# POLÍTICA DE USO ACEPTABLE

## Acceptable Use Policy (AUP)

Inversiones Uptech SPA — Servicios de Infraestructura Cloud y VPS

| Campo | Detalle |
|---|---|
| **Versión** | 6.2 |
| **Fecha de vigencia** | 03/01/2027 |
| **Última revisión** | 03/01/2026 |
| **Responsable** | Inversiones Uptech SPA |
| **Aplicable a** | Todos los servicios VPS, servidores dedicados, colocation, hosting y servicios gestionados provistos por Uptech |
| **Contacto AUP** | abuse@uptech.cl |
| **URL pública** | uptech.cl/aup |

⚠️ **Resumen ejecutivo**

Esta política define qué usos están permitidos y cuáles están prohibidos en la infraestructura de Uptech.

El incumplimiento puede resultar en suspensión inmediata del servicio, terminación del contrato y/o reporte a autoridades.

Para reportar abuso: abuse@uptech.cl | Para dudas: soporte@uptech.cl

## 1. ALCANCE Y APLICABILIDAD

Esta Política de Uso Aceptable (en adelante "AUP") establece las normas de uso para todos los servicios de infraestructura digital provistos por Inversiones Uptech SPA (en adelante "Uptech"), incluyendo, sin limitación: servidores privados virtuales (VPS), servidores dedicados, colocation, hosting compartido, servicios de almacenamiento, ancho de banda, direcciones IP y cualquier recurso de red asociado.

La AUP es de aplicación obligatoria para:

- El cliente titular del contrato de servicio.
- Cualquier usuario, empleado, contratista o tercero que acceda al servicio mediante credenciales del cliente.
- Cualquier usuario final de servicios o aplicaciones hospedadas en la infraestructura de Uptech.

El cliente es responsable de garantizar que todos los usuarios que acceden a su servicio conocen y cumplen esta política.

Esta AUP se complementa con los Términos y Condiciones del Contrato de Servicio y demás instrumentos contractuales vigentes. En caso de conflicto entre ellos, prevalecerá la interpretación más restrictiva para proteger la integridad de la red y los derechos de terceros.

## 2. DEFINICIONES

Para los efectos de esta AUP se entenderá por:

| Término | Definición |
|---|---|
| **Servicio** | Cualquier recurso de infraestructura provisto por Uptech al cliente mediante contrato. |
| **Cliente** | Persona natural o jurídica que suscribe un contrato de servicio con Uptech. |
| **Usuario** | Toda persona que accede o usa el Servicio, directa o indirectamente. |
| **Abuso** | Uso del Servicio que viola esta AUP, el contrato, o la ley aplicable. |
| **Spam** | Envío masivo o no solicitado de mensajes electrónicos, incluyendo e-mail, SMS, mensajes en redes sociales o cualquier otro canal. |
| **DDoS** | Ataque de denegación de servicio distribuido (Distributed Denial of Service) destinado a saturar recursos de red o aplicaciones. |
| **Malware** | Software malicioso de cualquier tipo: virus, troyanos, ransomware, spyware, rootkits, keyloggers, stealers, RATs, etc. |
| **Botnet** | Red de equipos comprometidos controlados remotamente para ejecutar ataques coordinados. |
| **Phishing** | Engaño dirigido a obtener credenciales, datos financieros u otra información sensible de terceros mediante suplantación de identidad. |
| **C2 / C&C** | Infraestructura de Comando y Control usada para operar malware o botnets. |
| **CSAM** | Material de abuso sexual infantil (Child Sexual Abuse Material), prohibido por ley en toda circunstancia. |
| **AUP** | Esta Política de Uso Aceptable. |
| **Uptech** | Inversiones Uptech SPA, RUT [●], con domicilio en Santiago de Chile. |
| **Abuso verificado** | Incidente documentado mediante logs, reportes de terceros, CERT, listas de reputación u otra evidencia técnica objetiva. |

## 3. USOS PERMITIDOS

El Servicio puede utilizarse para actividades lícitas, incluyendo a modo ejemplar:

- Hospedaje de sitios web, aplicaciones web, APIs, servicios SaaS y plataformas de e-commerce.
- Bases de datos, entornos de desarrollo, staging y producción de software.

- Almacenamiento de archivos, backups y sistemas de recuperación ante desastres.
- Streaming de contenido multimedia de origen legal y con los derechos correspondientes.
- Comunicaciones empresariales: servidores de correo, videoconferencia, VoIP, VPN corporativa.
- Procesamiento de datos, análisis, machine learning e inteligencia artificial.
- Investigación de seguridad ofensiva y defensiva dentro de entornos propios o con autorización escrita del objetivo ("pentest autorizado").
- Servicios DNS, proxies y CDN propios dentro de los límites de esta AUP.

