Política general de privacidad y tratamiento de datos personales

Soluciones de Confianza Digital Verifica IA S.A.S.

Dato del documento	Información
Responsable	Soluciones de Confianza Digital Verifica IA S.A.S. - NIT 901.739.560-4
Versión y vigencia	Versión 2.0 | Vigente desde el 15 de septiembre de 2026
Ámbito	Bases y tratamientos propios de Verifica como responsable
Canal de privacidad	juridico@verificaia.com | 314 258 9838

Esta Política explica cómo Verifica recolecta, usa, almacena, circula, transmite, transfiere, actualiza y suprime datos personales cuando decide las finalidades y los medios esenciales del tratamiento.

Regla de rol. Para todos los tratamientos descritos en esta Política, Verifica actúa como RESPONSABLE DEL TRATAMIENTO. Esta regla permite saber con claridad quién toma las decisiones, atiende tus derechos y responde por el cumplimiento.

Alcance excluido. En algunos proyectos empresariales Verifica puede prestar servicios tecnológicos siguiendo exclusivamente las instrucciones de otra organización. Esas operaciones no están reguladas por esta Política como tratamientos propios: se rigen por la política y el aviso del tercero responsable, el contrato de transmisión y las obligaciones legales que corresponden a Verifica como proveedor. Esta precisión no cambia el rol de Verifica en los tratamientos propios regulados aquí.

1. Lo esencial

- Verifica es el responsable de los tratamientos descritos en esta Política.
- Solo utilizamos datos adecuados, pertinentes y necesarios para finalidades informadas y legítimas.
- La biometría facial o de voz exige información previa y autorización expresa y separada, salvo una excepción legal documentada.
- Las comunicaciones comerciales son opcionales y pueden rechazarse sin perder el servicio principal.
- Puedes conocer, consultar, actualizar, corregir, suprimir tus datos o revocar la autorización cuando proceda.

- No vinculamos la identidad de una persona con el contenido secreto de su voto ni reutilizamos biometría para publicidad o entrenamiento de reconocimiento facial sin una finalidad nueva y autorización válida.

2. Quién responde por tus datos

Soluciones de Confianza Digital Verifica IA S.A.S. (Verifica), identificada con NIT 901.739.560-4 y domiciliada en Bogotá D.C., es el responsable del tratamiento de las bases y operaciones cubiertas por esta Política.

Canal	Información
Área responsable	Área Jurídica y de Protección de Datos de Verifica
Correo de privacidad	juridico@verificaia.com
Teléfono	301 8011067
Dirección	Carrera 13 No. 93-35, oficina 560, Bogotá D.C., Colombia
Sitio web	www.verificaia.com

El Área Jurídica y de Protección de Datos recibe y coordina las consultas, reclamos, solicitudes de actualización, rectificación, supresión y revocatoria, con apoyo de las áreas que administren la información.

3. A quiénes cubre esta Política

Grupo	Ejemplos
Visitantes, prospectos y asistentes	Personas que navegan el sitio web, usan formularios o WhatsApp, solicitan información, propuestas o demostraciones, descargan contenidos o participan en eventos.
Clientes y usuarios directos	Personas naturales y contactos, representantes, administradores o usuarios de organizaciones con las que Verifica mantiene una relación propia.
Usuarios de servicios propios	Firmantes, remitentes, destinatarios, titulares de credenciales, personas validadas, votantes o usuarios de soluciones cuando Verifica define las finalidades del tratamiento.
Proveedores, aliados y contratistas	Personas naturales y contactos de organizaciones que suministran bienes, servicios, integraciones, soporte o distribución.
Talento humano	Aspirantes, trabajadores, exempleados, practicantes, aprendices y beneficiarios o contactos relacionados con la relación laboral.
Accionistas y órganos corporativos	Accionistas, administradores, representantes, apoderados y miembros de órganos sociales, cuando corresponda.

4. Conceptos para entender la Política

Concepto	Qué significa aquí
Dato personal	Información vinculada o que pueda asociarse con una persona natural determinada o determinable.
Dato sensible	Información cuyo uso indebido puede afectar la intimidad o generar discriminación, incluida la biometría.
Tratamiento	Cualquier operación sobre datos, como recolectar, consultar, almacenar, actualizar, usar, circular, transmitir, transferir o suprimir.

