Vigilada MINEDUCACIÓN

UNIVERSIDAD
La Gran Colombia

POLÍTICA INSTITUCIONAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2021

UNIVERSIDAD LA GRAN COLOMBIA

PLENUM 2021

Rafael Antonio Chaves Posada

PRESIDENTE

José Alberto Bernal Calvo

VICEPRESIDENTE

- Álzate de López Mercy
- Arbeláez de Salazar Nelcy
- Avendaño Barreto José Helí
- Ávila Bottía Luis Segundo
- Azuero Isaza Vicente
- Bernal Calvo José Alberto
- Hno. Bolívar Rodríguez José Arcadio
- Cancino Bermúdez Hernán
- Chaves Posada Rafael Antonio
- Corsi Otálora Carlos Eduardo
- Pbro. García Álvarez Juan Guillermo
- García de Sáenz Martha Cecilia
- García Vásquez Carmenza
- Geithner Castrillón John Elkin
- González Chaves Ligia
- Herrera Soto Roberto
- Ledesma López German Darío
- Martínez de Samper Yolanda
- Montoya Barrera Nubia Marlén
- Mosquera Trejos Jorge Eliécer
- Noriega Santos Jorge
- Pava Lasprilla Fernando
- Peña Galvis Aura Felisa
- Quintero Pinilla Jorge Alberto
- Ramírez Gasca Abelardo
- Mons. Rueda Sierra Ismael
- Salas Toro Guillermo
- Salazar Vélez Carlos Ariel
- Toro Buitrago Luzmila
- Valderrama Álvarez Luis Enrique
- Valderrama Andrade Adán

Oswaldo Abril Casas

SECRETARIO

Oscar De Jesús Hernández Virviescas

REVISOR FISCAL

UNIVERSIDAD LA GRAN COLOMBIA

CONSILIATURA 2021

Abelardo Ramírez Gasca
PRESIDENTE

Rafael Antonio Cháves Posada
VICEPRESIDENTE

Carmenza García Vásquez
Fernando Pava Lasprilla
Rafael Antonio Cháves Posada
Abelardo Ramírez Gasca
REPRESENTANTES DEL HONORABLE PLENUM

Carlos Fernando Hincapié
REPRESENTANTE DE LOS PROFESORES

Jaime Mejía Ossman
REPRESENTANTE DE LOS EGRESADOS

Jeferson Alexander González
REPRESENTANTE DE LOS ESTUDIANTES

Adriana Ivonne Jiménez Barón
María Patricia Bautista Uribe
REPRESENTANTES DEL CONSEJO ACADÉMICO

Marco Tulio Calderón Peñaloza
RECTOR

Héctor Hugo Tabares Ramírez
SECRETARIO

UNIVERSIDAD LA GRAN COLOMBIA

DIRECTIVOS ACADÉMICOS Y DIRECTIVOS ADMINISTRATIVOS - AÑO 2021

Marco Tulio Calderón Peñaloza
RECTOR

Víctor Manuel Pérez Argüelles
VICERRECTOR DE INNOVACIÓN Y EMPRESARISMO

Mario Camilo Torres Suárez
VICERRECTOR DE DESARROLLO ACADÉMICO

Carlos Mauricio Cárdenas Méndez
VICERRECTOR DE GESTIÓN FINANCIERA

Héctor Hugo Tabares Ramírez
SECRETARIO GENERAL

Jorge Alberto Quintero Pinilla
RECTOR DELEGATARIO SECCIONAL ARMENIA

Bibiana Vélez Medina
VICERRECTORA ACADÉMICA SECCIONAL ARMENIA

Ángela María Narváez Osorio
SECRETARIA GENERAL SECCIONAL ARMENIA

Conrrado de Jesús Álvarez Chogó
DIRECTOR DE ASEGURAMIENTO DE CALIDAD

Félix Ancízar Ávila Arturo
COORDINADOR DE ASEGURAMIENTO DE LA CALIDAD

Martha Lucía Bahamón Jara
ASESORA EXTERNA

Daniel Andrés Rocha Ramírez
DIRECTOR DE SISTEMAS DE LA INFORMACIÓN

Fernando Jaime Escobar Botero
JEFE DE SISTEMAS DE LA INFORMACIÓN SECCIONAL ARMENIA

Contenido

1. Declaración de la política

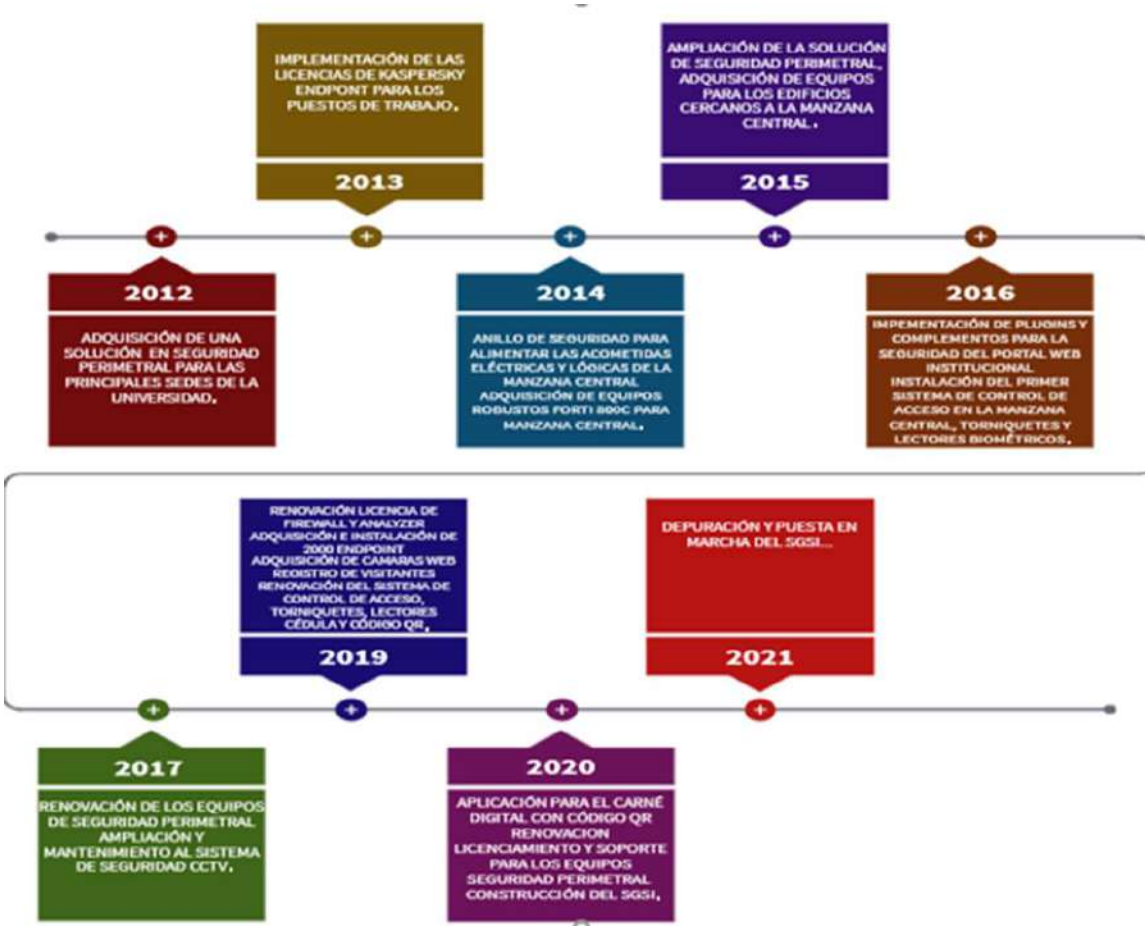
Conforme a la voluntad del fundador Julio César García, la Universidad La Gran Colombia inicia sus labores en febrero de 1951. Con el fin de atender a todos los frentes de la cultura y la formación humana, preferentemente el fomento de la investigación científica, tecnológica y la enseñanza a través de la calidad académico-administrativa basada en sus valores Cristianos, Bolivarianos, Hispánicos y Solidarios.

Por esta razón, en el año 2020 La Universidad La Gran Colombia se compromete con el diseño, elaboración e implementación de un Sistema de Gestión de Seguridad de la Información, el cual busca establecer un marco de confianza en el ejercicio de sus deberes con los estudiantes, los docentes, los administrativos y los aliados estratégicos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la institución.

Para la Universidad, la protección de la información busca disminuir el impacto generado sobre su información crítica ante los riesgos internos o externos que se puedan llegar a presentar, con el objetivo de mantener un nivel adecuado de seguridad que permita responder por la integridad, confidencialidad y disponibilidad de la información acorde con las necesidades de las partes interesadas. En esta implementación se da cumplimiento a la Resolución 61322 del Ministerio de Comercio, Industria y Turismo y de la Superintendencia de Industria y comercio, la cual exige estándares mínimos de seguridad para la información personal registrada en las diferentes bases de datos institucionales y que tienen como propósito el tratamiento de información para el cumplimiento de los objetivos institucionales, todo esto en concordancia con lo establecido en la norma ISO 27001: 2013.

