

Condiciones Específicas para Certificados SSL/TLS

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>

Tienda de certificados SSL: <https://micuenta.adaptixnetworks.com/store/certificados-ssl>

1. Objeto

Las presentes **Condiciones Específicas para Certificados SSL/TLS**, en lo sucesivo las “**Condiciones Específicas**”, regulan la contratación, emisión, instalación, renovación, validación, administración, vencimiento, cancelación y terminación de servicios relacionados con certificados digitales SSL/TLS proporcionados, gestionados o asistidos 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

Los certificados SSL/TLS permiten cifrar comunicaciones entre un sitio web, servidor, aplicación, servicio o dominio y los usuarios que acceden a éstos, sujeto a las características técnicas del certificado emitido, la configuración del servidor, la autoridad certificadora, el dominio, el navegador, el sistema operativo y el entorno donde se utilice.

Adaptix Networks podrá proporcionar, gestionar, instalar o asistir en el uso de certificados SSL/TLS gratuitos, comerciales o emitidos por terceros, según el servicio contratado y la disponibilidad técnica o comercial aplicable.

El Cliente reconoce que la emisión, renovación, validación, revocación y funcionamiento de los certificados SSL/TLS puede depender de autoridades certificadoras, proveedores externos, validaciones DNS, validaciones por correo electrónico, validaciones documentales, políticas de seguridad, reglas del ecosistema SSL/TLS y requisitos de terceros.

3. Tipos de certificados

Adaptix Networks podrá ofrecer o asistir, según el caso, con:

- a) Certificados gratuitos emitidos mediante Let's Encrypt desde Plesk u otras plataformas compatibles;
- b) Certificados SSL/TLS comerciales de pago disponibles en el portal de clientes;
- c) Certificados SSL/TLS emitidos por autoridades certificadoras como GlobalSign u otros proveedores disponibles;
- d) Certificados de validación de dominio, organización o validación extendida, cuando estén disponibles;
- e) Certificados wildcard o multidominio, cuando sean ofrecidos comercialmente;
- f) Certificados proporcionados directamente por el Cliente, sujetos a compatibilidad técnica.



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

+52 (222) 555-2355

Página 1 de 9

www.adaptixnetworks.com

La disponibilidad, precio, vigencia, validación, características, cobertura, garantía comercial, soporte y condiciones de cada certificado dependerán del producto contratado y de las políticas de la autoridad certificadora o proveedor correspondiente.

4. Let's Encrypt en Hospedaje Web

Cuando el Cliente cuente con un plan de **Hospedaje Web** administrado mediante Plesk, podrá utilizar certificados gratuitos de **Let's Encrypt** cuando la plataforma, dominio, DNS y configuración técnica lo permitan.

Adaptix Networks podrá asistir al Cliente en la instalación, activación o renovación de certificados Let's Encrypt dentro de Plesk, conforme a la **Política de Soporte Técnico** y al alcance razonable del servicio de Hospedaje Web contratado.

El Cliente reconoce que la emisión y renovación de certificados Let's Encrypt depende de validaciones automáticas, resolución DNS correcta, disponibilidad del dominio, configuración del servidor, respuesta HTTP/HTTPS, políticas de Let's Encrypt, límites de emisión y condiciones técnicas externas a Adaptix Networks.

La disponibilidad de Let's Encrypt no constituye garantía de emisión o renovación indefinida, ya que puede verse afectada por cambios de política, límites de la autoridad certificadora, errores de DNS, configuraciones incorrectas, cambios en el dominio, bloqueo de validaciones, migraciones o fallas de terceros.

5. Certificados SSL/TLS comerciales

Adaptix Networks podrá vender certificados SSL/TLS comerciales a través de su portal de clientes, incluyendo certificados emitidos por GlobalSign u otras autoridades certificadoras disponibles.

La contratación de certificados comerciales estará sujeta a:

- a) Disponibilidad del producto;
- b) Pago oportuno;
- c) Datos correctos del Cliente;
- d) Validación del dominio;
- e) Validación por correo electrónico, DNS o archivo, según corresponda;
- f) Validación documental o corporativa, cuando aplique;
- g) Políticas de la autoridad certificadora;
- h) Reglas técnicas y comerciales vigentes al momento de la emisión.

El Cliente reconoce que Adaptix Networks puede actuar como revendedor, gestor, intermediario técnico o proveedor de soporte, pero la emisión final del certificado dependerá de la autoridad certificadora correspondiente.