Concepto	Qué significa aquí
Responsable	Quien decide sobre la base de datos, sus finalidades y los aspectos esenciales del tratamiento. En esta Política es Verifica.
Encargado de Verifica	Proveedor que trata datos por cuenta de Verifica, bajo instrucciones documentadas y sin finalidades propias incompatibles.
Titular	Persona natural a quien pertenecen los datos.

5. Nuestros principios

Verifica aplica los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. En la práctica:

- informamos finalidades específicas antes o, a más tardar, al recolectar los datos;
- recolectamos únicamente información adecuada, pertinente y necesaria;
- mantenemos mecanismos para actualizar, corregir o controvertir la información;
- limitamos el acceso a personas y proveedores que necesitan los datos para una función autorizada;
- aplicamos privacidad desde el diseño, controles proporcionales al riesgo y medidas reforzadas para biometría, documentos, credenciales y menores;
- conservamos evidencia de autorizaciones, avisos, accesos, incidentes y atención de derechos para demostrar cumplimiento.

6. Qué datos podemos utilizar

Categoría	Información incluida
Identificación y contacto	Nombre, apellidos, tipo y número de documento, firma, correo, teléfono, dirección, empresa, cargo y datos de representación.
Comercial y contractual	Solicitudes, propuestas, contratos, licencias, productos, consumos, facturación, pagos, cartera, reuniones, preferencias y autorizaciones.
Financiera, contable y tributaria	Datos bancarios, tributarios, de pago, facturación y, cuando sea legal y necesario, información comercial, financiera, crediticia o de servicios.
Laboral y de selección	Hoja de vida, formación, experiencia, referencias, evaluaciones, contrato, nómina, seguridad social, beneficiarios, SST y demás información necesaria para la relación.
Documentos y transacciones	Documentos, mensajes, anexos, destinatarios, eventos de envío, entrega, lectura, aceptación o firma, sellos de tiempo, huellas digitales, certificados y evidencias.
Identidad y validación	Imágenes del documento, datos extraídos por OCR, fotografía o video del rostro, prueba de vida, comparación, puntajes, alertas y resultado de validación.
Biometría sensible	Plantillas o patrones faciales o de voz y grabaciones usadas para identificación o autenticación, cuando el servicio lo requiera y exista autorización expresa o excepción legal.
Credenciales y acceso	Cuenta, identificadores, roles, permisos, credenciales verificables, atributos de una wallet y registros de acceso o autenticación.

Categoría	Información incluida
Técnicos y seguridad	Dirección IP, fecha y hora, dispositivo, navegador, sistema operativo, cookies, logs, intentos de acceso, incidentes y geolocalización aproximada inferida de la IP cuando sea necesaria.
Soporte y atención	Consultas, tickets, archivos aportados, evidencia del incidente y grabaciones de llamadas o sesiones remotas cuando se haya informado y autorizado si corresponde.

Fuentes. Podemos obtener datos directamente del titular; de representantes, empleadores, contratantes, aliados o terceros legitimados; de sistemas y dispositivos utilizados; o de registros y fuentes de acceso público respecto de datos que tengan naturaleza pública. Verifica debe contar con autorización o con una excepción legal y conservar la trazabilidad de la fuente.

Minimización. Un documento, mensaje o archivo puede contener información adicional definida por quien lo crea. Verifica procurará limitar su tratamiento al contenido necesario para la finalidad informada y aplicará acceso restringido.

7. Para qué utilizamos la información

7.1 Sitio web, prospectos y comunicaciones

- Atender solicitudes, cotizaciones, demostraciones, preguntas, eventos y peticiones.
- Administrar formularios, agenda, descargas, preferencias y experiencia de navegación.
- Enviar comunicaciones comerciales propias o de aliados relacionados únicamente con autorización separada y posibilidad de retiro.
- Medir campañas y uso del sitio mediante cookies no necesarias solo después de obtener la decisión aplicable.