La estructura de alto nivel de las ISO permite a la Universidad tener una visión global del contexto interno y externo respecto a su gestión, mejora en la coordinación y priorización de las necesidades, reducción del nivel de documentación aplicable al sistema, unificación de controles y operaciones de los procesos, reducción de recursos y costos; por esta razón se identifica una política de gestión institucional. Ver la Figura 1 Línea de tiempo de la seguridad informática – Evolución en seguridad informática UGC.

Figura 1 Línea de tiempo de la seguridad informática – Evolución en seguridad informática UGC



Fuente: Sistemas de la información.

1.1. Identidad de la política

La Universidad La Gran Colombia se compromete a proveer las diferentes herramientas necesarias para la seguridad de los activos de información a través de procedimientos, lineamientos y buenas prácticas que permitan establecer un marco de protección entorno a la confidencialidad, integridad y disponibilidad de la información, promoviendo así una sensibilización en los diferentes procesos de la Universidad y garantizando la apropiación de una cultura orientada a la gestión de los riesgos.

2. Referentes

Con el fin de articular la política de la Universidad La Gran Colombia se toman como referencia análisis comparativos a nivel nacional e internacional, los cuales permiten orientar de forma estratégica la política de la Universidad, impactando su estructura y forma de implementación. A continuación, se presenta el comparativo entre tales referentes.

2.1. Referentes nacionales

En el contexto nacional se analizan diferentes universidades y sus respectivas políticas de seguridad de la información encontrando lo siguiente:

- Integración de las distintas buenas prácticas de seguridad de la información en los procesos institucionales.
- Articulación del sistema de gestión de seguridad de la información a la misión, la visión, las políticas y los objetivos Institucionales.
- Compromiso de la alta dirección con el cumplimiento de los objetivos del sistema de gestión de seguridad de la información.
- Fácil adaptación de los procesos con los objetivos propios del Sistema de Gestión de Seguridad de la Información.
- Definición clara de los roles y la responsabilidad dentro del Sistema de Gestión.
- Descripción clara del cumplimiento en los controles del Anexo A de la norma NTC ISO 27001: 2013.

2.2. Referentes Internacionales

En cuanto a la normatividad vigente en el contexto internacional, se identifica una clara unificación en la aplicabilidad del Sistema de Gestión de Seguridad de la Información entre los procesos académicos y administrativos, permitiendo de este modo comprender la implementación de la seguridad de la información en un ámbito institucional y dando una visión más clara para el cumplimiento de las necesidades de nuestras partes interesadas.

- Promueven una cultura de gestión del riesgo entre las partes interesadas a partir de la integración de lineamientos que garanticen la seguridad de la información en los procesos institucionales.
- Analizan el contexto de la organización, permitiendo identificar las debilidades, las oportunidades, las fortalezas y las amenazas que alteren el cumplimiento de los objetivos del Sistemas de Gestión de Seguridad de la Información.
- Descripción de roles y responsabilidades frente al Sistema de Gestión de Seguridad de la Información.
- Compromiso de la alta dirección con el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información.

Por otro lado, existen organizaciones como la ISO (International Organization for Standardization) que, como organismo internacional de normalización, ayuda en el aumento de conciencia sobre los estándares aplicables a cada necesidad organizacional, fortaleciendo diferentes competencias profesionales y permitiendo la implementación eficaz de un sistema de gestión estandarizado.

El Consejo Superior de Administración Electrónica de España elaboró MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para gestionar los riesgos de las TIC debido al creciente uso y dependencia de estas para alcanzar los objetivos que cada individuo u organización desea. Para esta metodología, la gestión de riesgos se divide en dos subprocesos que se presentan a continuación:

- Análisis de Riesgos: Permite determinar lo que posee la organización y que le podría suceder.
- Tratamiento de Riesgos: Organiza una defensa prudente para sobrevivir a los incidentes y seguir operando en las mejores condiciones, al no poder controlar se maneja un riesgo residual que es asumido por la alta dirección.

3. Fundamentación teórica del sistema de gestión de seguridad de la información

El Sistema de Gestión de Seguridad de la Información, se convierte en una herramienta que permite la identificación y el análisis oportuno de riesgos que puedan llegar a afectar los activos de la información, implementando procesos de evaluación, rendición de cuentas, información veraz y transparente sobre la Seguridad de la Información institucional, a continuación, se revisaran los elementos teóricos propios a entidades regulatorias.

3.1. Superintendencia de Industria y Comercio (SIC)

A través de la Dirección de Investigación de Protección de Datos Personales, la SIC exige a todas las entidades privadas o públicas implementar medidas de seguridad que garanticen la protección de los datos personales administrados por la misma, a su vez, la entidad debe estar en la capacidad de demostrar el cumplimiento de las diferentes responsabilidades consignadas en la Ley 1581 del 2012.

La protección está amparada en la Ley 1266 de 2008, también conocida como Ley de Habeas Data, la cual se aplica a todos los datos personales financieros, los crediticios, los comerciales y los de servicios registrados en un banco de datos. En este sentido, la aplicación de la Ley 1266 de 2008 está encaminada a regular el uso de esa información, exceptuando aquellos tipos de datos que por ejemplo se mantienen en un ámbito exclusivamente personal o doméstico.

Así mismo, en vista del carácter sectorial aplicable a la información relacionada con el sector financiero, se expide la Ley 1581 de 2012, la cual amplia el margen de aplicación de protección de datos a otros campos que no fueron cubiertos en la Ley de Habeas Data. Es decir, que todas las bases de datos que no se encuentran dentro del ámbito de aplicación de la Ley 1266 de 2008 se empiezan a regir por la Ley 1581 de 2012, cuyo ámbito de aplicación de acuerdo con su artículo 2 son todos los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. (Ley estatutaria 1581 de 2012, 2012)

3.2. Fiscalía General de la Nación

Los ataques de seguridad informática han dejado pérdidas cercanas a los 12 millones de dólares alrededor del mundo en los últimos años según cifras del Buró Federal de Investigaciones (FBI). En Colombia, la fiscalía general de la nación asegura que el monto de pérdidas oscila entre los 5 a 120 millones de pesos, dependiendo del tamaño de la empresa afectada. La fiscalía general de la nación como organismo de poder judicial condena cualquier delito consignado en la Ley 1273 de 2009 (Ley de delitos informáticos), brindando a los ciudadanos una cumplida y eficaz administración de la justicia. A continuación, se presentan las cifras consultadas en la página de la fiscalía general de la nación para el año 2021 en función de delitos informáticos reportados por un usuario. (Fiscalía General de la Nación, 2021)

Tabla 1 Registro de delitos informáticos.

DELITO	REGISTROS
Acceso abusivo a un sistema informático.	2804
Hurto por medios informáticos.	6468
Interceptación de datos informáticos.	280
Obstaculización de un sistema informático o red de telecomunicaciones.	60
Transferencia no consentida de activos valiéndose de alguna manipulación informática.	892

Nota. Esta tabla muestra la cantidad de registros almacenados en la página web oficial de la Fiscalía General de la Nación.

3.3. ISO 27001:2013 Sistemas de Gestión de Seguridad de la Información

La norma ISO 27001:2013 brinda un marco de referencia frente a la implementación de un Sistema de Gestión de Seguridad de la Información, lo cual permite a la organización una mejora en el desempeño de las actividades propias de cada proceso a través del ciclo PHVA, otorga una cultura basada en riesgos y fundamentos sólidos para la integración de los procesos mediante la identificación de sus activos de información críticos y la asignación de los controles correspondientes para prevenir la materialización de algún riesgo.

Cabe resaltar los beneficios que otorga la implementación de un Sistema de Gestión de Seguridad de la Información:

- Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos sobre los activos de información.
- Minimiza los riesgos en materia de confidencialidad, integridad y disponibilidad.
- Mejora continua de la seguridad de la información, mediante la supervisión, la revisión y la eficacia de los procesos implantados.

- Aporta un valor añadido y/o diferencial a la compañía.
- Exterioriza una clara vocación del cumplimiento de la normativa sobre protección de datos.
- Certifica una especial solvencia técnica en materia de seguridad de la información.
- Integra procesos lo que permite reducción del nivel de documentación que sea aplicable al sistema de gestión mejorando los tiempos de respuesta.
- Permite tomar decisiones estratégicas basadas en evidencias y en los resultados de las herramientas del Sistema de Gestión de Seguridad de la Información.
- Fomenta una cultura basada en la autoevaluación, autorregulación y mejoramiento, involucrando a sus colaboradores en la apropiación de los sistemas de gestión.

3.4. ISO 22301:2018 Continuidad de negocio:

La norma ISO 220301 tiene como objetivo mantener la continuidad de las actividades de la Universidad ante cualquier situación adversa que se pueda presentar, todo esto identificando las necesidades de la organización y de sus partes interesadas y priorizándolas ante cualquier eventualidad.

