RESOLUCIÓN No. 651

22 DE JULIO DE 2026

"Por medio de la cual se aprueba y adopta el alcance del Sistema de Gestión de Seguridad de la Información – SGSI 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 Universidad de Pamplona ha establecido la implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información – SGSI, como mecanismo para gestionar los riesgos asociados a la seguridad de la información y proteger los activos de información institucionales.

Que la Norma ISO/IEC 27001:2022 establece, en su numeral 4.3, los requisitos relacionados con la determinación del alcance del Sistema de Gestión de Seguridad de la Información.

Que para la determinación del alcance del SGSI se deben considerar el contexto interno y externo de la organización, las necesidades y expectativas de las partes interesadas pertinentes, así como las dependencias e interfaces entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.

Que la Universidad de Pamplona ha definido para esta primera etapa de implementación y certificación el Macroproceso de Transformación Digital como ámbito de aplicación del Sistema de Gestión de Seguridad de la Información – SGSI.

Que resulta necesario formalizar y aprobar el documento que establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad de Pamplona.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO. APROBACIÓN. Aprobar el documento denominado "Alcance del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad de Pamplona", cuyo contenido es el siguiente:

1. OBJETIVO, ALCANCE Y USUARIOS DEL DOCUMENTO

El objetivo del presente documento es establecer formalmente los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad de Pamplona, de conformidad con los requisitos establecidos en la Norma ISO/IEC 27001:2022.

Para determinar el alcance se consideran el contexto interno y externo de la Universidad, los requisitos de las partes interesadas pertinentes, las dependencias existentes entre las actividades desarrolladas por la Universidad y aquellas realizadas por terceros, así como los procesos, servicios, activos de información, infraestructura tecnológica y recursos que soportan el Macroproceso de Transformación Digital.

El presente documento aplica a la documentación, actividades, procesos, servicios, activos de información, recursos humanos, tecnológicos y físicos comprendidos dentro de los límites establecidos para el SGSI.

Los usuarios de este documento son la Alta Dirección de la Universidad de Pamplona, los responsables del Macroproceso de Transformación Digital, el responsable del SGSI, los líderes y responsables de los procesos incluidos en el alcance, el personal que participa en la implementación y operación del SGSI, los auditores y las demás partes interesadas internas o externas pertinentes.

2. DOCUMENTOS DE REFERENCIA

Para la definición y mantenimiento del alcance del SGSI se consideran, entre otros, los siguientes documentos:

- Norma ISO/IEC 27001:2022, numeral 4.3 – Determinación del alcance del Sistema de Gestión de Seguridad de la Información.
- Norma ISO/IEC 27001:2022, numeral 4.1 – Comprensión de la organización y de su contexto.
- Norma ISO/IEC 27001:2022, numeral 4.2 – Comprensión de las necesidades y expectativas de las partes interesadas.
- Política General de Seguridad de la Información de la Universidad de Pamplona.
- Contexto de la organización del SGSI.
- Matriz de partes interesadas y requisitos aplicables.
- Metodología de gestión de riesgos de seguridad de la información.
- Inventario y clasificación de activos de información.
- Declaración de Aplicabilidad – SoA.
- Mapa de procesos y estructura organizacional de la Universidad de Pamplona.
- Documentación institucional asociada al Macroproceso de Transformación Digital.
- Requisitos legales, reglamentarios, contractuales e institucionales aplicables.

3. DEFINICIÓN DEL ALCANCE DEL SGSI

La Universidad de Pamplona establece los límites y aplicabilidad de su Sistema de Gestión de Seguridad de la Información considerando la importancia de la información utilizada para la prestación de sus servicios, las características de los procesos involucrados, los activos de información, los riesgos de seguridad, la infraestructura tecnológica, las partes interesadas y dependencias existentes con otros procesos y terceros.

El Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad de Pamplona comprende el Macroproceso de Transformación Digital, incluyendo los procesos, servicios, activos de información, personal, infraestructura tecnológica, sistemas de información, redes de

comunicaciones y demás recursos que soportan las actividades comprendidas dentro de dicho macroproceso.

La información perteneciente al alcance deberá ser protegida durante todo su ciclo de vida, incluso cuando sea almacenada, procesada o transmitida mediante servicios, infraestructura o terceros que se encuentren fuera de los límites físicos u organizacionales directos del SGSI. En estos casos deberán establecerse los requisitos, responsabilidades y controles de seguridad correspondientes.

3.1. MACROPROCESO INCLUIDO

El alcance del Sistema de Gestión de Seguridad de la Información comprende el siguiente macroproceso:

Macroproceso de Transformación Digital

Este macroproceso integra los procesos y servicios tecnológicos destinados a soportar la transformación digital y la prestación de servicios tecnológicos de la Universidad de Pamplona.

