

Condiciones Específicas para Cloud Firewall, VPN y Seguridad Perimetral

Adaptix Networks, S.A. de C.V.

Versión vigente: Rev. 20260809

Fecha de entrada en vigor: 09 de agosto de 2026

Proveedor: Adaptix Networks, S.A. de C.V.

Sitio web: <https://www.adaptixnetworks.com>

Portal de clientes: <https://micuenta.adaptixnetworks.com>

1. Objeto

Las presentes **Condiciones Específicas para Cloud Firewall, VPN y Seguridad Perimetral**, en lo sucesivo las “**Condiciones Específicas**”, regulan la contratación, activación, uso, administración, soporte, configuración, operación, suspensión, cancelación y terminación de los servicios de firewall virtual, seguridad perimetral, filtrado web, VPN sitio-a-sitio, VPN sitio-a-cliente, alta disponibilidad y servicios relacionados proporcionados por **Adaptix Networks, S.A. de C.V.**, en lo sucesivo “**Adaptix Networks**”, “**Adaptix**” o “**el Proveedor**”.

Estas Condiciones Específicas forman parte integrante de los **Términos y Condiciones Generales de Servicio** de Adaptix Networks y complementan las políticas generales publicadas en la sección de Información Legal del sitio web de Adaptix Networks.

2. Naturaleza del servicio

El servicio de Cloud Firewall consiste en la provisión de una solución virtual o lógica de seguridad perimetral destinada a filtrar, permitir, denegar, registrar, enrutar, proteger o controlar tráfico de red conforme al plan contratado, configuración aplicada, reglas definidas y capacidades técnicas disponibles.

El servicio podrá incluir, según corresponda:

- a) Firewall virtual;
- b) Reglas de tráfico entrante y saliente;
- c) NAT;
- d) VPN sitio-a-sitio;
- e) VPN sitio-a-cliente o acceso remoto;
- f) Filtrado web;
- g) Políticas de seguridad;
- h) Alta disponibilidad, cuando aplique;
- i) Opciones de appliance virtual de terceros, como FortiGate u otras soluciones disponibles;
- j) Funciones adicionales conforme a la plataforma y plan contratado.

El Cloud Firewall es un servicio digital, intangible, tecnológico, recurrente y de provisión electrónica.

El servicio se considerará entregado cuando Adaptix Networks haya activado el firewall, puesto a disposición del Cliente la consola, credenciales, configuración inicial, conectividad, reglas base o acceso correspondiente.

3. Alcance del servicio



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

El alcance específico del servicio será el indicado en la tienda, cotización, orden de servicio, factura, descripción comercial, anexo técnico, configuración contratada o contrato particular aplicable.

De manera ordinaria, el Cloud Firewall podrá utilizarse para proteger servicios cloud, redes privadas, servidores virtuales, conexiones entre sitios, usuarios remotos, aplicaciones internas, acceso administrativo, tráfico corporativo o servicios asociados a la infraestructura del Cliente.

La contratación del servicio no implica, salvo pacto expreso, auditoría integral de seguridad, administración continua de sistemas internos, monitoreo SOC, respuesta a incidentes avanzada, análisis forense, hardening completo de servidores, pentesting, consultoría de ciberseguridad o garantía absoluta contra ataques.

4. Plataforma y tecnología utilizada

Adaptix Networks podrá prestar el servicio de Cloud Firewall mediante plataformas, fabricantes, appliances virtuales, soluciones de seguridad, herramientas propias o de terceros que considere adecuadas para la operación del servicio.

El Cliente reconoce que Adaptix Networks podrá modificar, sustituir, actualizar, migrar o reemplazar la tecnología utilizada para la prestación del servicio cuando resulte necesario por razones técnicas, comerciales, de seguridad, licenciamiento, soporte del fabricante, estabilidad, disponibilidad, fin de vida, mejora del servicio o continuidad operativa.

Las referencias a marcas, fabricantes, appliances o tecnologías específicas, incluyendo FortiGate u otras, se entenderán como opciones configurables o componentes técnicos disponibles, pero no limitarán la facultad de Adaptix Networks de utilizar tecnologías equivalentes o funcionalmente similares.

5. Administración del Cloud Firewall

La administración del Cloud Firewall podrá realizarse indistintamente por el Cliente o por Adaptix Networks, según el alcance contratado, permisos otorgados, modalidad operativa, solicitud expresa o acuerdo particular.

