Universidad Mariana
Res. MEN 1362 del 3 de febrero de 1983

Acreditada en Alta Calidad
VIGENCIA DE CUATRO AÑOS
Res. MEN 014045 del 19 de julio de 2022

ACUERDO 035
7 de diciembre de 2023

Por el cual se aprueba la Política de Seguridad de la Información de la Universidad Mariana

EL CONSEJO DIRECTIVO DE LA UNIVERSIDAD MARIANA
En uso de sus atribuciones legales y estatutarias y

CONSIDERANDO:

Que el Estado, de conformidad con la Constitución Política de Colombia en su artículo 69, garantiza la autonomía universitaria y vela por la calidad del servicio educativo a través del ejercicio de la suprema inspección y vigilancia de la educación superior. Las universidades podrán darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley.

Que la ley 1273 del 5 de enero de 2009, por medio de la cual se modifica el Código Penal, 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.

Que el documento Conpes 3995 del 1 de julio de 2020 - Política Nacional de Confianza y Seguridad Digital: "*Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías*".

Que la Universidad Mariana goza del principio constitucional de la autonomía, en conformidad con los principios y leyes que rigen la educación superior en Colombia, y se concibe como un derecho que favorece el libre intercambio de ideas, la búsqueda del conocimiento y la verdad, y como la capacidad para establecer sus propias reglas encaminadas a cumplir a cabalidad con su objetivo fundacional. PEI – 2023.

Que dentro de las funciones señaladas en el artículo 50 del Estatuto General, le corresponde al Consejo Administrativo y Financiero: orientar los planes, proyectos y actividades económicas, administrativas y financieras de acuerdo con lo establecido en los reglamentos de la universidad.

Que según el artículo 5, numeral 1, del Estatuto General, es función del Consejo Administrativo y Financiero, proponer y presentar al Consejo Directivo, las políticas relacionadas con la gestión administrativa y financiera de la universidad para su aprobación.

Que la Universidad Mariana siendo una institución de educación superior, católica y privada gestiona la seguridad de la información mediante la identificación, valoración y medición de los riesgos asociados a los activos de información que soporten la prestación de sus servicios de formación tanto presenciales como virtuales, donde se asegure la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentre bajo su responsabilidad y dominio.

Que es deber de la Universidad Mariana como institución de educación superior establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Universidad Mariana, en concordancia con su misión y propósitos institucionales en relación con la operación de sus procesos, objetivos estratégicos y los requisitos legales vigentes; al igual que la normatividad establecida por el Estado colombiano.

Que en mérito de lo expuesto,

ACUERDA:

ARTÍCULO PRIMERO: Aprobar la Política de Seguridad de la Información de la Universidad Mariana, según el documento que se adjunta al presente acuerdo como parte integral del mismo.

ARTÍCULO SEGUNDO: El presente Acuerdo rige a partir de la fecha.

COMUNÍQUESE Y CÚMPLASE

Dado en San Juan de Pasto, a los siete (7) días del mes de diciembre de dos mil veintitrés (2023).

UNIVERSIDAD MARIANA RECTORIA PASTO-NARIÑO

Hna. LILIANA ISABEL DÍAZ CABRERA, f.m.i.
Rectora

UNIVERSIDAD MARIANA SECRETARIA GENERAL SAN JUAN DE PASTO COLOMBIA

DORA LUCY ARCE HIDALGO
Secretaria General

Elaboró: Jonathan Almeyda Jácome, Consultor Externo

Revisó: Diana Mosquera Acosta, Directora Medios Educativos e Infraestructura Tecnológica

Aprobó: Hna. Dora Nancy Arcila Girado, Vicerrectora Administrativa y Financiera

POLÍTICA SEGURIDAD DE LA INFORMACIÓN

1. Declaración de la política:

La política de seguridad de la información es el acto mediante el cual se demuestra el compromiso por parte de la alta dirección de la Universidad Mariana en cuanto a la necesidad de proteger los activos de información (la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y desarrollo, generación y publicación de sus políticas, procesos, procedimientos, protocolos, manuales e instructivos. La universidad Mariana debe contar con plataformas apropiadas que protejan los mecanismos de tránsito, procesamiento, almacenamiento y comunicación que contienen y soportan sus servicios de registro, consulta, validación y realización de trámites ofertados, en tal sentido la universidad cuenta con personal idóneo humano y académicamente competente con sentido de compromiso alineado a la cultura de seguridad, reflejada en la aceptación y aplicación de las directrices establecidas por la alta dirección.

Con la implementación de la Política de seguridad de la información la Universidad Mariana busca dar cumplimiento a todo el compendio de disposiciones legales y regulatorias emitidas por los diferentes organismos del estado en lo que a tecnologías se refiere, así mismo contar con una metodología de gestión de riesgos como herramienta para actuar de manera proactiva ante las posibles situaciones que puedan afectar la continuidad de sus procesos.

