RESOLUCIÓN No. 650

22 DE JULIO DE 2026

"Por la cual se adopta la Política General de seguridad de la Información de la Universidad de Pamplona"

EL RECTOR (E) DE LA UNIVERSIDAD DE PAMPLONA, MEDIANTE RESOLUCION No. 639 DEL 17 DE JULIO DE 2026 EN USO DE SUS FACULTADES LEGALES Y ESTATUTARIAS EN ESPECIAL Y,

CONSIDERANDO

Que de conformidad con el literal e) del artículo 29 del Acuerdo No 027 del 23 de abril de 2002, Estatuto General, es función del Rector de la Universidad, "***Suscribir los contratos y/o convenios y expedir los actos que sean necesarios para el cumplimiento de los objetivos de la institución, atendiendo a las disposiciones vigentes"***

Que, en ejercicio de dicha facultad, corresponde al Rector expedir los actos administrativos necesarios para establecer, implementar, fortalecer, mantener y mejorar los mecanismos de gestión que contribuyan al cumplimiento de los objetivos institucionales, incluyendo aquellos orientados a la protección de la información, la gestión de los riesgos asociados a los activos de información y la continuidad y adecuada prestación de los servicios institucionales.

Que la Constitución Política de Colombia establece principios y derechos relacionados con la protección de la información, la intimidad, el buen nombre, el acceso a la información pública y el uso de medios tecnológicos para el desarrollo de las actividades de las instituciones.

Que el Articulo 15 de la Constitución Política de Colombia establece que todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, a su vez que el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

Que el Articulo 20 de la Constitución Política de Colombia garantiza a toda persona la libertad de expresar, difundir su pensamiento y opiniones, informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Que el artículo 69 de la Constitución Política de Colombia garantiza la autonomía universitaria y reconoce a las universidades la facultad de darse sus directivas y regirse por sus propios estatutos, de conformidad con la Constitución y la ley, en ejercicio de la autonomía académica, administrativa y demás ámbitos propios de su naturaleza institucional.

Que el Decreto reglamentario 1377 de 2013 y demás normas que lo adicionen modifiquen o sustituyan, establece los mecanismos y medios para la protección de los datos personales, sobre los cuales las entidades públicas y privadas, pueden hacer el manejo de los datos e información de los particulares en las bases de datos de las instituciones.

Que atendiendo los nuevos lineamientos emitidos por el MinTIC en general y la Resolución 500 de 2021 en particular, ***"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"***, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la cual tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital. Asimismo, establece las directrices y estándares para la estrategia de seguridad digital.

Que la Universidad de Pamplona, en cumplimiento de su misión institucional, genera, recibe, procesa, almacena, transmite, consulta, administra y custodia información de carácter

académico, administrativo, financiero, investigativo, de extensión, tecnológico y de apoyo a la gestión institucional.

Que la información constituye un activo estratégico y esencial para el cumplimiento de la misión, los objetivos institucionales y el desarrollo de los procesos estratégicos, misionales, de apoyo, evaluación y control de la Universidad de Pamplona.

Que la transformación digital, el uso creciente de sistemas de información, aplicaciones, bases de datos, plataformas académicas, infraestructura tecnológica, servicios en la nube, redes de comunicaciones y mecanismos electrónicos para el intercambio y procesamiento de información generan nuevos escenarios de riesgo y exposición frente a amenazas internas y externas.

Que dichas amenazas pueden afectar la confidencialidad, integridad y disponibilidad de la información y, en consecuencia, comprometer la continuidad de los procesos, la prestación de los servicios institucionales, el cumplimiento de las obligaciones legales y la confianza de las partes interesadas.

Que la Ley 527 de 1999 establece disposiciones relacionadas con los mensajes de datos, el comercio electrónico y las firmas digitales.

Que la Ley 1273 de 2009 incorporó disposiciones relacionadas con la protección de la información y de los datos y la preservación integral de los sistemas que utilizan tecnologías de la información y las comunicaciones.

Que la Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales y que la Universidad de Pamplona, en el ámbito de sus competencias, debe adoptar las medidas necesarias para garantizar su adecuado tratamiento y protección.

Que la Ley 1712 de 2014 establece disposiciones en materia de transparencia y derecho de acceso a la información pública, cuya aplicación debe armonizarse con las obligaciones de protección de la información, reserva, confidencialidad y protección de datos personales.

Que el Decreto 1078 de 2015 y las disposiciones que lo modifiquen, adicionen o sustituyan, establece el marco reglamentario aplicable al sector de Tecnologías de la Información y las Comunicaciones y contiene disposiciones relacionadas con Gobierno Digital.

Que la Universidad de Pamplona debe considerar el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones, así como los demás lineamientos y disposiciones que resulten aplicables a la institución.

Que la Norma Técnica Colombiana ISO/IEC 27001:2022 establece requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información – SGSI.

Que la Norma ISO/IEC 27002:2022 proporciona controles y buenas prácticas de referencia para la gestión de la seguridad de la información.

Que resulta necesario establecer un marco institucional que defina los principios, compromisos, responsabilidades y lineamientos generales para proteger los activos de información de la Universidad de Pamplona.