Cuando el Cliente cuente con acceso administrativo, será responsable de las configuraciones, reglas, cambios, políticas, VPN, NAT, objetos, usuarios, credenciales y demás ajustes que realice directamente en el firewall.

Cuando el Cliente solicite a Adaptix Networks realizar cambios, dichos cambios deberán solicitarse mediante ticket y por conducto de un contacto autorizado, conforme a la **Política de Soporte Técnico**.

Adaptix Networks podrá brindar asistencia técnica razonable para configuración, revisión, diagnóstico o modificación de reglas, VPN, NAT, filtrado o políticas, conforme al alcance contratado y disponibilidad técnica.

6. Acceso administrativo

El Cliente podrá recibir acceso administrativo o de gestión al Cloud Firewall, cuando el plan, plataforma y configuración lo permitan.

Toda acción realizada mediante credenciales, usuarios, llaves, tokens, direcciones IP, consola o accesos del Cliente se presumirá realizada o autorizada por el Cliente, salvo prueba en contrario.

El Cliente será responsable de:

- a) Proteger sus credenciales;
- b) Utilizar contraseñas robustas;
- c) Revocar accesos de personal que ya no deba tener permisos;
- d) Administrar usuarios autorizados;
- e) Evitar compartir accesos de forma insegura;



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

- f) Validar los cambios realizados en reglas, NAT, VPN o políticas;
- g) Mantener registro interno de sus propios cambios.

Adaptix Networks no será responsable por afectaciones causadas por configuraciones, cambios, errores, omisiones o accesos realizados por el Cliente, sus empleados, proveedores, técnicos, usuarios o terceros autorizados.

7. Cambios mediante ticket

Cuando el Cliente requiera que Adaptix Networks realice cambios en el Cloud Firewall, deberá solicitarlo mediante ticket en el portal de clientes:

<https://micuenta.adaptixnetworks.com>

El ticket deberá incluir, según corresponda:

- a) Servicio afectado;
- b) Regla, política, puerto, protocolo, dirección IP, red, NAT o VPN requerida;
- c) Justificación o propósito del cambio;
- d) Origen y destino del tráfico;
- e) Horario o ventana solicitada;
- f) Impacto esperado;
- g) Confirmación del contacto autorizado;
- h) Cualquier dato técnico necesario para ejecutar el cambio.

Adaptix Networks podrá solicitar aclaraciones antes de ejecutar un cambio cuando la solicitud sea ambigua, incompleta, riesgosa, técnicamente inviable, contradictoria o pueda afectar la seguridad o disponibilidad del servicio.

8. Responsabilidad sobre reglas y configuraciones

El Cliente será responsable de validar que las reglas, NAT, VPN, rutas, filtros, políticas, objetos y configuraciones solicitadas o realizadas sean correctas y correspondan a sus necesidades operativas.

Una regla mal definida puede exponer servicios, bloquear accesos legítimos, afectar aplicaciones, interrumpir conectividad, permitir tráfico no deseado, comprometer seguridad o afectar la operación del Cliente.

Adaptix Networks podrá orientar técnicamente al Cliente, pero no será responsable por consecuencias derivadas de instrucciones incorrectas, incompletas, ambiguas o inseguras proporcionadas por el Cliente, salvo responsabilidad directa imputable a Adaptix Networks.

9. VPN sitio-a-sitio

El servicio podrá incluir configuración o soporte para VPN sitio-a-sitio, conforme al plan contratado y compatibilidad técnica.

Las VPN sitio-a-sitio pueden depender de múltiples factores, incluyendo:

- a) Conectividad de Internet de ambos extremos;
- b) Direcciones IP públicas;
- c) NAT de terceros;
- d) Equipos firewall o routers del Cliente o terceros;
- e) Parámetros criptográficos;
- f) Políticas de fase 1 y fase 2;



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

- g) Rutas;
- h) Redes remotas;
- i) Proveedores de Internet;
- j) Estabilidad eléctrica y física de los sitios;
- k) Configuración correcta de ambos extremos.

Adaptix Networks no garantiza estabilidad absoluta de VPN cuando existan factores externos fuera de su control, incluyendo fallas del proveedor de Internet del Cliente, equipos remotos, configuraciones de terceros, enlaces inestables, cambios en dirección IP pública, bloqueos de puertos, NAT restrictivo o políticas de seguridad externas.

