UNIVERSIDAD DE CUNDINAMARCA

MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN A LA PRIVACIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2026

UNIVERSIDAD DE CUNDINAMARCA

MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN A LA PRIVACIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

FUSAGASUGÁ
2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento establece los lineamientos fundamentales para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI y el Programa Integral de Gestión de Datos Personales en la Universidad de Cundinamarca. Estos lineamientos se basan en lo dispuesto en el anexo A de la norma ISO/IEC 27001:2022, que define los requisitos para un sistema de gestión de seguridad de la información, y en el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC. Asimismo, se alinea con la normativa nacional vigente, en particular con la Ley Estatutaria 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, que regulan la protección de datos personales en Colombia.

En este contexto, el documento tiene como propósito garantizar el adecuado tratamiento de la información que la Universidad recolecta, almacena, usa, circula, suprime, transmite, transfiere y genera en el desarrollo de sus funciones misionales. Está dirigido a funcionarios administrativos, gestores de conocimiento, estudiantes, proveedores y demás partes interesadas que tengan acceso a la información, con el fin de asegurar su protección y cumplir con las obligaciones legales y técnicas que corresponden a la institución.

De esta manera, se busca no solo fortalecer la seguridad de la información y la privacidad de los datos personales, sino también promover una cultura de responsabilidad y transparencia en el manejo de la información, en concordancia con los estándares internacionales y las normativas nacionales aplicables.

2. OBJETIVO GENERAL

Enunciar los lineamientos que conforman el Sistema de Gestión de Seguridad de la Información – SGSI, Ciberseguridad y el Programa Integral de Gestión de Datos Personales, en articulación con lo establecido en el Manual de Políticas de Seguridad de la información como documento de referencia del habilitador No. 3 Seguridad y Privacidad de la información de la Política de Gobierno Digital.

2.1 OBJETIVOS ESPECÍFICOS

- Describir los lineamientos que forman parte del Sistema de Gestión de Seguridad de la Información y el Programa Integral de Gestión de Datos Personales –PIGDP.

- Dar a conocer la ubicación de los lineamientos que se encuentran actualmente formalizados en el Sistema de Gestión de la Calidad – SGC de la Universidad de Cundinamarca.

- Definir controles y responsabilidades para el uso, almacenamiento, transmisión y divulgación de la información, con el fin de prevenir accesos no autorizados, fuga de datos e incidentes que afecten la confidencialidad, integridad y disponibilidad de los activos institucionales.

3. ALCANCE

El alcance del presente manual y sus lineamientos aplica para todos los funcionarios administrativos, gestores de conocimiento, estudiantes, proveedores y demás partes interesadas de la Universidad de Cundinamarca que tengan acceso a la información, con el fin de asegurar su protección y cumplir con las obligaciones legales y técnicas.

4. DEFINICIONES

Para una mejor interpretación del presente manual, de la Ley 1581 de 2012 y los decretos reglamentarios, se recomienda tener en cuenta las siguientes definiciones:

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.[1]

AVISO DE PRIVACIDAD: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.[2]

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de tratamiento.[3]

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[4]

DATO PÚBLICO: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.[5]

DATOS SENSIBLES: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como

[1] RESOLUCIÓN 091 del 8 de agosto de 2023 – POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE PROTECCION DE DATOS PERSONALES DE LA UNIVERSIDAD DE CUNDINAMARCA

[2] Ídem

[3] Ídem

[4] Ídem

[5] Ídem

que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.[6]

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.[7]

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.[8]

TITULAR: Persona natural cuyos datos personales sean objeto de Tratamiento.[9]

TRANSFERENCIA: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país. [10]

TRANSMISIÓN: tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable. [11]

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[12]

VIDEOCÁMARA: Aparato que sirve para hacer fotografías, y que consta de un medio óptico, el objetivo, y de un medio mecánico, el obturador.[13]

VIDEOVIGILANCIA: Vigilancia por medio de un sistema de cámaras, fijas o móviles.[14]

---

6 Ibídem
7 Ídem
8 Ídem
9 Ídem
10 Ídem
11 Ídem
12 Ídem
13 REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.ª ed., [versión 23.7 en línea]. <https://dle.rae.es> 2024.
14 Ibídem

LINEAMIENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI

5.1 LINEAMIENTO DE PROTECCIÓN DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA

La Universidad de Cundinamarca adopto el lineamiento de Protección de Datos Personales de los Titulares de la Universidad de Cundinamarca, mediante la Resolución No 091 del 8 de agosto de 2023, el cual contempla:

La Universidad de Cundinamarca en cumplimiento con lo dispuesto en la Ley estatutaria 1581 de 2012, el Decreto Reglamentario 1074 de 2015 y demás normatividad que tengan reacción y regulen la materia, adopta el presente lineamiento de protección de datos personales, el cual será comunicado a todos los titulares.[15]

Fijar, adoptar y comunicar una "Política Institucional de Tratamiento de los datos personales" de los titulares de la Universidad de Cundinamarca, en desarrollo de las actividades de carácter académico, laboral y comercial, garantizando la protección de derechos como la privacidad, intimidad, el buen nombre y la imagen de nuestros interesados. En tal sentido, la recolección de datos se limitará a aquellos datos personales que son pertinentes y adecuados para la finalidad para lo cual son recolectados o requeridos.

5.1.1 FINALIDADES DEL TRATAMIENTO DE DATOS

La Universidad de Cundinamarca documenta en la guía **ESG-SSI-G007**, la finalidad por la cual recolecta almacena, usa y circula los datos personales de los titulares en el contexto de sus actividades académico-administrativas o cuando hay relación comercial con un tercero. Las finalidades serán recopiladas y agrupadas conforme al modelo de operación digital, es decir por Macroproceso y procesos a nivel institucional.

5.2 LINEAMIENTO DE TRATAMIENTO DE DATOS SENSIBLES

Se entiende como datos sensibles como aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[16]

[15] RESOLUCIÓN 091 del 8 de agosto de 2023 – POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD DE CUNDINAMARCA

[16] Decreto 1377 de 2013

La Universidad de Cundinamarca en el cumplimiento de lo dispuesto en la Ley 1581 de 2012 y acorde a su misión, recolecta datos personales de estudiantes, funcionarios administrativos y docentes, y personal externo a la Institución, entre la información recolectada, están los datos sensibles tales como el origen étnico racial, pertenencia a sindicatos, afiliaciones religiosas, entre otros. La recolección parte de la autorización y/o o aviso de privacidad, otorgada por el titular, siempre informando la finalidad para cual se recolectan los datos, el lugar y tiempo de almacenamiento, así como la disposición final, de acuerdo con el lineamiento de Protección de Datos Personales de los Titulares de la Universidad de Cundinamarca

5.3 LINEAMIENTO DE GESTIÓN DE ENCARGADOS DEL TRATAMIENTO.

El Responsable del Tratamiento (en adelante “El Responsable”) compartirá al Encargado del Tratamiento (en adelante “El Encargado”) determinada(s) base(s) de datos para llevar a cabo la ejecución de diversos programas y proyectos, todo enmarcado en un contrato principal debidamente suscrito por LAS PARTES. Lo anterior se traduce en que, el Encargado deberá entrar en contacto con los datos personales contenidos en las referidas bases de datos del Responsable, por lo que, a través de la presente política se establecen las obligaciones de protección de datos de las partes contratantes.

La presente política se adecua a cada uno de los preceptos normativos del Artículo 2.2.2.25.5.2 del Decreto 1074 de 2015. El encargado del tratamiento debe prestar la atención profesional necesaria para garantizar que todas las personas a las que se les confía el tratamiento o la ejecución de los contratos cumplen las disposiciones legales en materia de protección de datos.

5.3.1 Artículo primero. calidad de las partes. A efectos de la presente política y en armonía con el contrato principal suscrito, EL CONTRATANTE se denominará Responsable del tratamiento según la Ley 1581 de 2012 y demás normas que la modifiquen o adicionen. A efectos de la presente política y en armonía con el contrato principal suscrito, EL CONTRATISTA se denominará Encargado del tratamiento según la Ley 1581 de 2012 y demás normas que la modifiquen o adicionen.

5.3.2 Artículo segundo. Legislación aplicable. La adecuada prestación de los servicios citados en el contrato principal está condicionada al cumplimiento de la Ley General de Protección de Datos Personales – LGPD (Ley 1581 de 2012) y el resto de legislación complementaria en materia de protección y tratamiento de datos de carácter personal.