A continuación, se resaltan los beneficios que trae la implementación de la norma:

- Implantar la cultura de la continuidad del negocio dentro de la política de gestión de la organización.
- Generar confianza en las partes interesadas debido a las mejores prácticas internacionales para mantener la actividad de la institución con las mínimas interrupciones posibles.
- Ayuda eficaz para establecer indicadores medibles para alcanzar los objetivos previstos por una organización.
- Mejorar el conocimiento de los riesgos y oportunidades de la institución.
- Reducción de costos mediante la reducción de tiempos de inactividad.
- Ayuda a evitar consecuencias adversas de posibles responsabilidades derivadas de los riesgos de la actividad empresarial.

3.5. ISO 31000:2018 Gestión del riesgo

El objetivo principal de la norma ISO 31000: 2018 es ayudar a la organización a integrar la gestión de riesgos en sus actividades o procesos importantes, razón por la cual su efectividad se vuelve dependiente a la integración en las actividades de la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere

principalmente el apoyo de la alta dirección, así como de sus diferentes partes interesadas.

Adicionalmente, esta norma establece la base para la planificar y tomar decisiones estratégicas, lo que permite aumentar la probabilidad del cumplimiento de los objetivos estratégicos de la Universidad. Sus principales beneficios son:

- Identificar riesgos, causas, efectos y oportunidades.
- Integrar los procesos de la Universidad.
- Aumentar la confianza de las partes interesadas.
- Disminuir o prácticamente desaparecer incidentes inesperados
- Asignar y ejecutar recursos minimizando las posibles pérdidas de estos.
- Cumplir con las exigencias legales y reglamentarias, además de las normas internacionales.

3.6. ISO 19011:2018 Directrices para la auditoría de los sistemas de gestión

La norma ISO 19011: 2008 establece las directrices para una correcta auditoria a los sistemas de gestión, permitiendo evaluar de manera independiente y objetiva los procesos académicos y administrativos, asegurando el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información.

4. Fundamentación jurídica

Para la elaboración de la política se tomó la fundamentación jurídica algunos referentes nacionales, tales como el Gobierno Colombiano a través del Ministerio de Educación Nacional, Ministerio de TIC y organismos articulados a nuestro que hacer institucional. Estos se enumeran a continuación:

4.1. Fundamentos Jurídicos a nivel Nacional

- Constitución Política de Colombia 1991 Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. (Constitución Política de Colombia, 1991)
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor. “Sobre derechos de autor”. (Ley 23 de 1982, 1982)
- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado ‘de la protección de la información y de los datos’- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. (Ley 1273 de 2009, 2009)

- Ley 1581 de 2012. Congreso de la República. “Por la cual se regula el Régimen General de Protección de Datos”. (Ley 1581 de 2012, 2012)
- Decreto 1377 de 2013. “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”. (Ley 1377 de 2013, 2013)
- 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”. (Ley 1581 de 2012, 2012)
- Ley 1032 DE 2006. “Por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales”. (Ley 1032 de 2006, 2006)
- Decreto 1074 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”. (Ley 1074 de 2015, 2015)
- Circular externa 005. “Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única con el fin de incluir un país dentro de la lista de países contenida en dicho numeral, los cuales cuentan con un nivel adecuado de protección de datos personales de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio”. (Circular externa 005, s.f.)

4.2. Fundamentos Jurídicos a nivel Institucional

- Acuerdo 002 de 2008 de la Honorable Consiliatura, por la cual se ratifica el Estatuto Docente de la Universidad La Gran Colombia. Así mismo, es modificado por los Acuerdos números 003 del 10 de diciembre de 2014; 009 del 31 de octubre de 2017; 010, 011, 012 y 013 del 30 de noviembre de 2017; 001 del 23 de enero de 2018 y 003 del 15 de mayo de 2018 de la Honorable Consiliatura; 023 del 20 de noviembre de 2018 y 016 del 24 de septiembre de 2019 del Consejo Académico.
- Resolución 006 de 2009 de la Rectoría, por medio del cual se adopta el Modelo de Autoevaluación de la Universidad.
- Acuerdo 006 de 2011 del Consejo Académico, por el cual se expide el Reglamento Estudiantil de Posgrados.
- Resolución 17118 de 2014 de MEN, por el cual se ratifica la reforma estatutaria a la Universidad La Gran Colombia.
- Acuerdo 012 de 2015 del Consejo Académico, por el cual se expide el Reglamento Estudiantil de Pregrado.
- Proyecto Educativo Institucional (PEI) 2016 “Forjadores de la Nueva Civilización”.
- Plan Estratégico Institucional de Desarrollo (PEID) 2021 – 2027.

- Acuerdo 006 de 2020 de la Honorable Consiliatura, por medio del cual se adopta el Código de Ética y Buen Gobierno de la Universidad.
- Resolución 008 de 2020 de la Rectoría, por la cual se adoptan las políticas de tratamiento de la información y las tecnologías de la información y las telecomunicaciones de la Universidad.

5. Fundamentos institucionales

A través de las actividades institucionales, la Universidad La Gran Colombia busca fortalecer sus procesos de seguridad de la información en los procesos académicos y administrativos a través de la propuesta de los objetivos, propósitos y valores de la norma. A continuación, se listan los principios fundamentales del sistema de gestión de seguridad de la información.

5.1. Principios del Sistema de Gestión de Seguridad de la Información

La Política del Sistema de Gestión de Seguridad de la Información acoge todos los principios institucionales que centran la actuación de la comunidad académica en ser Cristianos, Bolivarianos, Hispánicos y Solidarios articulados con los sistemas de gestión y el quehacer institucional. Los principios por los que se rige esta política son:

- Integridad: Supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.
- Confidencialidad: Hace referencia a la necesidad de ocultar o mantener en secreto determinada información o recursos. Ello supone que la información sea accesible de forma única a las personas que se encuentran autorizadas, prevaleciendo siempre un proceso de control.
- Disponibilidad: supone que la información debe estar disponible para el usuario o sistema que lo requiera.
- Compromiso de las personas: Las personas competentes, empoderadas y comprometidas en toda la organización son esenciales para aumentar la capacidad de la organización para generar y proporcionar valor (Modelos de calidad: ISO 9000 vs EFQM 2020. Diferencias y alineación, 2020).
- Toma de decisiones basadas en la evidencia: Las decisiones basadas en el análisis y la evaluación de datos e información tienen mayor probabilidad de producir los resultados deseados (Modelos de calidad: ISO 9000 vs EFQM 2020. Diferencias y alineación, 2020).
- Trazabilidad: Conjunto de aquellos procedimientos que permiten conocer el histórico, la ubicación y la trayectoria de un producto.

- No repudio: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.
- Innovación: La Innovación es dar respuestas nuevas, significativamente diferentes a los retos de las Instituciones de Educación Superior. Mediante el pensamiento, la reflexión, la investigación, la gestión del conocimiento y del cambio, lograr con creatividad, apropiación de tecnologías emergentes y decisiones inteligentes; la creación, gestión y transferencia de nuevos o mejorados procesos y productos, que aporten interna y externamente al crecimiento, desarrollo, sostenibilidad; mayor productividad, competitividad y Prosperidad Social.
- Cumplimiento de la normativa legal: Articulado con toda la normatividad legal vigente a nivel gubernamental y de entes aseguradores que nos permitan la aplicación de las obligaciones, derechos y deberes en el sistema de gestión.
- Prevención: Busca que las acciones generadas en torno a cualquier proceso se dirijan a evitar o minimizar cualquier tipo de daño que se pueda presentar.
- Continuidad de negocio: Conjunto de procedimientos y medidas que adopta una organización para garantizar que las funciones esenciales puedan continuar durante y después de cualquier incidente, permitiendo que su operación no se vea afectada.

5.2. Valores del Sistema de Gestión de Seguridad de la Información.

Transparencia (Veraz, credibilidad, honestidad, Rendición de cuentas, Objetividad): capacidad de la institución para desarrollar sus actividades de manera visible, permitir el acceso a la información y rendir cuentas de manera veraz, oportuna y coherente con los principios y valores éticos de la Universidad.

- Integridad: Anteponer la honestidad y el compromiso ante las responsabilidades laborales.
- Autocritica: Tener la capacidad de analizar, cada cierto tiempo, las actividades y resultados de los procesos institucionales involucrados en el SGSI, de tal forma que se puedan evaluar las fortalezas y debilidades encontradas.
- Disciplina: Se relaciona con la puntualidad, seguir las normas, ser proactivo, proponerse alcanzar objetivos y ser exigente.

5.3. Objetivos de la política de seguridad de la Información.

Los objetivos de la política de seguridad de la información permiten promover la mejora continua en el sistema de gestión y garantizan una implementación eficaz en los

diferentes procesos de la universidad. A continuación, se presenta el objetivo general y los objetivos específicos del SGSI.