Las Políticas asociadas a la Seguridad de la Información se definen con base al Plan de Desarrollo Institucional según su orden de importancia, en primer lugar, la Política de Seguridad de la Información, debe ser una directriz global que establece el qué y el por qué se quiere proteger. Su definición y actualización debe estar alineada con la planeación estratégica de la institución, en este sentido el PEI establece como política general, el desarrollo de procesos permanentes de planeación estratégica y prospectiva, con el fin de fomentar el desarrollo institucional y el de sus programas académicos y procesos administrativos. En concordancia a lo anteriormente expuesto la Política General de Seguridad de la Información, debe establecer las responsabilidades generales aplicables a todas las áreas de la universidad en lo que respecta al uso adecuado de los activos de información y el proceso estratégico de gestión y aseguramiento de la calidad, esta Política enmarca el conjunto de políticas específicas enfocadas a las áreas, grupos, servicios y actividades particulares. Su definición y actualización debe reflejar cambios de índole institucional y tecnológica, teniendo en cuenta que la Universidad cuenta con infraestructura tecnológica de conectividad para las sedes y ampliaciones, además de incluir el uso de plataformas tecnológicas para la gestión analítica de datos y toma de decisiones.

Por lo anterior, la Universidad Mariana siendo una institución de educación superior, católica y privada gestiona la seguridad de la información mediante la identificación, valoración y medición de los riesgos asociados a los activos de información que soporten la prestación de sus servicios de formación tanto presenciales como virtuales, donde se asegure la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentre bajo su responsabilidad y dominio; esto alineado con las leyes, normas y regulaciones que apliquen al objeto social de la Universidad Mariana.

a. **Introducción:**

Al efectuar una revisión de conceptos de planeación en la literatura especializada reciente, se aprecia elementos comunes como el análisis retrospectivo, la evaluación presente de factores internos y externos, la previsión de los cambios y transformaciones futuras, la definición de objetivos, cursos alternativos de acción y formas para lograr los objetivos propuestos que, en general, sugieren el empleo de la planeación estratégica situacional corporativa.

A medida que el mundo entra en la cuarta revolución industrial, las necesidades de educación de los futuros profesionales están cambiando drásticamente, al igual que las exigencias de adaptación de las Instituciones de Educación Superior (IES), a esquemas de enseñanza y aprendizaje con el empleo de tecnologías emergentes. A la par, estos cambios suscitan tendencias y megatendencias relevantes para el entorno de la educación superior en el contexto global y local; entre muchas otras, destacan algunas pocas que aquí se expresan como la demanda de las denominadas habilidades blandas, como el trabajo en equipo, la toma de decisiones, la comunicación y la capacidad de planificar, organizar y priorizar el trabajo, la tendencia estudiantil hacia la transición entre los modos de aprendizaje estructurado y no estructurado que redefine los roles de los profesores; particularmente, se incrementa la demanda hacia el 'aprendizaje híbrido', que combina las modalidades presencial y digital con mayor frecuencia, utilizando el tiempo del aula para la discusión y la práctica y, brindando a los estudiantes, conferencias en formato de video y lecturas y otras herramientas digitales que pueden revisar en su propio tiempo. El Plan de Desarrollo Institucional 2021 – 2028 orienta los destinos de la Universidad Mariana, con la visión de convertirla en referente, por su compromiso demostrable de formación integral de ciudadanos, profesionales con perspectiva global y con capacidad de actuación en su contexto nacional y local. Una universidad que se destaque por los resultados de la gestión del conocimiento, con activos de discernimiento e innovación social, que contribuyan a la transformación del medio social mediante la apropiación social y transferencia del conocimiento en la solución de diversas problemáticas locales y, por sus procesos de excelencia soportados en talento humano de alto nivel, la apropiación de tecnologías y la adopción de las mejores prácticas de gobernanza. En vista de la importancia para el correcto desarrollo de los procesos de negocio, los sistemas de información deben estar protegidos adecuadamente. Una protección fiable permite a la institución percibir mejor sus intereses y llevar a cabo eficientemente sus obligaciones en seguridad de la información. Pues una inadecuada protección de la información afecta el rendimiento general de la institución y puede afectar negativamente su imagen, reputación y confianza de los estudiantes, pero, también, de los inversores que depositan su confianza, en el crecimiento estratégico de las actividades presentes y futuras de la institución a nivel local e internacional. El objetivo de la seguridad de la información es asegurar la continuidad del negocio y reducir al mínimo el riesgo de daño mediante la prevención de incidentes de seguridad de la información, así como reducir su impacto potencial cuando este sea inevitable. Para lograr este objetivo, la institución debe desarrollar una metodología de gestión del riesgo que le permita analizar regularmente el grado de exposición de sus activos de información más importantes frente a aquellas amenazas que puedan aprovechar ciertas vulnerabilidades que ocasionen impactos adversos a las actividades diarias de los profesionales, el estudiantado o

a los procesos importantes de la Universidad. El éxito en el uso de esta metodología parte de la propia experiencia y aportación de todos los empleados en materia de seguridad de la información, mediante la comunicación de cualquier consideración relevante a los responsables directos de los procesos, en las reuniones que se establezcan por parte de la alta dirección, con el objeto de localizar posibles cambios en los niveles de protección y poder así evaluar las opciones más eficaces de costo/beneficio de gestión del riesgo en cada momento, y según sea el caso. Los principios de seguridad presentados que acompaña a esta política fueron desarrollados por el área de educación e infraestructura tecnológica con el fin de garantizar que las futuras decisiones se basen en preservar la confidencialidad, integridad y disponibilidad de la información relevante de la institución. En tal sentido la institución cuenta con la colaboración de todos los empleados en la aplicación de las políticas y directivas de seguridad de la información propuestas.