De acuerdo con la estructura definida por la Universidad para el proyecto, el Macroproceso de Transformación Digital comprende los siguientes componentes:

a. Soporte

Comprende los servicios y actividades asociados con:

- Unipamplona.
- Académico IES.
- Organización a IES.
- Específico.
- PMO.

b. Desarrollo

Comprende los servicios y actividades asociados con:

- Unipamplona.
- Académico IES.
- Organización a IES.
- Pruebas.

c. Infraestructura de Servicios

Comprende los servicios y actividades relacionados con:

- Bases de datos.
- Servidores y herramientas.

d. Infraestructura de TI

Comprende los servicios y actividades relacionados con:

- Mantenimiento.
- Redes y comunicaciones.

e. Ciberseguridad

Comprende las actividades y servicios relacionados con la gestión y protección de la seguridad de la información y de los activos tecnológicos asociados al Macroproceso de Transformación Digital.

f. Experiencia de Usuario

Comprende los servicios y actividades asociados con:

- Diseño.
- Aulas virtuales.

Esta estructura corresponde al alcance que has definido gráficamente para el proyecto y permite que el documento formal del SGSI quede alineado con la presentación institucional.

3.2. PROCESOS Y SERVICIOS INCLUIDOS

Se encuentran comprendidos dentro del alcance del SGSI los procesos, actividades y servicios que conforman el Macroproceso de Transformación Digital, incluyendo aquellos necesarios para:

- Soporte y atención de servicios tecnológicos;
- Desarrollo, mantenimiento y pruebas de soluciones de software;
- Administración de bases de datos;
- Administración de servidores y herramientas tecnológicas;
- Administración y mantenimiento de infraestructura tecnológica;
- Administración de redes y comunicaciones;
- Gestión de ciberseguridad;
- Diseño y experiencia de usuario;
- Administración y soporte de aulas virtuales;
- Gestión de proyectos y actividades asociadas con la transformación digital;
- Gestión de los activos de información y recursos tecnológicos requeridos para la prestación de estos servicios.

También forman parte del alcance interdependencias con otros procesos institucionales cuando estas sean necesarias para la operación, seguridad o prestación de los servicios comprendidos dentro del SGSI.

3.3. UNIDADES ORGANIZATIVAS

El alcance comprende las unidades, grupos, equipos de trabajo y personas de la Universidad de Pamplona que participan directamente en la gestión, operación, administración, soporte, desarrollo, mantenimiento, seguridad o prestación de los servicios asociados con el Macroproceso de Transformación Digital.

Se incluyen igualmente las personas que, aunque pertenezcan a otras unidades organizacionales, tengan responsabilidades específicas sobre activos de información, riesgos, controles o servicios comprendidos dentro del alcance del SGSI.

Las unidades organizativas específicas serán identificadas y actualizadas de acuerdo con la estructura organizacional vigente de la Universidad y con las responsabilidades asignadas al Macroproceso de Transformación Digital.

3.4. ACTIVOS DE INFORMACIÓN

El alcance del SGSI comprende los activos de información necesarios para la operación y prestación de los procesos y servicios incluidos dentro del Macroproceso de Transformación Digital.

Entre otros, se consideran:

- Información digital y física;
- Bases de datos;
- Sistemas de información;
- Aplicaciones;
- Software;
- Servidores;
- Equipos de cómputo;
- Dispositivos de comunicaciones;
- Redes;
- Plataformas tecnológicas;
- Servicios en la nube;
- Herramientas de administración y monitoreo;
- Repositorios de código fuente;
- Documentación técnica y funcional;
- Configuraciones;
- Respaldos de información;
- Credenciales y mecanismos de autenticación;
- Servicios tecnológicos;
- Conocimiento del personal;
- Instalaciones e infraestructura de soporte.

Los activos específicos comprendidos dentro del alcance deberán estar identificados y administrados mediante el Inventario de Activos de Información del SGSI.

3.5. UBICACIONES

El alcance comprende las instalaciones físicas de la Universidad de Pamplona desde las cuales se administren, operen o presten los procesos y servicios incluidos dentro del Macroproceso de Transformación Digital, así como aquellas ubicaciones en las cuales se encuentren alojados activos de información o infraestructura tecnológica relevante para el SGSI.

También deberán considerarse los servicios tecnológicos prestados desde ubicaciones externas, centros de datos, servicios en la nube o instalaciones administradas por terceros cuando soporten procesos o activos comprendidos dentro del alcance.

Las ubicaciones específicas aplicables serán identificadas y documentadas como parte de la información del SGSI.

3.6. REDES E INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN

Se encuentra dentro del alcance toda la infraestructura tecnológica que soporte directa o indirectamente los procesos y servicios incluidos en el Macroproceso de Transformación Digital,

cuando se encuentre bajo responsabilidad de la Universidad o cuando su seguridad deba ser gestionada mediante acuerdos con terceros.

Esto incluye, según corresponda:

- Infraestructura de servidores;
- Infraestructura de almacenamiento;
- Bases de datos;
- Equipos de comunicaciones;
- Redes LAN y WAN;
- Redes inalámbricas;
- Conexiones a Internet;
- Enlaces de comunicaciones;
- Infraestructura de seguridad;
- Sistemas de información;
- Aplicaciones;
- Plataformas de virtualización;
- Servicios en la nube;
- Sistemas de respaldo;
- Herramientas de administración;
- Herramientas de monitoreo y seguridad;
- Ambientes de desarrollo, pruebas y producción.