7.2 Clientes, aliados y proveedores

- Conocer y vincular contrapartes; verificar identidad, representación, referencias, cumplimiento y conflictos de interés.
- Negociar, celebrar, ejecutar, administrar, facturar, recaudar, renovar o terminar contratos y licencias.
- Gestionar consumos, soporte, reuniones, entregables, garantías, auditoría, cobro y defensa de derechos.
- Administrar relaciones con proveedores, distribuidores, integradores, asesores y aliados comerciales.

7.3 Servicios de confianza digital propios

- Operar soluciones de identidad, validación documental, biometría, prueba de vida, wallet y control de acceso.
- Gestionar firma electrónica o digital, documentos protegidos, pagarés electrónicos, correo o SMS certificado, sellado de tiempo, custodia y trazabilidad.

- Administrar plataformas de votación electrónica, separar identidad y voto, prevenir duplicidades y producir resultados agregados.
- Autenticar usuarios, prevenir suplantación, fraude, abuso y accesos no autorizados; producir resultados, evidencias o reportes del servicio.

Estas finalidades se aplican cuando Verifica determina su propósito y medios esenciales. Si una organización distinta decide la finalidad y Verifica solo ejecuta instrucciones, esa operación se rige por la política del tercero responsable y por el aviso específico correspondiente.

7.4 Talento humano

- Recibir y evaluar postulaciones, verificar referencias y desarrollar procesos de selección y contratación.
- Administrar contratos, nómina, pagos, beneficios, seguridad social, formación, desempeño, bienestar, seguridad y salud en el trabajo y terminación de la relación.
- Cumplir deberes laborales, tributarios, contables, migratorios, de archivo, seguridad y atención de autoridades.
- Gestionar información de exempleados y beneficiarios durante los plazos legales y probatorios aplicables.

7.5 Seguridad, cumplimiento y mejora

- Monitorear disponibilidad, seguridad y rendimiento; investigar incidentes, gestionar vulnerabilidades y realizar auditorías.
- Conservar evidencia y atender requerimientos válidos de autoridades o procesos administrativos, judiciales y contractuales.
- Cumplir obligaciones contables, fiscales, societarias, laborales, contractuales, de archivo y protección de datos.
- Mejorar procesos con métricas agregadas o datos anonimizados de manera irreversible, sin intentar reidentificar a las personas.

8. Datos sensibles y biometría

Los datos sensibles incluyen aquellos que afectan la intimidad o cuyo uso indebido puede generar discriminación, como información de salud, origen étnico, orientación política, convicciones, afiliación sindical, vida sexual y datos biométricos.

Regla general. Verifica no solicita estas categorías para una consulta comercial ordinaria. Cuando un servicio, relación laboral o deber legal las requiera, explicará cuáles datos son sensibles, para qué se necesitan y qué ocurrirá si el titular decide no autorizarlos.

Verifica no condicionará una actividad al suministro de datos sensibles. Cuando la naturaleza de una funcionalidad o un deber legal exija validación biométrica, el aviso específico explicará una alternativa razonable o, si no existe por disposición legal, la norma aplicable y el efecto de la negativa.

Biometría. Antes de capturar un rostro, una voz, una prueba de vida o una plantilla biométrica, Verifica presentará un aviso específico y solicitará una autorización previa, expresa, informada, separada y verificable, salvo que exista una excepción legal aplicable y documentada.

El titular no está obligado a autorizar el tratamiento de datos sensibles. El aviso específico explicará la alternativa disponible o el efecto práctico de la negativa. La aceptación de esta Política no constituye por sí sola autorización biométrica.

Verifica no utilizará biometría para publicidad, inferir afinidades políticas, crear perfiles comerciales ni entrenar modelos de reconocimiento facial o de voz para una finalidad incompatible. Un nuevo uso exigirá información previa y una nueva autorización cuando corresponda.

9. Niños, niñas y adolescentes

Los servicios generales de Verifica no están dirigidos a menores de edad. Si una finalidad propia los involucra, Verifica verificará que el tratamiento sea excepcionalmente procedente, responda al interés superior del menor, respete sus derechos fundamentales y sea necesario y proporcional.