El hecho de que un uso no esté expresamente listado no lo hace automáticamente prohibido; en caso de duda, el cliente debe consultar a Uptech antes de proceder.

## 4. ACTIVIDADES PROHIBIDAS

Las siguientes actividades están estrictamente prohibidas. La enumeración no es taxativa; Uptech podrá determinar que otras actividades son igualmente prohibidas si contravienen el espíritu de esta política.

### 4.1 Spam y Comunicaciones Masivas No Solicitadas

🚫 **PROHIBIDO — Categoría: CRÍTICA**
Suspensión inmediata del servicio sin previo aviso.

- Envío de correos electrónicos en masa sin consentimiento explícito previo (opt-in) de los destinatarios.
- Uso del Servicio como relay abierto de correo (open relay).
- Generación de tráfico que resulte en la inclusión de las IPs de Uptech en listas negras como Spamhaus SBL/XBL/PBL, SORBS, Barracuda Reputation Block List u otras equivalentes.
- Campañas de SMS o mensajería masiva sin consentimiento verificable.
- Scraping masivo de direcciones de correo electrónico u otros datos personales.
- Uso de técnicas de evasión de filtros antispam (codificación especial, rotación de dominios, cuentas zombie, etc.).
- Hospedaje de listas de distribución de correo no gestionadas conforme al estándar CAN-SPAM, GDPR o legislación chilena aplicable.

### 4.2 Ataques y Actividad Maliciosa contra Terceros

🚫 **PROHIBIDO — Categoría: CRÍTICA**
Suspensión inmediata. Posible reporte a CSIRT, PDI y otras autoridades competentes.

- Ataques de denegación de servicio (DoS/DDoS) en cualquier forma, ya sea como origen, reflector o amplificador.
- Participación en botnets como nodo controlado o como infraestructura de C2/C&C.
- Escaneo masivo de puertos, fingerprinting o enumeración de vulnerabilidades en redes o sistemas de terceros sin autorización escrita del propietario.
- Explotación de vulnerabilidades en sistemas de terceros (hacking no autorizado).
- Ataques de fuerza bruta, credential stuffing o password spraying contra sistemas externos.

- Intercepción de tráfico de red (sniffing/spoofing) en segmentos de red compartida.
- Ataques de envenenamiento DNS (DNS poisoning/cache poisoning).
- Ataques Man-in-the-Middle (MitM) contra terceros.
- Exfiltración de datos de sistemas ajenos.
- Instalación o distribución de malware, ransomware, spyware, rootkits, keyloggers, troyanos o cualquier código malicioso.
- Hospedaje de kits de phishing, páginas de suplantación de identidad, formularios de captura fraudulentos o sitios de pharming.
- Participación en campañas de desinformación coordinada mediante infraestructura automatizada.

### 4.3 Contenido Ilegal o Dañino

🚫 **PROHIBIDO — Categoría: CRÍTICA**

Terminación inmediata del contrato. Reporte obligatorio a autoridades cuando la ley lo exija.

- Cualquier tipo de material de abuso sexual infantil (CSAM) o material que sexualice a menores de edad, sin excepción.
- Contenido que incite, promueva o facilite actos terroristas o de violencia extrema.
- Contenido que infrinja derechos de autor, marcas registradas u otros derechos de propiedad intelectual de terceros (incluyendo warez, cracks, seriales, piratería audiovisual o de software).
- Venta o distribución no autorizada de sustancias controladas, armas, documentos falsificados u otros bienes/servicios ilegales.
- Contenido que constituya discurso de odio en los términos de la legislación chilena e internacional aplicable.
- Esquemas de fraude, estafa, ponzi, phishing financiero o cualquier actividad de ingeniería social dirigida al robo de activos o identidad.
- Operación de plataformas de juego de azar sin las licencias reglamentarias exigidas en la jurisdicción de los usuarios.

### 4.4 Uso Abusivo de Recursos

⚠️ **PROHIBIDO — Categoría: ALTA**

Throttling, suspensión temporal o terminación según gravedad y reincidencia.

- Minería de criptomonedas que consuma recursos desproporcionados de CPU/GPU en planes no diseñados para ello, sin autorización previa de Uptech.
- Almacenamiento o distribución de torrents o contenido P2P de origen ilícito.
- Uso de ancho de banda de forma que degrade el servicio de otros clientes en la plataforma compartida.
- Ejecución de procesos que consuman de forma sostenida más del 80% de los recursos vCPU asignados durante periodos superiores a 30 minutos sin justificación técnica.
- Generación artificial de tráfico para sobrepasar umbrales de facturación o para degradar la calidad de servicio.
- Hospedaje de sitios de descargas masivas (cyberlockers) sin acuerdo previo con Uptech.