5.3.3 Artículo tercero. Objeto de la presente política. Constituye de la presente política determinar las condiciones de seguridad y confidencialidad en las cuales el

Encargado llevará a cabo el acceso y tratamiento de los datos de carácter personal bajo tutela del responsable.

5.3.4 Artículo cuarto. Condiciones del tratamiento. El Encargado únicamente tratará los datos conforme a los fines del desarrollo contractual y no los aplicará o utilizará con fin distinto al que figura en el contrato principal, ni los comunicará, ni siquiera para su conservación, a otras personas. No obstante, el Encargado no incurrirá en responsabilidad cuando, previa indicación expresa del Responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio. Cualquier otra finalidad de uso de los datos será incompatible con la presente política.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Responsable, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

5.3.5 Artículo quinto. Derechos de los titulares. Para garantizar a los titulares, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data, el Encargado gestionará las solicitudes relacionadas con los derechos de acceso, rectificación, cancelación y oposición, conforme a los términos y condiciones establecidos para la atención de consultas y reclamos en la normativa vigente sobre protección de datos personales.

5.3.6 Artículo Sexto. Seguridad. El Encargado conservará los datos personales que reciba del Responsable o que recaude en el desarrollo de sus obligaciones derivadas del contrato principal, en condiciones de seguridad de tal suerte que se evite su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Así mismo, informará en menos de dos (2) días hábiles al Responsable cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

5.3.7 Artículo Séptimo. Confidencialidad. El Encargado acepta, que la información confidencial que reciba o conozca con relación a la ejecución del acuerdo o contrato de prestación de servicios, tiene como única y exclusiva finalidad el permitir el cabal y correcto desempeño, de sus obligaciones, por lo tanto, se obliga a no difundir, comentar, copiar, entregar o comunicar a terceros o hacer un uso diferente de esta, por lo que la misma deberá ser manejada con absoluto cuidado y confidencialidad.

El deber de confidencialidad comprende la obligación de adoptar medidas de seguridad de carácter técnico, operativo, tecnológico y físico, así como comunicar cualquier sustracción, alteración o pérdida de la información confidencial. El Encargado solo podrá revelar la información confidencial cuando previamente se haya autorizado por escrito su divulgación.

Las anteriores obligaciones se extienden a toda persona que pudiera intervenir en cualquier fase de la prestación del servicio por cuenta del Encargado y subsistirán

aun después de finalizada la prestación del servicio efectuada en el marco del presente contrato principal.

5.3.8 Artículo Octavo. Política de tratamiento de datos. El Encargado se obliga a cumplir la política de tratamiento de la información del Responsable, la cual está disponible en el sitio web del Responsable.

El Encargado se obliga a suministrar copia de su Política de Tratamiento de la Información Personal en un término no mayor a los diez (10) días hábiles a la suscripción del presente contrato para cualquier fin de registro e inscripción ante la Superintendencia de Industria y Comercio – SIC.

5.3.9 Artículo Noveno. De la información del Encargado. En el caso en que el encargado aporte documentos que contengan datos de carácter personal de sus trabajadores o de terceros en la ejecución del contrato, garantiza que dicha información procede del consentimiento de los interesados para llevar a cabo el tratamiento de datos a el responsable.

El Encargado únicamente comunicará a El Responsable datos de carácter personal adecuados, pertinentes y no excesivos en relación con las necesidades de la prestación del servicio objeto del presente contrato, garantizando que dichos datos sean exactos y puestos al día, y obligándose a comunicar a El Responsable en el plazo legalmente establecido al efecto, aquellos que hayan sido rectificados y/o deban ser cancelados según proceda.

5.4 LINEAMIENTO DE USO ADECUADO DE CORREO INSTITUCIONAL

La Universidad de Cundinamarca cuenta con el **ASIM005**, que tiene como propósito garantizar el adecuado manejo de los datos e información de titulares a los que se les ha asignado un correo institucional con fines académicos, laborales y/o comerciales. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso de Apoyo, Proceso Gestión Sistemas y Tecnología, procedimiento **ASIP20**.

