



Documento Corporativo de Políticas, Privacidad y Servicio

People Intelligence S.A.S

Versión 1.0

Documento Corporativo de Políticas, Privacidad y Servicio

Tabla de Contenido:

1. INTRODUCCIÓN GENERAL	4
2. OBJETIVO GENERAL.....	5
2.1. OBJETIVOS ESPECÍFICOS.....	5
3. ALCANCE	6
4. MARCO NORMATIVO Y CUMPLIMIENTO	6
5. POLÍTICAS TÉCNICAS Y DE SEGURIDAD.....	7
5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	7
5.2. POLÍTICA DE USO ACEPTABLE	8
5.3. POLÍTICA DE CONTROL DE ACCESOS.....	8
5.4. POLÍTICA DE GESTIÓN DE VULNERABILIDADES.....	9
5.5. POLÍTICA DE CLASIFICACIÓN DE DATOS.....	9
5.6. POLÍTICA Y PLAN DE RESPUESTA A INCIDENTES	9
5.7. PRUEBAS DE PENETRACIÓN DE RED	10
5.8. DESARROLLO SEGURO Y GESTIÓN DE CAMBIOS.....	10
6. POLÍTICAS DE PRIVACIDAD	11
6.1. INTRODUCCIÓN.....	11
6.2. ACEPTACIÓN	11
6.3. ACTUALIZACIONES	11
6.4. INFORMACIÓN RECOLECTADA.....	11
6.5. COOKIES Y TECNOLOGÍAS SIMILARES	12
6.6. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES	12
6.7. USO, ACCESO, RETENCIÓN Y DESTRUCCIÓN DE DATOS	12
6.8. DERECHOS DE LOS USUARIOS	12
6.9. EDAD MÍNIMA REQUERIDA	12
6.10. ALOJAMIENTO Y TRANSFERENCIA INTERNACIONAL DE DATOS	13
6.11. SITIOS DE TERCEROS	13
6.12. TRANSFERENCIAS DEL NEGOCIO.....	13
6.13. MODIFICACIONES	13
6.14. NOTIFICACIONES Y CONTACTO	13
6.15. PROTECCIÓN DE DATOS PERSONALES.....	13
7. POLÍTICAS DEL SERVICIO.....	15
7.1. INTRODUCCIÓN Y ACEPTACIÓN DE CONDICIONES.....	15
7.2. ACTUALIZACIONES	15
7.3. OBJETO DEL SERVICIO Y ALCANCE FUNCIONAL	15
7.4. OBLIGACIONES DEL USUARIO.....	15
7.5. OBLIGACIONES DE LA COMPAÑÍA.....	16

7.6.	LIMITACIONES DEL SERVICIO Y EXCLUSIONES DE RESPONSABILIDAD	16
7.7.	SEGURIDAD Y CONFIDENCIALIDAD	16
7.8.	MODIFICACIONES DEL SERVICIO	16
7.9.	CONTACTO Y NOTIFICACIONES	16
7.10.	ROLES Y RESPONSABILIDADES	16
7.11.	PROCEDIMIENTOS Y ANEXOS.....	17
8.	CONTROL DE CAMBIOS.....	18

1. Introducción General

People Intelligence es una plataforma tecnológica para la escucha de la voz del colaborador (Voice of Employee), con capacidad de creación, gestión y análisis de encuestas organizacionales, utilizando metodologías de people analytics para visualización de resultados y relacionamiento de los mismos con información externa o incluso entre las mismas encuestas, generando reportes a través de tableros interactivos de Power BI.

Mediante alianzas con departamentos de Recursos Humanos de distintas empresas, permite diseñar encuestas, recopilar respuestas y analizar resultados. La plataforma cuenta con dos áreas principales: área administrativa (configuración, gestión de encuestas y generación de reportes) y área de usuario final (rellenado de encuestas y visualización de resultados).

La infraestructura está alojada en Microsoft Azure, utilizando servicios de autenticación, almacenamiento y respaldo en la nube. Los usuarios acceden mediante credenciales y, según su perfil, tienen permisos diferenciados.