b. Antecedentes:

La rápida evolución y adopción de las Tecnologías de la Información y Comunicación como base para cualquier actividad socioeconómica, el creciente uso de las mismas por toda la sociedad, la rápida expansión de las redes de telecomunicaciones, y el fenómeno de convergencia, han marcado la dinámica del sector de las TIC y las economías de los países durante los últimos años; y la seguirán marcando, ya que las tendencias internacionales muestran que el entorno digital es dinámico y crece continuamente. Entorno donde se ha consolidado una economía basada en tecnologías (economía digital), cuya evolución y maduración genera impactos positivos en todos los ámbitos de la sociedad y en todos los sectores económicos que han estado a la vanguardia de esta tendencia para lograr mayor conocimiento de sus clientes, mayor productividad, competitividad y creación de nuevos modelos de negocio. En este sentido la Universidad Mariana logra ser un referente de alta calidad, con adhesión a estándares internacionales en la oferta académica, con especial énfasis en áreas de innovación social y por contar con: i) Plataformas de Tecnologías de la Información alineadas a las necesidades de aseguramiento del aprendizaje, ii) redes académicas de docencia y proyección social y, iii) activos de conocimiento y capital estructural en innovación social, alcanzando su participación en redes de conocimiento especializado y de fomento a la apropiación social de conocimiento. Esto ha permitido que la Universidad Mariana sea reconocida en la región por su oferta académica alineada con las tendencias en nuevas áreas del conocimiento y estándares internacionales, representada en diez nuevos pregrados, además de diez nuevas maestrías propias, tanto de profundización como con énfasis en investigación y, doctorados, entre los que destaca la oferta de cinco y tres posdoctorados, multiplicando por 10X la absorción de estudiantes de otras regiones del país y extranjeros y, la posibilidad de ampliar cobertura en diversas modalidades (presencial, virtual, dual y de registro único).

En tal razón la Universidad Mariana ha definido indicadores institucionales de calidad, en concordancia con estándares internacionales y la normativa nacional. Cuenta con un Sistema Interno de Aseguramiento de la Calidad, fortalecido con mecanismos y herramientas

computacionales para la sistematización, gestión y uso de la información, la medición de la evolución de los resultados académicos y el análisis de la apreciación de sus grupos de interés. Resultado de ello, ha implementado mecanismos de autoevaluación y mejoramiento periódicos que le han significado la renovación del registro calificado del 100% de los programas, la acreditación de calidad del 60 % de acreditables y la acreditación internacional de ocho programas académicos. En la actualidad la Universidad Mariana cuenta con una plataforma robusta de tecnología educativa emergente, entre la que se incluye laboratorios virtuales con tecnologías de simulación, realidad virtual y realidad aumentada para el desarrollo de prácticas formativas, recursos educacionales abiertos y MOOC, así como el uso de inteligencia artificial en plataformas de aprendizaje personalizado y de seguimiento y, evaluación al aprendizaje estudiantil de la que hace uso el 100% de los programas académicos. Así, el portafolio de servicios formativos combina modalidades presencial, virtual y mixta, favoreciendo el aprendizaje mediado por las Tecnologías de Información y Comunicación, esto permite que la Universidad Mariana sea transformada por la implementación de procesos formativos basados en la apropiación de plataformas tecnológicas inteligentes. De esta manera ha incrementado la eficacia de sus procesos en el logro de resultados de aprendizaje. La dinamización de la cooperación internacional y las redes académicas de docencia y proyección social, de investigación, de conocimiento especializado y, de fomento a la apropiación social y transferencia del conocimiento en nuevas áreas de tipo interdisciplinario e innovación, le han permitido a la Universidad, incrementar 15X la interacción de su comunidad educativa con comunidades académicas internacionales.

Hoy por hoy la Universidad Mariana es reconocida por contar con activos de conocimiento expresados en productos de innovación social, desarrollo tecnológico, generación de nuevo conocimiento, de formación de recurso humano y de apropiación social del conocimiento resultantes de su actividad en I+D+I, con los cuales ha incrementado en 5X su participación en redes de conocimiento especializado y de fomento a la apropiación social del conocimiento en el ámbito nacional e internacional.