10. VPN sitio-a-cliente o acceso remoto

El servicio podrá incluir VPN sitio-a-cliente, acceso remoto o conexión de usuarios remotos, conforme al plan contratado, plataforma disponible y configuración aplicable.

El funcionamiento del acceso remoto puede depender de:

- a) Equipo del usuario;
- b) Sistema operativo;
- c) Cliente VPN instalado;
- d) Conexión a Internet del usuario;
- e) Antivirus, firewall local o políticas corporativas;
- f) Credenciales correctas;
- g) Certificados, llaves o perfiles;
- h) NAT o restricciones del proveedor de Internet;
- i) Cambios de red;
- j) Compatibilidad de software;
- k) Autorizaciones internas del Cliente.

Adaptix Networks podrá asistir razonablemente en la configuración del acceso remoto, pero no garantiza compatibilidad con todos los equipos, sistemas operativos, dispositivos móviles, redes, antivirus, firewalls locales, proveedores de Internet o políticas de terceros.

11. Filtrado web

Cuando el servicio incluya filtrado web, éste podrá utilizarse para permitir, bloquear, clasificar o restringir acceso a sitios web, categorías, dominios, URLs, contenidos o aplicaciones conforme a las capacidades técnicas disponibles.

El Cliente reconoce que los sistemas de filtrado web pueden depender de motores de clasificación, bases de datos, reputación, categorías, firmas, heurística, terceros, fabricantes o proveedores externos.

Ningún sistema de filtrado web es perfecto. Pueden existir falsos positivos, falsos negativos, sitios no clasificados, clasificación errónea, evasión mediante cifrado, proxies, VPNs externas, cambios de dominio, CDNs, aplicaciones móviles o tecnologías ajenas al control de Adaptix Networks.

Adaptix Networks podrá modificar políticas, categorías, reglas o mecanismos de filtrado cuando resulte necesario por razones técnicas, de seguridad, operativas o por solicitud autorizada del Cliente.

12. Monitoreo interno y notificaciones



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

Adaptix Networks podrá recibir notificaciones internas relacionadas con el estado del Cloud Firewall, incluyendo, de manera enunciativa, alertas de nuevo firmware, cambios de estado de VPN, eventos de conectividad, disponibilidad, actualizaciones o avisos de plataforma.

Dichas notificaciones tienen finalidad operativa interna y no constituyen, salvo contratación expresa, un servicio de monitoreo dedicado, SOC, vigilancia permanente, respuesta administrada a incidentes, reporte periódico al Cliente o garantía de intervención inmediata.

El Cliente podrá solicitar revisiones, diagnósticos, cambios, reportes o asistencia mediante ticket, conforme a la Política de Soporte Técnico y al alcance del servicio contratado.

13. Logs y reportes

Los logs, eventos, reportes o registros generados por el Cloud Firewall podrán revisarse cuando exista una incidencia, solicitud del Cliente, diagnóstico técnico, revisión de seguridad, reporte de abuso o necesidad operativa.

Salvo contratación expresa, Adaptix Networks no garantiza conservación histórica indefinida de logs, reportes personalizados, exportación periódica, análisis forense, correlación avanzada, monitoreo continuo ni almacenamiento probatorio.

Los logs pueden rotarse, sobrescribirse, depurarse, limitarse o eliminarse conforme a la capacidad técnica, configuración de la plataforma, políticas internas, licenciamiento, volumen de eventos y operación ordinaria del servicio.

El Cliente será responsable de contratar o implementar soluciones específicas si requiere retención extendida, cumplimiento regulatorio, auditoría, SIEM, análisis forense, evidencia probatoria o monitoreo de seguridad avanzado.

14. Bloqueo preventivo y mitigación de amenazas

Adaptix Networks podrá bloquear, limitar, filtrar, aislar o modificar tráfico, direcciones IP, países, puertos, protocolos, sesiones, amenazas, reglas o servicios sin autorización previa del Cliente cuando exista riesgo técnico, operativo, reputacional, de seguridad o legal.

