CONSEJO SUPERIOR
ACUERDO N° 4
10 ABR 2026

POR MEDIO DEL CUAL SE ACTUALIZA Y ADOPTA LA POLÍTICA DE GESTIÓN DE LA INFORMACIÓN DE LA CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES

El Consejo Superior de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, en uso de sus facultades legales otorgadas por sus Estatutos y,

CONSIDERANDO:

Que en ejercicio de la autonomía universitaria establecida en el artículo 69 de la Constitución Política de Colombia y la ley 30 de 1992 a las Instituciones de Educación Superior sobre la Autonomía Universitaria para proceder en la decisión de sus estructuras administrativas y académicas, que a la letra expresa en el artículo 29 que las instituciones podrán *"definir y organizar sus labores formativas, académicas, docentes, científicas, y culturales*..."

Que los Estatutos de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, le asigna al Consejo Superior la función de expedir, modificar las políticas que considere necesarias para el funcionamiento de la institución previo cumplimento de la legislación vigente.

Que según la adopción del Marco General del Plan de Desarrollo Institucional 2018-2025 de la UNICUCES, sirve como un referente para proyectar las acciones de las funciones misionales de la institución, donde se formulan políticas, objetivos estratégicos y metas relacionadas con la Educación y Formación, la que permitirá el alcance de los logros propuestos por cada una de las dependencias adscritas.

Que el decreto 1330 del 25 de Julio de 2019, en su artículo 2.5.3.2.3.1.3, establece que las Instituciones de educación superior deben dar cuenta de la existencia de política que permitan el desarrollo estructurado de los programas académicos que oferta y desarrolla la UNICUCES.

Que la UNICUCES fortalecer la capacidad institucional para el uso, apropiación y aprovechamiento de la información (interna y externa), en el mejoramiento de la toma de decisiones basadas en información oportuna y veraz, en la transparencia institucional y en la rendición de cuentas.

Que la Política de Gestión de la Información de la UNICUCES, tiene como propósito la efectiva gestión de la información, teniendo en cuenta la importancia del fortalecimiento e integración de los sistemas de información para el mejoramiento de la gestión y la toma de decisiones basadas en evidencia, la gestión del ciclo de vida del dato, la institucionalización del modelo de gestión de información reconociendo las necesidades de las dependencias, la definición del esquema de gobernabilidad para la gestión de la información, y la introducción de conceptos como gestión eficiente, gobernabilidad, interoperabilidad y calidad de los datos.

Que la presente actualización de la Política de Gestión de la Información de la UNICUCES, debe ser conocida, comprendida y aplicada por toda la comunidad universitaria, incluyendo estudiantes, docentes, investigadores, funcionarios administrativos, contratistas y terceros que presten servicios o mantengan algún tipo de vinculación con la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES.

Que la actualización de la Política de Gestión de la Información de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, tiene como propósito la efectiva gestión de la información, teniendo en cuenta la importancia del fortalecimiento e integración de los sistemas de información para el mejoramiento de la gestión y la toma de decisiones basadas en evidencia, la gestión del ciclo de vida del dato, la institucionalización del modelo de gestión de información UNICUCES, reconociendo las necesidades de las dependencias, la definición del esquema de gobernabilidad para la gestión de la información, y la introducción de conceptos como gestión eficiente, gobernabilidad, interoperabilidad y calidad de los datos.

Que acogiendo las diversas disposiciones en el marco normativo vigente tanto del Ministerio de Educación Nacional mediante el Decreto 1330 de julio de 2019, la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, aprueba la actualización Política de Gestión de la Información, por lo cual,

ACUERDA:

ARTICULO PRIMERO: Constituir por este acuerdo, la actualización de la Política de Gestión de la Información de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR.

ARTÍCULO SEGUNDO. El presente acuerdo rige a partir de la fecha de su expedición.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dado en la ciudad de Santiago de Cali, a los diez (10) días del mes de abril de dos mil veintiséis (2026).

