1. Introducción

La información constituye un activo de primer orden para **CIMA LAB Diagnostics**, siendo imprescindible para la prestación de los servicios que ofrece a terceras partes. Así mismo, las tecnologías de la información y las comunicaciones (TIC) se han hecho indispensables para las organizaciones, ya que contribuyen a la eficacia del tratamiento de la misma.

Sin embargo, las mejoras que aportan las TIC vienen acompañadas de nuevos riesgos y amenazas. Por esa razón, es necesario tenerlas en cuenta, e introducir medidas específicas para proteger tanto la información como los servicios que dependen de ella.

A tal fin, se introduce el concepto de seguridad de la información, con el objetivo de proteger la información y los servicios, reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable, siendo sus bases establecidas en el presente documento.

2. Misión y objetivos de la política

La presente política tiene como propósito el establecimiento de las directrices y principios que rigen la gestión de los activos e información de CIMA LAB Diagnostics, en base a la norma ISO 27001, y al resto de normas implementadas en la organización, ISO 9001 e ISO 15189.

Además, debiéndose alinear y ajustar a lo dispuesto por las Políticas en Seguridad de la Información desarrolladas por parte de la Universidad de Navarra y la Clínica Universidad de Navarra, en caso de conflicto, lo dispuesto en los documentos anteriores prevalecerá sobre lo descrito en el presente documento.

Para ello, se establecen los siguientes objetivos generales en materia de seguridad de la información:

- Establecer unas bases robustas sobre las que los empleados y terceras partes puedan acceder a la información vinculada a los servicios de **CIMA LAB Diagnostics** de forma segura.
- Contribuir desde la dirección al cumplimiento de la misión y objetivos establecidos por **CIMA LAB Diagnostics**.
- Asegurar la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad de la Información.
- Asegurar la continuidad en la prestación de servicios, tanto de manera preventiva como reactiva ante incidentes de seguridad.
- Proteger los activos de la información de **CIMA LAB Diagnostics** frente a cualquier amenaza, intencionada o accidental, interna o externa, con el fin de asegurar la Confidencialidad, Integridad y Disponibilidad de los mismos.
- Asegurar la correcta formación de sus empleados en las diferentes áreas de la seguridad de la información.

Esta Política de Seguridad de la Información refleja el compromiso explícito y constante de la dirección de **CIMA LAB Diagnostics** para difundir y consolidar la cultura de la seguridad en sus entornos y actividades.

2. Alcance

Este documento será de aplicación a toda la información de **CIMA LAB Diagnostics** vinculada a los sistemas de información que dan soporte a los servicios del laboratorio de Tumores Sólidos y Enfermedades Hereditarias, de acuerdo a la declaración de aplicabilidad vigente.

Esta política no se limita a los datos de carácter personal, y es independiente de que el tratamiento sea manual o automatizado.

3. Distribución

Aprobada por la Dirección de **CIMA LAB Diagnostics**, esta Política debe ser accesible a todas las personas y entidades afectadas dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), mediante los canales adecuados.

4. Marco normativo

La legislación en materia de seguridad de la información que debe servir de referencia se actualiza de forma continua y queda reflejado en el documento **"PM01_R04_Listado de Legislación y PM01_R05_Listados de normas y guías de referencia generales".**

5. Revisión de la política

Se distinguen dos tipos de actividades relacionadas con las posibles revisiones que puedan llevarse a cabo sobre este documento:

- Revisiones periódicas sistemáticas. Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política. La revisión de la Política de Seguridad de la Información deberá garantizar que se encuentra alineada con la estrategia, la misión y visión de **CIMA LAB Diagnostics**, y que asegura el cumplimiento de los objetivos de control establecidos.

  Las revisiones periódicas se realizarán al menos con una periodicidad anual.

- Revisiones no planificadas. Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o haya causado un impacto en la seguridad de la información de **CIMA LAB Diagnostics**.