Estas medidas podrán aplicarse cuando Adaptix Networks detecte o tenga indicios razonables de:

- a) Ataques;
- b) Escaneos maliciosos;
- c) Tráfico anómalo;
- d) Abuso;
- e) Malware;
- f) Phishing;
- g) Botnets;
- h) DDoS;
- i) Intentos de intrusión;
- j) Compromiso de credenciales;
- k) Vulnerabilidades explotadas;
- l) Riesgo para otros clientes;
- m) Afectación a la infraestructura;
- n) Requerimientos de proveedor, centro de datos, fabricante, autoridad o tercero legitimado.

La aplicación de medidas preventivas o de mitigación no generará responsabilidad para Adaptix Networks cuando se realice de buena fe para proteger su infraestructura, servicios, clientes, proveedores o terceros.



15. Seguridad no absoluta

El Cliente reconoce que un firewall, VPN, filtrado web o mecanismo de seguridad perimetral reduce riesgos, pero no garantiza seguridad absoluta.

Aunque Adaptix Networks emplee buenas prácticas, herramientas de seguridad, configuraciones razonables, segmentación, filtrado, políticas, actualizaciones o mecanismos preventivos, ningún sistema de seguridad puede garantizar protección total contra ataques, errores humanos, vulnerabilidades, malware, phishing, ransomware, credenciales comprometidas, fallas de terceros o amenazas nuevas.

El Cliente deberá mantener medidas complementarias de seguridad, incluyendo:

- a) Contraseñas robustas;
- b) Actualizaciones de servidores y aplicaciones;
- c) Respaldos;
- d) Antivirus o EDR cuando aplique;
- e) Control de usuarios;
- f) Revisión de permisos;
- g) Capacitación de usuarios;
- h) Políticas internas de seguridad;
- i) Hardening de sistemas;
- j) Monitoreo adicional cuando su operación lo requiera.

El Cloud Firewall no sustituye la responsabilidad del Cliente sobre la seguridad interna de sus servidores, aplicaciones, usuarios, credenciales, dispositivos, redes, contenidos y sistemas.

16. Responsabilidad del Cliente sobre su infraestructura interna

El Cliente seguirá siendo responsable de la seguridad, administración, actualización y configuración de sus servidores, sistemas operativos, aplicaciones, bases de datos, usuarios, contraseñas, servicios, dispositivos, redes internas y datos.

El Cloud Firewall no corrige vulnerabilidades internas, contraseñas débiles, aplicaciones desactualizadas, plugins vulnerables, configuraciones inseguras, malware ya instalado, usuarios mal capacitados, errores de permisos, exposición indebida de servicios o malas prácticas de administración.

Adaptix Networks podrá advertir, recomendar o asistir técnicamente al Cliente cuando detecte riesgos evidentes, pero no estará obligada a auditar de forma permanente la infraestructura interna del Cliente, salvo contratación expresa.

17. Alta disponibilidad

Cuando el servicio incluya alta disponibilidad, redundancia o configuración equivalente, dicha funcionalidad estará sujeta a la arquitectura contratada, disponibilidad de plataforma, configuración correcta, licenciamiento, conectividad, recursos y condiciones técnicas aplicables.

La alta disponibilidad reduce riesgos de interrupción, pero no garantiza continuidad absoluta, ausencia de fallas, conmutación instantánea, cero pérdida de sesiones, cero pérdida de paquetes, continuidad de VPN o disponibilidad ininterrumpida.

Los mecanismos de alta disponibilidad pueden verse afectados por mantenimientos, actualizaciones, fallas simultáneas, errores de configuración, fallas de terceros, dependencias de red, comportamiento de aplicaciones, licenciamiento, bugs de fabricante o eventos de fuerza mayor.



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

Página 6 de 10

www.adaptixnetworks.com

18. Licencias y fabricantes

Cuando el servicio utilice licencias, appliances, software, suscripciones, firmas, filtrado, antivirus, IPS, VPN, seguridad o componentes de terceros, el Cliente reconoce que su disponibilidad, precio, funcionalidades, actualizaciones, soporte y continuidad podrán depender del fabricante o proveedor correspondiente.

Adaptix Networks podrá trasladar al Cliente cambios de precio, condiciones, restricciones, fin de vida, sustituciones, modificaciones de licenciamiento o discontinuación de productos de terceros.

