



CONDICIONES DE USO Y DECLARACIÓN DE PRIVACIDAD – ANTON.IA LEAD NAVIGATOR

Última actualización: 27-08-2025

1. QUIÉNES SOMOS Y ALCANCE

- ANTON.IA Lead Navigator es una plataforma SaaS de automatización de ventas B2B que ayuda a identificar leads, enriquecer información, investigar empresas con IA y enviar correos personalizados a través de la cuenta de Microsoft Outlook del propio usuario.
- ROLES: Para efectos de protección de datos, ANTON.IA (el proveedor) actúa normalmente como ENCARGADO/PROCESADOR respecto del tratamiento de datos de leads ejecutado en nombre del CLIENTE (la organización usuaria), quien es el RESPONSABLE/CONTROLADOR al definir las finalidades (prospección y contacto B2B). En módulos propios de cuenta/facturación, ANTON.IA puede actuar como responsable respecto de sus usuarios administrativos.
- ALCANCE: Este documento aplica al uso del sitio, de la aplicación web y de las integraciones con proveedores externos descritos en el Anexo 1. Salvo que se indique lo contrario, las integraciones operadas para la prospección (p. ej., scraping/obtención de datos públicos) son configuradas y administradas por ANTON.IA como subencargado en nombre del CLIENTE.

2. RESUMEN DE PRIVACIDAD

- Principio de mínimo privilegio: pedimos exclusivamente permisos delegados de Microsoft Graph necesarios para operar. Por defecto: User.Read (identidad) al conectarse; Mail.Send (enviar) solo al momento de enviar un correo; Mail.Read (leer) es opcional y se solicita únicamente si el usuario activa el tracking por acuses/seguimiento desde su propia bandeja. No se usan permisos de aplicación ni *.Read.All.

- Autenticación segura: OAuth 2.0/OIDC con PKCE. Tokens de acceso se almacenan en sessionStorage del navegador; no guardamos contraseñas ni refresh tokens de larga duración (sin offline_access).
- Envío de correos: el correo se crea y envía vía Microsoft Graph en la cuenta del usuario. ANTON.IA no almacena las credenciales ni copia el contenido en sus servidores; guarda metadatos mínimos para seguimiento (p. ej., internetMessageId, conversationId) cuando el usuario lo permite.
- Transparencia y control: el usuario puede desconectar su cuenta Outlook, borrar leads y reportes; el administrador del CLIENTE puede revocar consentimientos desde Microsoft Entra.

3. DATOS QUE TRATAMOS

A) Datos de cuenta y autenticación (usuario):

- Identificadores de Microsoft (id, nombre, email) obtenidos con User.Read.
- Tokens de acceso (sessionStorage del navegador del usuario; vida corta).
- B) Datos de leads y empresas (B2B):
 - Identificadores públicos o de negocio: nombre, cargo, empresa, industria, ubicación aproximada, URLs públicas (p. ej., LinkedIn), correo profesional, dominio, tamaño de empresa, tecnologías declaradas, etc.
 - Origen: i) entradas manuales del usuario;
 - ii) servicios de búsqueda/enriquecimiento operados por ANTON.IA como subencargado (p. ej., actores de Apify administrados por ANTON.IA) y otras fuentes autorizadas;
 - iii) opcionalmente, fuentes/conectores que el CLIENTE decida integrar por su cuenta y bajo su responsabilidad.

C) Contenido y metadatos de comunicación:

- Asunto y cuerpo del email redactado por el usuario (o generado por IA a petición del usuario) y destinatarios/CC/BCC.
- Metadatos de Graph: messageId, internetMessageId, conversationId; acuses estándar de entrega/lectura y –si se activa– mensajes de la misma conversación del buzón del propio usuario (Mail.Read opcional).
- D) Datos técnicos y de uso:
 - Registros de actividad (timestamps, IP aproximada, agente de usuario/navegador), eventos técnicos y métricas de rendimiento.