5.5 LINEAMIENTO DE SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el desarrollo de todas las actividades académicas, administrativas y/o comerciales, los funcionarios administrativos, gestores del conocimiento y estudiantes de la Universidad de Cundinamarca, recibirán la sensibilización y, en caso de requerirse según las funciones contractuales, el respectivo entrenamiento en todos los temas relacionados con seguridad y privacidad de la información; es decir, los requerimientos necesarios para la implementación de la Ley de Protección de Datos Personales y el Sistema de Gestión de Seguridad de la Información. La Coordinadora de Seguridad de la Información con el apoyo del equipo táctico operativo, con el aval

de la Dirección de Planeación Institucional y cuando se requiera la Comisión de Gestión, serán los encargados de coordinar las acciones de Sensibilización y Entrenamiento, así como de evaluar la pertinencia de su actualización, según el nivel de avance en la implementación y las necesidades propias de la Institución, adicionalmente se compromete a proporcionar los recursos necesarios para desarrollar y mantener el presente plan, con el fin de proteger los activos de información contra cualquier amenaza o vulnerabilidad.

Los grupos de interés serán sensibilizados y entrenados durante la vigencia contractual, indicando las directrices y buenas prácticas en lo que respecta a seguridad y privacidad de la información. Por lo que es obligatorio para todos asistir y completar los escenarios de sensibilización, entrenamiento y cursos de capacitación programados por el SGSI y la Dirección de Talento Humano. La no participación sin justificación será considerada como incumplimiento de las políticas de seguridad de la información de la universidad. Esto según lo establecido en el **ESG-SSI-PL01**. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, macroproceso estratégico, proceso gestión de sistemas integrados, seguridad de la información.

5.6 LINEAMIENTO DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Universidad de Cundinamarca reconoce la información como un activo esencial para el cumplimiento de sus objetivos institucionales. En este sentido, afirma su compromiso con una gestión integral, eficiente y segura de la información, mediante la implementación de un lineamiento para la Gestión de Activos de Información. Este lineamiento adopta los principios de Confidencialidad, Integridad y Disponibilidad de la información, directrices y responsabilidades para la administración, protección y uso adecuado de los activos de la información.

Como parte de este compromiso, el Sistema de Gestión de Seguridad de la Información – SGSI, cuenta con el procedimiento **ESG-SSI-P01**, el cual define los lineamientos para la gestión de los activos. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, Seguridad de la información.

5.7 LINEAMIENTO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION.

La Universidad de Cundinamarca asume el compromiso de administrar los riesgos de seguridad de la información que puedan afectar de manera negativa el alcance de los objetivos estratégicos y objetivos de procesos de la institución; del mismo modo busca forjar una institución más proactiva que reactiva, previniendo y reduciendo los efectos no deseados promoviendo la mejora continua, propendiendo una organización basada en la acción preventiva automática enfocada en la administración del riesgo,

con control en todos los niveles de la institución, brindando seguridad razonable destinando los esfuerzos necesarios para administrar los riesgos que se puedan presentar en la Universidad de Cundinamarca.

Así mismo desde el Sistema de Gestión de Seguridad de la Información - SGSI actualmente se cuenta con el procedimiento **ESG-SSI-P12**, en el que se describen las actividades a seguir en relación con las fases descritas en la ilustración 1 del numeral 5, que inicia con el contexto organizacional y termina con la documentación del proceso de la gestión de riesgos, este proceso se realiza de manera periódica anualmente o cuando surgen cambios en el contexto de la institución (cambios en los procesos, activos de información o materialización de incidentes).

5.8 LINEAMIENTO DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

La Universidad de Cundinamarca cuenta con el documento **ESG-SSI-M006**, el cual tiene como propósito, establecer directrices claras y obligatorias para todos los funcionarios administrativos, docentes, contratistas y visitantes, en cuanto a buenas prácticas en el manejo de documentos impresos y el uso de dispositivos digitales en los espacios de trabajo, con el fin de asegurar que toda información crítica o no, sea adecuadamente resguardada, garantizando así que la manipulación y visualización de la información confidencial se maneje de manera segura y conforme a los requisitos legales y contractuales aplicables. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, del procedimiento **ESG-SSI-P08**.