La autorización deberá ser otorgada por el representante legal después de permitir que el menor sea escuchado y valorar su opinión según la madurez, autonomía y capacidad para comprender el tratamiento. Los datos sensibles o biométricos requerirán información y controles reforzados.

10. Automatización e inteligencia artificial

Algunos servicios pueden usar OCR, comparación biométrica, detección de vida, análisis de señales de fraude u otras herramientas automatizadas. Verifica documentará su finalidad, necesidad, riesgos, fuentes, calidad de datos, controles de seguridad y supervisión humana cuando el tratamiento esté bajo su responsabilidad.

Si una decisión automatizada de Verifica puede producir efectos jurídicos o afectar significativamente a una persona, el aviso específico explicará su existencia, los criterios principales comprensibles, las consecuencias previstas y el canal para solicitar revisión humana o controvertir el resultado.

Una alerta, puntaje o coincidencia técnica no producirá por sí sola una exclusión definitiva cuando sea necesaria una valoración contextual, exista riesgo relevante de error o la ley, el contrato o el servicio exijan revisión humana.

11. Con quién puede circular la información

Destinatario	Finalidad y condición
Clientes o contrapartes vinculadas	Reciben datos, resultados, documentos o evidencias necesarios para la relación propia de Verifica cuando exista autorización del titular o una habilitación legal aplicable. El contrato delimita el alcance y las obligaciones de las partes.

Destinatario	Finalidad y condición
Proveedores de servicios	Operación y funcionamiento de la plataforma tecnológica que se brinde.
Proveedores tecnológicos	Nube, alojamiento, mensajería, firma, sellado de tiempo, ciberseguridad, soporte, analítica y continuidad, con acceso limitado a lo necesario.
Aliados, distribuidores e integradores	Participan en una solución o relación comercial cuando exista autorización del titular o una habilitación legal aplicable. El acuerdo con el aliado limita el uso de la información.
Autoridades, auditores y asesores	Acceden ante un deber legal, orden válida, auditoría, defensa de derechos o gestión profesional sujeta a reserva.

Verifica seleccionará y supervisará a sus encargados, celebrará acuerdos que definan instrucciones y finalidades, y exigirá confidencialidad, seguridad, atención de derechos, reporte de incidentes, subcontratación controlada y devolución, supresión o anonimización al terminar el servicio.

12. Transmisiones y transferencias internacionales

Algunos servicios pueden requerir procesamiento en México, Italia, Estados Unidos, la Unión Europea u otros países identificados en el aviso o documentación específica del servicio. Verifica informará los destinos materiales y el tipo de operación cuando sea necesario para que el titular tome una decisión informada.

13. Cookies y tecnologías similares

Categoría	Para qué sirve
Necesarias	Permiten seguridad, funcionamiento, sesión, balanceo y preferencias esenciales. No se usan para publicidad.
Preferencias	Recuerdan idioma, configuración o elecciones para mejorar la experiencia.
Analítica	Ayudan a entender cómo se usa el sitio y dónde debe mejorarse. Se activan según la decisión aplicable.
Publicidad	Miden campañas o personalizan comunicaciones. Solo se activan después de obtener autorización cuando sea exigible.

El panel de cookies permitirá aceptar, rechazar o modificar las categorías no necesarias. El inventario vigente deberá identificar proveedor, finalidad, duración y tratamiento internacional. Los enlaces o aplicaciones de terceros, incluido WhatsApp, se rigen además por sus propias políticas.

14. Cuánto tiempo conservamos los datos

Tipo de información	Criterio de conservación
Clientes, proveedores y contrapartes	Durante la relación y los plazos legales, contables, fiscales, contractuales, probatorios o de archivo posteriores.

Tipo de información	Criterio de conservación
Prospectos y comunicaciones opcionales	Mientras exista una autorización vigente o sea necesario atender una solicitud iniciada por el titular; después del retiro, se conservará únicamente la evidencia mínima de la decisión cuando corresponda.
Talento humano	Durante la selección o relación y por los plazos laborales, de seguridad social, SST, tributarios, probatorios y de archivo aplicables.
Biometría y documentos	Por el plazo mínimo necesario explicado en el aviso específico; después se eliminan, bloquean o anonimizan, salvo deber legal o probatorio.
Logs, autorizaciones y evidencias	Según el riesgo, la necesidad de trazabilidad, la vigencia del servicio y los plazos para investigar incidentes, atender derechos o defender reclamaciones.

