POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Blumind Technologies, S.L.

Marca «Waterbenchmarks» — www.waterbenchmarks.ai

Versión 1.0 — 20 de junio de 2026 · Aprobada por la Dirección · Documento público

1. Objeto y aprobación

Esta Política de Seguridad de la Información establece el compromiso de la Dirección de Blumind Technologies, S.L. (en adelante, "la Empresa"), responsable del proyecto y marca **Waterbenchmarks**, con la protección de la información que maneja y de los sistemas que la soportan.

La presente política ha sido aprobada por la Dirección y es efectiva desde su fecha de aprobación, manteniéndose vigente hasta que sea sustituida por una versión posterior. Es de obligado cumplimiento para todas las personas incluidas en su alcance.

2. Alcance

Alcance subjetivo. Esta política obliga a todas las personas del equipo de Waterbenchmarks, así como a colaboradores y proveedores que accedan a su información o sistemas, tanto en local como en remoto.

Alcance objetivo. Se aplica a los activos de información del proyecto, en particular:

- el sitio web **www.waterbenchmarks.ai** y sus formularios;
- los **servicios de terceros (SaaS y alojamiento en la nube)** en los que se apoya la operación (por ejemplo, plataforma de email/marketing, alojamiento web y herramientas de productividad);
- los sistemas y datos empleados para la **evaluación y comparativa (benchmark) de modelos de IA**;
- los **datos personales** tratados: suscriptores de la newsletter, consultas del formulario de contacto y usuarios registrados.

3. Principios de seguridad

La gestión de la seguridad de la información en Waterbenchmarks se rige por los siguientes principios:

- **Seguridad como proceso continuo.** La seguridad no es una acción puntual, sino una práctica permanente que abarca personas, herramientas y procesos.
- **Gestión basada en riesgos.** Identificamos y valoramos los riesgos sobre nuestra información de forma proporcionada a nuestro tamaño y actividad, y priorizamos las medidas en función de ellos.
- **Mínimo privilegio.** Cada persona y cada servicio accede únicamente a la información y funciones que necesita para su tarea.
- **Protección de datos desde el diseño.** Aplicamos minimización de datos, control de accesos y conservación limitada en todo tratamiento de datos personales.

- **Responsabilidad sobre los proveedores.** Al apoyarnos en servicios de terceros, exigimos y verificamos que ofrezcan garantías de seguridad adecuadas.
- **Mejora continua.** Revisamos y actualizamos nuestras medidas cuando cambian la tecnología, los riesgos o nuestra actividad.

4. Objetivos de seguridad

Esta política persigue garantizar, de forma proporcionada, la **confidencialidad, integridad y disponibilidad** de la información, y en concreto:

- proteger los datos personales de suscriptores, contactos y usuarios registrados;
- controlar quién accede a las cuentas y herramientas del proyecto;
- asegurar que los proveedores que tratan datos por nuestra cuenta ofrecen garantías suficientes;
- mantener la disponibilidad del sitio web y los servicios esenciales;
- detectar y responder adecuadamente a los incidentes de seguridad.

5. Marco normativo y de referencia

La Empresa se compromete a cumplir la normativa aplicable a su actividad, en particular el **Reglamento General de Protección de Datos (RGPD)**, la **LOPDGDD** y la normativa de servicios de la sociedad de la información (**LSSI**).

Como referencia de buenas prácticas, esta política se inspira en los principios de la norma **ISO/IEC 27001**, adaptados al tamaño y la madurez actuales del proyecto.

> **Sobre el Esquema Nacional de Seguridad (ENS).** Waterbenchmarks no presta actualmente servicios al sector público, por lo que el ENS (RD 311/2022) no le resulta de aplicación obligatoria a día de hoy. En caso de contratar con administraciones públicas en el futuro, la Empresa adaptará esta política y adoptará los roles, controles y documentación adicionales que el ENS exija antes de iniciar dicha actividad.

6. Organización y responsabilidades

Dada la estructura actual del proyecto (equipo reducido), la organización de la seguridad se mantiene sencilla y proporcionada:

- **Dirección.** Aprueba esta política, asigna los recursos necesarios y asume la responsabilidad última sobre la seguridad de la información.
- **Responsable de Seguridad.** Persona designada por la Dirección que coordina las medidas de seguridad, gestiona los accesos y los proveedores, y lidera la respuesta a incidentes. Función asignada a: **[COMPLETAR: nombre del Responsable de Seguridad]**.

- **Todo el equipo y colaboradores.** Conocen y aplican esta política, usan los sistemas de forma responsable y comunican cualquier incidente o sospecha al Responsable de Seguridad.

A medida que el equipo crezca o cambie la actividad, estos roles podrán ampliarse o formalizarse (por ejemplo, mediante un comité de seguridad).

7. Seguridad de proveedores y terceros

Dado que la operación de Waterbenchmarks se apoya en servicios de terceros, la gestión de proveedores es un elemento central de esta política. La Empresa se compromete a:

- seleccionar proveedores que ofrezcan garantías adecuadas de seguridad y cumplimiento del RGPD;
- suscribir, cuando proceda, los **contratos de encargo de tratamiento** correspondientes con quienes traten datos personales por su cuenta;
- verificar que las transferencias internacionales de datos, si las hubiera, cuenten con las garantías exigidas por el RGPD;
- limitar el acceso de cada proveedor a lo estrictamente necesario.

8. Protección de datos personales

El tratamiento de datos personales se realiza conforme a la Política de Privacidad del proyecto y al RGPD: con base jurídica, minimización, conservación limitada y respeto a los derechos de las personas. Las solicitudes y consultas en esta materia se atienden a través de **alvaro@blumind.es**.

9. Gestión de incidentes

La Empresa establece mecanismos razonables para **prevenir, detectar, responder y recuperarse** de los incidentes de seguridad. Cualquier incidente que afecte a datos personales se gestionará conforme a las obligaciones del RGPD, incluida, cuando corresponda, la notificación a la Agencia Española de Protección de Datos (AEPD) y a las personas afectadas.

10. Vigencia y revisión

Esta política se revisará al menos una vez al año, y adicionalmente cuando cambien las circunstancias legales, técnicas u organizativas que la fundamentan. Está disponible públicamente y se facilita a quien la solicite. Cada versión queda registrada y las anteriores se archivan.

La Dirección de Blumind Technologies, S.L.

Alvaro Diaz del Rio Redondo — Administrador

20 de junio de 2026

Blumind Technologies, S.L. · CIF B26982181 · Calle Ponzano 52, 2ºB, 28003 Madrid

DIAZ DEL RIO REDONDO ALVARO - 53615746D

Firmado digitalmente por DIAZ DEL RIO REDONDO ALVARO - 53615746D
Fecha: 2026.06.20 20:28:52 +02'00'