4. FINALIDADES DEL TRATAMIENTO

- Operar la plataforma: autenticación, permisos, envío de correos desde la cuenta del usuario, gestión de leads/oportunidades, ejecución de flujos de investigación/IA a petición del usuario.
- Soporte y seguridad: depuración de errores, prevención de fraude/abuso, mantener disponibilidad y rendimiento.
- Analítica operativa agregada: uso de funciones a nivel de producto sin identificar personas.
- Cumplimiento legal y contractual.

5. BASES LEGALES

- Ejecución de contrato o medidas precontractuales: brindar el servicio solicitado por el CLIENTE (autenticación, envío de correos, investigación, etc.).
- Interés legítimo del CLIENTE en actividades B2B de prospección, siempre con salvaguardas y respeto de normas anti-spam y de datos aplicables.
- Consentimiento del usuario final para conectar su cuenta de Microsoft y, si corresponde, para activar el tracking que requiere Mail.Read.
- Cumplimiento de obligaciones legales (p. ej., atención de derechos).

6. CÓMO ENVIAMOS CORREOS Y CÓMO SEGUIMOS RESULTADOS

- Envío: ANTON.IA solicita un token de Mail.Send y crea un borrador en /me/messages, luego invoca /me/messages/{id}/send en Microsoft Graph. El correo se envía desde la cuenta del usuario.
- Seguimiento: por defecto se pueden solicitar acuses estándar (entrega/lectura) sin píxeles. Opcionalmente, si el usuario activa tracking, ANTON.IA pide el permiso Mail.Read y consulta mensajes de la misma conversación en el buzón del propio usuario. Esto puede desactivarse en cualquier momento.
- Limitación: ANTON.IA no accede a otros buzones de la organización ni a directorios globales. No se usan permisos de aplicación.

7. CONSERVACIÓN

- Metadatos de envío/seguimiento, leads y reportes: se conservan mientras la cuenta del CLIENTE esté activa o hasta que CLIENTE/usuario los elimine.
- Registros técnicos: se conservan mientras la cuenta del CLIENTE esté activa o hasta que CLIENTE/usuario los elimine.

8. TRANSFERENCIAS Y UBICACIÓN DE DATOS

- Microsoft Graph (Microsoft Corporation) opera infraestructura global; el tratamiento se realiza conforme a los términos estándar de Microsoft.
- Proveedores tercerizados (subencargados) utilizados por ANTON.IA para funciones específicas se listan en el Anexo 1, con su ubicación y garantías (p. ej., SCCs/RGPD, cláusulas tipo, etc.).

9. SEGURIDAD

- Capa de transporte cifrada (HTTPS/TLS); autenticación OIDC con PKCE.
- Tokens en sessionStorage (sin offline_access) y sesión revocable. No almacenamos contraseñas de Microsoft.
- Principio de mínimo privilegio (solo /me/* y permisos delegados). Auditorías de permisos en Azure/Entra.
- Controles internos razonables: gestión de vulnerabilidades, control de accesos, registro de eventos e incidencia.

10. DERECHOS DE TITULARES

- Dependiendo de la jurisdicción, los usuarios pueden ejercer derechos de acceso, rectificación/actualización, cancelación/supresión, oposición/limitación y portabilidad.
- Solicituds: contacte a nicolas.yarur.q@gmail.com o utilice los canales internos que el CLIENTE disponga. Cuando ANTON.IA actúe como encargado, derivará la solicitud al responsable (CLIENTE).

11. OBLIGACIONES DEL CLIENTE Y DEL PROVEEDOR

- Del CLIENTE: declara y garantiza que posee base legal para tratar datos de leads y contactarlos (p. ej., interés legítimo B2B, consentimiento o excepción aplicable) y que cumplirá la normativa anti-spam/canales (CAN-SPAM, RGPD ePrivacy, LGPD, normas locales, etc.). Gestionará mecanismos de opt-out/unsubscribe cuando corresponda. El contenido y destinatarios de cada correo son responsabilidad del CLIENTE.
- De ANTON.IA (proveedor): configura y opera los flujos de búsqueda/enriquecimiento (p. ej., actores de Apify) como subencargado, obteniendo exclusivamente datos lícitos (fuentes públicas o con licencia) y respetando términos de uso de las fuentes. Ajustará o desactivará flujos ante avisos de incumplimiento o requerimientos del CLIENTE o de la autoridad competente.