6. Validación del certificado

La emisión de un certificado SSL/TLS puede requerir validaciones de distinto tipo, incluyendo:

- a) Validación por correo electrónico;
- b) Validación mediante registro DNS;
- c) Validación mediante archivo publicado en el servidor;
- d) Validación documental;
- e) Validación de identidad;
- f) Validación de organización;
- g) Validación telefónica;
- h) Validación de titularidad o control del dominio;
- i) Cualquier otra validación requerida por la autoridad certificadora.



Adaptix Networks podrá asistir al Cliente en la gestión de dichas validaciones cuando sea técnicamente posible y conforme al servicio contratado.

El Cliente deberá cooperar oportunamente proporcionando información, documentos, autorizaciones, accesos, registros DNS, confirmaciones de correo o cualquier elemento requerido para completar la validación.

La falta de cooperación, información incorrecta, datos inconsistentes, correos no atendidos, DNS mal configurado, bloqueo del dominio o retrasos del Cliente podrán impedir, retrasar o cancelar la emisión del certificado sin responsabilidad para Adaptix Networks.

7. Validaciones DNS

Cuando la emisión o renovación de un certificado requiera validación mediante registros DNS, el Cliente será responsable de crear, autorizar o permitir la creación de los registros correspondientes.

Cuando el dominio utilice Hospedaje Web con Plesk y la zona DNS se administre desde dicha plataforma, el Cliente podrá gestionar los registros DNS mediante Plesk, o solicitar asistencia a Adaptix Networks mediante ticket.

Cuando el DNS sea administrado por un tercero, el Cliente será responsable de realizar los cambios necesarios con su proveedor DNS externo.

Adaptix Networks no será responsable por retrasos, fallas de emisión, vencimientos o rechazos derivados de DNS administrado fuera de su control, registros incorrectos, propagación incompleta, TTL, errores del Cliente o restricciones de terceros.

8. Validaciones por correo electrónico

Cuando la autoridad certificadora requiera validación por correo electrónico, el Cliente será responsable de atender oportunamente los mensajes enviados a las direcciones autorizadas para el dominio o a los correos administrativos definidos por la autoridad certificadora.

La falta de recepción, lectura, respuesta o confirmación del correo de validación podrá impedir la emisión, renovación o reemisión del certificado.

Adaptix Networks no será responsable por fallas de validación derivadas de buzones inexistentes, correos filtrados, antispam, cuentas no revisadas, datos incorrectos, dominios vencidos, problemas de correo del Cliente o causas no imputables directamente a Adaptix Networks.

9. Instalación en Hospedaje Web

En servicios de Hospedaje Web administrados por Adaptix Networks mediante Plesk, Adaptix Networks podrá asistir al Cliente con la instalación o activación de certificados SSL/TLS sobre el dominio correspondiente.

La instalación estará sujeta a:

- a) Que el dominio apunte correctamente al servicio de Hospedaje Web;
- b) Que la zona DNS permita la validación;
- c) Que el certificado haya sido emitido correctamente;
- d) Que el dominio, subdominio o alias esté configurado en Plesk;
- e) Que no existan conflictos técnicos, errores de configuración o restricciones de la plataforma.



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

+52 (222) 555-2355

La asistencia para instalación de SSL/TLS en Hospedaje Web no implica garantía de corrección de problemas externos, desarrollo del sitio web, corrección de contenido mixto, cambios de aplicación, redirecciones avanzadas, reparación de CMS, limpieza de malware o soporte fuera del alcance contratado.

10. Instalación en Cloud Server

En servicios de **Cloud Server**, VPS o servidores virtuales, la instalación, configuración, renovación y administración del certificado SSL/TLS corresponderá al Cliente, salvo que haya contratado expresamente un servicio administrado o solicite asistencia técnica adicional a Adaptix Networks.

Adaptix Networks podrá asistir al Cliente mediante ticket en la instalación o configuración de certificados en Cloud Server, sujeto a disponibilidad técnica, sistema operativo, panel, aplicación, servidor web, permisos, accesos, complejidad y condiciones comerciales aplicables.

La asistencia en Cloud Server podrá generar cargos adicionales cuando implique administración interna del servidor, configuración avanzada, troubleshooting de aplicaciones, servidores web, balanceadores, contenedores, proxies, servicios de correo, APIs, bases de datos, plataformas de terceros o intervenciones fuera del soporte razonable incluido.

11. Renovación de certificados

La renovación de certificados SSL/TLS dependerá del tipo de certificado contratado.

Los certificados gratuitos de Let's Encrypt suelen renovarse de forma automática cuando la plataforma, dominio, DNS y validaciones técnicas lo permiten.

Los certificados comerciales deberán renovarse conforme a su vigencia, producto contratado, pago oportuno, validaciones requeridas y políticas de la autoridad certificadora.