Las bases de datos cubiertas por esta Política permanecerán vigentes mientras subsistan las finalidades informadas y las obligaciones legales o contractuales asociadas. El tratamiento no será indefinido por el solo hecho de que la autorización no haya sido revocada.

Cuando termine la finalidad y no exista deber de conservación, Verifica y sus encargados eliminarán, devolverán, bloquearán o anonimizarán los datos de forma segura. Las copias de respaldo saldrán de rotación conforme al ciclo técnico documentado.

15. Cómo protegemos y gobernamos la información

Verifica aplicará medidas administrativas, humanas, técnicas y contractuales proporcionales a la naturaleza, volumen y riesgo de la información. Ningún sistema puede prometer seguridad absoluta.

- gestión de accesos por rol, mínimo privilegio y autenticación reforzada para cuentas críticas;
- cifrado en tránsito y, cuando corresponda, en almacenamiento; separación de ambientes, clientes y categorías de información;
- registros de eventos, monitoreo, pruebas, gestión de vulnerabilidades, respaldos, continuidad y recuperación;
- acuerdos de confidencialidad, formación del personal, evaluación y supervisión de proveedores;
- evaluaciones de impacto y privacidad desde el diseño para biometría, IA, menores u otros tratamientos de riesgo alto;
- procedimientos de actualización, conservación, eliminación segura y respuesta a incidentes.

Incidentes. Verifica investigará, contendrá y documentará los eventos que puedan comprometer datos personales. Informará a las autoridades, clientes afectados y titulares cuando corresponda y realizará los reportes exigibles por los canales y términos aplicables.

16. Tus derechos

- Conocer, consultar y acceder gratuitamente a tus datos en los términos legales.

- Solicitar actualización, rectificación o corrección de información parcial, inexacta, incompleta, fraccionada, que induzca a error o cuyo tratamiento esté prohibido o no autorizado.
- Pedir prueba de la autorización, salvo que la ley exceptúe ese requisito.
- Ser informado sobre el uso dado a los datos y los destinatarios relevantes.
- Solicitar la supresión o revocar la autorización cuando proceda. La solicitud puede negarse si existe un deber legal o contractual de conservación o una excepción legal aplicable.
- No responder preguntas sobre datos sensibles y decidir separadamente sobre biometría, publicidad y otras finalidades opcionales.
- Solicitar revisión humana de una decisión automatizada significativa cuando corresponda.
- Presentar consultas y reclamos y acudir ante la Superintendencia de Industria y Comercio después de agotar el trámite aplicable.

El acceso será gratuito al menos una vez por cada mes calendario y cada vez que existan cambios sustanciales en esta Política que motiven nuevas consultas. Verifica solo podrá cobrar los costos de reproducción o envío adicionales permitidos por la normativa.

17. Cómo ejercer tus derechos

Puedes escribir al Área Jurídica y de Protección de Datos en juridico@verificaia.com, utilizar los canales publicados en www.verificaia.com o radicar tu solicitud en la dirección indicada en la sección 2.

Quién puede solicitar. El titular, sus causahabientes, su representante o apoderado y las personas autorizadas por el titular o por la ley. Quien actúe por otra persona deberá acreditar su calidad.

Contenido. Indica nombre e identificación, explica con claridad lo que consultas o reclamas, señala un canal de respuesta y adjunta los soportes disponibles. En un reclamo, identifica los hechos que originan la solicitud.

17.1 Consultas

Verifica responderá las consultas dentro de los diez (10) días hábiles siguientes a su recibo. Si no es posible responder en ese término, informará antes de su vencimiento el motivo de la demora y la nueva fecha, que no podrá superar cinco (5) días hábiles adicionales.