El desarrollo de una economía digital sólida y segura es primordial para el país, ya que esta contribuye positivamente a la prosperidad económica y social del mismo. Su crecimiento y correcto funcionamiento requiere la construcción de un entorno digital abierto, seguro y confiable, acorde con el aumento y dinamismo de las actividades digitales de los individuos. Características que se logran más efectivamente desde un enfoque de gestión del riesgo que involucra a todas las partes interesadas, lo cual es estratégico al permitirles tomar decisiones socioeconómicas informadas para maximizar las oportunidades en el entorno digital. Para esto, se debe abordar el riesgo de seguridad digital como un reto económico y social en lugar de un reto puramente técnico.

c. **Marco Normativo:**

El marco normativo es un instrumento trascendental de la seguridad de la información, toda vez que aporta conocimiento en el cumplimiento de las regulaciones y su aplicación en los

procesos y procedimientos operacionales, así mismo nos instruye en los procesos de adquisición de tecnologías y servicios, negociación, contratación, y exigencia a nuestros proveedores y cumplimiento a nuestros acreedores, del mismo modo nos guía en la integración de las políticas, principios y valores institucionales a través de los procesos y procedimientos en procura de mejorar el desarrollo y cuidado de los mismos, en este sentido nace la necesidad de construir una serie de documentos anexos que complementen y apalanquen la Política de Seguridad de la Información para su eficaz cumplimiento y operatividad, soportados en protocolos, manuales, guías e instructivos, y políticas asociadas con el propósito de evitar la ocurrencia de vulnerabilidades y amenazas que conllevan a la materialización de sus riesgos asociados. Su integración se da a través del desarrollo e interacción de los procesos y procedimientos institucionales y se fortalecen con el eficaz desarrollo de los planes de capacitación, inducción, reinducción y campañas de sensibilización, las cuales se deben llevar a cabo de manera permanente y continua, así como la aplicación y verificación del cumplimiento de las demás políticas asociadas.

Es así como el Proyecto Educativo Institucional (PEI) define la gestión institucional como el conjunto de procesos y actividades encaminados a buscar la calidad, la racionalización y la optimización de los recursos físicos, financieros, tecnológicos y del capital humano, como soportes fundamentales que garanticen el normal funcionamiento de las diferentes dependencias de la Universidad, y faciliten el cumplimiento de la Misión y Visión Institucional. Para alcanzar los objetivos descritos, el PEI establece como política general, el desarrollo de procesos permanentes de planeación estratégica y prospectiva, con el fin de fomentar el desarrollo institucional y el de sus programas académicos y procesos administrativos. Así mismo, para adelantar el seguimiento y evaluación al desarrollo de cada uno de los objetivos y estrategias establecidas, prevé la definición e implementación de indicadores de gestión, que permitan el análisis de los resultados en forma permanente y faciliten la toma de decisiones de manera oportuna y con enfoque prospectivo. En tal sentido se describe la planeación como la etapa que forma parte del proceso administrativo mediante la cual se establecen directrices, se definen estrategias y se seleccionan alternativas y cursos de acción, en función de objetivos y metas generales[…] tomando en consideración la disponibilidad de recursos reales y potenciales que permitan establecer un marco de referencia necesario para concretar programas y acciones específicas en tiempo y espacio, logrando una predicción lo más probable del futuro para generar planes que puedan garantizar el éxito".

El Plan de Desarrollo Institucional 2021 - 2028 se basa en este enfoque y, específicamente, en la corriente de la escuela voluntarista o escuela francesa, fundada por Gastón Berger y Bertrand de Jouvenel. Esta corriente "propone analizar las posibles evoluciones de una organización […] en un horizonte de tiempo determinado, teniendo en cuenta las interacciones con sus entornos endógenos y exógenos, para elegir su mejor alternativa de futuro posible, a través de un ejercicio colectivo en el que convergen todas las voluntades de los actores relacionados con dicha organización. De este modo, el desarrollo institucional articula diferentes elementos con los que la universidad puede alcanzar sus objetivos, entre los que se cuenta el crecimiento, cambios estructurales como la cultura organizacional, el liderazgo,

la gestión del conocimiento e innovación, como lo manifiestan Delfín Pozos y Acosta Márquez (2016), además de la transformación de su oferta académica, el aseguramiento de la calidad de los resultados académicos, su capacidad de relacionamiento en entornos académicos competitivos nacionales e internacionales, su interacción e impacto en el medio social, su infraestructura y medios educativos, la formación integral de sus estudiantes, entre otros. Así mismo el marco normativo nos ayuda en el propósito de fortalecer la capacidad estructural y relacional de la Universidad con la implementación de estructuras y mecanismos de aseguramiento de la calidad; de infraestructura física y tecnológica para la gestión académica y administrativa, el seguimiento a egresados, la gestión de la permanencia estudiantil y la gestión del entorno laboral, así como, fortalecer la capacidad de relacionamiento con usuarios de servicios especializados y la comercialización del portafolio de productos de investigación, innovación, emprendimiento y servicios de proyección social, como estrategia de apalancamiento financiero y sostenibilidad institucional. Teniendo en cuenta el modelo de gestión, el cual Incluye la identificación de los ámbitos de actuación académicos y administrativos basados en meta prospectiva, la implementación de las tecnologías de la industria 4.0, tales como: computación en la nube, automatización de productos y procesos, simuladores para laboratorios de ciencias de la salud y de ingeniería, sistemas de información para la consulta de datos institucionales, analítica de datos y tableros de control, como soporte para el desarrollo de las funciones sustantivas, la gestión administrativa y la toma de decisiones; y la vinculación, cualificación, desarrollo, evaluación y retiro del personal a través de la implementación efectiva de los siete programas que integran el modelo Talentos, así como la Implementación del plan maestro de fortalecimiento de la infraestructura tecnológica con conectividad para las sedes y ampliaciones de la Universidad y la incorporación de plataformas tecnológicas con certificaciones ISO mínimas en ciberseguridad, para la analítica de datos, gestión y toma de decisiones académicas y administrativas a través de desarrollo de software propio y licenciamiento de terceros, son factores que demandan un esfuerzo mayor en el cumplimiento normativo y regulatorio del uso y aplicación de tecnologías de información y comunicación, en tal sentido la Política de Seguridad de la Información se debe alinear a las estrategias que la Universidad ha incorporado como estructuras y mecanismos de autorregulación y autoevaluación permanente y relaciones de cooperación internacional con pares evaluadores, es por ello que existe un sistema de atención al usuario adecuado que responde a los estándares de calidad y a las necesidades de los grupos de interés, sobre el cual ha consolidado procesos de evaluación, seguimiento y mejoramiento permanentes los cuales deben incluir el monitoreo, seguimiento, evaluación y actualización de la Política de Seguridad de la información.