General

Consolidar un ambiente seguro que facilite la protección de los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, garantizando la confidencialidad, disponibilidad e integridad de la información, así como de la continuidad de los servicios que brinda la institución.

Objetivos específicos

- Establecer lineamientos y buenas prácticas en el marco de referencia para la gestión y toma de decisiones en la seguridad de la información de la Universidad.
- Fomentar una cultura organizacional orientada al tratamiento de los riesgos mediante campañas de sensibilización y capacitación a las diferentes partes interesadas.
- Planear e implementar estrategias orientadas a la mejora del Sistema de Gestión de Seguridad de la Información.
- Gestionar los riesgos y oportunidades de seguridad de la información permitiendo la continuidad de los procesos y el cumplimiento de los objetivos institucionales.
- Implementar estrategias de medición que permitan monitorear el cumplimiento de los requisitos de seguridad de la información.

6. Estrategias de implementación.

La estrategia de implementación de la política de Seguridad de la información articula sus partes interesadas fortaleciendo la colaboración, el apoyo y la determinación en las actividades de seguridad de la información en la institución. A continuación, se muestra la integración de las partes interesadas que permite a la Universidad La Gran Colombia a implementar y fomentar una cultura orientada a la gestión de los riesgos en los diferentes procesos institucionales.

Figura 2 Incorporación de las partes interesadas con las líneas de acción

Fuente: Sistemas de la información

6.1. Sistema de Gestión de seguridad de la información.

Un sistema de gestión de seguridad de la información es un conjunto de políticas, directrices y procedimientos orientados a la protección y el adecuado manejo de la información, garantizando siempre la confidencialidad, integridad y disponibilidad de los activos de información críticos en cada proceso.

Gestión de accesos a los sistemas de información

Gestionar de manera adecuada los accesos a los diferentes sistemas de información críticos que maneja la Universidad, para lo cual se definen criterios de seguridad que garanticen que el acceso a la información se realice estrictamente por la persona que se encuentra autorizada, asegurando así la Confidencialidad, Integridad y Disponibilidad de la información.

Los anteriores criterios se definen bajo la estructura de la norma ISO 27001:2013 (Norma ISO/IEC 27001:2013, 2013), abordando los controles del Anexo A y los subgrupos que se muestran a continuación:

- Requisitos del negocio para control de acceso

Establecer y documentar los procesos de control de acceso con base en los requisitos del negocio y de seguridad de la información, que permita garantizar el acceso de los usuarios a la red y a los servicios para los que hayan sido autorizados específicamente.

- Gestión de acceso de usuarios

Implementar estrategias que garanticen la correcta asignación, cancelación o ajuste de los derechos de acceso a cualquier sistema de información.

- Responsabilidades de los usuarios

Definir y socializar las responsabilidades frente al correcto uso de las credenciales de acceso a los sistemas de información.

- Control de acceso a sistemas y aplicaciones

Establecer una adecuada definición de roles para el acceso a los sistemas de información, manteniendo la respectiva segregación de funciones para cada cargo y evitando posibles accesos no autorizados a la información.

- Sistema de gestión de contraseñas

Apropiar la confidencialidad de la información, haciendo uso de lineamientos para una correcta gestión de contraseñas que permitan interactuar con los sistemas de aplicación y permitan la recuperación o asignación de las mismas.

- Inicio de sesión seguro:

Garantizar que las plataformas tecnológicas realicen una validación de datos de entrada donde permita certificar que los datos recolectados y procesados sean correctos y apropiados, como la confirmación de tipos, los formatos, las longitudes, la pertinencia, la cantidad, el uso.

- Control de acceso a información personal sensible:

Definir disposiciones específicas que garanticen el correcto tratamiento de los datos sensibles recolectados y almacenados por la Universidad, en cumplimiento de sus funciones institucionales.

A continuación, en la figura 3 Fases de gestión de accesos, se muestran las fases de la gestión de accesos a los sistemas de información:

Figura 3 Fases de gestión de accesos.

Fuente: Sistema de la información

- Registro: Cada usuario que requiera el acceso a un sistema de información lo debe solicitar por medio del aplicativo Help Desk.
- Verificación: La Dirección de Sistemas de la Información analiza la solicitud con el fin de identificar si es viable asignar el permiso de acceso que solicita el funcionario.
- Validación: Seguridad de la Información realiza validaciones que pretenden identificar si la matriz de perfiles se encuentra debidamente diligenciada, así como si los cambios registrados por sistemas de la información se encuentran autorizados por el jefe directo.
- Aplicación: La Dirección de Sistemas de la información aplica los permisos inicialmente solicitados en el sistema toda vez que seguridad de la información confirme la matriz de perfiles y su correcto diligenciamiento.
- Evaluación: Se monitorean de forma periódica los accesos autorizados vs los aplicados en cada sistema, identificando posibles accesos no autorizados o inconsistencias sobre la asignación de perfiles.

Gestión de incidentes SI

En cuanto a la gestión de incidentes el proceso determina una adecuada gestión de incidentes y eventos de seguridad de la Información por parte del responsable, con el objetivo de obtener respuestas rápidas y eficaces ante cualquier evento que ponga en riesgo la información de la Universidad. Todo esto abordando lo establecido en la norma y que se encuentra descrito en el documento Manual de Lineamientos de Seguridad de la Información de la Universidad La Gran Colombia.

Figura 4 Fases de gestión de incidentes de Seguridad de la Información

Fuente: Sistemas de la información.

Gestión de activos de la información

En la protección de los activos de información de cada proceso institucional se busca soportarlo en un inventario actualizado, consistente y con la clasificación correspondiente según el modelo definido con la Unidad de Archivo General e Histórico, permitiendo dar cumplimiento a lo descrito en la norma y a los objetivos mencionados a continuación:

- Responsabilidad por los activos

Gestionar la identificación, el uso y la disposición final de los activos de información, definiendo estrategias que permitan orientar a los usuarios sobre el manejo aceptable de los mismos y garantizando que sean de uso exclusivo para la ejecución de actividades definidas en el rol de cada funcionario.

- Clasificación de la información

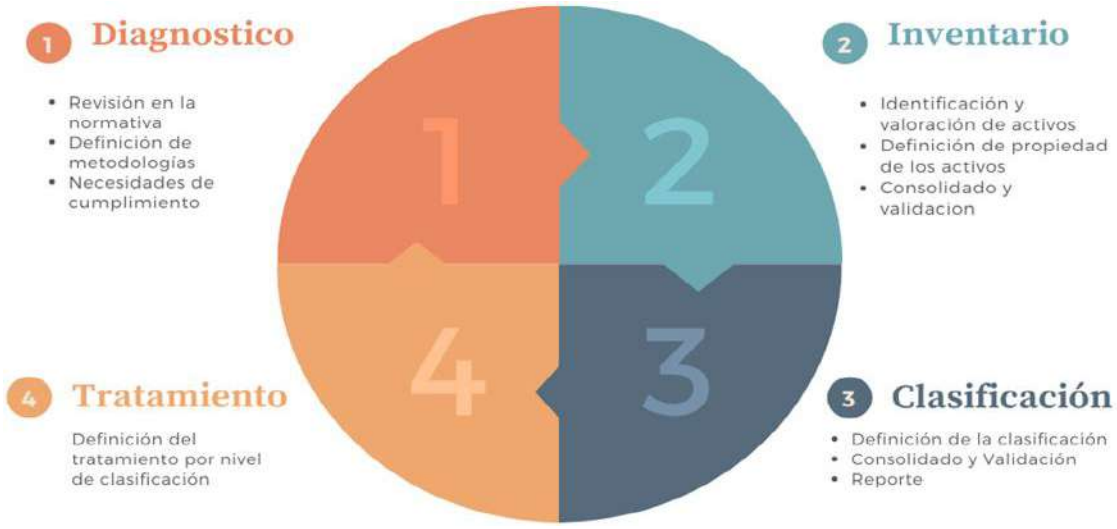
Preservar la confidencialidad e integridad de la información realizando de forma coherente la clasificación de los activos de información en función de su sensibilidad y criticidad para la Universidad.

- Manejo de los medios

Garantizar el adecuado manejo de los medios de almacenamiento de información tales como USB´s o discos duros que son utilizados en los diferentes procesos de la universidad, elaborando procedimientos de borrado seguro que permitan proteger información contra amenazas internas o externas.

A continuación, en la figura 5 Proceso de gestión de activos, se muestran las fases de la gestión de accesos a los sistemas de información:

Figura 5. Proceso de gestión de activos.



Fuente: Sistemas de la información.