### 4.5 Infraestructura de Red y Seguridad

⚠️ **PROHIBIDO — Categoría: ALTA**
Suspensión de red inmediata ante amenaza activa. Investigación posterior.

- Uso de IPs de Uptech para operaciones de proxy anónimo o exit-node de redes de anonimato (Tor, I2P, etc.) sin autorización explícita de Uptech.
- ARP spoofing, MAC flooding u otros ataques a la capa de enlace en entornos de red compartida.
- Publicación de rutas BGP falsas o secuestro de prefijos IP (BGP hijacking).
- Intentos de acceso a la infraestructura de gestión de Uptech (hipervisores, switches, consolas de gestión, APIs de administración).
- Uso de IPs adicionales o subredes asignadas para fines distintos a los declarados al momento de la solicitud.
- Instalación de backdoors o accesos persistentes no declarados en el VPS que puedan comprometer la seguridad de la plataforma.

### 4.6 Actividades Financieras Irregulares

⚠️ **PROHIBIDO — Categoría: ALTA**
Terminación del contrato y reporte a organismos financieros reguladores si corresponde.

- Hospedaje de plataformas de fraude financiero, skimmers de tarjetas de crédito (carding), intercambio de datos robados o compraventa de información financiera ilícita.
- Operación de exchanges de criptomonedas sin registro ante el regulador competente cuando sea requerido.
- Uso del Servicio para lavado de activos o evasión de sanciones internacionales (OFAC, ONU, UE).

### 4.7 Privacidad y Datos Personales

ℹ️ **PROHIBIDO — Categoría: MEDIA-ALTA**
Notificación formal y plazo de corrección. Suspensión si no se remedia.

- Recopilación, procesamiento o almacenamiento de datos personales sin base legal conforme a la Ley N° 19.628 o legislación equivalente del país de los titulares.
- Operación de sistemas de vigilancia masiva o stalkerware dirigidos a monitorear a personas sin su conocimiento y consentimiento.
- Venta o transferencia de bases de datos de personas sin consentimiento de los titulares.

## 5. CLASIFICACIÓN DE INFRACCIONES Y CONSECUENCIAS

La siguiente matriz define el nivel de severidad asociado a cada tipo de infracción y la respuesta estándar de Uptech. Uptech se reserva el derecho de escalar la respuesta ante reincidencia o circunstancias agravantes.

| Infracción | Severidad | Respuesta estándar de Uptech |
|---|---|---|
| Spam / open relay detectado | CRÍTICA | Suspensión inmediata de red. Aviso por email. 24h para remediar. |
| DDoS activo originado desde el VPS | CRÍTICA | Null-route inmediato. Investigación. Posible terminación. |
| C2/Botnet / malware distribuido | CRÍTICA | Aislamiento de red. Terminación del contrato. Reporte a CSIRT. |
| CSAM o contenido ilegal grave | CRÍTICA | Terminación inmediata. Reporte obligatorio a PDI/MPCH. |
| Phishing / suplantación de identidad | CRÍTICA | Suspensión inmediata. Notificación al dominio afectado. |
| Hackeo activo de sistemas de terceros | CRÍTICA | Suspensión inmediata. Cooperación con autoridades. |
| Escaneo masivo no autorizado de puertos | ALTA | Bloqueo de puerto/IP atacante. Advertencia formal. |
| Minería abusiva de CPU/GPU | ALTA | Throttling. Advertencia. Suspensión si reincide. |
| Abuso de ancho de banda | ALTA | Rate limiting. Advertencia. Cobro por exceso si aplica. |
| Proxy anónimo / exit-node Tor no autorizado | ALTA | Bloqueo de puertos. Advertencia. Suspensión si reincide. |
| Infracción de derechos de autor (DMCA/IP) | MEDIA | Notificación. Plazo 72h para retirar contenido. |
| Datos personales sin base legal | MEDIA | Notificación formal. Plazo 7 días para remediar. |
| Reventa no autorizada del servicio | MEDIA | Advertencia. Renegociación o terminación. |

## 6. PROCEDIMIENTO DE RESPUESTA A INCIDENTES DE ABUSO

### 6.1 Detección

Uptech puede detectar infracciones por los siguientes medios, entre otros:

- Monitoreo automatizado de tráfico de red (análisis de patrones, volúmenes, puertos y protocolos).
- Alertas de listas de reputación externas (Spamhaus, AbuseIPDB, SURBL, PhishTank, etc.).
- Reportes de abuso enviados a abuse@uptech.cl por terceros afectados.
- Notificaciones de CERTs nacionales o internacionales (CSIRT Chile, US-CERT, etc.).
- Requerimientos legales o judiciales de autoridades competentes.
- Auditorías internas periódicas de seguridad.