La falta de disponibilidad de una función específica de fabricante no constituirá incumplimiento de Adaptix Networks cuando se deba a causas externas, fin de vida, cambios de licenciamiento, políticas del fabricante o sustitución razonable de tecnología.

19. Actualizaciones y firmware

Adaptix Networks podrá aplicar actualizaciones, parches, firmware, upgrades, cambios de versión o ajustes de seguridad cuando lo considere necesario para mantener la estabilidad, seguridad, compatibilidad o soporte del servicio.

Cuando sea razonablemente posible, Adaptix Networks procurará notificar mantenimientos programados con anticipación.

No obstante, podrá realizar actualizaciones urgentes sin aviso previo cuando exista riesgo de seguridad, vulnerabilidad crítica, falla operativa, requerimiento de fabricante, riesgo de explotación, incidente activo o causa justificada.

El Cliente reconoce que las actualizaciones pueden requerir reinicios, reconexión de VPN, cambios temporales de disponibilidad, ajustes de configuración o ventanas de mantenimiento.

20. Dependencias externas

El funcionamiento del Cloud Firewall, VPN, filtrado o seguridad perimetral puede depender de servicios, equipos o condiciones externas a Adaptix Networks, incluyendo:

- a) Proveedores de Internet del Cliente;
- b) Equipos del Cliente;
- c) Firewalls, routers o módems remotos;
- d) Sistemas operativos de usuarios;
- e) Clientes VPN;
- f) Proveedores de DNS;
- g) Proveedores cloud externos;
- h) Fabricantes de software o hardware;
- i) Autoridades certificadoras;
- j) Operadores de red;
- k) Proveedores de energía;
- l) Configuraciones de terceros.

Adaptix Networks no será responsable por interrupciones, degradaciones, fallas o incompatibilidades causadas por dichos terceros o elementos fuera de su control razonable.

21. Servicios no incluidos salvo contratación expresa

Salvo pacto expreso por escrito, no se consideran incluidos dentro del Cloud Firewall:



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

- a) Monitoreo SOC 24/7 dedicado;
- b) Respuesta a incidentes avanzada;
- c) Análisis forense;
- d) Pentesting;
- e) Auditoría integral de seguridad;
- f) Hardening de servidores;
- g) Administración continua de endpoints;
- h) Limpieza de malware en equipos del Cliente;
- i) Capacitación de usuarios finales;
- j) Consultoría de cumplimiento regulatorio;
- k) SIEM o correlación avanzada;
- l) Retención extendida de logs;
- m) Reportes personalizados periódicos;
- n) Administración de redes internas del Cliente;
- o) Soporte presencial;
- p) Soporte a equipos de terceros no gestionados por Adaptix Networks.

Estas actividades podrán cotizarse por separado como servicios administrados, consultoría, bolsa de horas, proyecto especial o servicio profesional.

22. Uso aceptable

El Cliente deberá utilizar el Cloud Firewall, VPN y servicios de seguridad perimetral conforme a la **Política de Uso Aceptable**.

Queda prohibido utilizar el servicio para:

- a) Ocultar actividades ilícitas;
- b) Facilitar ataques;
- c) Realizar escaneos no autorizados;
- d) Evadir controles de seguridad de terceros;
- e) Distribuir malware;
- f) Ejecutar phishing;
- g) Participar en botnets;
- h) Facilitar fraude;
- i) Afectar redes, sistemas o servicios de terceros;
- j) Realizar actividades que comprometan la reputación o infraestructura de Adaptix Networks.

Adaptix Networks podrá suspender, limitar o terminar el servicio cuando detecte uso indebido, abuso, riesgo o incumplimiento de las políticas aplicables.

23. Suspensión por abuso, riesgo o incumplimiento

Adaptix Networks podrá suspender, limitar, aislar o cancelar total o parcialmente el Cloud Firewall, VPN, reglas, accesos o servicios relacionados cuando exista:

- a) Falta de pago;
- b) Incumplimiento contractual;
- c) Uso abusivo o ilícito;
- d) Riesgo de seguridad;
- e) Ataques originados desde el servicio;
- f) Compromiso del firewall o credenciales;
- g) Afectación a terceros;
- h) Requerimiento de autoridad;



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

- i) Requerimiento de proveedor o centro de datos;
- j) Incumplimiento de la Política de Uso Aceptable;
- k) Riesgo para infraestructura, reputación, direcciones IP, redes, clientes o proveedores de Adaptix Networks.