El Cliente será responsable de revisar avisos de vencimiento, atender validaciones, renovar oportunamente certificados comerciales, mantener datos correctos, conservar acceso a los correos de validación y verificar que el certificado se encuentre correctamente instalado y vigente.

Adaptix Networks podrá enviar avisos de renovación o vencimiento cuando sea técnicamente posible, pero la falta de recepción o lectura de dichos avisos por causas no imputables a Adaptix Networks no exime al Cliente de su responsabilidad de renovar y validar oportunamente.

12. Vencimiento del certificado

El vencimiento de un certificado SSL/TLS puede generar advertencias de seguridad, errores de navegador, interrupción de servicios, pérdida de confianza, fallas en APIs, problemas de correo, afectación de aplicaciones, problemas de posicionamiento, abandono de usuarios o afectaciones comerciales.

El Cliente reconoce que los certificados vencidos por falta de renovación, falta de validación, falta de pago, falta de cooperación, errores de DNS, datos incorrectos, falta de acceso al correo de validación o causas no imputables directamente a Adaptix Networks serán responsabilidad del Cliente.

Adaptix Networks no será responsable por daños, pérdidas, interrupciones, reclamaciones o afectaciones derivadas de certificados vencidos por causas imputables al Cliente o a terceros.



13. Reemisión de certificados

La reemisión de un certificado puede ser necesaria por:

- a) Cambio de clave privada;
- b) Cambio de servidor;
- c) Cambio de dominio o subdominio permitido;
- d) Compromiso de seguridad;
- e) Error de instalación;
- f) Cambio de datos;
- g) Requerimiento de la autoridad certificadora;
- h) Reinstalación o migración del servicio;
- i) Pérdida de archivos del certificado.

La reemisión estará sujeta a las políticas de la autoridad certificadora, producto contratado, validaciones aplicables, disponibilidad técnica y cooperación del Cliente.

Adaptix Networks podrá asistir en la reemisión cuando sea posible, pero no garantiza que la autoridad certificadora apruebe, permita o procese la reemisión en todos los casos.

14. Revocación de certificados

Un certificado SSL/TLS podrá ser revocado por causas como:

- a) Compromiso de la clave privada;
- b) Solicitud del Cliente;
- c) Orden o instrucción de autoridad competente;
- d) Requerimiento de la autoridad certificadora;
- e) Información falsa, incorrecta o no verificable;
- f) Incumplimiento de políticas de la autoridad certificadora;
- g) Uso indebido, fraude, phishing, malware o suplantación;
- h) Riesgos de seguridad.

Adaptix Networks no será responsable por revocaciones ordenadas o ejecutadas por autoridades certificadoras, registros, autoridades competentes o terceros cuando deriven de causas ajenas a Adaptix Networks.

15. Compatibilidad técnica

La instalación y funcionamiento correcto de un certificado SSL/TLS depende de múltiples factores, incluyendo:

- a) Servidor web;
- b) Sistema operativo;
- c) Panel de control;
- d) Navegadores;
- e) Cadena intermedia;
- f) Protocolos TLS habilitados;
- g) Ciphers;
- h) Configuración de red;
- i) Balanceadores, proxies, firewalls o CDN;
- j) Aplicaciones del Cliente;
- k) Redirecciones HTTP/HTTPS;
- l) Contenido mixto;
- m) Compatibilidad de clientes antiguos.



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

+52 (222) 555-2355

Adaptix Networks podrá asistir en la instalación básica cuando corresponda, pero no garantiza compatibilidad con todos los navegadores, dispositivos, sistemas antiguos, aplicaciones, clientes, integraciones, APIs o configuraciones especiales, salvo pacto expreso.

16. Contenido mixto y errores de aplicación

La instalación de un certificado SSL/TLS no garantiza que el sitio web o aplicación funcione completamente bajo HTTPS.

Pueden existir errores de contenido mixto, enlaces internos en HTTP, recursos externos inseguros, scripts, imágenes, hojas de estilo, APIs, plugins, temas, CMS o aplicaciones que requieran ajustes adicionales.

La corrección de contenido mixto, redirecciones, configuración de aplicaciones, cambios de CMS, ajustes de código, depuración de plugins, hardening o modificaciones avanzadas no se considera incluida salvo que el servicio contratado lo contemple expresamente o se cotece por separado.

17. Claves privadas

El Cliente será responsable de proteger las claves privadas asociadas a sus certificados SSL/TLS cuando dichas claves sean generadas, almacenadas o administradas por el Cliente o dentro de servicios bajo su control.

El compromiso, pérdida, exposición o uso indebido de una clave privada puede requerir la revocación y reemisión del certificado.