7. Los actores de la política

Los actores de la política son todos aquellos individuos que intervienen directa o indirectamente con el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la información. A continuación, se establecen los actores de la política de seguridad de la información:

- Estudiante: De acuerdo con el reglamento estudiantil, artículo 31 el estudiante es la persona que, cumpliendo con los requisitos de admisión, se matricula para cursar un programa o un curso de extensión en la Universidad. (Reglamento Estudiantil, 2020)
- Profesor: Según lo definido por el Decreto 1278 de 2002 en su artículo 5 un docente es la persona que desarrolla labores académicas directa y personalmente con los estudiantes. Estos también son responsables de las actividades curriculares no lectivas complementarias de la función docente de aula, entendidas como administración del proceso educativo, preparación de su tarea académica, investigación de asuntos pedagógicos, evaluación, calificación, planeación, disciplina y formación de los alumnos, reuniones de profesores, dirección de grupo, actividades formativas, culturales y deportivas, atención a los padres de familia y acudientes, servicio de orientación estudiantil y actividades vinculadas con organismos o instituciones del sector que incidan directa o indirectamente en la educación (Art.5 Decreto 1278, 2002, Junio 19).
- Directivo: Es la persona encargada “formalmente” de la unidad organizacional. Esta autoridad formal le confiere un estatus especial dentro de la estructura de la Empresa ante funciones interpersonales, informativas y decisorias.

- Administrativo: Empleado o funcionario de una Empresa privada u organismo público que trabaja en tareas de administración o gestión y trabaja en una oficina.
- Aliados empresariales: Son personas naturales o jurídicas con las que se pueden llegar a tener acuerdos comerciales para lograr un objetivo individual o común para beneficio de ambas partes.
- Aliados académicos: Son lazos entre personas, IES o entidades para lograr propósitos comunes en caminados al mejoramiento de la calidad académica, a través de convenios estratégicos.
- Egresado: Persona natural que ha cursado y aprobado satisfactoriamente la totalidad del plan de estudios reglamentado para un programa o carrera, pero que aún no ha recibido el título académico (Glosario Ministerio de Educación Nacional, s.f.)
- Superintendencia de Industria y Comercio (SIC): La Superintendencia de Industria y Comercio es la autoridad nacional de protección de la competencia, los datos personales y la metrología legal, protege los derechos de los consumidores y administra el Sistema Nacional de Propiedad Industrial a través del ejercicio de sus funciones administrativas y jurisdiccionales.
- Ministerio de Tecnologías de la Información y las Comunicaciones: De acuerdo a la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones y a sus beneficios.

7.1. Roles del Sistema de Gestión de Seguridad de la Información.

Todo el equipo de la Universidad La Gran Colombia es responsable de la seguridad de la información, no obstante, existen varios roles y responsabilidades específicas dentro del SGSI, las cuales se presentan a continuación:

- Alta dirección
  - Aprobar la política de seguridad y privacidad de la información.
  - Promover la gestión de la seguridad de la información mediante el compromiso de la dirección y la asignación de los recursos adecuados.
  - Estudiar y aprobar las iniciativas de seguridad de la información que le sean propuestas.
- Responsable del funcionamiento del SGSI

El responsable del funcionamiento del SGSI en la Universidad La Gran Colombia es el director de Sistemas de la Información. Sus principales responsabilidades son:

- Asegurar la disponibilidad de los recursos necesarios para la definición, la implementación y el mantenimiento del SGSI.
- Revisar periódicamente los documentos y controles del SGSI para asegurar que el sistema logre los resultados previstos.
- Definir lineamientos que den guía al oficial de seguridad de la información.

- Ingeniero de seguridad informática:

Es un encargado designado por el responsable del funcionamiento del SGSI. Sus principales responsabilidades son:

- Coordinar con los propietarios de los activos de información y los dueños de procesos las acciones para el cumplimiento del SGSI.
- Hacer el seguimiento a la implementación y el cumplimiento de los controles de seguridad en la Universidad La Gran Colombia.
- Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al SGSI.
- Liderar el proceso de gestión de incidentes de seguridad de la información en la Universidad La Gran Colombia.

- Propietario de los activos de información

Es el funcionario, tercero o área de la Universidad La Gran Colombia al que se le asignó la responsabilidad formal sobre un activo de información. Sus principales responsabilidades son:

- Cumplir con la política de seguridad de la información aprobada por el Comité de Seguridad de la Información.
- Identificar y establecer el alcance, el valor o la criticidad de los activos de información de los cuales es propietario.
- Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos, aprobada por el responsable del funcionamiento del SGSI.
- Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.
- Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.
- Informar las demandas y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.
- Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

- Custodio de los activos de información

Es el funcionario, tercero o área de la Universidad La Gran Colombia responsable de hacer efectivos los controles que el propietario del activo de la información haya definido. Sus principales responsabilidades son:

  - Implementar y mantener los controles requeridos en los medios donde se encuentren almacenados los activos de información que se encuentren a su cargo.
  - Administrar los recursos donde residen los activos de información, dando los permisos definidos por el propietario del activo a los usuarios interesados.
  - Proteger los activos de información presentes en los medios a su cargo en la situación que corresponda: almacenamiento, transporte y procesamiento.

- Responsable del proceso

Es el funcionario, tercero o área de la Universidad La Gran Colombia al cual se le asignó la responsabilidad sobre un proceso de la entidad. Sus principales responsabilidades son:

  - Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.
  - Validar los activos de información identificados, junto con las características básicas de cada uno de ellos.
  - Apoyar y validar la identificación y designación de los propietarios de los activos de información de su proceso.

- Usuario de la información:

Se define como el funcionario o tercero de la Universidad La Gran Colombia que utiliza la información para desempeñar sus funciones diarias. Sus principales responsabilidades son:

  - Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera de la Universidad La Gran Colombia.
  - Conocer la clasificación de los activos de información que maneja.
  - Preservar la seguridad de la información utilizada en el desempeño de sus funciones y obligaciones.
  - No divulgar la información clasificada sin autorización del propietario del activo de información.
  - Procurar el buen manejo de todos los activos, protegiéndolos en relación con los principios de seguridad.

8. Comité de seguridad de la información

El comité se encarga de determinar las estrategias para el desarrollo del Sistema de Gestión de Seguridad de la Información garantizando que se cumplan los lineamientos

y objetivos establecidos, para nuestro sistema de gestión establecemos dos comités principales los cuales se describirán a continuación.

8.1. Comité Institucional de Seguridad de la Información

En el marco de las actividades relacionadas con la seguridad de la información, el Sistema de Gestión de Seguridad de la Información opera a través de las estrategias definidas en el Comité Institucional de Seguridad de la Información.

A continuación, se definen los objetivos del comité institucional de seguridad de la información:

Objetivo del Comité Institucional de Seguridad de la Información

Evaluar las estrategias para el desarrollo del Sistema de Gestión de Seguridad de la Información, determinando y garantizando que se cumplan los lineamientos y los objetivos establecidos.

En la Tabla 2 se definen los cargos que participaran en el comité institucional de seguridad de la información.

Tabla 2 Integrantes del Comité Institucional de Seguridad de la Información

Sede Bogotá	Seccional Armenia
• Rector o delegado • Secretario Académico • Vicerrector de Desarrollo Académico • Vicerrector de Innovación y Empresarismo • Vicerrector de Gestión Financiera • Director Nacional de Sistema de la Información • Representante de los Decanos • Representante de los administrativos • Representante de seguridad física	• Rector delegatario o delegado • Secretario Académico • Vicerrector de Desarrollo Académico • Jefe departamento de Informática • Representante de los Decanos • Representante de los administrativos • Representante de seguridad física

Fuente: Sistemas de la información

Funciones del Comité Institucional de Seguridad de la Información

- Proponer políticas, estrategias y actividades encaminadas la seguridad de la información de los Activos de la Universidad.
- Evaluar y aprobar las iniciativas sobre seguridad de la información.
- Prevenir pérdidas mayores o que comprometan los activos de información.

- Velar por el cumplimiento de los estándares de seguridad establecidos por la Superintendencia de Industria y Comercio.
- Promover el apoyo a la Seguridad de la Información dentro de la Organización, así como también, coordinar el proceso de administración de la continuidad de las actividades.
- Hacer seguimiento a los indicadores establecidos dentro del SGSI verificando su correcto cumplimiento.
- Fomentar la apropiación de la cultura de la seguridad de la información en todas las dependencias y en los miembros que conforman la comunidad académica.
- Aprobar las principales iniciativas para incrementar la Seguridad de la Información de acuerdo con las competencias y responsabilidades asignadas a cada gerencia, así como acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

8.2. Comité Operativo de Seguridad de la Información

La gestión de la seguridad de la información al interior de los diferentes procesos de la Universidad se organiza y orienta en el marco del Comité Operativo de Seguridad de la Información, el cual siempre actúa en articulación con las orientaciones emanadas por el Comité Institucional de Seguridad de la Información y la Dirección de Sistemas de la Información.

Objetivo del Comité Operativo de Seguridad de la Información

Contribuir por el cumplimiento de las actividades de seguridad de la información de cada proceso administrativo, académico e institucional, permitiendo así la generación de estrategias en la implementación y mejora continua.

En la Tabla 3 se definen los cargos que participaran en el comité operativo de seguridad de la información.

Tabla 3 Integrantes del comité operativo de seguridad de la información.