(Original firmado por)

CARLOS AUGUSTO NARVAEZ DIAZ
Presidente

(Original firmado por)

ALEJANDRA DIAZ MANZANO
Secretario

UNICUCES

CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR

Política de Gestión de la Información

Gestionamos la información de manera ética, segura, íntegra y oportuna para la toma de decisiones, la transparencia y la mejora continua institucional.

- Protegemos la confidencialidad, integridad y disponibilidad de la información.
- Garantizamos la calidad, veracidad y oportunidad de la información.
- Cumplimos la normatividad vigente en materia de protección de datos y seguridad de la información.
- Promovemos una cultura de uso responsable y transparente de la información.
- Utilizamos la información como activo estratégico para la innovación y la mejora continua.

Información que nos conecta, decisiones que transforman, futuro que construimos juntos.

Información confiable, institución transparente y eficiente.

2025

CAPÍTULO I

ASPECTOS GENERALES

Artículo 1º. **Definición**. La presente política detalla la forma como la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, dará el adecuado tratamiento a la información que sea remitida, analizada y procesada por la UNICUCES.

Artículo 2º. Objetivo. GENERAL: Fortalecer la capacidad institucional de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR. UNICUCES para el uso, apropiación y aprovechamiento de la información (interna y externa), en el mejoramiento de la toma de decisiones basadas en información oportuna y veraz, en la transparencia institucional y en la rendición de cuentas.

Artículo 3º. Objetivos. ESPEFICICOS: Los objetivos específicos de la Política de Gestión de la Información en la UNICUCES, son:

- Establecer un gobierno de la información efectivo, eficiente y eficaz de los datos y la información que permita tener la capacidad de tomar decisiones basadas en evidencia.

- Definir los lineamientos para el desarrollo de una arquitectura de datos que apoye la obtención de los objetivos de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR. UNICUCES y que permita que las personas vinculadas o con algún tipo de relación con ella puedan usar y actualizar los datos de la manera correcta.

- Introducir controles y definir criterios de estandarización de datos dentro de las prácticas de gestión de la información en la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR. UNICUCES.

- Brindar lineamientos generales para las prácticas de diseño e implementación de modelos de gestión de datos para una apropiada gestión de la información en la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES.

Artículo 4º. Autorización. Cuando se trate de diferentes documentos de personas naturales o jurídicas, se solicitará previamente la autorización para el tratamiento de por cualquier información que permita ser utilizado como prueba. Según el caso, dicha autorización puede ser parte de un documento más amplio como, por ejemplo, de un contrato, o de un documento especifico (formato, formulario etc…).

Artículo 5º. Alcance. Esta política regula la gestión integral de los datos estructurados de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES., es decir, aquellos contenidos en bases de datos, tablas y sistemas de información que soportan los procesos institucionales. El Modelo de Gobierno de los Datos y la Información y el Modelo de Gestión de la Información se aplican a los datos organizacionales estructurados necesarios para la gestión académica, administrativa, de investigación y de extensión de la UNICUCES.

Artículo 6º. **Finalidad del documento a tratar**. En caso de tratarse de datos de carácter personal privados correspondientes a personas naturales, la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES realizará la descripción de la finalidad del tratamiento de los datos y se informará mediante un documento específico, así mismo se informará al titular de los datos lo siguiente:

a) El Tratamiento al que serán sometidos sus datos personales y la finalidad específica del mismo.
b) Los derechos que le asisten como titular.
c) La página web, correo electrónico, dirección física y demás canales de comunicación por los cuales podrá formular consultas y/o reclamos ante el Responsable o encargado del Tratamiento.

Artículo 7º. **Términos y Definiciones.** la Política de Gestión de la información presenta elementos que contribuyen con la construcción de sistemas cuya arquitectura se fundamenta en la calidad del dato y de la información, para lo cual se identifican términos y definiciones para la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES así:

- **Activo:** Recurso tangible o intangible que se genera a través de una operación, se puede controlar y permite obtener un beneficio.

