ANEXO III AL DPA - MEDIDAS TECNICAS Y ORGANIZATIVAS
AIKIT RESEARCH, S.A.

Version vigente desde: abril 2026

El presente Anexo III forma parte indisociable del Acuerdo de Procesamiento de Datos (DPA) suscrito entre el Cliente (Responsable del Tratamiento) y AIKIT RESEARCH, S.A. (Encargado del Tratamiento) y describe las medidas tecnicas y organizativas adoptadas por AIKIT RESEARCH, S.A. para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, conforme al articulo 32 del Reglamento (UE) 2016/679 (RGPD).

1. CONFIDENCIALIDAD

1.1. Control de acceso fisico

Los centros de datos en los que se aloja la informacion del Cliente son operados por proveedores cloud certificados con controles fisicos de acceso, vigilancia 24/7 y registro de visitas. AIKIT RESEARCH, S.A. no aloja informacion del Cliente en instalaciones propias.

1.2. Control de acceso logico

- Autenticacion robusta de usuarios mediante credenciales individuales y autenticacion multifactor (MFA) en las cuentas con acceso a sistemas que tratan informacion del Cliente.
- Politicas de complejidad y rotacion de contrasenas.
- Bloqueo automatico de sesion tras periodo de inactividad.
- Cifrado de los dispositivos corporativos (endpoints) en los que se almacene informacion del Cliente.
- Acceso administrativo bajo principios Zero-Trust.

1.3. Control de autorizacion

- Modelo de control de acceso basado en roles (RBAC) con aplicacion del principio de minimo privilegio.
- Revision periodica (al menos anual) de los accesos.
- Registro de los accesos a sistemas que tratan informacion del Cliente.
- Revocacion inmediata de los accesos al cesar la relacion laboral o contractual del personal autorizado.

1.4. Separacion (multi-tenant)

La plataforma esta disenada con segregacion logica de datos entre clientes. La informacion de cada Cliente se aisla mediante identificadores unicos y controles de acceso a nivel aplicativo y de almacenamiento.

1.5. Separacion de entornos

Los entornos de desarrollo, preproduccion y produccion estan segregados. Los datos del Cliente se procesan exclusivamente en el entorno de produccion.

1.6. Cifrado

- Cifrado en transito: TLS 1.2 o superior en todas las comunicaciones entre el Cliente y la plataforma, asi como entre los componentes internos del servicio.
- Cifrado en reposo: AES-256 o equivalente para los datos del Cliente almacenados de forma persistente, incluidos los

backups.
- Gestion centralizada de claves y secretos con politica de rotacion.

2. INTEGRIDAD

2.1. Control de transferencias

- Comunicaciones cifradas mediante HTTPS/TLS.
- Web Application Firewall (WAF) frente a trafico malicioso.
- Filtrado y proteccion frente a amenazas en correo electronico corporativo.
- Soluciones EDR/Antivirus en endpoints corporativos.

2.2. Control de entrada

- Registro de actividad (audit trail) con identificador unico de usuario para las acciones relevantes sobre datos del Cliente.
- Marcas temporales y conservacion de logs durante el periodo necesario para fines de seguridad y cumplimiento.

2.3. Desarrollo seguro

- Practicas de Secure Software Development Lifecycle (SDLC).
- Revision de codigo entre pares antes de despliegue a produccion.
- Analisis automatizado de dependencias y vulnerabilidades en el ciclo de integracion continua.
- Infraestructura como codigo (IaC) versionada.
- Testing automatizado.

3. DISPONIBILIDAD Y RESILIENCIA

3.1. Hosting y arquitectura

- Infraestructura cloud certificada (Microsoft Azure y proveedores conforme al Anexo II) con redundancia geografica dentro del EEE en el despliegue estandar.
- Monitorizacion continua y alertas automaticas de disponibilidad y rendimiento.
- Proteccion frente a denegacion de servicio (CDN + bot management).

3.2. Recuperacion

- Backups automatizados con periodicidad adecuada al riesgo.
- Cifrado de los backups (AES-256 o equivalente).
- Pruebas periodicas de recuperacion.
- Plan de continuidad y recuperacion documentado.

4. PROCEDIMIENTOS DE REVISION

4.1. Gestion de proteccion de datos

- Contacto en materia de proteccion de datos: admin@aikit.io.
- Revision al menos anual de las medidas tecnicas y organizativas.
- Formacion periodica del personal en proteccion de datos y seguridad de la informacion.
- Realizacion de Evaluaciones de Impacto (DPIA) cuando proceda conforme al articulo 35 del RGPD.

4.2. Gestion de vulnerabilidades

- Escaneos automatizados de vulnerabilidades.
- Pruebas de penetracion (pentests) periodicas, al menos anuales, realizadas por terceros independientes.
- Politica publica de divulgacion responsable de vulnerabilidades (Vulnerability Disclosure Policy).

4.3. Respuesta a incidentes

- Gestion centralizada de logs y alertas (SIEM).
- Capacidad de bloqueo inmediato de cuentas comprometidas.
- Procedimiento de respuesta a incidentes documentado, con intervencion de la Direccion y del equipo tecnico.
- Notificacion al Cliente de brechas de seguridad sin dilacion indebida y, en todo caso, dentro de las setenta y dos (72) horas siguientes a su conocimiento, conforme al DPA.

4.4. Privacy by design / by default

- Aplicacion de los principios de privacidad desde el diseno y por defecto en el desarrollo de nuevas funcionalidades.
- Minimizacion de datos: la plataforma trata unicamente los datos necesarios para la prestacion del servicio.

4.5. Gestion de subencargados

- Revision previa y diligencia debida de los subencargados.
- Suscripcion de contratos de encargado del tratamiento con los subencargados, replicando las obligaciones del presente DPA.
- Suscripcion de garantias de transferencia internacional (Clausulas Contractuales Tipo, EU-U.S. DPF) cuando proceda.

5. ORGANIZACION

5.1. Politicas internas

AIKIT RESEARCH, S.A. mantiene un sistema de politicas internas que incluyen, entre otras, una Politica de Seguridad de la Informacion, una Politica de Proteccion de Datos y una Politica de Inteligencia Artificial.

5.2. Personal

Todo el personal de AIKIT RESEARCH, S.A. y sus colaboradores externos quedan sujetos a obligaciones contractuales de confidencialidad y a los estandares de seguridad recogidos en los protocolos internos.

5.3. Compromiso de no entrenamiento

AIKIT RESEARCH, S.A. NO utiliza los datos personales del Cliente, los Inputs ni los Outputs para entrenar modelos de inteligencia artificial propios ni de terceros, ni para ningun fin distinto del estrictamente necesario para ejecutar el servicio.

6. ACTUALIZACION DE LAS MEDIDAS

AIKIT RESEARCH, S.A. revisa y actualiza las medidas tecnicas y organizativas del presente Anexo cuando lo justifiquen cambios en la tecnologia, en los riesgos identificados, en la normativa aplicable o en las mejores practicas del sector. Las actualizaciones no podran reducir el nivel de proteccion previsto.

==========
CONTACTO
==========

Contacto de protección de datos: admin@aikit.io
Cuestiones operativas: admin@aikit.io
Reporte de incidentes: admin@aikit.io

==========
Fin del documento - Anexo III al DPA: Medidas Tecnicas y Organizativas
==========