2. Objetivo General

Dar a conocer a todos nuestros empleados, clientes, usuarios finales, proveedores, aliados y accionistas, y en general a todas las partes interesadas que intervienen en el desarrollo del negocio, las políticas de seguridad, privacidad y tratamiento de datos personales que rigen la **Suite People Intelligence**; establecer los principios, responsabilidades y controles técnicos y organizativos que garantizan el ejercicio de los derechos de los titulares (conocer, actualizar, rectificar, suprimir y oponerse) respecto de la información que repose en nuestras bases de datos o aquellas que tratemos por cuenta de nuestros clientes; y asegurar el cumplimiento de la Constitución Política de 1991 (arts. 15 y 20), la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas aplicables, así como los principios de ISO/IEC 27001 y, cuando corresponda, del GDPR.

2.1. Objetivos específicos

- Publicar de forma clara y accesible las políticas y términos que aplican al uso de la Plataforma y sus canales asociados.
- Definir responsabilidades, métricas (SLA) y mecanismos de control documental y revisión periódica.
- Establecer procedimientos para el ejercicio de derechos de los titulares (ARCO) y canales de contacto.
- Alinear el tratamiento de datos con los principios de finalidad, legalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

3. Alcance

Estas políticas aplican a todos los usuarios, roles, infraestructura tecnológica y datos procesados en la plataforma, incluyendo:

- Todos los colaboradores, contratistas y terceros que accedan o procesen información a través de la plataforma.
- Usuarios con roles como Admin, Journey, Multicompañía, PowerBI Administrator, Sentimental, Dynamic, PowerBI Dashboard, Management.
- Todos los datos personales y sensibles tratados.
- Toda la infraestructura tecnológica utilizada.

4. Marco Normativo y Cumplimiento

People Intelligence cumple con:

- Ley 1581 de 2012 y Decreto 1377 de 2013 (Habeas Data – Colombia).
- ISO/IEC 27001 y 27002 (controles y buenas prácticas).
- Principios del Reglamento General de Protección de Datos (GDPR).
- Requisitos contractuales con clientes.
- Buenas prácticas de Microsoft Azure Security.

Declaración de aplicabilidad (SoA): Los controles descritos a continuación aplican salvo que un contrato o evaluación de riesgos documentada defina excepciones con tratamiento de riesgo aprobado por la Dirección de Analítica y Tecnología.

5. Políticas Técnicas y de Seguridad

Esta sección detalla las políticas alineadas con ISO/IEC 27001, que cubren seguridad de la información, uso aceptable, control de accesos, gestión de vulnerabilidades, clasificación de datos, respuesta a incidentes y pruebas de penetración.

5.1. Política de Seguridad de la Información

Objetivo: Proteger la confidencialidad, integridad y disponibilidad de la información y de los servicios de People Intelligence.

Alcance: Toda la información y activos de información en la plataforma y servicios de soporte.

Lineamientos y controles mínimos:

- Gobierno de seguridad: roles definidos, SoA, gestión de riesgos al menos anual.
- Las comunicaciones entre clientes, la aplicación y las APIs se realizan mediante TLS (HTTPS)..
- Principio de mínimo privilegio, segregación de funciones y revisión periódica de permisos.
- cualquier copia de seguridad en producción se genera como operación ad-hoc y su creación debe registrarse como tal. Esta política no describe copias de seguridad automatizadas ni pruebas de restauración documentadas como controles existentes..
- Gestión de proveedores y subprocesadores (due diligence y cláusulas de seguridad).
- Concientización y capacitación anual obligatoria para personal con acceso a datos.

Responsables: Dirección de Analítica y Tecnología ; Equipo de Desarrollo.

Revisión: Anual o ante cambios sustanciales.

5.2. Política de Uso Aceptable

Objetivo: Establecer reglas de uso de la plataforma y activos tecnológicos.