6. Organización interna de la seguridad

La seguridad de la información corresponde, con las funciones que se señalan para cada uno en este apartado, a los siguientes órganos:

- Comisión de Seguridad de la Información de CIMA LAB Diagnostics

  La Comisión de Seguridad de la Información es el organismo que centraliza la gestión de la seguridad de la información en **CIMA LAB Diagnostics**.
  Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán crearse Comisiones de Seguridad delegadas, dependientes funcionalmente de la Comisión de Seguridad de la Información de **CIMA LAB Diagnostics**, que serán responsables en su ámbito de las actuaciones que se les deleguen.
  La comisión de seguridad de **CIMA LAB Diagnostics** depende funcionalmente del Comité de Seguridad y Protección de Datos de la Universidad de Navarra (UNAV) y de la Clínica Universidad de Navarra (CUN).

- Representante de la Dirección

  Es responsable de liderar y promover la seguridad de la información en la organización. Esto implica establecer políticas, asignar recursos, comunicar las expectativas de la alta dirección, supervisar la implementación del SGSI y garantizar el cumplimiento de los requisitos legales y

normativos. Además, juega un papel clave en la identificación y mitigación de riesgos de seguridad de la información, contribuyendo así a proteger los activos de la organización y alcanzar los objetivos empresariales.

- Responsable del SGSI

  El Responsable del SGSI se encarga de mantener actualizado el sistema, asegurando su conformidad con los estándares y requisitos de aplicación, realizando auditorías para evaluar su eficacia. Este rol abarca desde el diseño e implementación de medidas de seguridad hasta la gestión de riesgos, la formación del personal en aspectos de seguridad y la coordinación en respuesta ante incidentes.

- Responsable del Servicio

  El responsable del Servicio será la persona con competencia suficiente para decidir sobre la finalidad y prestación de dicho servicio y determinará los requisitos de seguridad de los servicios prestados dentro del marco establecido que regula la ISO27001. A tal efecto:

  a. Realizará los preceptivos análisis de riesgos, y seleccionará las salvaguardas que se han de implantar.
  b. Aceptará los riesgos residuales respecto de la información calculada en el análisis de riesgos.
  c. Realizará el seguimiento y control de los riesgos, con la participación del Responsable del SGSI.
  d. Suspenderá la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

7. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el Comité de Dirección de CIMA LAB Diagnostics, y prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

8. Clasificación de la información

CIMA LAB Diagnostics clasificará y llevará inventario de los activos de la información en virtud de su naturaleza. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

9. Datos de carácter personal

Cuando un sistema maneje datos de carácter personal, le será de aplicación lo dispuesto en el Reglamento Europeo 679/2026 de protección de datos y en la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, sin perjuicio de los requisitos establecidos en el marco regulatorio establecido. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

10. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos.

Para la armonización de los análisis de riesgos, se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

11. Instrumentos de desarrollo

Se establece un marco normativo en materia de seguridad de la información estructurado por diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico.

La política de seguridad estructurará su marco normativo en los siguientes niveles:

- La presente Política de Seguridad de la Información que establece los requisitos y criterios de protección de carácter global.
- Las normas de seguridad que definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.
- Los procedimientos de seguridad en los que se describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

Además, se podrán establecer guías con recomendaciones y buenas prácticas.

12. Obligaciones del personal

Todo el personal con responsabilidad en el uso, operación, o administración de sistemas de tecnologías de la información tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, independientemente del tipo de relación jurídica que les vincule con **CIMA LAB Diagnostics.**

El incumplimiento de la Política de Seguridad de la Información y su normativa de desarrollo dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

13. Relaciones con terceros

Cuando **CIMA LAB Diagnostics** preste servicios o ceda información a terceras partes, se les hará partícipe de esta Política de Seguridad de la Información y de las normas e instrucciones derivadas.

Asimismo, cuando **CIMA LAB Diagnostics** utilice servicios de terceros o ceda información a terceros se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información. Los terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.