Protocolo de Tratamiento y Proteccion de Datos Personales

Politica detallada de privacidad, datos, documentos temporales, metadatos, eliminacion y seguridad.

Producto	TestingAsking
Titular/propietario comercial	MapaTech
Codigo de documento	TA-LEGAL-003
Version	0.1 - Borrador preliminar para revision legal
Fecha	2026-06-09
Clasificacion	Publico una vez revisado / Privacidad y cumplimiento

Advertencia: este documento es un borrador legal preliminar preparado con base en el estado tecnico y comercial actual del proyecto. Debe ser revisado, adaptado y aprobado por un abogado habilitado antes de publicarse, firmarse, incorporarse a la app, usarse en Play Store/App Store o presentarse a usuarios, instituciones, inversionistas o autoridades. Nada en este documento debe interpretarse como garantia de blindaje absoluto frente a reclamos, sanciones o demandas.

Control del documento

Campo	Detalle	Campo	Detalle
Responsable	MapaTech	Revision legal	Representante legal / asesor legal pendiente
Estado	Borrador no vinculante	Uso	Preproduccion / preparacion de politicas
Contacto	[correo de contacto legal/privacidad pendiente]	Pais base	Ecuador
Actualizacion	Cada vez que cambien funciones, proveedores, pagos o normativa	Aceptacion	Click-wrap / checkbox expreso en app y web

Indice de contenido

1. Objeto y alcance del protocolo

Este Protocolo de Tratamiento y Proteccion de Datos Personales describe como TestingAsking recolecta, usa, almacena, protege, comparte, conserva, elimina o anonimiza datos personales, datos educativos, documentos temporales, examenes generados, actividad, dispositivos, soporte, facturacion y metadatos no personales.

El protocolo debe alinearse con la Ley Organica de Proteccion de Datos Personales de Ecuador, su reglamentacion, las politicas de Google Play y App Store, terminos de proveedores de IA, contratos institucionales y cualquier normativa aplicable en los paises donde se ofrezca el servicio.

Este documento no sustituye el aviso de privacidad resumido que debe mostrarse en la app ni la politica publica completa que debe estar disponible antes de recolectar datos personales.

2. Roles de tratamiento

MapaTech, como operador comercial de TestingAsking, podra actuar como responsable del tratamiento respecto de usuarios particulares y como responsable, corresponsable o encargado respecto de usuarios institucionales, segun el contrato firmado con la universidad, colegio, academia, empresa u organizacion.

En planes institucionales, la entidad contratante puede determinar finalidades propias, por ejemplo crear usuarios, asignar licencias, revisar reportes, gestionar grupos o medir progreso. En tal caso, el contrato debe definir obligaciones, permisos, base legal, canales de atencion y limites de acceso a informacion.

Proveedores como hosting, IA, tiendas de aplicaciones, pasarelas de pago, correo, analitica o soporte podran actuar como encargados, subencargados, responsables independientes o proveedores tecnicos, segun sus terminos y contratos.

3. Principios de tratamiento

- Transparencia: informar al usuario que datos se tratan y para que.
- Finalidad: usar los datos para fines legitimos, especificos y comunicados.
- Minimizacion: evitar solicitar datos innecesarios.
- Seguridad: aplicar medidas razonables para proteger los datos.
- Confidencialidad: limitar el acceso al personal o proveedores que lo necesiten.
- Conservacion limitada: mantener datos personales solo por el tiempo necesario o legalmente justificado.
- Responsabilidad demostrada: documentar decisiones, proveedores, medidas y cambios.
- Control del usuario: habilitar acceso, rectificacion, eliminacion y otros derechos aplicables.

4. Categorias de datos tratados

TestingAsking puede tratar las siguientes categorias de datos, actuales o futuras, segun las funciones utilizadas por el usuario:

- Datos de cuenta: correo electronico, nombre de usuario, nombre o alias, hash de contraseña, ID interno, plan, rol, estado y fechas de creacion o actualizacion.
- Datos de dispositivo: device_key, plataforma, nombre del dispositivo, app_version, estado activo, ultimo uso, limite de dispositivos y senales de heartbeat.
- Datos de actividad: login, generacion de examenes, intentos, resultados, publicaciones, errores, eventos de uso y navegacion basica.
- Datos educativos: documentos temporales, texto extraido, tema detectado, banco de preguntas, respuestas, puntajes, progreso e historial.
- Datos de IA: modelo usado, prompt o contenido enviado, respuesta generada, tokens, costo estimado, tiempo de respuesta, errores, cantidad solicitada y dificultad.
- Datos de comunidad: examenes publicados, titulo, descripcion, autor, categoria, vistas, inicios, completados, valoraciones y reportes.
- Datos institucionales: administracion, entidad, usuarios asociados, roles, facturacion estimada, estado, reportes y actividad agregada o permitida.
- Datos de soporte: mensajes, asunto, prioridad, estado, responsable, historial del ticket y archivos enviados voluntariamente.
- Datos de facturacion: producto, precio, moneda, periodo, estado de suscripcion, recibo, identificador de compra, datos de factura y medio de pago segun corresponda.