## 6.2 Evaluación

Una vez detectada una posible infracción, el equipo de seguridad de Uptech:

- Recopila y preserva evidencia técnica (logs, capturas de tráfico, reportes externos).
- Clasifica la infracción según la matriz de severidad de la Sección 5.
- Determina si se requiere acción inmediata (suspensión preventiva) o si puede gestionarse con notificación previa.

## 6.3 Notificación al Cliente

Salvo en casos de severidad CRÍTICA donde la suspensión inmediata sea necesaria para proteger la red o a terceros, Uptech notificará al cliente por correo electrónico al domicilio registrado antes de tomar medidas. La notificación incluirá:

- Descripción de la infracción detectada.
- Evidencia resumida disponible.
- Plazo para remediar (variable según severidad: 2-72 horas para casos graves, hasta 7 días para infracciones moderadas).
- Consecuencias si no se remedia en el plazo indicado.

## 6.4 Plazos de Remediación Estándar

| Severidad | Plazo para remediar |
|---|---|
| **CRÍTICA** | 0–24 horas (suspensión inmediata posible) |
| **ALTA** | 24–48 horas |
| **MEDIA** | 72 horas – 7 días hábiles |
| **BAJA** | 10 días hábiles |

## 6.5 Acciones de Mitigación de Uptech

Uptech podrá aplicar, de forma unilateral y proporcional a la amenaza, las siguientes medidas técnicas:

- Null-route de IPs: bloqueo de todo el tráfico hacia/desde una dirección IP específica a nivel de red troncal.
- Rate limiting: limitación del ancho de banda disponible para el servicio afectado.
- Bloqueo selectivo de puertos: cierre de puertos específicos (ej. 25/SMTP, 6881-6889/BitTorrent) asociados al abuso.
- Aislamiento de red: desconexión del VPS de la red pública, manteniendo acceso de gestión (KVM/consola) para que el cliente pueda limpiar el sistema.
- Snapshot y suspensión: captura del estado del VPS y suspensión completa del servicio.
- Terminación del contrato y eliminación de datos conforme a la Cláusula 9 del contrato.

## 6.6 Reactivación del Servicio

Tras la resolución del incidente, el cliente podrá solicitar la reactivación del servicio acreditando que:

- La causa raíz del abuso ha sido identificada y eliminada.

- Se han tomado medidas para evitar la recurrencia (actualización de software, cambio de credenciales, corrección de configuración, etc.).
- Si corresponde, se ha notificado a los afectados y/o a las autoridades pertinentes.

Uptech se reserva el derecho de exigir un informe técnico de remediación antes de proceder a la reactivación. Se podrá cobrar un cargo de reactivación según lo indicado en el contrato vigente.

## 7. CANAL DE REPORTE DE ABUSO

Cualquier persona o entidad que detecte actividad abusiva originada desde la infraestructura de Uptech puede reportarla a través de los siguientes canales:

| Canal | Contacto / URL |
|---|---|
| **E-mail (principal)** | abuse@uptech.cl |
| **Formulario web** | uptech.cl/abuse |
| **E-mail soporte** | soporte@uptech.cl |
| **Emergencias 24/7** | [●] (número de contacto de guardia) |

Para agilizar la atención, los reportes deben incluir:

- Dirección IP de origen del abuso (con zona horaria UTC).
- Fecha y hora del incidente (preferentemente en formato ISO 8601).
- Logs o evidencia técnica relevante.
- Descripción del impacto observado.
- Datos de contacto del reportante (para seguimiento).

Uptech se compromete a acusar recibo de los reportes dentro de las 4 horas hábiles siguientes y a comunicar el resultado de la investigación.

## 8. INVESTIGACIÓN DE SEGURIDAD Y PENTESTING

Uptech reconoce la importancia de la investigación de seguridad responsable y admite las siguientes actividades bajo las condiciones indicadas:

### 8.1 Actividades Permitidas sin Autorización Previa

- Pentesting sobre sistemas de exclusiva propiedad del cliente, alojados en su propio VPS.
- Uso de herramientas de seguridad (nmap, Metasploit, etc.) dentro del propio VPS, sin que el tráfico resultante impacte sistemas de terceros.
- Laboratorios de seguridad, honeypots y entornos de análisis de malware en entornos aislados y debidamente contenidos.