La infraestructura específica deberá identificarse mediante los inventarios de activos y documentación técnica correspondiente.

3.7. PERSONAS

Se encuentran dentro del alcance las personas que desarrollen actividades relacionadas con los procesos y servicios del Macroproceso de Transformación Digital, incluyendo, según corresponda:

- Funcionarios y/o servidores públicos;
- Contratistas;
- Personal técnico;
- Administradores;
- Desarrolladores;
- Personal de soporte;
- Responsables de infraestructura;
- Responsables de bases de datos;
- Personal de ciberseguridad;
- Responsables de servicios;
- Proveedores y terceros con acceso autorizado.

Las responsabilidades de seguridad deberán establecerse de acuerdo con las funciones desempeñadas y los activos de información a los cuales cada persona tenga acceso.

3.8. PROVEEDORES Y TERCEROS

Los proveedores y terceros que suministren servicios tecnológicos, infraestructura, comunicaciones, software, servicios en la nube, soporte, mantenimiento u otros servicios

relacionados con activos incluidos dentro del alcance deberán ser considerados dentro de la gestión de riesgos del SGSI.

Cuando un activo o servicio comprendido dentro del alcance sea administrado total o parcialmente por un tercero, la Universidad establecerá los requisitos y responsabilidades de seguridad correspondientes mediante contratos, acuerdos, niveles de servicio u otros mecanismos aplicables.

3.9. DEPENDENCIAS

El SGSI reconoce la existencia de dependencias entre el Macroproceso de Transformación Digital y otros procesos de la Universidad de Pamplona.

Estas relaciones deberán identificarse y gestionarse cuando puedan afectar la confidencialidad, integridad o disponibilidad de la información o el cumplimiento de los objetivos del SGSI.

De igual manera, deberán identificarse las dependencias relacionadas con proveedores, servicios externos, telecomunicaciones, servicios en la nube, infraestructura compartida y demás terceros necesarios para la prestación de los servicios comprendidos dentro del alcance.

3.10. EXCLUSIONES DEL ALCANCE

Para esta primera etapa de implementación y certificación del SGSI, los procesos y macroprocesos institucionales diferentes al Macroproceso de Transformación Digital no forman parte directamente del alcance del SGSI, salvo cuando actúen como dependencias, propietarios, usuarios o partes interesadas de los procesos, servicios o activos incluidos en el alcance.

Esta delimitación no implica que la información institucional ubicada fuera del alcance carezca de medidas de protección ni que las disposiciones generales de seguridad de la información de la Universidad dejen de ser aplicables.

Las exclusiones específicas deberán encontrarse debidamente justificadas y no podrán afectar la capacidad de la Universidad para proporcionar seguridad adecuada a la información, procesos y servicios incluidos dentro del alcance del SGSI.

4. REVISIÓN DEL ALCANCE

El presente alcance deberá ser revisado como mínimo una vez al año y adicionalmente cuando se presenten cambios significativos que puedan modificar los límites o aplicabilidad del SGSI, incluyendo:

- Cambios en el Macroproceso de Transformación Digital;
- Incorporación o eliminación de procesos o servicios;
- Cambios en la estructura organizacional;
- Cambios significativos en infraestructura tecnológica;
- Incorporación de nuevos sistemas o plataformas;
- Cambios de ubicación;
- Contratación o modificación de servicios de terceros;
- Cambios en servicios en la nube;
- Cambios significativos en riesgos;
- Modificaciones legales, reglamentarias o contractuales;
- Resultados de auditorías;

• Decisiones de la Alta Dirección.

Los cambios realizados al alcance deberán ser documentados, revisados y aprobados mediante los mecanismos establecidos por la Universidad.

ARTÍCULO SEGUNDO. ÁMBITO DE APLICACIÓN. El alcance aprobado mediante la presente Resolución será aplicable a las actividades, procesos, servicios, activos de información, recursos humanos, tecnológicos y físicos comprendidos dentro de los límites establecidos para el Sistema de Gestión de Seguridad de la Información – SGSI.

ARTÍCULO TERCERO. RESPONSABILIDAD. La implementación, operación, mantenimiento, revisión y mejora del alcance aprobado se desarrollará de conformidad con las responsabilidades asignadas dentro del Sistema de Gestión de Seguridad de la Información – SGSI y la estructura organizacional vigente de la Universidad de Pamplona.

ARTÍCULO CUARTO. ACTUALIZACIÓN Y CONTROL. El alcance del SGSI deberá mantenerse actualizado de acuerdo con las condiciones establecidas en el documento aprobado y con los cambios que puedan afectar sus límites o aplicabilidad.

ARTÍCULO QUINTO. PUBLICACIÓN Y DIVULGACIÓN. La presente Resolución deberá ser comunicada y publicada de acuerdo con los mecanismos institucionales establecidos por la Universidad de Pamplona.

ARTÍCULO SEXTO. VIGENCIA. La presente Resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias.

PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE.

HERIBERTO JOSE RANGEL NAVIA
Rector (E)

V.B. José Enrique Duran Granados- director CIADTI

Elaboró: Anny Castillejo- Apoyo jurídico- CIADTI