Que la seguridad de la información constituye una responsabilidad institucional que requiere la participación de la Alta Dirección, funcionarios, docentes, investigadores, estudiantes, contratistas, proveedores, operadores, practicantes, pasantes y demás terceros o partes interesadas que tengan acceso a información o activos de información de la Universidad.

Que la Universidad de Pamplona reconoce la necesidad de establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información – SGSI, alineado con su direccionamiento estratégico, la gestión integral de riesgos y los requisitos legales, reglamentarios, contractuales e institucionales aplicables.

Que la Universidad de Pamplona reconoce la importancia de proteger la información que genera, recibe, procesa, transmite, almacena, consulta, custodia y administra, independientemente de su formato, ubicación o medio de tratamiento.

Que, en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO. OBJETO.

Adoptar la Política General de Seguridad de la Información de la Universidad de Pamplona, como marco institucional para orientar la gestión y protección de la información y de los activos de información de la Universidad.

ARTÍCULO SEGUNDO.OBJETIVOS

Establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad de Pamplona, tomando como marco de referencia la NTC-ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información – MSPI y los requisitos legales, reglamentarios, contractuales e institucionales aplicables.

El SGSI estará articulado con el direccionamiento estratégico, la gestión institucional de riesgos y los demás sistemas, modelos y mecanismos de gestión aplicables en la Universidad.

ARTÍCULO TERCERO. ÁMBITO DE APLICACIÓN.

La Política General de Seguridad de la Información será de aplicación institucional y deberá ser observada, según corresponda, por los directivos, servidores públicos, personal administrativo, docentes, investigadores, estudiantes, contratistas, proveedores, practicantes, pasantes y demás terceros o partes interesadas que tengan acceso, administren, procesen, almacenen, transmitan, custodien o utilicen información o activos de información de la Universidad.

La Política será aplicable a la información independientemente de su formato, ubicación o medio de tratamiento.

PARÁGRAFO. El alcance específico del SGSI será establecido y mantenido como información documentada independiente, considerando el contexto de la Universidad, los procesos, servicios, sedes, infraestructura, tecnologías, interfaces, dependencias y partes interesadas pertinentes.

ARTÍCULO CUARTO. RESPONSABILIDADES.

La Alta Dirección demostrará liderazgo y compromiso con el SGSI, promoverá su integración con los procesos institucionales y gestionará, de acuerdo con las capacidades y mecanismos institucionales, los recursos necesarios para su establecimiento, implementación, mantenimiento y mejora continua.

La instancia o responsable que sea designado para liderar el SGSI coordinará su implementación, mantenimiento, seguimiento y mejora, así como la gestión de riesgos, objetivos, controles y demás actividades necesarias para su adecuado funcionamiento.

El Centro de Investigación Aplicada y Desarrollo en Tecnologías de Información – CIADTI, dentro del ámbito de sus competencias, apoyará la implementación, operación y mantenimiento de los controles tecnológicos requeridos para la protección de la infraestructura, sistemas, aplicaciones, plataformas, redes y servicios tecnológicos bajo su responsabilidad.

Los líderes de proceso, propietarios de activos de información y demás personas vinculadas con la Universidad serán responsables del cumplimiento de las disposiciones de seguridad de la información que les resulten aplicables.

La revisión y aprobación de los documentos relacionados con el SGSI de acuerdo al alcance definido serán responsabilidad del director de CIADTI y será el encargado de gestionar su publicación a las partes interesadas.

ARTÍCULO QUINTO. DESARROLLO Y CUMPLIMIENTO DE LA POLÍTICA.

Para el desarrollo de la Política General de Seguridad de la Información y la operación del SGSI, la Universidad establecerá y mantendrá las políticas específicas, procedimientos, metodologías, estándares, manuales, instructivos, guías, controles y demás información documentada que resulte necesaria.

Estas disposiciones serán de obligatorio cumplimiento para las personas y partes interesadas a quienes resulten aplicables, de conformidad con su relación, funciones, responsabilidades y nivel de acceso a los activos de información de la Universidad.

ARTÍCULO SEXTO. SEGUIMIENTO Y MEJORA CONTINUA.

El SGSI será objeto de seguimiento, medición, evaluación, auditoría y revisión a intervalos planificados, con el propósito de verificar su desempeño, cumplimiento y eficacia y promover su mejora continua.

La Política General de Seguridad de la Información será revisada periódicamente y cuando se presenten cambios significativos en el contexto institucional, los riesgos, los procesos, las tecnologías, el alcance del SGSI o los requisitos aplicables.

ARTÍCULO SEPTIMO. VIGENCIA

La presente Política General de Seguridad de la Información de la Universidad de Pamplona entrará en vigencia a partir de su expedición y deroga las normas que le sean contrarias.

El responsable designado para la gestión del SGSI deberá promover su revisión periódica, actualización, comunicación y disponibilidad para las partes interesadas pertinentes.

PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE.

HERIBERTO JOSE RANGEL NAVIA
Rector (E)

V.B. José Enrique Durán Granados- director CIADTI

Elaboró: Anny Castillejo- Apoyo jurídico- CIADTI