Seccional Bogotá	Seccional Bogotá
● Director Nacional de Sistemas de la Información ● Coordinador de Infraestructura Tecnológica ● Ingeniero de Seguridad Informática ● Ingeniero de centro de datos ● Webmaster ● Técnico de soporte	● Jefe del departamento de Informática ● Ingeniero sistemas de información ● Ingeniero de redes y telecomunicaciones ● Ingeniero soporte técnico

Fuente: Sistemas de la información

Funciones del Comité Operativo de Seguridad de la Información

A continuación, se definen cuáles son las funciones del comité operativo de seguridad de la información.

- Definir proyectos de tecnología que impliquen la aplicación de Seguridad de la Información en el contexto del negocio (Servicio, Producto e Información).
- Generar informes de actividades en el marco de la Seguridad de la Información para ser presentadas ante el Comité Institucional de Seguridad de la Información.
- Emanar las orientaciones desde el Comité Institucional de Seguridad de la Información y la Dirección de Sistemas de la Información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la institución frente a posibles amenazas, sean internas o externas.
- Evaluar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios de la institución, sean preexistentes o nuevos.
- Elaborar el plan anual de actividades del Comité Operativo de Seguridad de la Información con su respectivo cronograma, hacer seguimiento del plan y establecer los correctivos necesarios.
- Validar y aprobar las nuevas iniciativas englobadas en el marco de Seguridad de la Información
- Realizar el seguimiento al desarrollo de las actividades de Seguridad de la Información en los procesos académicos y administrativos, proponiendo los correctivos necesarios.
- Gestionar la asignación de recursos a las metas trazadas para el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información.
- Socializar los resultados derivados de los diferentes indicadores trazados dentro del SGSI.
- Informar periódicamente al Comité Institucional de Seguridad de la información y la Dirección de Sistemas de la información sobre el desarrollo de sus labores.

9. Seguimiento y evaluación

El seguimiento y la evaluación del cumplimiento de las estrategias de la política de seguridad de la información a través de las siguientes actividades:

9.1. Seguimiento y acciones

Se busca enmarcar diferentes acciones encaminadas a fortalecer la Política de Seguridad de la información y el Sistema de Gestión de Seguridad de la Información en cada una de las etapas teniendo en cuenta los recursos físicos, financieros y tecnológicos, razón por la cual se definen las siguientes líneas de acción.

Línea de acción: Gestión de accesos a los sistemas de información.

Este proceso busca gestionar los accesos a los sistemas de información promoviendo buenas prácticas de todos los usuarios. Por tal motivo se despliegan diferentes objetivos en el cumplimiento de las actividades que fortalecen el acceso a los sistemas de información de la UGC, a saber:

- Evaluar la asignación de permisos en los Sistemas de información críticos de la Universidad, teniendo en cuenta la periodicidad determinada en el proceso
- Validar el cumplimiento de los lineamientos de Seguridad de la Información definidos en el documento para la gestión de activos de la información, mediante auditorias o revisiones planificadas a intervalos regulares.
- Revisar los lineamientos de seguridad de la información, garantizando que su contenido sigue vigente y alineado con las necesidades de la Institución.

Línea de acción: Gestión de incidentes Sistema de Información

En cuanto a la gestión de incidentes de sistema de la información busca atender los diferentes casos detectados a través de los sistemas de la UGC, promoviendo así elementos preventivos en el respaldo de las tecnologías. A continuación, se presentan los diferentes propósitos en el proceso:

- Evaluar el funcionamiento de las acciones y actividades realizadas dentro de la Gestión de incidentes de seguridad de la información.
- Validar el cumplimiento de los lineamientos definidos en el documento Manual de lineamientos de Seguridad de la Información para la gestión de activos de la información, mediante auditorías o revisiones planificadas a intervalos regulares.
- Revisar de forma periódica los lineamientos de seguridad de la información, garantizando que su contenido sigue vigente y está alineado con las necesidades de la Institución.

Línea de acción: Gestión de activos de la información.

La gestión de activos de la información busca garantizar un adecuado uso de la información crítica utilizada en cada proceso, resaltando los componentes más

importantes de cada activo y fortaleciendo las estrategias de seguridad para prevenir cualquier materialización de riesgo que se puedan presentar, tales estrategias implican:

- Establecer mecanismos que permitan mejoras en el proceso de identificación de Activos de información en las diferentes áreas de la Universidad.
- Solicitar de forma periódica la actualización de los Inventarios de Activos de información, garantizando la vigencia de estos en cada proceso.
- Validar el cumplimiento de los lineamientos definidos en el documento Manual de Lineamientos de Seguridad de la Información para la gestión de activos de la información, mediante auditorías o revisiones planificadas a intervalos regulares.

9.2. Indicadores estratégicos

A continuación, se presentan los diferentes indicadores que dan respuesta a los previsto en la normatividad legal vigente que pretende demostrar la implementación y resultados e implementación de las estrategias.

En la Tabla 4. Indicadores de la Política, se pueden ver los indicadores junto con su estrategia, línea de acción y responsable.

Tabla 4 Indicadores de la Política.

Denominación	Nombre del Indicador	Estrategia	Línea de Acción	Área Responsable del Indicador
Identificar el nivel de cultura de seguridad en los administrativos, docentes y terceros de la Universidad de La Gran Colombia.	Sensibilización de Seguridad de la Información.	Realizar Campañas de sensibilización a las partes involucradas en el proceso para evaluar el conocimiento en seguridad de la información.	Gestión de incidentes Gestión de Activos de información	Talento humano Sistemas de la información
Identificar el nivel de cumplimiento de los lineamientos de seguridad de la información en cada proceso.	Nivel de implementación del SGSI.	Medir el cumplimiento de los lineamientos establecidos dentro del marco de gestión de la Seguridad de la información.	Gestión de incidentes Gestión de Activos de información	Sistemas de la información

Denominación	Nombre del Indicador	Estrategia	Línea de Acción	Área Responsable del Indicador
			Gestión de control de acceso a los sistemas de información	
Hacer seguimiento a la gestión de incidentes.	Incidentes de seguridad de la información.	Realizar un análisis de la gestión de incidentes de seguridad de la información.	Gestión de incidentes	Sistemas de la información
Identificar el compromiso de los procesos con la gestión de riesgos.	Gestión de riesgos de seguridad de la información.	Medir el cumplimiento de las actividades definidas durante la identificación del riesgo.	Gestión de incidentes Gestión de Activos de información Gestión de control de acceso a los sistemas de información	Sistemas de la información
Gestión de la remediación de vulnerabilidades técnicas encontradas en el proceso de análisis.	Vulnerabilidades	Medir el cumplimiento de la remediación de vulnerabilidades técnicas.	Gestión de incidentes Gestión de Activos de información Gestión de control de acceso a los sistemas de información	Sistemas de la información

Fuente: Sistemas de la información

10. Compromisos de la Alta Dirección

Para lograr lo anterior, la alta dirección se compromete a impulsar el cumplimiento de la política entre las partes interesadas y en todos sus lugares de desarrollo destinando los recursos necesarios para la mejora continua y la sostenibilidad del Sistema de Gestión de Seguridad de la Información SGSI. Tal política está a disposición de las partes interesadas y del público en general propio a la Universidad la Gran Colombia y está sujeta a revisión periódica.

_____

Firma
Rector
Universidad La Gran Colombia
Fecha: dd/mm/aaaa

BIBLIOGRAFÍA

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2013). Norma Técnica Colombiana NTC-ISO 27001 técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI). requisitos. [Archivo PDF]. http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2018). Norma Técnica Colombiana NTC-ISO 31001 Gestión de Riesgos. Directrices. [Archivo PDF]. http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf

ISO. (7 de marzo de 2021). ISO is an independent, non-governmental international organization with a membership of 165 national standards bodies. https://www.iso.org/about-us.html

ISOTools. (7 de marzo de 2021). Sistemas de Gestión de Riesgos y Seguridad. https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301/

ISOTools. (7 de marzo de 2021). ISO 27001: Pilares fundamentales de un SGSI. . https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

Ministerio De Ciencia, Tecnología e Innovación. (2020). MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. https://minciencias.gov.co/sites/default/files/ckeditor_files/D103M01%20Manual%20Pol%C3%ADticas%20Seguridad%20y%20Privacidad%20Informaci%C3%B3n%20V00.pdf

Ministerio de Educación Nacional. (s. f.). Glosario Ministerio de Educación Nacional. https://www.mineducacion.gov.co/1621/article-136473.html#:~:text=%2D%20EGRESADO&text=Persona%20natural%20que%20ha%20cursado,ha%20recibido%20el%20t%C3%ADtulo%20acad%C3%A9mico

Ministerio de Tecnologías de la información y las comunicaciones. (7 de marzo de 2021). Acerca del MinTIC.https://www.mintic.gov.co/portal/inicio/Ministerio/Acerca-del-MinTIC/

Organización Internacional de Normalización (ISO). (2018). Norma Internacional ISO 19011 Directrices para la auditoría de los sistemas de gestión [Archivo PDF]. https://www.cecep.edu.co/documentos/calidad/norma-iso-19011-2018.pdf .