- **Activo de Información:** Cualquier componente (humano, hardware, software, información digital o física o de infraestructura) que soporta uno o más procesos de la Institución y, en consecuencia, debe ser protegido.

- **Acuerdo de Confidencialidad:** Es un documento en el que los funcionarios de Referencia o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, comprometiéndose a no divulgar, usar o explotar la información confidencial restringida o confidencial a la que tengan acceso en virtud de la labor o contrato que desarrollan dentro y fuera de la misma.

- **Amenazas:** Se entiende por amenaza, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo de seguridad de la información. Son amenazas el talento humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Las amenazas en un contexto de seguridad de la información incluyen actos dirigidos, amenazas en un contexto de seguridad de la información incluyen actos dirigidos deliberados (por ejemplo, por *crackers*) y sucesos no dirigidos, aleatorios o impredecibles (como puede ser un rayo), amenaza es la causa de riesgo que crea aptitud dañina sobre personas y bienes de la UNICUCES.

- **Análisis de Riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- **Análisis de Riesgos de Seguridad de la Información**: Proceso sistemático de identificación de fuentes (amenazas y vulnerabilidades), estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las

consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información de la UNICUCES.

- **Autenticación:** Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **Ciberseguridad:** Es el conjunto de procedimientos, prácticas y técnicas para la protección, prevención de daños y restauración tanto de los servicios tecnológicos y sistemas de comunicaciones electrónicas, como la información digital allí gestionada, mitigando riesgos asociados a amenazas y ataques cibernéticos (*malware, phishing, ramsomware*, denegación de servicio, y otras formas de intrusión), asegurando que la UNICUCES pueda operar de manera segura y resiliente en entornos digitales.

- **Cifrado:** Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

- **Confidencialidad:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Contraseña:** Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso, por lo general una herramienta tecnológica o accesos físicos que son validados por herramientas tecnológicas. Las claves suelen tener limitaciones en sus caracteres (no aceptan algunos) y su longitud.

- **Controles:** Medidas dispuestas para reducir el nivel de riesgo, tales como políticas, procedimientos, directrices, prácticas o estructuras de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- **Criptografía:** Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

- **Dato:** Representación convencional de un hecho o idea que puede ser tratada por el ordenador.

- **Derechos de Autor:** Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada cuando esta la requiera.

- **Equipo de Cómputo:** Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

- **Evento de Seguridad de la Información:** Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un incumplimiento posible de la política de seguridad de la información, una falla de controles, de la política de seguridad de la información una falla de controles o una situación previamente desconocida que puede ser pertinente para la seguridad.

- ***Hacking* Etico (*Ethical Hacking*):** Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

- **Incidente de Seguridad de la Información**: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES y amenazar la seguridad de la información.

- **Información:** Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

- **Información sensible:** Información o cualquier tipo de dato que si se difunde podría resultar perjudicial para personas u organizaciones. Los datos sensibles pueden incluir información personal identificable (IPI), datos financieros, entre otros, Particularmente en datos personales los datos sensibles son aquellos que afectan la intimidad de su titular o cuyo uso indebido puede generarle discriminación, vulneración a su derecho de igualdad.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

- **Medio Removible:** Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros USR entre otras removibles, CDS, DVDs y unidades de almacenamiento USB, entre otras.

- **Mitigar el Riesgo:** Cuando se decide prevenir o reducir el impacto o probabilidad del riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo a un nivel aceptable. Se consigue, por ejemplo: mediante la optimización de los procedimientos, la implementación de controles, fortalecimiento del ejercicio del autocontrol, fortalecimiento del ejercicio de la autoevaluación de la gestión, las auditorías internas, entre otros. Existen dos formas de reducir el riesgo: prevenir, que apunta a la disminución de laprobabilidad o proteger.