5.9 LINEAMIENTO DE CONTROL DE ACCESO FISICO A AREAS SEGURAS

La Universidad de Cundinamarca cuenta con un documento denominado **ESG-SSI-M010**, el cual establece diversas directrices encaminadas a controlar el acceso físico a las áreas seguras de la Universidad de Cundinamarca, buscando reducir y/o minimizar los riesgos de accesos no autorizados a las áreas seguras de la institución, que pueden exponerla a pérdidas de información por confidencialidad, integridad o disponibilidad, daños a recursos técnicos y/o tecnológicos, fuga de información por un indebido tratamiento de datos personales de los titulares, entre otros. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, procedimiento **ESG-SSI-P08**.

5.10 LINEAMIENTO DE USO DE DISPOSITIVOS MÓVILES Y BYOD

La Universidad de Cundinamarca cuenta con el documento **ESG-SSI-M007**, mediante el cual se definen las condiciones generales para el uso adecuado de los activos de información, para este caso específicamente los tipificados como activo tipo "Hardware", al interior de las instalaciones de la institución, este tipo de activo en este documento de denominará "dispositivo móvil institucional". Así mismo en este lineamiento se reconoce el uso de los dispositivos móviles institucionales fuera de las instalaciones de la Universidad, este escenario se da siempre y cuando se cumpla el conducto regular definido y se proporcionen las condiciones óptimas de uso. Por lo tanto, los diferentes grupos de interés deben conocer y acatar los lineamientos descritos en este lineamiento, pero no limitado a estos, con el fin de garantizar la seguridad de la información cuando se administre, transmita o almacene información en dichos dispositivos. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, procedimiento **ESG-SSI-P08**.

5.11 LINEAMIENTO DE VIDEOVIGILANCIA

La Universidad de Cundinamarca comprende la importancia de establecer lineamientos claros en la instalación, mantenimiento y funcionamiento de cada uno de los circuitos de videovigilancia con los que cuenta la institución en sus diferentes ubicaciones geográficas, garantizando la seguridad y privacidad de la información de todas los titulares que utilizan las instalaciones universitarias, documentado mediante la guía de la Oficina de Recursos Físicos y Servicios Generales denominada **ABSG006**.

5.12 LINEAMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de Cundinamarca, entiende la importancia de gestionar los incidentes del Sistema de Gestión de Seguridad de la información - SGSI, por lo tanto, establece los lineamientos y acciones necesarias para la protección de la información a nivel institucional, articulado al ciclo de vida de Gestión de Incidentes del MinTIC definido en el Anexo 1 de la Resolución 500 de 2021, actualizado mediante la Resolución 02277 de 2025, partiendo de la preparación, el análisis, la evaluación, la contención, la erradicación y la recuperación del incidente que se presente en los distintos procesos que conforman el Modelo de Operación Digital de la Universidad de Cundinamarca, minimizando el impacto que estos puedan generar, como también evitar que conlleven a la materialización de los riesgos de los activos de la información de la institución.

Así mismo desde el Sistema de Gestión de Seguridad de la Información - SGSI actualmente se cuenta con el procedimiento **ESG-SSI-P09**, en el que se describen las actividades para garantizar la adecuada gestión de eventos y/o incidentes de

seguridad de la información en la Universidad de Cundinamarca. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, Seguridad de la información.

5.13 LINEAMIENTO DE GESTIÓN DE RESPALDO DE LA INFORMACIÓN

La Universidad de Cundinamarca, comprendiendo la importancia de garantizar la integridad y disponibilidad de la información a nivel institucional, establece el lineamiento para la gestión de copias de respaldo de la información a nivel institucional, por medio del documento **ASIM008**, en donde del mismo establece como se realizarán de manera periódica las copias de respaldo en los recursos y servicios informáticos, conforme a los parámetros definidos y utilizando las herramientas designadas por el área de Servicios Tecnológicos. Asimismo, se efectuarán pruebas regulares para verificar la integridad y correcto almacenamiento de los datos respaldados, garantizando la continuidad operativa y la protección de los activos de información ante posibles incidentes. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso de Apoyo, Sistemas y Tecnología, dentro del procedimiento **ASIP25**.

5.14 LINEAMIENTO DE RELACION CON LOS PROVEEDORES

La Universidad de Cundinamarca comprendiendo la importancia de garantizar la confidencialidad, integridad y disponibilidad de la información en la relación con los proveedore y/o terceros, estableció por medio del documento **ESG-SSI-M013**, en donde por medio del cual establece que los proveedores, contratistas deberán diligenciar los acuerdos de confidencialidad y definir de manera consensuada con la Universidad de Cundinamarca la implementación, mantenimiento y revisión a intervalos planificados de los controles de seguridad que permitan mitigar los riesgos derivados de la interacción entre las partes. Además, los proveedores; contratistas deberán cumplir en todos los aspectos del lineamiento de Seguridad de la Información y del tratamiento de datos personales vigente en la Institución. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, procedimiento **ESG-SSI-P08**.