17.2 Reclamos

- Si el reclamo está incompleto, Verifica solicitará la corrección dentro de los cinco (5) días hábiles siguientes a su recepción. Si transcurren dos (2) meses desde el requerimiento sin respuesta, se entenderá desistido.
- Si Verifica no es competente respecto de una parte de la solicitud, la trasladará a quien corresponda dentro de los dos (2) días hábiles siguientes, cuando sea posible identificarlo, e informará al interesado.

- Una vez recibido el reclamo completo, Verifica incluirá en la base la leyenda Reclamo en trámite y el motivo dentro de los dos (2) días hábiles siguientes. La mantendrá hasta decidir el reclamo.
- Verifica resolverá el reclamo dentro de los quince (15) días hábiles contados desde el día siguiente a su recibo. Si requiere más tiempo, informará antes del vencimiento el motivo y la nueva fecha, que no podrá superar ocho (8) días hábiles adicionales.

Antes de presentar una queja ante la SIC, el titular deberá agotar el procedimiento de consulta o reclamo cuando la ley así lo exija.

18. Avisos de privacidad y autorizaciones

Antes o, a más tardar, al momento de recolectar los datos, Verifica identificará su calidad de responsable, informará los datos y finalidades específicas, explicará los derechos y canales y solicitará la autorización cuando sea necesaria.

La publicación o aceptación de esta Política no reemplaza, por sí sola, la autorización para tratar datos personales. Cuando la autorización sea necesaria, Verifica la solicitará de forma previa, expresa e informada y conservará prueba de ella.

Los formularios, contratos, plataformas y servicios podrán usar avisos específicos. Estos complementan esta Política y concretan los datos, proveedores, países, tiempos y consecuencias del caso; no pueden reducir los derechos del titular ni convertir una finalidad opcional en necesaria.

Decisiones separadas. Las finalidades necesarias, la publicidad, la biometría, las grabaciones y cualquier uso nuevo que exija consentimiento se presentarán de forma diferenciada mediante casillas desmarcadas u otro mecanismo claro.

Sin aceptación implícita. El silencio, la inactividad, la navegación posterior o una casilla marcada por defecto no equivalen a autorización. La autorización podrá constar por escrito, de forma oral o mediante una conducta inequívoca que permita consultarla posteriormente.

Verifica conservará evidencia de la versión del aviso y la política, identidad asociada, fecha, hora, canal, finalidades presentadas y decisión adoptada. La autorización no se exigirá en los casos exceptuados por la ley, pero los principios y demás obligaciones seguirán aplicándose.

19. Deberes de Verifica como responsable

- Garantizar el ejercicio efectivo de los derechos del titular y suministrarle información sobre el uso de sus datos.
- Solicitar y conservar prueba de la autorización cuando sea necesaria e informar las finalidades y derechos.
- Mantener información veraz, completa, exacta, actualizada, comprobable y comprensible; corregirla oportunamente.

- Tramitar consultas y reclamos, registrar las leyendas exigidas y atender las instrucciones de la SIC.
- Adoptar políticas, procedimientos y medidas de seguridad; demostrar su implementación y gestionar incidentes.
- Registrar y actualizar las bases de datos y reportar incidentes ante el Registro Nacional de Bases de Datos (RNBD), cuando la normativa lo exija.
- Entregar a sus encargados solo información autorizada, impartir instrucciones y exigir el cumplimiento de esta Política.
- Circular los datos únicamente a personas autorizadas o habilitadas por la ley y respetar la confidencialidad incluso después de terminar la relación.

20. Cambios, vigencia y marco aplicable

Esta Política entra en vigencia el 15 de septiembre de 2026. La versión vigente estará disponible en www.verificaia.com. Verifica identificará cada actualización con número de versión y fecha.

Los cambios sustanciales relacionados con la identificación del responsable, nuevas finalidades, categorías sensibles, destinatarios, países o riesgos serán comunicados de manera eficiente antes de aplicarse. Verifica solicitará una nueva autorización cuando cambie la finalidad o la ley así lo exija.

El tratamiento se rige principalmente por el artículo 15 de la Constitución Política; la Ley Estatutaria 1581 de 2012; el capítulo 25 del Decreto 1074 de 2015 y sus modificaciones y las instrucciones vigentes de la Superintendencia de Industria y Comercio, además de cualquier otra norma colombiana aplicable.