- **No Repudio:** Condición en la que quien envía un mensaje o realiza una operación con los sistemas de información no puede negar la validez del resultado del proceso que se utilizó para autenticar la información.

- **Política:** Directrices y normas que deben cumplir los integrantes de una institución las cuales reflejan las intenciones y dirección de una institución.

- **Propietario de la Información:** Es la unidad organizacional o proceso donde se crean los activos de información.

- **Recursos Tecnológicos:** Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES.

- **Riesgo:** Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas o de imagen por deficiencias, fallas o inadecuaciones, en el talento humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.

- **Servicios tecnológicos:** Conjunto de soluciones o recursos que se ofrecen a través del uso de tecnologías de información y comunicación (TIC). Puede incluir desde software, infraestructura tecnológica, almacenamiento y procesamiento de datos, redes y comunicaciones, hasta nuevas tecnologías (inteligencia artificial, *blockchain*, etc), dispuestos físicamente en la institución o "en nube", y administrados directamente por la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES o a través de un tercero.

- **Sistema de gestión de seguridad de la información:** se refiere a un conjunto de procesos sistemáticos y estructurados que, a través de políticas, procedimientos y controles basado en el riesgo, protege de manera proactiva y continua la confidencialidad, integridad y disponibilidad de la información crítica en la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES.

- **Sistema de Información:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por referencia o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado a la medida para la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES.

- **Sistemas de Control Ambiental:** Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características de este, emito fundamentalmente humedad y temperatura y de manera adicional, también permite controlar su pureza y su movimiento.

- **Software Malicioso:** Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

- **Grupos de interés:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES entidad.

- **Vulnerabilidad:** Es el grado de debilidad de un activo frente a una amenaza, hace referencia a la capacidad que tiene la amenaza de afectar el activo.

Parágrafo: Que la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES en su cultura y desarrollo Digital, reconoce que la seguridad digital es componente esencial de un desarrollo digital sólido y sostenible, además que la Política de Seguridad de la Información y el Sistema de Gestión de Seguridad de la Información constituyen el marco mediante el cual se consolida el gobierno de Seguridad de información en la UNICUCES con el objetivo de minimizar el riesgo de seguridad de información en sus procesos y proteger su información ante amenazas de ciberseguridad.

CAPÍTULO II

DERECHO DE TITULARES DE LA INFORMACIÓN

Artículo 8º. **Del Derecho de Acceso**. La CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES garantiza el derecho de acceso conforme a
la Ley 1581 de 2012, los decretos reglamentarios asociados, así como las resoluciones y lineamientos expedidos por el Ministerio TIC que orientan la implementación de controles, la gestión de incidentes y la relación con terceros y proveedores tecnológicos, donde solamente a los Titulares de datos personales privados que correspondan a personas naturales, previa acreditación de la identidad del titular, legitimidad, o personalidad de su representante, poniendo a disposición de éste, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales tratados, a través de cualquier medio de comunicación, incluyendo los electrónicos que permitan el acceso directo del titular.

Artículo 9º. **Del Derecho a Consulta**. Los titulares de los datos personales podrán consultar la información de carácter personal que repose en cualquiera de las bases de datos de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, excepto las bases de datos de los registros públicos, cuya consulta atenderá a lo dispuesto por el Código de Comercio, el Decreto 898 de 2002 y las demás normas que regulen sobre esta materia.

En consecuencia, la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES garantiza el derecho de consulta conforme a lo dispuesto en la Ley 1581 de 2012 exclusivamente sobre los datos personales privados, sensibles y de menores correspondientes a personas naturales, suministrando a los titulares de estos datos personales la información contenida en cada una de las bases de datos correspondientes y que estén bajo el control de UNICUCES.