5.15 LINEAMIENTO DE INTEGRIDAD

La Universidad de Cundinamarca reafirma su compromiso con la integridad mediante la implementación de controles y auditorías efectivas que aseguren la responsabilidad individual en el manejo de la información. Cada usuario es responsable de sus acciones en los sistemas de información, garantizando que la creación, modificación, recepción o envío de información en los intercambios electrónicos se realice de manera ética, transparente y conforme a las normativas establecidas. Estos controles asegurarán la autenticidad, veracidad y trazabilidad de los datos, promoviendo una cultura de integridad en toda la institución. Este documento se encuentra formalizado

en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, manual **ESG-SSI-M018**.

5.16 LINEAMIENTO NO REPUDIO

La Universidad de Cundinamarca se compromete a implementar mecanismos de control y auditoría para las actividades de los usuarios en los sistemas de información. Esto asegura que ningún usuario pueda negar su responsabilidad sobre la creación, modificación, recepción o envío de información en el intercambio electrónico. La seguridad será una parte integral del ciclo de vida de los sistemas de información nuevos o existentes. Este documento se encuentra formalizado en el Sistema de Gestión de la Calidad, Macroproceso Estratégico, Proceso Gestión Sistemas integrados, manual **ESG-SSI-M019**.

5. CICLO DE VIDA DEL DATO

La Universidad de Cundinamarca, establece los siguientes numerales que corresponden a los procedimientos y a las diferentes fases, para enmarcar la gestión del ciclo de vida del dato, teniendo en cuenta que es proceso indispensable para alcanzar el máximo aprovechamiento de los datos recolectados, almacenados y dispuestos en la infraestructura técnica y tecnológica, con que cuenta la institución.

De esta forma, el ciclo de vida se divide en cuatro etapas:

6. RECOLECCIÓN Y ALMACENAMIENTO DE DATOS

Como proceso estratégico, el SGSI ha documentado el Procedimiento **ESG-SSI-P03**, en el que establece las actividades pertinentes para la obtención o captura de los datos mediante el uso de diferentes mecanismos tales como formularios impresos o digitales, diligenciamiento de encuestas, toma de muestras, grabación de audio y video, sensores, entre otros. y el respectivo almacenamiento en las bases de datos manuales o automatizadas.

7. USO Y CIRCULACIÓN DE LOS DATOS

Como proceso estratégico, el SGSI ha documentado el Procedimiento **ESG-SSI-P05**, el que establece las actividades pertinentes para, una vez almacenados los datos, realizar las diferentes actividades derivadas de cada uno de los planes, programas y procedimientos asociados a los Macroproceso Estratégico, Misional, de Apoyo y de Seguimiento, Medición, Análisis y Evaluación y que reúnen todas las operaciones misionales de la U Cundinamarca.

8. TRANSFERENCIA Y/O TRANSMISIÓN DE LOS DATOS A UN TERCERO PARA SU TRATAMIENTO.

Como proceso estratégico, el SGSI ha documentado el Procedimiento **ESG-SSI-P07**, el que establece las actividades pertinentes cuando el tratamiento sea realizado por una entidad o persona externa a la Institución a fin de dar cumplimiento a un requerimiento o necesidad específica de esta, dependiendo el caso se realiza una transmisión o transferencia de los datos, cuya restricción de uso está condicionada al objeto contractual y el acuerdo de confidencialidad firmado.

9. SUPRESIÓN DE LOS DATOS:

Como proceso estratégico, el SGSI ha documentado el Procedimiento **ESG-SSI-P06**, que establece las actividades pertinentes para la eliminación total o parcial de los datos almacenados en las bases de datos de la Institución, ya sea porque se cumplió la finalidad para la que fueron solicitados o por solicitud expresa del Titular.

APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Los lineamientos aquí definidos se harán efectivos a partir de su aprobación por la Alta Dirección y serán revisadas a intervalos planificados y por los menos una (1) vez al año, cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de La Universidad de Cundinamarca.