NORMOGRAMA
Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.
Directiva Presidencial 02 Febrero 24 de 2022 “Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (Min TIC).

Decreto 338 Marzo 8 de 2022 "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
Resolución 746 Marzo 11 de 2022 "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
Decreto 767 Mayo 16 de 2022 “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”.
Directiva Presidencial 03 Marzo 15 de 2021 Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos.
Resolución 500 Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
Conpes 3995 Julio 1 de 2020 Política Nacional de Confianza y Seguridad Digital “Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías”.
Resolución 1519 Agosto 24 de 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.
Decreto 1008 Junio 14 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 número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Ley 1915 Julio 12 de 2018 Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Conpes 3854 abril 11 de 2016 Política Nacional de Seguridad Digital. Busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
Decreto 103 de 2015 Enero 20 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1068 mayo 26 de 2015 Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Capítulo 26.
Decreto 886 Mayo 13 de 2014 Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 1377 Junio 23 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1581 octubre 17 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.
Ley 1273 Enero 05 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.

d. Justificación:

La Universidad Mariana en su contexto institucional tiene Implementadas diversas estrategias para el desarrollo de competencias interculturales e internacionales en estudiantes y profesores y de capacidades institucionales de generación y aplicación del conocimiento global a la solución de problemas locales, con lo cual busca, gestionar de manera eficaz y eficiente los recursos económicos, financieros, tecnológicos, administrativos, de infraestructura física y del talento humano, y desarrollar un sistema administrativo de apoyo eficiente a los procesos misionales de la Universidad, apoyada en los mecanismos de aseguramiento de la calidad; de infraestructura física y tecnológica para la gestión académica y administrativa, el seguimiento a egresados, la gestión de la permanencia estudiantil y la gestión del entorno laboral, así como, fortalecer la capacidad de relacionamiento con usuarios de servicios especializados y la comercialización del portafolio de productos de investigación, innovación, emprendimiento y servicios de proyección social, como estrategia de apalancamiento financiero y sostenibilidad institucional. Bajo esta premisa y en virtud de la rápida evolución y adopción de las Tecnologías de Información y Comunicación como base para cualquier actividad socioeconómica, el creciente uso de las mismas por toda la sociedad, la rápida expansión de las redes de telecomunicaciones, y el fenómeno de convergencia, han marcado la dinámica del sector de las TIC y las economías de los países durante los últimos años.

Tabla 1. Proyecciones de algunos indicadores de uso de las TIC a nivel global

Proyecciones	2015	2020	Incremento porcentual
Más usuarios de banda ancha móvil	3 mil millones	4 mil millones	33%
Más terminales conectados	16,3 mil millones	24,4 mil millones	49%
Más datos generados	8,8 zettabytes	44 zettabytes	400%
Más tráfico IP de red (mensual)	72,4 exabytes	168 exabytes	132%
Dispositivos (Internet de las cosas	15 mil millones	200 mil millones(a)	1200%
Tamaño del mercado de la nube pública global	USD 97 mil millones	USD 159 mil millones	63%

Fuente: Adaptado de INTEL SECURITY (2015a). Nota: (a) Proyección a 2018.

No obstante, a lo anterior, la creciente relevancia del entorno digital sobre las actividades socioeconómicas, y su alto dinamismo, ha traído consigo un conjunto de incertidumbres, riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos, a los que se encuentran

expuestos los individuos y las organizaciones, públicas y privadas. En tal sentido las organizaciones a nivel global se han visto en la imperiosa necesidad de implementar mecanismos de protección que les permitan contrarrestar y controlar todos estos fenómenos a los cuales están permanentemente expuestas, con base a lo anterior se resalta la importancia de desarrollar una Política de Seguridad de la Información que se adapte y contribuya al logro de lo expuesto en el direccionamiento estratégico de la Universidad Mariana (2011), la cual parte de los propósitos declarados en la Visión y Misión institucionales, los objetivos institucionales expresados en el PEI que explicitan los propósitos misionales y los lineamientos estratégicos, programas, proyectos y planes operativos que materializan el propósito estratégico.