5. Documentos subidos y procesamiento temporal

El documento original subido por el usuario se procesa con el objetivo de extraer texto y generar un examen. La politica tecnica prevista es no conservar permanentemente el archivo original, salvo que se active una funcion futura de almacenamiento y el usuario la acepte de forma clara.

Durante el procesamiento, el documento puede permanecer temporalmente en memoria, almacenamiento temporal del servidor, cola de procesamiento, registros tecnicos controlados o servicio de extraccion. Deben implementarse mecanismos para eliminar archivos temporales al finalizar el proceso o ante error.

El texto extraido puede enviarse al proveedor de IA para generar preguntas. Por ello, el usuario no debe subir contenido sensible, confidencial, reservado, de terceros o protegido por derechos de autor sin autorizacion.

El examen generado, a diferencia del archivo original, puede guardarse para permitir la operacion normal de la app, historial, intentos, comunidad, soporte, sincronizacion, estadisticas y mejora.

6. Finalidades del tratamiento

- Crear y administrar cuentas de usuario.
- Autenticar sesiones y proteger credenciales.
- Procesar documentos temporalmente y generar examenes mediante IA.
- Guardar examenes generados, intentos, resultados e historial.
- Mostrar progreso, graficos, retroalimentacion y resultados.
- Operar comunidad, publicaciones, reportes y moderacion.
- Administrar planes, cuotas, pagos, suscripciones e instituciones.
- Controlar limites de dispositivos, seguridad, abuso y fraude.
- Enviar comunicaciones operativas, soporte, cambios legales y avisos importantes.
- Medir rendimiento tecnico, tokens, costos de IA, errores y disponibilidad.
- Mejorar producto, experiencia, algoritmos, modelos internos, analitica y decisiones comerciales.
- Crear metricas agregadas, anonimizadas o disociadas para reportes, investigacion, presentaciones, benchmarking o comercializacion no personalizada.
- Cumplir obligaciones legales, fiscales, contables, contractuales, de tiendas, autoridades o defensa frente a reclamos.

7. Base legal o fundamento de tratamiento

La base legal especifica debe validarse con asesor legal. De forma preliminar, el tratamiento puede apoyarse en consentimiento del usuario, ejecucion de contrato o terminos aceptados, cumplimiento de obligaciones legales, interes legitimo para seguridad y mejora, autorizacion institucional o bases equivalentes permitidas por la normativa aplicable.

El consentimiento debe ser libre, informado, especifico e inequivoco cuando corresponda, especialmente para aceptacion de terminos, tratamiento de datos, envio a proveedores externos de IA, comunicaciones comerciales y uso de datos para finalidades no estrictamente necesarias.

En el caso de menores o instituciones educativas, puede requerirse autorizacion del representante legal, contrato institucional, base legal educativa u otra condicion validada juridicamente.

8. Datos sensibles y datos de terceros

TestingAsking no esta disenado para solicitar datos sensibles. Sin embargo, el usuario podria subir documentos que contengan informacion sensible o de terceros. Esta accion esta prohibida salvo que el usuario tenga autorizacion expresa, base legal suficiente y cumpla los requisitos aplicables.

- No subir datos de salud, diagnosticos, tratamientos, discapacidad, informacion genetica o biometrica.
- No subir datos financieros sensibles, claves, tarjetas, estados bancarios o informacion patrimonial privada.
- No subir datos de menores, calificaciones privadas, expedientes educativos o identificaciones sin autorizacion.
- No subir datos sobre vida sexual, orientacion, religion, politica, etnia, afiliacion, antecedentes o informacion intima.
- No subir datos de terceros, empresas o instituciones sin permiso.

Si TestingAsking detecta o recibe reporte de tratamiento indebido de datos sensibles, podra eliminar contenido, suspender cuentas, solicitar informacion, bloquear funciones y cooperar con autoridades competentes cuando corresponda.

9. Metadatos, datos agregados y datos anonimizados

TestingAsking podra conservar y utilizar metadatos no personales, datos agregados, anonimizados o disociados que no permitan identificar directa ni indirectamente a una persona. Estos datos pueden permanecer aun despues de eliminada una cuenta, porque dejan de estar asociados a un titular identificable.

Estos datos podran usarse para mejorar la plataforma, optimizar algoritmos, entrenar modelos internos, evaluar rendimiento, planificar funciones, medir demanda, crear reportes comerciales, analizar tendencias educativas, presentar resultados a aliados, negociar convenios o comercializar informacion estadistica no identificable.