Artículo 10º. **Del Derecho a Reclamar**. El Titular de datos personales privados que correspondan a una persona natural y considere que la información contenida o almacenada en una base de datos que no corresponda a los registros públicos de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR UNICUCES, puede ser objeto de corrección, actualización, o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes y principios contenidos en la normatividad sobre Protección de Datos Personales. En tal sentido, podrán presentar reclamación

ante el Responsable o Encargado del tratamiento en la UNICUCES.

Artículo 11º. **Del Derecho a la Rectificación y Actualización de datos**. La CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES, se obliga a rectificar y actualizar a solicitud del Titular, la información de carácter personal que corresponda a personas naturales, que resulte incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados. Lo anterior, siempre y cuando, no se trate de datos contenidos en los registros públicos. Al respecto, UNICUCES tendrá en cuenta lo siguiente:

a) En las solicitudes de rectificación y actualización de datos personales, el Titular debe indicar las correcciones a realizar y aportar la documentación que avale su petición.

b) La CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES, tiene plena libertad de habilitar mecanismos que le faciliten el ejercicio de este derecho, siempre y cuando beneficien al Titular de los datos personales. En consecuencia, se podrá habilitar medios electrónicos u otros que UNICUCES considere pertinentes y seguros.

c) La CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES, podrá establecer formularios, formatos, sistemas y otros métodos que serán informados en el Aviso de Privacidad y que se pondrán a disposición de los interesados en la página web u oficinas de la UNICUCES.

CAPÍTULO III

OTRAS DISPOSICIONES

Artículo 12º. **Protección de datos en los contratos**. En los contratos laborales, UNICUCES incluirá cláusulas con el fin de autorizar de manera previa y general el tratamiento de datos personales relacionados con la ejecución del contrato, lo que incluye la autorización de recolectar, modificar o corregir, en momentos futuros, datos personales del Titular correspondientes a personas naturales.

También incluirá la autorización para que algunos de los datos personales, en caso dado, puedan ser entregados o cedidos a terceros con los cuales UNICUCES tenga contratos de prestación de servicios, para la realización de tareas tercerizadas. En estas cláusulas, se hará mención de la presente Política y de su ubicación en el sitio web institucional, para su debida consulta.

En los contratos de prestación de servicios externos, cuando el contratista requiera de datos personales, UNICUCES le suministrará dicha información siempre y cuando exista autorización previa y expresa del Titular de los datos personales para esta transferencia, quedando excluida de esta autorización, los datos personales de naturaleza pública definidos en el numeral 2° del artículo 3° del Decreto Reglamentario 1377 de 2013 y los contenidos en los registros públicos.

Dado que en estos casos, los terceros son Encargados del tratamiento de datos y sus contratos incluirán cláusulas que precisan los fines y los tratamientos autorizados por UNICUCES y delimitan de manera precisa el uso que estos terceros le pueden dar a aquellos, así como las obligaciones y deberes establecidos en la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, incluyendo las medidas de seguridad necesarias que garanticen en todo momento la

confidencialidad, integridad y disponibilidad de la información de carácter personal encargada para su tratamiento.

El contexto nacional presenta un escenario de transformación digital acelerada que incide directamente en la gestión de la seguridad y privacidad de la información de las IES, es así como la consolidación de la estrategia de digital, y de fortalecimiento de los servicios en línea y la creciente dependencia de plataformas tecnológicas han incrementado la exposición a riesgos asociados a la ciberseguridad, la protección de datos personales y la continuidad de los servicios digitales.

En esta dinámica, se evidencia un aumento sostenido de amenazas cibernéticas, incidentes de seguridad de la información y vulnerabilidades derivadas del uso intensivo de tecnologías emergentes, la tercerización de servicios tecnológicos y la interoperabilidad entre sistemas de información. Este contexto exige a las instituciones de educación superior el fortalecimiento integral de sus capacidades de prevención, detección y respuesta, adoptando enfoques articulados de gestión del riesgo y de protección de los activos de información en la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES.