Superintendencia de industria y comercio. (7 de marzo de 2021). Misión y Visión. https://www.sic.gov.co/mision-y-vision.

Universidad La Gran Colombia. (7 de marzo de 2021). Misión Institucional. https://www.ugc.edu.co/sede/bogota/index.php/mision

Universidad La Gran Colombia. (7 de marzo de 2021). Visión Institucional. https://www.ugc.edu.co/sede/bogota/index.php/vision

Universidad La Gran Colombia. (7 de marzo de 2021). Valores. https://www.ugc.edu.co/sede/bogota/index.php/valores

Fiscalía General de la Nación (7 de marzo de 2021). ESTADÍSTICA DE DENUNCIAS POR DELITOS. https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

ISOTools. (2020). Modelos de calidad: ISO 9000 vs EFQM 2020. https://www.isotools.org/2020/02/28/modelos-de-calidad-iso-9000-vs-modelo-efqm-2020-diferencias-y-alineacion/

UNIVERSIDAD LA GRAN COLOMBIA

CONSILIATURA

A C U E R D O N°. 007

28 de julio de 2021

Por el cual se aprueban las Políticas Institucionales de la Universidad La Gran Colombia

LA HONORABLE CONSILIATURA

de la UNIVERSIDAD LA GRAN COLOMBIA, en uso de las facultades y atribuciones legales y estatutarias, en especial, los numeral 2, 3 y 4 del Artículo 21 de los Estatutos de la Universidad, ratificados por la resolución N° 001159 de fecha del 21 de enero de 2021 del Ministerio de Educación Nacional que la faculta para *"Desarrollar las políticas administrativas y financieras de la Universidad (...) Dictar los reglamentos generales de la Universidad y los especiales de carácter administrativo y financiera"* y,

C O N S I D E R A N D O

Que la Constitución Política, en el artículo 69, garantiza la autonomía universitaria y establece que las universidades podrán darse sus directrices y regirse por sus propios estatutos de acuerdo con la Ley.

Que la Ley 30 de 1992 desarrolla los alcances de la autonomía universitaria y regula la educación superior en los aspectos generales de los programas académicos.

Que la Ley 30 de 1992, en los artículos 53, 54 y 55, creó el Sistema Nacional de Acreditación e información para las Instituciones de Educación Superior cuyo objetivo es garantizar a la sociedad que las instituciones que hacen parte del sistema cumplen con los más altos requisitos de calidad; por su parte, el Consejo Nacional de Acreditación - CNA estableció que la autoevaluación institucional es un proceso inherente a la educación superior y una tarea permanente en las instituciones de educación superior que fundamentan su actuación en el mejoramiento continuo y en la gestión de la calidad académica.

Que la Ley 1188 de 2008 regula el registro calificado de los programas de educación superior y Se dictan otras disposiciones

Que el Decreto 1075 de 2015 modificado por el Decreto 1330 de 2019, establece la necesidad contar y fortalecer las Políticas que orienten el desarrollo administrativo y académico para orientar las funciones de la Universidad.

Que el Decreto 1075 de 2015 modificado por el Decreto 1330 de 2019, en su artículo 2.5.3.2.3.1.4, establece la estructura administrativa y académica como una de las condiciones institucionales de calidad necesarias para el otorgamiento de registros calificados y gestión a nivel institucional.

Que la Resolución 015224 de 2020 regula los parámetros de autoevaluación, verificación y evaluación de las condiciones de calidad de carácter institucional reglamentadas en el Decreto 1075 de 2015, modificado por el Decreto 1330 de 2019, para la obtención y renovación del registro calificado.

Que el Decreto 1330 de 2019 en su Artículo 2.5.3.2.1.1, define la calidad como el conjunto de atributos articulados, interdependientes, dinámicos, construidos por la comunidad académica como referentes y que responden a las demandas sociales, culturales y ambientales. Dichos atributos permiten hacer valoraciones internas y externas a las Instituciones, con el fin de promover su transformación y el desarrollo permanente de sus labores formativas, académicas, docentes, científicas, culturales y de extensión.

Que según el artículo 21 de los Estatutos de la Universidad, ratificados por la resolución N° 001159 de fecha del 21 de enero de 2021 del Ministerio de Educación Nacional, corresponde la Honorable Consiliatura de la Universidad Desarrollar las políticas administrativas y financieras de la Universidad, velar por la buena marcha de la Universidad, dictar los reglamentos generales de la Universidad y los especiales de carácter administrativo y financiero.

Que en atención a las necesidades identificadas para la implementación del Decreto 1330 de 2019, la Universidad La Gran Colombia priorizó el proceso de construcción de una visión conjunta de calidad y del sistema interno de aseguramiento de la calidad, a través de ejercicios participativos de reflexión con la comunidad académica. Dichos encuentros permitieron consolidar la estructura, la identidad, el reconocimiento de las estrategias y líneas de acción, entre otros, en las que se deben enmarcar los procesos de gestión en atención al mejoramiento continuo propio de la Institución.

Que las Políticas Institucionales referenciadas a continuación contaron con escenarios de reflexión y construcción en el marco de los órganos colegiados de los Consejos de Facultad de cada una de las unidades académicas de la Universidad:

1. Política Institucional de Gestión de la Infraestructura Física
2. Política Institucional de Gestión de Seguridad de la Información

3. Política de Gestión de la Infraestructura de las Tecnologías de la Información y las Comunicaciones
4. Política de Investigación, Desarrollo Tecnológico, Innovación y Creación Artística y Cultural
5. Política Institucional de Comunicación Estratégica y Marca
6. Política Institucional de Internacionalización
7. Política Institucional de Permanencia y Graduación Soy y Seré UGC

Política Institucional de Gestión de la Infraestructura Física

Que la Universidad La Gran Colombia cuenta con el respaldo y compromiso de los directivos para la creación de una política institucional que permita la planificación, ejecución, seguimiento y control de la infraestructura física de la universidad a nivel nacional, buscando la consolidación de propuestas vanguardistas en el diseño y la construcción de nuevas estructuras inteligentes, sostenibles e inclusivas, articuladas a los requerimientos de la comunidad educativa.

Que, desde su planeación, los proyectos de infraestructura física de la Universidad son concebidos de tal forma que respondan a las condiciones de funcionabilidad, espacialidad, inclusión, garantía de movilidad de manera segura, eficiencia y preservación del patrimonio arquitectónico y urbanístico del sector en donde se encuentren ubicadas en las sedes de la institución, dando cumplimiento a las normas y procedimientos que reglamenten su uso y conservación.

Que en la búsqueda de niveles óptimos de confort para el disfrute de los espacios por parte de la comunidad educativa grancolombiana, las acciones institucionales están orientadas al mejoramiento progresivo de la infraestructura, y a garantizar el control de los aspectos ambientales y sus impactos asociados.

Que los ejes estratégicos del PEID, persiguen consolidar entornos diferenciales de enseñanza, invertir recursos operacionales en proyectos de infraestructura, expandir la infraestructura de la universidad a nivel nacional y complementar el avance y los programas de permanencia de la presencia regional de nuevos programas y nuevas modalidades de formación, garantes de sostenibilidad y transformación digital.

Que el Decreto 1330 de 2019 en el artículo 2.5.3.2.3.1.7, refiere la existencia, gestión y dotación de los recursos tangibles e intangibles que le permiten desarrollar a la institución sus labores formativas, académicas, docentes, científicas, culturales y de extensión, teniendo en cuenta criterios arquitectónicos, urbanísticos, ambientales, paisajísticos y de innovación, que

vayan en concordancia y garanticen los procesos orientados a cumplir con los ejes misionales de la institución.

Política Institucional de Gestión de Seguridad de la Información

Que la Universidad La Gran Colombia reconoce la importancia de la información, como uno de sus activos más preciados, por lo cual proporciona los recursos necesarios para su adecuada gestión en términos de integridad, disponibilidad y confidencialidad.

Que desde el año 2020, La Universidad La Gran Colombia ha optado por fortalecer la seguridad de la información en cada proceso institucional, implementando un Sistema de Gestión de Seguridad de la información que permita servir como marco de control y referencia para la ejecución segura de las actividades misionales, de apoyo, estratégicas y de evaluación.

Que mediante las leyes 1581 de 2012 y 1712 de 2014, se establecen disposiciones generales para la protección de datos personales y se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública Nacional respectivamente.

Que la Ley 1581 del 2012 en el artículo 19 y el procedimiento de Registro Nacional de Bases de datos frente a la Superintendencia de Industria y Comercio, solicita la creación, ejecución y continuo monitoreo de medidas de seguridad que garanticen la protección adecuada de la información utilizada en los procesos institucionales de la Universidad La Gran Colombia.