La anonimización debe realizarse con criterios razonables para impedir reidentificacion. Si un dato permite identificar al usuario, debera tratarse como dato personal y estara sujeto a derechos, limitaciones y obligaciones aplicables.

Redaccion recomendada para la app

Al eliminar tu cuenta, eliminaremos o anonimizaremos tus datos personales conforme a la ley. Podremos conservar informacion agregada o anonimizada que no te identifique para mejorar TestingAsking, generar estadisticas, entrenar algoritmos internos y desarrollar productos o reportes no personalizados.

10. Conservacion y eliminacion de datos

Los plazos de conservacion deben definirse tecnicamente antes de produccion. Como base preliminar:

- Documento original: procesamiento temporal y eliminacion al finalizar la generacion o tras ventana tecnica breve.
- Texto extraido: conservacion temporal o limitada, salvo que forme parte del examen generado.
- Examen generado: mientras la cuenta este activa, hasta eliminacion por el usuario o segun politica de retencion.
- Intentos y resultados: mientras el usuario requiera historial o hasta eliminacion/anonymizacion de cuenta.
- Examenes publicos: hasta despublicacion, eliminacion por moderacion o retiro solicitado conforme a politicas.
- Logs tecnicos: periodo limitado necesario para seguridad, diagnostico y auditoria.
- Facturacion y contratos: periodo legal, contable o fiscal correspondiente.
- Soporte: periodo necesario para resolver casos, auditoria y mejora de atencion.
- Datos anonimizados/agregados: conservacion indefinida o de largo plazo al no identificar titulares.

11. Eliminacion de cuenta

El usuario podra solicitar eliminacion de cuenta mediante la app, web, correo o canal habilitado. Una vez validada la identidad, TestingAsking eliminara o anonimizara datos personales asociados, incluyendo nombre, correo, identificadores de cuenta, credenciales, perfiles y datos personales directamente vinculados.

La eliminacion no sera inmediata sobre copias de seguridad, registros de seguridad, logs tecnicos, comprobantes contables, evidencias de fraude, reclamos activos, contratos, obligaciones legales o informacion necesaria para defensa juridica. Dichos datos se conservaran por el plazo justificado y luego se eliminaran o anonimizaran.

La eliminacion tampoco alcanzara informacion agregada, anonimizada, disociada, estadistica o no personal que no permita identificar al usuario. Este punto debe explicarse de forma transparente antes de que el usuario acepte el servicio.

12. Derechos del titular

El titular de datos podra ejercer los derechos que le reconozca la normativa aplicable, incluyendo acceso, rectificacion, actualizacion, eliminacion, oposicion, suspension, portabilidad, no ser objeto de decisiones automatizadas cuando aplique y revocatoria de consentimiento en los casos permitidos.

Para ejercer derechos, el usuario debera comunicarse al canal de privacidad indicado, acreditar su identidad y especificar la solicitud. TestingAsking debera responder dentro de los plazos legales aplicables o informar razones de demora, rechazo o imposibilidad cuando corresponda.

En usuarios institucionales, algunas solicitudes pueden requerir coordinacion con la entidad contratante si esta actua como responsable o corresponsable del tratamiento.

13. Transferencias y proveedores externos

TestingAsking puede utilizar proveedores nacionales o internacionales para hosting, base de datos, inteligencia artificial, tiendas de aplicaciones, pagos, correo, soporte, analitica, seguridad, backups y otros servicios necesarios para operar la plataforma.

Proveedores actuales o previstos incluyen Hostinger para infraestructura VPS, Google Gemini API para generacion de examenes, Google Play y App Store para distribucion y pagos, proveedores de correo, pasarelas de pago, sistemas de soporte y herramientas de analitica futuras.

El usuario entiende que algunos datos pueden ser tratados fuera de Ecuador o del pais de residencia. MapaTech debera implementar las medidas contractuales, tecnicas y organizativas razonables para dichas transferencias, conforme a la normativa aplicable y terminos del proveedor.

14. Seguridad tecnica y organizativa

TestingAsking debe aplicar medidas proporcionales al riesgo, incluyendo cifrado en transito mediante HTTPS, almacenamiento de contraseñas con hash seguro, proteccion de claves en variables de entorno, base de datos no expuesta publicamente, acceso administrativo restringido, registros de seguridad, separacion por administracion y controles de permisos.

Tambien se recomiendan backups, snapshots, rotacion de claves, rate limiting, auditoria de panel administrativo, validacion de archivos, limites de tamano, limpieza de temporales, monitoreo, gestion de vulnerabilidades, control de CORS, logs sin datos sensibles y protocolos de respuesta ante incidentes.