El marco normativo nacional ha evolucionado para responder a estos desafíos, estableciendo mayores responsabilidades para las entidades de educación superior en materia de seguridad digital, tratamiento de datos personales, gestión de proveedores tecnológicos y aseguramiento de la información.

Lineamientos como el Modelo de Privacidad y Seguridad de la Información (MSPI), el Modelo Integrado de Planeación y Gestión (MIPG) y las disposiciones asociadas a la estrategia de Gobierno Digital refuerzan la necesidad de contar con planes estructurados, medibles y alineados con la planeación institucional en la UNICUCES.

En el sector educativo, y particularmente en la educación superior con modalidades presencial, virtual, digital e hibrida, hacen que estos retos se intensifican debido al manejo de grandes volúmenes de información académica, administrativa y personal, así como a la prestación de servicios educativos en entornos virtuales.

La UNICUCES en este contexto, reflexiona en la Política de Gestion de la Informacion y los planes de seguridad y privacidad de la Información se constituye en un instrumento clave para responder a las tendencias nacionales y garantizar la confianza de los usuarios de la UNICUCES en los servicios institucionales, en coherencia con los objetivos del desarrollo educativo y la transformación digital del país.

Artículo 13º. **Marco Legal**. La presente política de Gestión de la Información ha sido elaborada en concordancia con las siguientes normas y documentos:

- Constitución Política, artículo 15.
- Ley 1581 de 2012
- Ley 1273 de 209
- Ley 1266 de 2008
- Decretos Reglamentarios 1727 de 2009 y 2952 de 2010
- Decreto Reglamentario parcial No 1377 de 2013
- Sentencias de la Corte Constitucional C–1011 de 2008, y C-748 del 2011

- Avisos de privacidad y Reglamento Interno de Trabajo
- Decreto 612 de 2018. Decreta lineamientos y planes de acción que las entidades del estado deben implementar para gestionar sus acciones institucionales.
- Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 2710 de 2017. Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Título 9 Políticas y Lineamientos de TI, Capitulo 1 Política de Gobierno Digital, Sección 2, Componentes, Instrumentos y Responsables de SPI. Manual Estrategia de Gobierno en Línea
- Decreto 103 de 2015. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 1377 de 2013 Por la cual se reglamenta parcialmente la Ley 1581 de 2012 para la protección de datos personales.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012 Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 2693 de 2012 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. Manual para la implementación de la estrategia de gobierno en línea 2012-2015
- Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y aplicación de criterios de seguridad.
- Ley 1341 de 2009, Marco General del Sector de TIC. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones-TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Decreto 1151 de 2008 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones: Manual para la implementación de la estrategia de gobierno en línea.
- Acuerdo 060 de 2001 Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.

- Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
- Decreto 1360 de 1989 Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Norma ISO/IEC 27001, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4

Artículo 14º. **Organización de archivos y tablas de retención documental.** Adicionar a esta política la normatividad establecida sobre las normas para la organización del archivo y las tablas de retención documental de la CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES, La declaración de la política de seguridad de la información para la UNICUCES, constituye un recurso estratégico en el cumplimiento de su misión y es su prioridad protegerla y tratarla apropiadamente, teniendo en cuenta los principios de disponibilidad, integridad y confidencialidad, buscando asegurar el cumplimiento de los requisitos operativos, técnicos, normativos y regulatorios, a los cuales está sujeta la información, tomando como base la gestión de riesgos que, de manera continua, redunde en la mejora y eficacia del Sistema de gestión de Seguridad de la Información y el SIGU.

Artículo 15º. Mecanismos de autenticación. La CORPORACIÓN UNIVERSITARIA CENTRO SUPERIOR, UNICUCES establecerá mecanismos de autenticación seguros, apropiados según su uso y posibilidades tecnológicas, que restrinjan el acceso no autorizado a los servicios de tecnología de información; todos los servicios tecnológicos deben contar con los mecanismos de autenticación y protección de la autenticación que la UNICUCES considere, establezca e informe.