC. Se debe implementar mecanismos que les permitan comunicarse de manera eficiente con los titulares afectados, sobre el incidente de seguridad relacionadas con sus datos personales y las posibles consecuencias, y proporcionar herramientas a dichos titulares afectados para minimizar el daño potencial o causado.

LISTA VERIFICACIÓN RESPONSABILIDAD DEMOSTRADA EN PROTECCIÓN DE DATOS PERSONALES	
	45. Se debe informar como mínimo, el tipo de incidente, la fecha en que ocurrió, y la fecha en la que se tuvo conocimiento del mismo, la causal, el tipo de datos personales comprometidos y la cantidad de titulares afectados.
2.7 Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales	46. Contar con disposiciones que incluyan requisitos para que los encargados cumplan con las normas colombianas de protección de datos y las políticas de tratamiento.
	47. Disponer de mecanismos para que el Encargado reporte al Responsable los incidentes de seguridad de la información.
	48. Garantizar una formación y educación en temas de protección de datos personales para los empleados del Encargado que tengan acceso a la información personal.
	49. Exigir la adherencia a las políticas de tratamiento si se utilizan subcontratistas.
	50. Realizar auditorías internas o externas.
	51. Celebrar acuerdos con los encargados y sus empleados donde se acepte el cumplimiento de las políticas y protocolos del responsable del tratamiento.
2.8 Comunicación externa	52. Informar a los titulares de datos personales, sus derechos, de acuerdo con lo establecido en el artículo 11 de la ley 1581 de 2012, la Política de Tratamiento de Información, así como los programas de control que se han implementado. Las comunicaciones dirigidas a los titulares deben ser claras y comprensibles, y no limitarse a una simple repetición de las normas que rigen la materia.
3. **Evaluación y revisión continua**	
3.1. Desarrollar un plan de supervisión y revisión	53. El Oficial de seguridad y Cumplimiento debe desarrollar un plan de supervisión y revisión anual. El plan debe establecer las medidas de desempeño e incluir un calendario de cuándo deben ser revisadas las políticas y los controles del programa, por lo menos una vez al año.
3.2 Evaluar y revisar los controles del programa	54. El monitoreo es un proceso continuo que debe abordar por lo menos las siguientes preguntas ¿Cuáles amenazas y riesgos al tratamiento de datos personales detectados en la Institución?, ¿los controles del programa están teniendo en cuenta las nuevas amenazas y reflejando las quejas más recientes, o los hallazgos de las auditorias, o las orientaciones de la autoridad de protección de datos?, ¿se están ofreciendo nuevos servicios que involucran una mayor recolección, uso o divulgación de la información personal?, ¿se está llevando a cabo una capacitación eficaz?, ¿se están cumpliendo las políticas y procedimientos establecidos?, y ¿el Programa Integral de Gestión de Datos Personales – PIGD se encuentra actualizado?

7. Divulgación, Socialización y Capacitación

La Dirección de Tecnología y Sistemas de Información, en coordinación con la Dirección Jurídica, definirá los procesos, procedimientos, controles y demás mecanismos necesarios, para la divulgación, socialización y capacitación del Programa Integral de Gestión de Datos Personales – PIGD.

ARTÍCULO SEGUNDO. La presente resolución rige a partir de la fecha de su expedición.

Dada en Bogotá D.C, el día 19 de noviembre de 2020.

Comuníquese y cúmplase.

El Rector General,

P. HAROLD CASTILLA DEVOZ, cjm.
Rector General

Proyectó: Ricardo Ramirez Rivera- Oficial de seguridad y cumplimiento
Aprobó: Saúl Reyes Aria- Director de Tecnología y Sistemas de Información
Revisó: Dirección Jurídica.