10. BIBLIOGRAFÍA Y WEBGRAFÍA

ALEGSA. Diccionario de informática y tecnología. [sitio web] Santa Fe, Argentina. [Consultado: 23 de agosto de 2022]. Disponible en: https://www.alegsa.com.ar/Dic/ups.php.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Santa Fe de Bogotá, D.C.: Diario Oficial 2012. Nro. 48587. [Consultado: agosto 25 de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

REAL ACADEMIA ESPAÑOLA. Diccionarios. [sitio web] Madrid, España. [Consultado: 23 de agosto de 2022]. Disponible en https://www.rae.es/.

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2021	02	23	Emisión del documento. Transición del ASIM004.
2	2021	03	09	Inclusión de Política de Datos Sensibles y Ciclo de Vida del Dato
3	2021	10	13	Inclusión de finalidad referente a la medición de clima y cultura organizacional
4	2021	12	06	Inclusión de finalidad de la Dirección de Planeación
5	2022	08	31	Inclusión de finalidad de la Oficina Servicio De Atención Al Ciudadano e interacción social universitaria, actualización de introducción y objetivo.
6	2023	02	20	En el numeral 5.1 FINALIDADES DEL TRATAMIENTO, se crea una guía denominada ESG-SSI-G007 GUÍA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA en donde se documentan las finalidades agrupadas por macroproceso y proceso.
7	2023	03	31	Inclusión de Política de gestión de Incidentes de Seguridad de la Información
8	2024	02	16	Se realizó la actualización del contenido y la redacción de la introducción, el objetivo general, el alcance, los numerales 5, 8, 15 y 16 del documento de lineamientos de seguridad y privacidad de la información, además de sustituir el término “política” por “lineamiento” la mayoría de su contenido.
9	2025	04	07	Se actualizo el contenido de la introducción, objetivo general, objetivos específicos, alcance, se agregó el numeral 5.13 y 5.14 y el 7. Además, se reestructuro el manual dejando todos los lineamientos en el numeral 5. Según la resolución rectoral 074 del 22 de julio del 2024, dando cumplimiento a la ley 2345 del 2023 "chao marcas" y dando alcance a la circular 006 "Cambio de identificador visual en los documentos de gestión documental" se realiza el cambio de logo en el documento.
10	2025	12	05	-Se incorporó un tercer objetivo específico, en coherencia con los lineamientos establecidos en el manual. -En el ítem 5.3.5 – Derechos de los

				Titulares, se realizó un ajuste en la redacción del párrafo, debido a que el término *"decepcionará"* alteraba el sentido del contenido; en consecuencia, se efectuó la corrección correspondiente. -Adicionalmente, en el numeral 5.4, se actualizó la denominación del formato ASIP20, el cual figuraba como *"Gestión de acceso a usuarios de servicios informáticos"*, cambiándose a *"Gestión de acceso a los sistemas de información, recursos y servicios tecnológicos"*, conforme al Modelo de Operación Digital.
11	2026	04	10	Cambia el nombre del manual y pasa de "MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" a "MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN A LA PRIVACIDAD DE LA INFORMACIÓN." -Se realizo un ajuste en la redacción en el numeral 5.6 LINEAMIENTO DE GESTIÓN DE ACTIVOS DE INFORMACIÓN en los términos, en el párrafo 1 se elimina la palabra "estratégico", se cambia la palabra "reafirma" por "afirma" y la oración final por "Este lineamiento adopta los principios de Confidencialidad, Integridad y Disponibilidad de la información, directrices y responsabilidades para la administración, protección y uso adecuado de los activos de la información." para dar claridad en la redacción del lineamiento. Se realizo un ajuste en el numeral 5.12 LINEAMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN para actualizar los lineamientos de gestión de incidentes conforme a la normatividad y los requisitos legales vigentes. Se agrega los lineamientos de Integridad y No Repudio, en los apartados 5.15 y 5.16

ELABORÓ	
NOMBRES Y APELLIDOS	**CARGO**
Brenda Camila Mesa Rozo	Profesional I
Brian Steven Cubillos Cubillos	Técnico
REVISÓ	
NOMBRES Y APELLIDOS	**CARGO**

María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información - SGSI

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información - SGSI	2026	04	10