La suspensión preventiva no libera al Cliente de pagar importes devengados, servicios recurrentes, cargos pendientes o costos asociados.

24. Cancelación y eliminación de información

La cancelación del Cloud Firewall deberá solicitarse conforme a la **Política de Cancelación, Reembolso, Suspensión y Reactivación**.

Una vez cancelado, vencido, suspendido por falta de pago o terminado el servicio, Adaptix Networks podrá eliminar de forma definitiva configuraciones, reglas, objetos, usuarios, VPN, logs, respaldos, snapshots, licencias asociadas o cualquier información relacionada con el servicio.

Salvo que una condición específica indique otro plazo, Adaptix Networks podrá eliminar la información después de **30 días naturales** contados a partir de la suspensión, vencimiento, cancelación o terminación del servicio.

Una vez eliminada la información, su recuperación podrá ser imposible.

25. No reembolsos

Conforme a la **Política de Cancelación, Reembolso, Suspensión y Reactivación**, Adaptix Networks mantiene una política general de **no reembolsos**.

No procederán reembolsos por Cloud Firewall ya activado, aprovisionado, entregado, renovado, configurado, utilizado, suspendido por incumplimiento o puesto a disposición del Cliente.

La falta de uso del Cloud Firewall, VPN, filtrado, appliance virtual o funciones de seguridad no dará derecho a devolución, crédito, descuento o cancelación retroactiva.

26. Limitación de responsabilidad

Salvo dolo, mala fe, culpa grave o responsabilidad que legalmente no pueda limitarse, Adaptix Networks no será responsable por daños indirectos, pérdida de negocio, pérdida de ingresos, pérdida de reputación, pérdida de oportunidad, pérdida de datos, interrupción operativa, incidentes de seguridad, accesos no autorizados, malware, ransomware, phishing, fraude, ataques, indisponibilidad de VPN o afectaciones derivadas de causas no imputables directamente a Adaptix Networks.

La responsabilidad de Adaptix Networks, en su caso, se limitará conforme a lo establecido en los **Términos y Condiciones Generales de Servicio**.

27. Relación con otros documentos

Estas Condiciones Específicas complementan los siguientes documentos:

- a) Términos y Condiciones Generales de Servicio;
- b) Aviso de Privacidad;



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355

- c) Política de Uso Aceptable;
- d) Política de Soporte Técnico;
- e) Política de Cancelación, Reembolso, Suspensión y Reactivación;
- f) Política de Respaldos, Retención y Recuperación de Información;
- g) Política de Validación y Entrega de Accesos Administrativos;
- h) Condiciones Específicas para Cloud Server, VPS y Servidores Virtuales;
- i) Condiciones Específicas para Direcciones IP públicas;
- j) Cotización, orden de servicio, factura, anexo técnico o contrato particular aplicable.

En caso de contradicción entre estas Condiciones Específicas y los Términos y Condiciones Generales de Servicio, prevalecerán estas Condiciones Específicas únicamente respecto del servicio de Cloud Firewall, VPN y Seguridad Perimetral, salvo disposición legal irrenunciable en contrario.

28. Modificaciones

Adaptix Networks podrá modificar, actualizar o sustituir estas Condiciones Específicas en cualquier momento para atender cambios legales, regulatorios, técnicos, operativos, comerciales, de seguridad, de plataforma, fabricantes, proveedores o prácticas internas.

Las modificaciones serán publicadas en la sección de Información Legal del sitio web de Adaptix Networks.

La versión vigente será la publicada en:

<https://www.adaptixnetworks.com/informacion-legal/>

El uso continuado del servicio después de la publicación de modificaciones implicará la aceptación de las Condiciones Específicas actualizadas.

29. Vigencia

Las presentes Condiciones Específicas para Cloud Firewall, VPN y Seguridad Perimetral entrarán en vigor a partir de la fecha indicada al inicio del documento y permanecerán vigentes hasta que sean modificadas, sustituidas o actualizadas por Adaptix Networks.

Adaptix Networks, S.A. de C.V.
Condiciones Específicas para Cloud Firewall, VPN y Seguridad Perimetral
Rev. 20260809



37 Poniente 2701 Segundo Piso
Col. Benito Juárez
Puebla, Pue. 72410

+52 (222) 555-2355