En 2022 las ciber amenazas han aumentado en un 28% con respecto a 2021 y el próximo año se espera que nuevos ciber incidentes ataquen a empresas, administraciones y usuarios.

Durante este año, empresas y profesionales como administraciones y organismos públicos han tenido que hacer frente a diferentes ciber amenazas. Y es que, aunque existen compañías muy bien dotadas que han implementado nuevas tecnologías y han capacitado al personal, lo cierto es que todavía son muchas las que continúan siendo una presa fácil y atractiva para sufrir un ciberataque.

De hecho, los ataques informáticos durante 2022 han aumentado en un 28% en comparación con 2021, según datos de un informe de Sophos y recogido por la tecnológica española NUUBB, especializada en servicios cloud para empresas y agentes digitalizadores.

Los ataques de ransomware a minoristas fueron los grandes protagonistas, con un incremento del 75% desde el año 2020.

Los ciber delincuentes consiguieron cifrar los archivos de los minoristas atacados.	68% de los casos
Los minoritas mostró que el ataque afectó a su capacidad para operar	92% de los casos
Supuso una pérdida en el negocio o sus ingresos.	89%
Pagó un rescate para recuperar los datos.	49%
Usó otros medios para restaurarlos.	32%

e. Objetivos de la política:

Objetivo General:

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Universidad Mariana, en concordancia con su misión y propósitos institucionales en relación con la operación de sus procesos, objetivos estratégicos y los requisitos legales vigentes.

Objetivos Específicos:

a. Definir las expectativas de la universidad con respecto al correcto uso que el personal realice con los recursos de información de la institución, así como de las medidas que se deben adoptar para la protección de los mismos.
b. Establecer para todo el personal de la institución la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.
c. Determinar e implementar medidas esenciales de seguridad de la información para la Universidad con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando el riesgo de pérdida o mal uso de dichos activos, protegiendo la reputación como organismo estratégico y asegurando la continuidad sin interrupciones significativas de los procesos esenciales.

Este objetivo se enfoca en abordar las siguientes consecuencias potenciales:

1. Pérdida o mal uso de activos de información:

- Identificar y clasificar los activos críticos de información.
- Implementar controles de acceso y autenticación para prevenir accesos no autorizados.
- Establecer políticas de gestión de datos y procedimientos de respaldo regular para prevenir pérdidas.

2. Pérdida de imagen como organismo estratégico:

- Desarrollar un marco de políticas de seguridad de la información alineado con estándares reconocidos.
- Implementar programas de concienciación y formación en seguridad para personal y estudiantes.
- Establecer un plan de respuesta a incidentes para abordar rápidamente cualquier brecha de seguridad.

3. Interrupción total o parcial de procesos:

- Realizar evaluaciones de riesgos para identificar posibles amenazas y vulnerabilidades.
- Implementar medidas de mitigación, como sistemas de respaldo y redundancia, para garantizar la continuidad del negocio.
- Desarrollar y probar planes de contingencia para responder eficazmente a interrupciones inesperadas.

Al alcanzar este objetivo, la Universidad estará mejor equipada para enfrentar amenazas a la seguridad de la información, proteger sus activos, preservar su reputación y garantizar la continuidad de sus operaciones esenciales.

d. Proporcionar a todo el personal de la universidad las herramientas que faciliten la toma de decisiones apropiadas, en situaciones relacionadas con la preservación de la seguridad de la información.

Para cumplir con estos objetivos el Sistema de Gestión de Seguridad de la Información SGSI se basa en la identificación de los activos de información involucrados en los procesos de estratégicos, misionales y de apoyo de la universidad, lo cual implica llevar a cabo junto a los responsables de los diferentes procesos de la institución las siguientes actividades esenciales:

- Identificar, para todos los procesos, los activos de información involucrados, catalogados como información Hardware, Software, información, instalaciones, redes y personas.
- Para cada activo de información identificar un responsable que vele por su disponibilidad, confidencialidad e integridad.
- Analizar el riesgo al cual están expuestos, con la ayuda de la metodología NTC-ISO/IEC 27005:2020.
- Difundir en forma planificada entre todo el personal de la universidad el objetivo de preservación de la información, sus características y las responsabilidades individuales para lograrlo.
- Insertar esto en los planes de capacitación anual de la institución como actividades permanentes y en el proceso de inducción del nuevo personal.

f. Diagnóstico:

Según la Superintendencia Financiera de Colombia (2015), el número de operaciones financieras (monetarias y no monetarias) en Colombia mediante el canal Internet aumentó en un 45% de 2012 a 2014 y mediante el canal Telefonía móvil en un 252%. En el primer semestre de 2015, el sistema financiero colombiano realizó 2.026 millones de operaciones por 3.237,8 billones de pesos, de los cuales mediante el canal Internet se realizaron 863 millones de operaciones (un 43% del total) por valor de 1.092,61 billones de pesos (un 34% del total). 2 Según el Programa Gobierno en línea del Ministerio de Tecnologías de la Información y las Comunicaciones, el porcentaje de ciudadanos colombianos que usan canales o medios electrónicos para (i) obtener información, (ii) realizar trámites, (iii) obtener servicios, (iv) presentar peticiones, quejas o reclamos, o (v) participar en la toma de decisiones, pasó del 30% en 2009 al 65% en 2014. Lo mismo sucedió con las empresas colombianas, pasando del 24% en 2009 al 81% en 2014. Adicionalmente, por medio del portal del Estado colombiano se realizaron 1.038 trámites en línea en el 2015.