### 8.2 Actividades que Requieren Autorización Escrita Previa de Uptech

- Simulación de ataques DDoS desde el VPS (incluso si el objetivo pertenece al cliente).
- Operación de exit-nodes, proxies de anonimato o nodos Tor.
- Pentesting sobre sistemas de terceros, aunque el cliente cuente con autorización del propietario del objetivo.

- Cualquier actividad que genere tráfico masivo que pueda ser confundido con un ataque real.

Las solicitudes de autorización deben enviarse a abuse@uptech.cl con al menos 48 horas de anticipación, describiendo el alcance, la metodología, las IPs involucradas y el período de tiempo de las pruebas.

## 9. PRIVACIDAD EN LA APLICACIÓN DE ESTA POLÍTICA

Uptech aplica esta política con el mínimo impacto posible sobre la privacidad del cliente. El monitoreo de red se realiza a nivel de metadatos de tráfico (IP de origen/destino, puertos, volúmenes, protocolos) y no implica inspección del contenido de los paquetes (DPI), salvo cuando sea estrictamente necesario para confirmar un abuso grave y con registro formal del acceso.

Los datos recopilados durante una investigación de abuso serán tratados de forma confidencial y utilizados exclusivamente para:

- Confirmar o descartar la existencia de la infracción.
- Notificar a las partes afectadas.
- Dar cumplimiento a requerimientos legales o judiciales.

Uptech no vende ni comparte datos de investigación con terceros con fines comerciales.

## 10. COOPERACIÓN CON AUTORIDADES

Uptech cooperará plenamente con las autoridades competentes en la investigación de actividades ilegales. En los siguientes casos, Uptech podrá divulgar información del cliente sin notificación previa:

- Requerimiento judicial o fiscal legalmente válido (orden de allanamiento, oficio judicial, exhorto).
- Situación de emergencia que implique riesgo vital para personas (art. 222 bis del Código Procesal Penal u equivalente).
- Obligación legal expresa de reporte (ej. CSAM conforme a la Ley N° 19.927).

Fuera de estos casos, Uptech procurará notificar al cliente sobre cualquier requerimiento de información, salvo que exista prohibición legal expresa o que la notificación pueda frustrar la investigación.

## 11. CUMPLIMIENTO CON REGÍMENES DE SANCIONES INTERNACIONALES

Uptech no proveerá servicios a personas, entidades o jurisdicciones sujetas a sanciones internacionales vigentes, incluyendo las listas OFAC (EE.UU.), ONU, Unión Europea y cualquier organismo equivalente. El cliente declara y garantiza que ni él ni sus usuarios finales se encuentran en dichas listas.

Si Uptech determina que un cliente está incurso en alguna de estas restricciones, terminará el servicio de inmediato y retendrá los fondos que corresponda conforme a la normativa aplicable.

## 12. MODIFICACIONES A ESTA POLÍTICA

Uptech podrá modificar esta AUP en cualquier momento. Los cambios sustantivos serán notificados al cliente con un mínimo de 15 días de anticipación mediante:

- Correo electrónico al domicilio registrado del cliente.
- Publicación en uptech.cl/aup con indicación de la versión y fecha de vigencia.

Si el cliente continúa usando el Servicio una vez transcurrido el plazo de preaviso, se entenderá que acepta la versión actualizada de la AUP. Si no acepta los cambios, deberá notificarlo por escrito antes del vencimiento del preaviso, en cuyo caso podrá terminar el contrato sin penalidad.

El historial de versiones de esta AUP estará disponible en uptech.cl/aup/historial.

## 13. DISPOSICIONES FINALES

Esta AUP se rige por la legislación chilena. En lo no previsto expresamente, se aplicarán supletoriamente las normas de la Ley N° 19.223 (Delitos Informáticos), la Ley N° 19.628 (Protección de Datos), la Ley N° 17.336 (Propiedad Intelectual), el Código de Comercio, el Código Civil y los tratados internacionales ratificados por Chile que resulten aplicables.

Si alguna disposición de esta AUP fuera declarada inválida o inaplicable, el resto de sus disposiciones mantendrán plena vigencia.

La tolerancia ocasional de Uptech ante alguna infracción no constituirá renuncia al derecho de exigir el cumplimiento estricto de esta política en el futuro.

📬 **Contactos clave de Uptech**

Reporte de abuso: abuse@uptech.cl
Soporte técnico: soporte@uptech.cl
Consultas legales: legal@uptech.cl
Sitio web AUP: uptech.cl/aup
Versión de este documento: 1.0 | Vigente desde: [DD/MM/AAAA]

*— Fin del documento —*