Lineamientos:

- Prohibido: compartir credenciales; intentar acceso no autorizado; subir malware; uso para actividades ilícitas; cargar datos de menores sin consentimiento; introducir datos excesivos/no necesarios.
- Obligatorio: proteger credenciales; usar MFA cuando esté habilitado; reportar incidentes o sospechas; respetar propiedad intelectual.
- Contenidos prohibidos: material discriminatorio, violento, sexual explícito, o que viole derechos de terceros.

Sanciones: Suspensión o terminación de acceso; reporte al empleador/cliente; acciones legales cuando aplique.

5.3. Política de Control de Accesos

Objetivo: Asegurar que solo personal autorizado acceda a sistemas y datos según rol.

Lineamientos:

- Gestión de identidades mediante proveedor de identidad corporativo (p. ej., Azure AD) y perfiles por rol.
- MFA obligatorio para cuentas administrativas/privilegiadas; recomendado para usuarios finales; bloqueo por intentos fallidos y por inactividad configurable.
- Revisiones trimestrales de permisos y accesos privilegiados; evidencias archivadas.
- Segregación de ambientes (DEV/QA/PROD) y datos en no-prod anonimizados o seudonimizados.

5.4. Política de Gestión de Vulnerabilidades

Objetivo: Reducir el riesgo por vulnerabilidades técnicas.

Lineamientos:

- Escaneos automatizados mensuales en infraestructura y aplicaciones; monitoreo continuo cuando sea posible.
- Pruebas de seguridad en el SDLC: análisis SCA/SAST para código/paquetes; revisiones de dependencias; controles de hardening.
- Ventanas de parcheo regulares; excepciones con aceptación de riesgo formal y fecha de remediación.

5.5. Política de Clasificación de Datos

Objetivo: Establecer categorías y reglas de manejo de datos.

Categorías: Público · Interno · Confidencial (incluye Datos Personales y datos sensibles).

Reglas de manejo:

- Confidencial: cifrado en tránsito y reposo; control de acceso por rol; registro de acceso; uso de entornos seguros; compartición mínima necesaria.
- Interno: acceso limitado a personal autorizado; no divulgación externa sin autorización.
- Público: sin restricciones, evitar mezclar con datos personales.
- No-prod: prohibido usar datos reales sin anonimización/seudonimización.
- Prevención de fuga de datos (DLP) proporcional al riesgo.

5.6. Política y Plan de Respuesta a Incidentes

Objetivo: Detectar, contener, erradicar y recuperar ante incidentes; comunicar a interesados según ley/contrato.

Flujo: Detección → Notificación → Triage → Contención → Erradicación → Recuperación → Lecciones aprendidas (RCA).

Comunicación: Canal de seguridad, correo dedicado y mesa de ayuda; designación de vocero; conservación de evidencias.

5.7. Pruebas de Penetración de Red

Objetivo: Evaluar la seguridad mediante pruebas controladas internas y/o por terceros independientes.

Alcance: Perímetro externo, APIs, aplicaciones web y móviles, y segmentación/red interna (según contrato y ventana autorizada).

Lineamientos:

- Periodicidad: al menos anual y tras cambios sustanciales.
- Metodologías OWASP/NIST; evidencia de correcciones y retesting de hallazgos críticos/altos.
- Informe entregable con severidad, PoC y recomendaciones; plan de remediación y fecha objetivo.
- Gestión de riesgos y aceptación formal cuando

5.8. Desarrollo Seguro y Gestión de Cambios

Objetivo: Asegurar que cambios a la plataforma no introduzcan riesgos indebidos.

Lineamientos:

- SDLC con revisión de código por pares; pipelines con análisis SAST/SCA/DAST proporcional al riesgo.
- Separación de funciones: desarrollo ≠ despliegue ≠ operación.
- Gestión de cambios: RFC con evaluación de riesgo, plan de reversión, ventana de mantenimiento y aprobación.
- Gestión de secretos: almacenamiento en bóvedas; rotación periódica; prohibido en repositorios.
- Inventario de dependencias y SBOM disponible bajo solicitud contractual.