Adaptix Networks no será responsable por incidentes derivados de claves privadas compartidas indebidamente, almacenadas sin seguridad, filtradas, eliminadas, copiadas por terceros o comprometidas por causas no imputables directamente a Adaptix Networks.

18. Certificados proporcionados por el Cliente

Cuando el Cliente proporcione un certificado SSL/TLS propio para instalación o uso en servicios de Adaptix Networks, el Cliente será responsable de:

- a) Contar con derecho de uso del certificado;
- b) Proporcionar el certificado correcto;
- c) Proporcionar clave privada, cadena intermedia y archivos necesarios;
- d) Verificar la vigencia;
- e) Renovarlo oportunamente;
- f) Asegurar que cubra el dominio, subdominio o servicio correspondiente;
- g) Cumplir las condiciones de la autoridad certificadora que lo emitió.

Adaptix Networks podrá rechazar la instalación de certificados incompletos, inválidos, inseguros, vencidos, incompatibles, mal emitidos o que generen riesgo técnico o de seguridad.

19. Dependencia de terceros

El Cliente reconoce que la emisión, validación, renovación, reemisión, revocación, compatibilidad y funcionamiento de certificados SSL/TLS puede depender de terceros, incluyendo:



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

+52 (222) 555-2355

- a) Let's Encrypt;
- b) GlobalSign;
- c) Otras autoridades certificadoras;
- d) Registradores de dominio;
- e) Proveedores DNS;
- f) Navegadores;
- g) Sistemas operativos;
- h) Fabricantes de software;
- i) Proveedores de correo;
- j) Proveedores de infraestructura o seguridad.

Adaptix Networks no será responsable por fallas, rechazos, retrasos, cambios de política, límites de emisión, revocaciones, incompatibilidades, bloqueos, vencimientos, discontinuaciones, errores o decisiones atribuibles a dichos terceros, salvo en la medida en que exista responsabilidad directa imputable a Adaptix Networks.

20. Uso prohibido

El Cliente no podrá utilizar certificados SSL/TLS gestionados, instalados o contratados a través de Adaptix Networks para:

- a) Phishing;
- b) Malware;
- c) Fraude;
- d) Suplantación de identidad;
- e) Sitios engañosos;
- f) Distribución de contenido ilícito;
- g) Actividades prohibidas por la Política de Uso Aceptable;
- h) Infracción de derechos de terceros;
- i) Ocultar actividades maliciosas o abusivas.

Adaptix Networks podrá suspender servicios, retirar certificados, negar asistencia, reportar abuso o colaborar con autoridades certificadoras, proveedores o autoridades competentes cuando detecte uso indebido.

21. 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 certificados SSL/TLS ya solicitados, emitidos, renovados, validados, instalados, reemitidos, puestos a disposición o gestionados correctamente.

El Cliente reconoce que los certificados SSL/TLS comerciales dependen de autoridades certificadoras y terceros, y que una vez procesados pueden no ser cancelables, reversibles o reembolsables.

La falta de uso del certificado, errores de configuración imputables al Cliente, falta de validación, falta de instalación por causas ajenas a Adaptix Networks o cancelación anticipada no dará derecho a devolución.

22. Cancelación

La cancelación de un certificado SSL/TLS deberá realizarse conforme a la **Política de Cancelación, Reembolso, Suspensión y Reactivación** y mediante el portal de clientes de Adaptix Networks.



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

+52 (222) 555-2355

La cancelación podrá evitar renovaciones futuras cuando sea procesada oportunamente, pero no implica reembolso de certificados ya emitidos, renovados, validados, instalados o puestos a disposición.

El Cliente reconoce que cancelar un certificado puede afectar el funcionamiento seguro del sitio web, aplicación, servidor, correo, API o servicio asociado.

23. 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, interrupción operativa, errores de navegador, fallas de aplicación, advertencias de seguridad, pérdida de datos, reclamaciones de terceros 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**.

24. Relación con otros documentos

Estas Condiciones Específicas complementan los siguientes documentos:

- a) Términos y Condiciones Generales de Servicio;
- b) Aviso de Privacidad;
- 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 Registro, Renovación y Transferencia de Dominios;
- i) Condiciones Específicas para Hospedaje Web;
- j) Condiciones Específicas para Cloud Server, VPS y Servidores Virtuales;
- k) 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 certificados SSL/TLS, salvo disposición legal irrenunciable en contrario.

25. 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 registradores, registros, 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.



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

+52 (222) 555-2355

26. Vigencia

Las presentes Condiciones Específicas para Certificados SSL/TLS 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 Certificados SSL/TLS
Rev. 20260809



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

+52 (222) 555-2355