12. COOKIES Y ALMACENAMIENTO LOCAL

- ANTON.IA utiliza cookies/tokens estrictamente necesarios para autenticación y seguridad. No emplea cookies de terceros con fines publicitarios en la versión empresarial, salvo que el CLIENTE las incorpore en su propio dominio.
- El almacenamiento local empleado por la app es el sessionStorage del navegador del usuario; su contenido se elimina al cerrar la pestaña o expirar la sesión.

13. MENORES DE EDAD

- ANTON.IA es un servicio B2B y no está dirigido a menores. No recopilamos conscientemente datos de menores.

14. CAMBIOS A ESTA POLÍTICA

- Podremos actualizar este documento para reflejar mejoras o cambios regulatorios. Se informará al CLIENTE mediante los canales acordados. La continuidad del uso implica la aceptación de la versión actualizada.

15. CONTACTO

- Responsable de privacidad/seguridad: Nicolas Fuelles Yarur Gongora , nicolas.yarur,g@gmail.com.

CONDICIONES DE USO (TÉRMINOS)

16. CUENTA Y ACCESO

- El usuario debe mantener la confidencialidad de sus credenciales y de los tokens de acceso. Cualquier actividad realizada desde su sesión se presume autorizada por él.
- ANTON.IA puede suspender o restringir el acceso ante indicios de abuso, incumplimiento o riesgo de seguridad.

17. LICENCIA Y PROPIEDAD INTELECTUAL

- ANTON.IA otorga al CLIENTE una licencia limitada, no exclusiva e intransferible para usar el servicio conforme a estos términos y a la documentación. El software, marcas, modelos y contenidos pertenecen a sus respectivos titulares.

18. USOS PROHIBIDOS

- Enviar correo no solicitado en contravención de las leyes aplicables; recopilar datos de manera ilícita; intentar acceder a buzones o datos de terceros; vulnerar medidas de seguridad; ingeniería inversa salvo lo permitido por ley; sobrecargar o interferir con el servicio.

19. CONTENIDOS Y RESPONSABILIDAD

- El CLIENTE es responsable del contenido de los correos, de la selección de destinatarios y del tratamiento de datos de leads. ANTON.IA no responde por usos indebidos del servicio ni por la disponibilidad de servicios de terceros (Microsoft, Apify u otros) fuera de su control.

20. DISPONIBILIDAD Y SOPORTE

- El servicio se presta “como está” y “según disponibilidad”. Se ofrecerá soporte razonable en los canales definidos. Cualquier SLA específico debe constar en un anexo comercial/contrato de servicio.

ANEXO 1 — PROVEEDORES Y SUBENCARGADOS (REFERENCIAL)

- Microsoft Corporation (Microsoft Graph / Outlook 365): autenticación y envío de correos del usuario.
- Apify (administrado por ANTON.IA): ejecución de actores configurados por ANTON.IA para obtención de datos públicos autorizados.

- n8n Cloud o infraestructura orquestada por ANTON.IA: flujos de investigación/IA.

ANEXO 2 — RETENCIÓN Y CONTROLES (EJEMPLO – ADAPTAR)

- Leads y empresas: vigencia del contrato o eliminación a solicitud.
- Metadatos de correos (IDs/conversaciones): vigencia o eliminación a solicitud.
- Registros técnicos (logs): vigencia o eliminación a solicitud.
- Backups: cifrados; rotación conforme a política interna.

ANEXO 3 — DERECHOS Y CANALES DE ATENCIÓN

- Canal para solicitudes de derechos: nicolas.yarur.g@gmail.com.
- Plazos de respuesta: 2 días prorrogables cuando la ley lo permita.

ANEXO 4 — CONFIGURACIÓN DE PRIVACIDAD RECOMENDADA

- Azure/Entra: permisos delegados User.Read y Mail.Send; Mail.Read solo si se habilita tracking. Sin *.Read.All ni permisos de aplicación. Sin offline_access.
- Enterprise Applications: “User assignment required = Yes” (opcional) y revocar consentimientos innecesarios. Auditorías periódicas.
- App: tokens en sessionStorage, logout visible, panel que indique scopes activos y opción para desactivar tracking.