POLÍTICA DE SEGURIDAD Y LIMITACIÓN DE RESPONSABILIDAD

Última actualización: 12 de mayo de 2025

La presente Política de Seguridad y Limitación de Responsabilidad describe las medidas técnicas y organizativas que **Wymo** ("nosotros", "nos" o "nuestro") implementa para proteger la información de sus usuarios, así como los límites de nuestra responsabilidad ante eventos de seguridad que escapen a nuestro control directo. Al utilizar nuestros Servicios, el usuario reconoce haber leído, comprendido y aceptado los términos aquí establecidos.

ÍNDICE

1. COMPROMISO DE SEGURIDAD DE WYMO

En resumen: La seguridad de sus datos es una prioridad fundamental para Wymo.

Wymo considera la protección de los datos personales y la información de sus usuarios como una prioridad estratégica y operativa. Hemos diseñado nuestra infraestructura tecnológica y nuestros procesos internos con un enfoque de seguridad por defecto y desde el diseño (*security by default & by design*), incorporando múltiples capas de protección que actúan de forma simultánea y complementaria para minimizar los riesgos de acceso no autorizado, alteración, divulgación o pérdida de datos.

Nuestro equipo de seguridad realiza revisiones periódicas de todos los sistemas, aplica actualizaciones de forma proactiva y evalúa continuamente nuevas amenazas para adaptar nuestras defensas a un entorno digital en constante evolución.

2. MEDIDAS TÉCNICAS DE PROTECCIÓN

En resumen: Utilizamos tecnología de última generación para proteger su información en todas las etapas.

Wymo implementa, entre otras, las siguientes medidas técnicas:

- **Cifrado en tránsito:** toda la comunicación entre el usuario y nuestros servidores se realiza mediante protocolos TLS (Transport Layer Security) actualizados, garantizando que los datos no puedan ser interceptados durante su transmisión.
- **Cifrado en reposo:** la información almacenada en nuestras bases de datos se cifra utilizando algoritmos estándar del sector (AES-256), de modo que resulte ilegible para cualquier persona no autorizada que pudiera acceder físicamente a los servidores.
- **Autenticación multifactor (MFA):** ofrecemos y promovemos el uso de autenticación de múltiples factores para el acceso a las cuentas de usuario, añadiendo una capa adicional de verificación más allá de la contraseña.
- **Firewalls y sistemas de detección de intrusiones (IDS/IPS):** nuestros entornos de producción están protegidos por cortafuegos de última generación y sistemas automatizados que detectan y bloquean patrones de tráfico anómalos o maliciosos en tiempo real.
- **Segmentación de redes:** separamos lógica y físicamente los distintos entornos de nuestra infraestructura para limitar la propagación de cualquier incidente de seguridad.
- **Copias de seguridad (backups):** realizamos respaldos automáticos y periódicos de todos los datos críticos, almacenados en ubicaciones geográficamente distribuidas y cifradas, para garantizar la recuperación ante cualquier eventualidad.
- **Gestión de vulnerabilidades:** ejecutamos análisis de vulnerabilidades y pruebas de penetración (*pentesting*) de forma regular para identificar y remediar posibles debilidades antes de que puedan ser explotadas.
- **Monitoreo continuo 24/7:** contamos con sistemas de vigilancia permanente que alertan a nuestro equipo ante cualquier actividad sospechosa, permitiendo una respuesta ágil.

3. MEDIDAS ORGANIZATIVAS

En resumen: La seguridad no es solo tecnología; también son procesos y personas.

Wymo complementa sus medidas técnicas con controles organizativos sólidos:

- **Principio de mínimo privilegio:** solo el personal estrictamente necesario tiene acceso a los datos de los usuarios, y dicho acceso está limitado al mínimo imprescindible para el desempeño de sus funciones.
- **Formación continua:** todos los empleados y colaboradores de Wymo que manejan datos reciben formación periódica en buenas prácticas de seguridad, gestión de contraseñas y reconocimiento de amenazas como el phishing.
- **Acuerdos de confidencialidad:** todo el personal con acceso a datos sensibles está vinculado por acuerdos de confidencialidad y no divulgación.
- **Auditorías internas:** realizamos revisiones internas periódicas de nuestros procesos y controles de seguridad para asegurar su correcta aplicación y detectar áreas de mejora.
- **Política de gestión de accesos:** contamos con procedimientos formales para la concesión, revisión y revocación de accesos, especialmente ante cambios en el equipo.

4. GESTIÓN DE INCIDENTES DE SEGURIDAD

En resumen: Contamos con un protocolo estructurado para responder ante cualquier incidente.

Wymo dispone de un Plan de Respuesta a Incidentes de Seguridad documentado y probado, que establece los procedimientos a seguir ante cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de los datos. Este plan contempla fases de identificación, contención, erradicación, recuperación y análisis post-incidente, con el objetivo de minimizar el impacto y el tiempo de resolución.

5. LIMITACIÓN DE RESPONSABILIDAD ANTE ATAQUES EXTERNOS

En resumen: A pesar de nuestras robustas medidas, ciertos eventos fuera de nuestro control directo nos eximen de responsabilidad.