Ningun sistema es absolutamente seguro. El usuario acepta que existen riesgos inherentes al uso de internet, proveedores externos, IA, dispositivos personales y cargas de archivos. TestingAsking notificara incidentes cuando sea legalmente obligatorio o razonablemente necesario.

15. Heartbeat, usuarios online y trazabilidad

TestingAsking puede implementar senales de heartbeat para registrar que una app esta activa, por ejemplo al abrir la app, iniciar sesion, volver de segundo plano, generar un examen o cada cierto intervalo mientras la app este en uso.

Estos registros pueden incluir user_id, device_key, plataforma, app_version, marca temporal, ultimo uso, estado de sesion y datos tecnicos razonables. Su finalidad es seguridad, limite de dispositivos, soporte, usuarios online, diagnostico, analitica, facturacion institucional y prevencion de abuso.

La politica de privacidad debe comunicar esta funcion antes de activarla en produccion.

16. Reportes institucionales

En planes institucionales, TestingAsking puede entregar reportes a administradores autorizados. Los reportes podran ser agregados o individuales segun contrato, base legal, permisos, configuracion y consentimiento o informacion previa aplicable.

Los reportes pueden incluir usuarios activos, examenes generados, intentos, progreso, tiempos, temas, niveles de dificultad, resultados, uso de IA, actividad por periodo, facturacion estimada y datos necesarios para soporte o administracion.

Cada administracion debera ver solo la informacion que le corresponde. Debe evitarse filtracion entre instituciones mediante filtros, permisos, tokens, validaciones backend y auditoria.

17. Incidentes, contenido ilegal y autoridades

Si se detecta contenido ilegal, datos personales expuestos, material sexual explicito, explotacion infantil, amenazas, fraude, malware, infraccion de derechos o riesgo para usuarios, TestingAsking podra bloquear contenido, preservar evidencias, suspender cuentas, investigar, notificar a proveedores, atender requerimientos y cooperar con autoridades competentes.

La entrega de informacion a autoridades se realizara cuando exista requerimiento legal valido, orden competente, obligacion normativa, emergencia razonable o fundamento permitido por ley. TestingAsking procurara entregar solo la informacion necesaria y documentar la respuesta.

18. Aviso corto para incorporar en la app

Texto sugerido para mostrar antes de aceptar privacidad:

TestingAsking procesa tus documentos temporalmente para convertirlos en examenes inteligentes. El documento original no se conserva de forma permanente. El examen generado, tus respuestas, resultados, historial y datos tecnicos de uso pueden guardarse para permitirte practicar, medir progreso, recibir soporte, usar comunidad y mejorar el servicio. El texto

extraido puede enviarse a proveedores externos de IA. No subas informacion sensible, confidencial o documentos sobre los que no tengas derechos o autorizacion.

19. Checklist minimo antes de produccion

Antes de publicar una nueva APK, activar planes de pago o abrir convenios institucionales, se recomienda completar este checklist de privacidad y datos:

- Publicar politica de privacidad completa en una URL estable y accesible desde la app, landing y ficha de tienda.
- Agregar pantalla de aceptacion expresa de terminos, privacidad y aviso de IA antes de subir documentos.
- Implementar mecanismo visible para solicitar eliminacion de cuenta y datos personales.
- Separar claramente documento original temporal, examen generado, intentos, resultados y metadatos anonimizados.
- Registrar fecha, version y evidencia de aceptacion de terminos por usuario.
- Configurar eliminacion automatica de archivos temporales y logs rotativos.
- Documentar proveedores externos, finalidades y transferencias internacionales.
- Completar Data Safety de Google Play y requisitos equivalentes de App Store.
- Implementar reportes y moderacion para contenido de comunidad.
- Validar que cada administracion institucional solo vea los datos que le corresponden.
- Crear procedimiento de respuesta a incidentes, solicitudes de autoridades y reclamos de propiedad intelectual.

Anexo final: aprobacion antes de publicacion

Antes de usar este documento en produccion, MapaTech deberia completar los datos pendientes de identificacion, domicilio, RUC o identificacion fiscal, correo de privacidad, contacto de soporte, jurisdiccion aplicable, politica de reembolsos definitiva, mecanismo de eliminacion de cuenta y canal de reclamos de propiedad intelectual.

El documento deberia validarse con un abogado de Ecuador y, si la app se publica fuera del pais, con asesoria de cada jurisdiccion relevante. Tambien deberia revisarse contra las politicas vigentes de Google Play, App Store, proveedores de IA, proveedores de hosting y pasarelas de pago aplicables.

Preparado por	TestingAsking / MapaTech - borrador asistido
Revisado por abogado	[pendiente]
Aprobado por representante legal	[pendiente]
Fecha de entrada en vigencia	[pendiente]