6. Políticas de Privacidad

6.1. Introducción

Estas Políticas de Privacidad (en adelante, las “Políticas de Privacidad”) rigen el tratamiento de la información recopilada de los Usuarios en el Sitio: **peopleintelligence.app** (en adelante, el “Sitio”) y la aplicación móvil “People Intelligence” (en adelante, la “Aplicación”), conjuntamente, la “Plataforma”, propiedad de People Intelligence (en adelante, “People Intelligence” o la “Compañía”) y forman parte de los Términos y Condiciones del Sitio. El propósito de estas Políticas de Privacidad es describir qué tipos de datos e información personal (en adelante, “Información Personal”) reúne People Intelligence, los propósitos para los que la misma es utilizada, bajo qué circunstancias puede llegar a revelarse y los derechos que tienen los Usuarios con respecto a su protección.

6.2. Aceptación

El acceso a la Plataforma y la utilización del Servicio implican la aceptación plena de estas Políticas de Privacidad y de los Términos y Condiciones. Si el Usuario no está de acuerdo, no debe acceder ni utilizar el Servicio.

6.3. Actualizaciones

People Intelligence se reserva el derecho de modificar estas Políticas de Privacidad en cualquier momento. Los cambios serán notificados por los medios que la Compañía considere más oportunos.

6.4. Información Recolectada

- **Información Personal:** Nombre, apellidos, fecha de nacimiento, fecha de contratación, nivel de estudios, ubicación de oficina, división/área, género y otros datos demográficos.
- **Información General:** Datos técnicos (IP, URL, cookies, tipo de navegador, sistema operativo, idioma, etc.) y datos de navegación (páginas visitadas, uso

de la Plataforma).
El Usuario se compromete a proporcionar datos exactos, actuales y completos.

6.5. Cookies y Tecnologías Similares

Uso de cookies operativas, analíticas y de publicidad para mejorar la experiencia del Usuario y optimizar la Plataforma.

6.6. Seguridad de la Información y Datos Personales

Implementación de medidas de seguridad siguiendo estándares aceptados por la industria. No obstante, People Intelligence no puede garantizar la seguridad absoluta de la información transmitida o almacenada.

6.7. Uso, Acceso, Retención y Destrucción de Datos

La Información Personal se utiliza para:

- Prestación y mejora de la Plataforma.
 - Resolución de disputas y atención al cliente.
 - Soporte técnico y personalización de servicios.
- La retención de datos será únicamente durante el tiempo legal o necesario; posteriormente serán eliminados o destruidos.

6.8. Derechos de los Usuarios

Derecho de acceso, rectificación, supresión y oposición al tratamiento de datos.
Solicitudes al correo: contacto@peopleintelligence.co.

6.9. Edad Mínima Requerida

Se requiere tener al menos 18 años, salvo consentimiento expreso de padres o tutores.

6.10. Alojamiento y Transferencia Internacional de Datos

Datos alojados en servidores de Azure. Pueden ser transferidos internacionalmente bajo las leyes aplicables.

6.11. Sitios de Terceros

Enlaces a sitios externos no están cubiertos por estas Políticas. People Intelligence no se responsabiliza por el contenido o prácticas de terceros.

6.12. Transferencias del Negocio

En caso de fusión, adquisición o venta, la Información Personal podrá ser transferida al nuevo propietario.

6.13. Modificaciones

Cualquier modificación tendrá efecto inmediato tras su publicación en la Plataforma.

6.14. Notificaciones y Contacto

Notificaciones a través de correo electrónico o en la Plataforma. Consultas a: contacto@peopleintelligence.co.

6.15. Protección de Datos Personales

People Intelligence, en calidad de Responsable del Tratamiento de Datos Personales, adopta las medidas administrativas, técnicas y organizativas necesarias para garantizar la protección de la información personal de sus usuarios, clientes, colaboradores y terceros.

Estas medidas se implementan en cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013, demás normas concordantes, y los estándares internacionales aplicables (incluyendo principios de ISO/IEC 27001 y del Reglamento General de Protección de Datos - GDPR).