A pesar de que **Wymo** implementa y mantiene un conjunto exhaustivo de medidas de seguridad técnicas y organizativas conforme a los estándares del sector, el entorno digital presenta riesgos inherentes que ninguna organización puede eliminar completamente. En consecuencia, **Wymo** no asume responsabilidad por los daños o perjuicios derivados de los siguientes supuestos, que se consideran fuera del alcance de nuestro control razonable:

- **Ataques de terceros malintencionados** de naturaleza sofisticada o sin precedentes (ataques de día cero, amenazas persistentes avanzadas — APT, etc.) que logren vulnerar las defensas implementadas pese a haber adoptado las precauciones razonables del sector.
- **Fallos en infraestructura de terceros** sobre los que Wymo no ejerce control, incluyendo proveedores de servicios en la nube, centros de datos, proveedores de telecomunicaciones o redes de entrega de contenido (CDN).
- **Interceptación de datos en redes no controladas por Wymo**, tales como redes WiFi públicas o no seguras utilizadas por el propio usuario para acceder al servicio.
- **Eventos de fuerza mayor**, incluyendo desastres naturales, conflictos armados, actos terroristas, pandemias, cortes masivos de energía o cualquier otro evento extraordinario e imprevisible que afecte a la integridad de los sistemas.
- **Vulnerabilidades en software de terceros** integrado en nuestra plataforma que no hayan sido públicamente divulgadas por sus fabricantes al momento del incidente (vulnerabilidades de día cero).
- **Acciones u omisiones del propio usuario**, incluyendo el uso de contraseñas débiles, la no habilitación de la autenticación multifactor disponible, la instalación de software malicioso en sus dispositivos o la divulgación voluntaria o negligente de sus credenciales.

En todos los supuestos descritos, **Wymo** se compromete a actuar con la mayor diligencia posible una vez detectado el incidente, colaborando con las autoridades competentes cuando así se requiera y adoptando las medidas correctivas necesarias para mitigar el impacto y prevenir su repetición. La limitación de responsabilidad aquí establecida no excluye los derechos que la normativa aplicable reconoce de forma imperativa a los usuarios.

6. RESPONSABILIDADES DEL USUARIO

En resumen: La seguridad es compartida; el usuario también tiene un papel fundamental.

Para garantizar la máxima protección de su cuenta e información, el usuario se compromete a:

- Utilizar contraseñas robustas, únicas para su cuenta de Wymo y actualizarlas periódicamente.

- Activar la autenticación multifactor cuando esté disponible.
- No compartir sus credenciales de acceso con terceros bajo ninguna circunstancia.
- Mantener actualizados los dispositivos y navegadores que utiliza para acceder al servicio.
- Notificar de forma inmediata a contact@wymoperu.com ante cualquier sospecha de acceso no autorizado a su cuenta.
- Evitar el acceso a los Servicios de Wymo desde redes WiFi públicas o no seguras.

7. SERVICIOS Y PROVEEDORES TERCEROS

En resumen: Seleccionamos cuidadosamente a nuestros proveedores, pero no controlamos sus sistemas.

Wymo trabaja exclusivamente con proveedores de servicios tecnológicos que acreditan el cumplimiento de estándares reconocidos de seguridad (como ISO 27001, SOC 2 u equivalentes). No obstante, dichos proveedores operan sus propios sistemas e infraestructuras, sobre los cuales Wymo no ejerce control directo. En consecuencia, Wymo no asume responsabilidad por incidentes de seguridad que se originen en los sistemas de proveedores terceros, sin perjuicio de las reclamaciones que Wymo pueda ejercer contra dichos proveedores conforme a los acuerdos contractuales vigentes.

8. NOTIFICACIÓN DE BRECHAS

En resumen: Le informaremos de forma transparente y oportuna si sus datos se ven afectados.

En caso de que **Wymo** detecte o sea notificada de una brecha de seguridad que implique un riesgo significativo para los derechos y libertades de los usuarios afectados, procederemos a notificar a dichos usuarios y, cuando así lo exija la normativa aplicable, a las autoridades competentes de protección de datos, dentro de los plazos legalmente establecidos. La notificación incluirá, en la medida de lo posible, la naturaleza del incidente, los datos afectados, las medidas adoptadas y las recomendaciones para que el usuario proteja su información.

Si usted sospecha o detecta cualquier vulnerabilidad en nuestros sistemas, le instamos a comunicárnoslo de forma responsable a través de contact@wymoperu.com, absteniéndose de divulgar la información públicamente antes de que hayamos tenido la oportunidad de evaluar y remediar el problema.

9. ACTUALIZACIONES DE ESTA POLÍTICA

Wymo se reserva el derecho de actualizar la presente política en cualquier momento para reflejar cambios en nuestras prácticas de seguridad, en la normativa aplicable o en el entorno tecnológico. Las versiones actualizadas se publicarán en nuestra plataforma con indicación de la fecha de revisión. Le recomendamos consultar esta página periódicamente.

10. CONTACTO

Para cualquier consulta, reporte de incidente o ejercicio de derechos relacionado con esta política:

Wymo — Equipo de Seguridad y Privacidad
Lima, Perú
contact@wymoperu.com
www.wymo.com/seguridad