h. Grupos de interés:

Grupos de interés internos:

Grupo	Intervención	Descripción
Regentes	Directa	La Regencia al velar por la estabilidad, desarrollo y progreso de la Universidad Mariana participa de

		manera activa en el desarrollo y manutención de la política de seguridad de la información.
Autoridades Colegiadas	Directa	Los órganos colegiados cuentan con la responsabilidad de tener funciones de gobierno y responsabilidades designadas a través de los estatutos de la Universidad, por lo cual ejecutan un rol activo en el mantenimiento y ejecución de la política de seguridad de la información.
Autoridades Personales	Directa	Las autoridades de gobierno personal desempeñan un rol directo de resultado en la política de seguridad de la información puesto que hacen las veces de cumplir y hacer cumplir las orientaciones del Concejo Máximo.
Personal Administrativo	Directa	Estos grupos generan una alta influencia en el desarrollo y resultados de la implementación de la política de seguridad de la información, debido a que son la primera línea en cuanto a su cumplimiento y punto de retroalimentación de cualquier aspecto u oportunidad de mejora que se tenga de la misma.
Profesores	Directa	
Estudiantes	Directa	
Egresados	Indirecta	Los egresados a no estar de manera presencial dentro de la universidad no generan un rol que impacte en el desarrollo y resultados de la aplicación de la política de seguridad de la información.

Grupos de interés externos:

Grupo	Intervención	Descripción
Proveedores y contratistas	Directa	Este grupo genera una alta influencia en el desarrollo y resultados de la implementación de la política de seguridad de la información, debido a que son la primera línea en cuanto a su cumplimiento y punto de retroalimentación de cualquier aspecto u oportunidad de mejora que se tenga de la misma.
El estado	Indirecta	Solo a través de las leyes lograría influir en el desarrollo de la política de seguridad de la información por lo que su influencia es baja.
Padres de familia	Indirecta	Estos grupos de interés para aspectos de seguridad de la información no tienen influencia por sus campos de acción y objetivos sociales y académicos.
Sector productivo	Indirecta	
Comunidades sociales	Indirecta	
Comunidades científicas	Indirecta	
Comunidades académicas	Indirecta	
Otras instituciones	Indirecta	Otras universidades pueden tener un rol de influencia al ser un referente en el ambiente académico de gestión de seguridad de la información que la Universidad Mariana pueda llegar a usar como ejemplo.

i. Definición de los lineamientos:

A continuación, se listan los lineamientos que se desglosarían a partir del objetivo de la Política de seguridad de la información de la Universidad Mariana:

Lineamientos para la preservación de la Seguridad Física y del entorno:

- Perímetro de Seguridad Física
- Controles de Acceso Físico
- Protección de Oficinas, Recintos e Instalaciones
- Desarrollo de Tareas en Áreas Protegidas
- Aislamiento de las Áreas de Recepción y Distribución
- Ubicación y Protección del Equipamiento y Copias de Seguridad
- Suministros de Energía
- Seguridad del Cableado
- Mantenimiento de Equipos
- Seguridad de los Equipos Fuera de las Instalaciones
- Desafectación o Reutilización Segura de los Equipos
- Políticas de Escritorios y Pantallas Limpias
- Retiro de los Bienes

Lineamiento para el Uso de las Tecnologías de la Información y Comunicaciones de la Universidad:

- Uso de las redes informáticas institucionales
- Uso de Cuentas de Servicios Informáticos Institucionales
- Uso Adecuado del correo electrónico
- Uso de contraseñas
- Uso de los Recursos Tecnológicos
- Administración de Bases de Datos
- Uso de la infraestructura física de telecomunicaciones
- Uso de las Tecnologías de Información y Comunicación de la Universidad para el personal administrativo
- Gestión de auditorías informáticas de manera periódica sobre los Sistemas de Información

Lineamientos para los Activos de seguridad de la información:

- Inventario de activos

Lineamientos para la Clasificación de la información:

- Información Restringida
- Información Confidencial
- Información de Uso Interno
- Información Pública
- Administración de la información física y electrónica de acuerdo a definición de las tablas de retención documental

Lineamientos para la Administración de Contraseñas de Acceso, Perfiles y Roles de Usuario:

- Seguridad y control de acceso
- Acceso a la Información
  Niveles de Acceso:
  a) Nivel de consulta de la información
  b) Nivel de mantenimiento de la información
- Asignación o cambio de contraseñas, perfiles o roles de usuarios
- Administración de contraseñas

Lineamientos para la Seguridad del Recurso Humano:

- Incorporación de la Seguridad en los Puestos de Trabajo
- Control y Política del Personal
- Compromiso de Confidencialidad
- Términos y Condiciones de Empleo
- Formación y Capacitación en Materia de Seguridad de la Información

Lineamientos para la respuesta a Incidentes y Anomalías en Materia de Seguridad:

- Comunicación de Incidentes Relativos a la Seguridad
- Comunicación de Debilidades en Materia de Seguridad
- Comunicación de Anomalías del Software
- Aprendiendo de los Incidentes

Las acciones a realizar en la política para cumplir el objetivo son: la implementación de los lineamientos expuestos y el monitoreo del cumplimiento de los mismos, los cuales se deben realizar a través de un equipo dedicado a este fin bajo la supervisión de la Dirección de Medios Educativos e Infraestructura Tecnológica.