En particular, People Intelligence garantiza que:

- **Finalidad y Minimización de Datos:**
La recolección y tratamiento de datos se realizará únicamente para los fines autorizados, evitando la recopilación de información excesiva o no necesaria.
- **Seguridad y Confidencialidad:**
la plataforma utiliza tokens para autenticación entre componentes. Las cuentas administrativas aplican mecanismos de autenticación fuerte donde están configuradas.
- **Derechos del Titular:**
Los titulares podrán ejercer sus derechos de acceso, rectificación, actualización, supresión y oposición al tratamiento de sus datos, mediante solicitud enviada a contacto@peopleintelligence.co , siguiendo los procedimientos definidos en estas políticas.
- **Transferencia y Transmisión:**
La transferencia internacional de datos se realizará únicamente cuando el país receptor ofrezca niveles adecuados de protección o se cuente con las garantías contractuales y legales exigidas.
- **Tratamiento de Datos Sensibles y de Menores de Edad:**
Se recolectarán únicamente cuando sea estrictamente necesario y con la autorización expresa de su titular, o de los padres o tutores en el caso de menores.
- **Responsable de Protección de Datos:**
La Dirección de Analítica y Tecnología actuará como responsable de velar por el cumplimiento de esta política y la atención de consultas y reclamos relacionados con la protección de datos personales.

7. Políticas del Servicio

7.1. Introducción y Aceptación de Condiciones

El acceso y uso de la Plataforma implica la aceptación de las presentes Políticas del Servicio y de los Términos y Condiciones. Si el Usuario no acepta, debe abstenerse de utilizar la Plataforma.

7.2. Actualizaciones

People Intelligence podrá actualizar o modificar las presentes Políticas del Servicio y los Términos y Condiciones en cualquier momento, notificando los cambios por medios que considere apropiados.

7.3. Objeto del Servicio y Alcance Funcional

La Plataforma permite a las empresas crear, administrar y visualizar encuestas, recopilar respuestas y acceder a reportes de análisis de datos mediante tableros de Power BI. Incluye funcionalidades administrativas, de usuario final y de visualización de resultados.

7.4. Obligaciones del Usuario

Usar la Plataforma de manera lícita y conforme a estas políticas.

- No compartir credenciales de acceso.
- Proporcionar datos veraces y actualizados.
- Respetar los derechos de propiedad intelectual.

7.5. Obligaciones de la Compañía

- Garantizar la disponibilidad de la Plataforma, salvo interrupciones por mantenimiento o fuerza mayor.
- Proteger la Información Personal conforme a la Política de Privacidad.
- Mantener medidas de seguridad técnica y organizativa.

7.6. Limitaciones del Servicio y Exclusiones de Responsabilidad

- People Intelligence no garantiza la ausencia de interrupciones o errores.
- No se responsabiliza por daños derivados del mal uso de la Plataforma.
- El acceso puede ser suspendido por incumplimiento de las políticas.

7.7. Seguridad y Confidencialidad

La Compañía aplica controles técnicos y organizativos para proteger la información, incluyendo cifrado y control de accesos.

7.8. Modificaciones del Servicio

La Compañía podrá modificar las funcionalidades, interfaz o condiciones de uso de la Plataforma en cualquier momento.

7.9. Contacto y Notificaciones

Consultas o notificaciones deben dirigirse a contacto@peopleintelligence.co o mediante los canales oficiales publicados en la Plataforma.

7.10. Roles y Responsabilidades

- Dirección de Analítica y Tecnología: Aprobar y revisar políticas.

	Documento Corporativo de Políticas, Privacidad y Servicio	Código: POL001 Versión: 1.0 Fecha: 03/03/2025
---	--	---

- Administradores: Implementar controles y gestionar accesos.
- Usuarios: Cumplir las políticas y reportar incidentes.
- Auditor Interno: Verificar cumplimiento.

7.11. Procedimientos y Anexos

Incluye formatos de alta/baja de usuarios, procedimiento de habeas data, procedimiento de gestión de incidentes, procedimiento de respaldo y restauración.

8. Control de Cambios

Versión: 1.0	Fecha de Versión: 03 de Marzo de 2025
Descripción de cambios: Creación del documento	
Fecha de Aprobación: Marzo 2025	Fecha Divulgación: Marzo 2025