Política de Gestión de la Infraestructura de las Tecnologías de la Información y las Comunicaciones

Que la institución desde mediados del 1980 apoyó sus procesos académicos y administrativos en las tecnologías de la información y la comunicación orientando su política de infraestructura de la tecnología a brindar un servicio de disponibilidad integridad y proyección tecnología de esta.

Que la Universidad La Gran Colombia cuenta con una infraestructura tecnológica amplia y suficiente para el correcto desarrollo de las actividades académicas y administrativas, infraestructura que es gestionada a través de la adquisición, actualización e implementación de los recursos tecnológicos necesarios para atender sus procesos.

Que mediante las leyes 1581 de 2012 y 1712 de 2014, se establecen disposiciones generales para la protección de datos personales y se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública Nacional respectivamente.

Que el Decreto Único Reglamentario del Sector de Tecnologías de la información y las Comunicaciones define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

Que mediante la Ley 1341 de 2009. "Por la cual se definen 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".

Que la institución considera pertinente realizar la modernización de la infraestructura tecnológica, los sistemas de información, los recursos de hardware y los recursos de software de acuerdo con las necesidades de la comunidad académica y promueve su aprovechamiento para fortalecer cada vez más los procesos académicos y administrativos.

Que se hace necesario fortalecer la apropiación de lo dispuesto en la 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 base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

Que se hace necesario fortalecer la apropiación de lo dispuesto en la Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Política de Investigación, Desarrollo Tecnológico, Innovación y Creación Artística y Cultural

Que la Universidad debe proyectarse como escenario para la formación de una mejor ciudadanía, aliada con el Estado, las empresas, la sociedad civil y las comunidades.

Que a través de la investigación la Universidad cumple con el propósito de brindar formación integral y permanente a todos los miembros de su comunidad académica.

Que la investigación es uno de los cinco ejes estratégicos contemplados en el Plan Estratégico Institucional de Desarrollo, PEID 2021-2027.

Que el eje estratégico de investigación se muestra en el PEID 2021-2027 como una apuesta clara por la generación de nuevo conocimiento, de producto de investigaciones aplicadas en las que participa toda la comunidad y que se desprenden de un amplio y flexible proceso de formación para la investigación, en la que participen profesores, estudiantes y la administración.

Política Institucional de Comunicación Estratégica y Marca

Que la Universidad la Gran Colombia reconoce como pilar de su proyección, la construcción de un acertado modelo de gestión estratégica desde la comunicación, el posicionamiento de marca y la proyección comercial de la oferta académica como generadores de valor académicos y productivos para el país y la región.

Que la proyección es uno de los cinco ejes estratégicos propuestos en el Plan Estratégico Institucional de Desarrollo, PEID 2021 -2027 en el que la Dirección de Comunicación Estratégica y Marca es un actor fundamental al visibilizar a la Universidad La Gran Colombia en el sector educativo a nivel nacional e internacional.

Que a través de la comunicación se genera repercusión positiva en los medios de comunicación, aliados, patrocinadores, grupos de interés, gobierno y opinión pública en general, logrando la participación de representantes de organizaciones y medios de comunicación en los eventos académicos y actividades dirigidos al posicionamiento de la Universidad.

Que mediante las estrategias de comunicación, difusión y posicionamiento de marca se fortalezca la estrategia comercial que genere un crecimiento en el número de estudiantes en pregrado, posgrado y formación continuada.

Que por medio de las acciones de comunicación se fortalezca la comunicación interna y el orgullo de marca entre directivos, colaboradores, estudiantes, docentes y egresados a través de los diferentes medios y canales.

Política Institucional de Internacionalización

Que la internacionalización es un proceso que fomenta los lazos de cooperación e integración de las Instituciones de Educación Superior con sus pares en otros lugares del mundo, con el fin de alcanzar mayor presencia y visibilidad internacional en un mundo cada vez más globalizado.

Que el Ministerio de Educación Nacional resalta la necesidad de establecer mecanismos para la articulación y desarrollo de las labores formativas, académicas, docentes, científicas, culturales y de extensión de las instituciones para promover de manera eficiente y eficaz la regionalización, equidad e inclusión, la internacionalización, la movilidad de estudiantes y profesores.

Que la Universidad La Gran Colombia tiene como eje estratégico el desarrollo de la internacionalización, definiéndola como "una visión global que impacte todas las disciplinas y que se construya a partir de experiencias internacionales y activa participación en redes académicas, empresariales, gremiales y organismos multilaterales.

Que la Política de Internacionalización de la Universidad La Gran Colombia se inscribe en el contexto regional, nacional e internacional y que debe estar acorde con las condiciones cambiantes del entorno desde lo legal, lo político y lo social, respondiendo a los nuevos enfoques, definiciones y dinámicas de la educación superior.

Política Institucional de Permanencia y Graduación Soy y Seré UGC

Que la universidad La Gran Colombia, en cumplimiento de los objetivos fundamentales de la Educación Superior construye, su perspectiva pedagógica como eje central de sus políticas institucionales, trabajando articuladamente con las áreas académica y administrativa, las cuales proporcionan las herramientas que promueven la sostenibilidad de la Política de permanencia y graduación, a través del acompañamiento, apoyo y servicios a los estudiantes, mediante el desarrolla de procesos formativos y la implementación de estrategias de intervención pertinentes en cada etapa del ciclo del estudiante en la educación superior, desde su ingreso hasta su graduación.

Que dichas estrategias se ejecutan en concordancia con sus principios institucionales desde una visión Cristiana, Bolivariana, Hispánica y Solidaria; cuyo fin se enfoca hacia la formación integral, perfeccionamiento de profesionales y cumplimiento del proyecto de vida de todos los estudiantes, en diferentes áreas del conocimiento para contribuir a la construcción de una civilización más humana y cristiana.

Que La Universidad La Gran Colombia entiende la permanencia y la graduación como el proceso de acompañamiento y apoyo al estudiante en el cumplimiento de su proyecto académico y personal, mediante el desarrollo de programas, planes e instrumentos en cada una de las etapas del proceso de formación, que van desde antes de su ingreso a la institución hasta después de su graduación.

UNIVERSIDAD LA GRAN COLOMBIA

Que La Universidad concibe la permanencia y graduación para sus estudiantes, como eje estratégico y transversal dentro de sus políticas institucionales, desarrollando y fortaleciendo a través de estrategias, una sana convivencia, un trato amigable reforzando el correcto y adecuado clima en la comunidad universitaria, creando modelos de mejoramiento continuo transversales e interdisciplinares en todos los niveles, y cuyo objetivo primordial es disminuir la tasa de deserción.

Que la Consiliatura de la Universidad aprobó Acuerdo No. 007 del 12 de mayo de 2020, la política de inclusión del sector social de menores recursos económicos, grupos minoritarios como parte importante de la política de Permanencia y Graduación.

Que el Consejo Académico de la Universidad La Gran Colombia Seccional Armenia aprobó mediante Acuerdo No 002 del 20 de marzo de 2013 la Política de Inclusión, Permanencia y Graduación Estudiantil en su segunda versión.

Que el Consejo Académico de la Universidad La Gran Colombia en sesión 15 de junio de 2021, realizó las reflexiones sobre las diferentes Políticas presentadas para su consideración.

Que la Universidad La Gran Colombia requiere adoptar las Políticas referidas anteriormente, garantizando el aseguramiento de la calidad institucional y de los programas académicos, el mejoramiento continuo y la excelencia académica, por lo tanto:

A C U E R D A:

ARTÍCULO PRIMERO: Aprobar las Políticas Institucionales relacionadas a continuación, las cuales fueron construidas en conjunto con la comunidad académica de la Universidad y presentadas a consideración del Consejo Académico:

1. Política Institucional de Gestión de la Infraestructura Física
2. Política Institucional de Gestión de Seguridad de la Información
3. Política de Gestión de la Infraestructura de las Tecnologías de la Información y las Comunicaciones
4. Política de Investigación, Desarrollo Tecnológico, Innovación y Creación Artística y Cultural
5. Política Institucional de Comunicación Estratégica y Marca
6. Política Institucional de Internacionalización
7. Política Institucional de Permanencia y Graduación Soy y Seré UGC

UNIVERSIDAD LA GRAN COLOMBIA

ARTÍCULO SEGUNDO: Los documentos de Políticas Institucionales adjuntas hacen parte integral del presente acuerdo y para su modificación deben ser discutidas por las partes interesadas y aprobadas por la Honorable Consiliatura de la Universidad.

ARTÍCULO TERCERO: Las Políticas Institucionales referidas en el Artículo Primero deben ser socializadas permanentemente con la comunidad académica que conforma la Universidad.

ARTÍCULO CUARTO: El presente Acuerdo rige a partir de la fecha de su aprobación y deroga todas las normas que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE,

En Bogotá, D.C, a los veintiocho (28) días del mes de julio de dos mil veintiuno (2021).

ABELARDO RAMÍREZ GASCA
Presidente Honorable Consiliatura

HÉCTOR HUGO TABARES RAMÍREZ
Secretario Honorable Consiliatura