En cuanto a los **indicadores**, se establecen los siguientes para medir el avance y desarrollo de la política de seguridad de la información al cabo de un año:

- Porcentaje de la implementación de la política de seguridad de la información, que dentro del plazo establecido debería estar a un 100% implementada.

- Nivel de madurez de la política de seguridad de la información, que cuyo nivel sería medido a través de metodología COBIT que para el año de implementada debería tener un nivel de dos (2) “Repetible”, siendo desde cero (0) a cinco (5) los niveles posibles.

  El detalle de los niveles COBIT es el siguiente: 0 Inexistente; 1 Inicial; 2 Repetible; 3 Definida; 4 Administrada; 5 Optimizada.

- Gestión de incidentes de seguridad de la información, que para el plazo establecido, se deberían poder haber gestionado el 100% de los incidentes que se puedan presentar dentro de ese lapso de tiempo.

j. Mecanismos de monitoreo y seguimiento:

El monitoreo y seguimiento a la política de seguridad de la información se debe realizar dando cumplimiento a la totalidad de los lineamientos expuestos en el literal anterior, actividad que se materializaría a través de la Dirección de Medios Educativos e Infraestructura Tecnológica; dado que esto alimentaria de gran manera a los indicadores "**Porcentaje de la implementación de la política de seguridad de la información**" y "**Nivel de madurez de la política de seguridad de la información**" los cuales contando con estas fuentes de información podrán ser medidos mediante la metodología de nivel de madurez COBIT; metodología que puede ser aplicada con una periodicidad semestral, la cual por medio de un plan de trabajo consistente entrevistas a diferentes áreas de la institución, el análisis documental y la verificación con la alta dirección de la institución se obtiene la calificación correspondiente.

k. Mecanismo de evaluación de la Política:

La política de seguridad de la información es aplicable al mecanismo de "Evaluación de resultados", la cual determina los efectos intencionales de la política, una vez se ha terminado la vigencia de la política. Las técnicas utilizadas para recolectar información son: la entrevista, el análisis documental y los grupos de discusión con la comunidad universitaria. La aplicación de esta metodología facilita la comprensión, la credibilidad y aceptación de los resultados.

l. Mecanismos de validación o socialización:

La socialización de la política que se espera aprobar estaría dirigida a todos los grupos de interés Internos (Regentes, Autoridades Colegiadas, Autoridades Personales, Personal Administrativo, Profesores, Estudiantes y Egresados); en cuanto a los grupos de interés externos, solo sería socializada a los proveedores y contratistas.

Los canales por los cuales se puede hacer esta socialización una vez sea aprobada por los grupos de gobierno de la Universidad Mariana deben ser los siguientes:

- Portal Web
- Intranet
- Correo electrónico institucional

m. Referencias bibliográficas:

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf Documento Conpes - Lineamientos de política para ciberseguridad y ciberdefensa

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf Documento Conpes - Política Nacional de Seguridad Nacional

https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html Ceupe - Política de seguridad de la información y SGSI

https://www.minambiente.gov.co/wp-content/uploads/2023/01/Plan-de-Seguridad-y-Privacidad-de-la-Informacion-DS-E-GET-29.pdf Ministerio de ambiente y desarrollo sostenible - Plan de Seguridad y Privacidad de la Información -2023

https://www.20minutos.es/tecnologia/ciberseguridad/los-6-ciberataques-que-seran-mas-habituales-en-2023-5086823/ 20 Minutos - Los 6 ciberataques que serán más habituales en 2023

http://serviap2009.umariana.edu.co/Biblioteca/frm_resultados.aspx?xi=63567 Universidad Mariana – Implementación de políticas de seguridad en redes informáticas usando tecnológicas CISCO

4. CONSERVACIÓN DE INFORMACIÓN DOCUMENTADA

Ver listado maestro de documentos y de registros.

Ver Tablas de Retención Documental.

5. CONTROL DE CAMBIOS

Control de Cambios		
Versión	**Vigencia**	**Descripción**
01	23/06/2023	Elaboración del documento.
02	09/11/2023	Ajuste del documento a nivel de estructura informada por la Dirección de planeación
03	05/12/2023	Modificación al documento de acuerdo a observaciones del Consejo administrativo y financiero.

Elaborado: Jonathan Almeyda Jácome	**Cargo:** Consultor Externo	**Fecha:** 09/11/2023
Revisado: Diana Mosquera Acosta	**Cargo:** Directora Medios Educativos e Infraestructura Tecnológica	**Fecha:** 05/12/2023
Aprobado: Hna. Dora Arcila Giraldo	**Cargo:** Vic. Administrativa y Financiera	**Fecha:** 05/12/2023