

CALL HARMONY

Política de Uso Aceptable (AUP)

callharmony.online · Versión 2.0 · Documento oficial · Operado por Ser Energia Universal Ltda.

| 0. Propósito

Esta política define qué usos de la plataforma Call Harmony están permitidos y cuáles no, desde una perspectiva técnica y de seguridad. Complementa los Términos y Condiciones y la Política Antifraude, sin superponerse con ellos. Aplica a todos los usuarios y especialistas independientes que acceden a Call Harmony por cualquier medio.

| 1. Usos Permitidos

- Acceder a la plataforma mediante los canales oficiales (sitio web, aplicación móvil) usando credenciales propias y válidas.
- Utilizar los tokens adquiridos para acceder a sesiones de consulta de tarot en tiempo real, en las modalidades disponibles: **videollamada** o **llamada de voz**.
- Interactuar con la plataforma de forma manual, mediante dispositivos personales y conexión propia.
- Reportar errores, vulnerabilidades o comportamientos inesperados al equipo de soporte.

| 2. Usos Prohibidos

2.1 Acceso y autenticación

- Crear cuentas falsas, múltiples o bajo identidades de terceros sin su consentimiento.
- Compartir credenciales de acceso con terceros.
- Acceder a cuentas ajenas sin autorización.
- Intentar recuperar contraseñas de cuentas que no son propias.
- Usar VPN o proxies para evadir restricciones geográficas o de acceso de la plataforma.

2.2 Automatización y manipulación técnica

- Usar bots, scripts, crawlers o cualquier herramienta automatizada para interactuar con la plataforma.
- Realizar scraping de contenido, perfiles, precios o cualquier dato de la plataforma.
- Realizar ataques de denegación de servicio (DoS/DDoS) o solicitudes masivas automatizadas.
- Manipular el sistema de asignación aleatoria de especialistas mediante cualquier medio técnico.
- Intentar interceptar, modificar o redirigir comunicaciones dentro de la plataforma.

2.3 Integridad del sistema

- Intentar acceder a zonas de la plataforma para las que no se tienen permisos (paneles administrativos, bases de datos, APIs no públicas).
- Explotar vulnerabilidades del sistema en beneficio propio o de terceros sin reportarlas previamente al equipo.
- Inyectar código malicioso, virus, malware o cualquier elemento que afecte el funcionamiento de la plataforma.
- Intentar descompilar, hacer ingeniería inversa o copiar el código fuente de la plataforma.

2.4 Pagos y tokens

- Intentar manipular el sistema de tokens mediante vulnerabilidades técnicas.
- Usar métodos de pago robados, fraudulentos o no autorizados.
- Realizar chargebacks fraudulentos después de haber consumido el servicio.
- Intentar duplicar tokens o transferirlos entre cuentas por medios no autorizados.

2.5 Datos y privacidad

- Recolectar, almacenar o compartir datos personales de otros usuarios o especialistas obtenidos a través de la plataforma.
- Grabar sesiones por cuenta propia sin consentimiento expreso de la otra parte. Las grabaciones realizadas por Call Harmony para control interno se conservan durante 15 (quince) días, conforme a la Política de Privacidad vigente.
- Usar información obtenida dentro de la plataforma para fines externos o comerciales no autorizados.

| 3. Responsabilidad del Usuario / Especialista

- Cada usuario y especialista independiente es responsable de toda actividad que ocurra bajo sus credenciales de acceso.
- El desconocimiento de esta política no exime de responsabilidad ante su incumplimiento.
- Call Harmony se reserva el derecho de investigar cualquier uso que resulte sospechoso, incluso si no está explícitamente listado en este documento.

| 4. Gestión de Acceso por Incumplimiento

El incumplimiento de esta política podrá derivar en medidas de gestión de acceso a la infraestructura de la plataforma, proporcionales a la naturaleza y gravedad del incidente:

Clasificación	Ejemplos	Medida aplicable
Leve	Uso de VPN, intento de acceso no autorizado sin éxito	Notificación contractual y suspensión temporal de acceso
Grave	Scraping, manipulación de tokens, cuenta falsa	Suspensión de acceso por plazo determinado
Crítico	Ataque técnico, fraude de pagos, robo de datos	Rescisión contractual y eventual notificación a las autoridades competentes

Las medidas adoptadas tienen naturaleza de gestión de infraestructura y seguridad de la plataforma, y no constituyen relación de empleo ni poder disciplinario laboral.

| 5. Reporte Responsable de Vulnerabilidades

Si encontrás una vulnerabilidad técnica en la plataforma, reportala de forma responsable antes de divulgarla públicamente:

- **Correo electrónico:** sistemcallharmony@gmail.com
- **WhatsApp (solo mensajes):** +55 22 99290-7887 — 10:00 a 22:00 hs (BRT)

Call Harmony se compromete a investigar todos los reportes de buena fe y a no tomar acciones contra quienes reporten vulnerabilidades de forma responsable.

| 6. Actualizaciones

Esta política puede ser actualizada. Los cambios serán notificados con antelación razonable. El uso continuado de la plataforma implica la aceptación de la versión vigente.

