

Seguridad y confianza operativa

Para entornos regulados y de alta disponibilidad

SynapseTel Cloud diseña, moderniza y opera infraestructura crítica de telecomunicaciones y nube empresarial. Trabajamos con elementos de núcleo de red, centros de datos híbridos y pipelines CI/CD de producción. La seguridad rige el acceso a su entorno, el desarrollo y la entrega de código y el control de los flujos automatizados.

v7.0 · Política actualizada: 19 de octubre de 2026

Entidad contratante	Registro	Jurisdicción
SYNAPSETEL CLOUD LLC	L26000459009	Florida, United States

1. Ejecución dentro del perímetro del cliente y sin custodia de datos de producción

El aislamiento de perímetros es nuestro principal control de prestación. Los datos propietarios, topologías y código permanecen dentro de su perímetro de seguridad aprobado.

Ingeniería dentro de su entorno

La evaluación, migración e implementación se ejecutan en sus cuentas/VPC en la nube, su infraestructura VMware/vSAN local o sus clústeres Red Hat OpenShift. Los ingenieros acceden mediante bastiones, VDI o pasarelas ZTNA aprobados por usted.

Sin extracción de datos de producción

No copiamos, almacenamos ni tratamos CPNI, datos personales de abonados, bases de producción ni capturas de paquetes de red en vivo en infraestructura propiedad de SynapseTel.

Gestión controlada de artefactos

Diagramas, grafos de dependencias y procedimientos permanecen en repositorios y almacenes documentales del cliente. Los metadatos de diagnóstico ajenos a producción expresamente autorizados para análisis local se cifran y eliminan al terminar el encargo según el procedimiento acordado, mediante borrado criptográfico cuando sea compatible.

Este límite se aplica al material técnico de producción. El portal administrativo separado trata contactos, cuentas, servicios y facturación autorizados; su funcionamiento se describe más abajo.

2. Identidad, acceso y gobierno de cambios

El acceso técnico utiliza su IdP, sus procesos PAM y cuentas nominativas. Usted conserva la aprobación, revisión y revocación del acceso.

Mínimo privilegio y acceso temporal

Limitamos los roles a la tarea aprobada y admitimos elevación just-in-time. La grabación de sesiones SSH, API Kubernetes y consola cloud se configura mediante sus controles de acceso y registro compatibles.

Autenticación respaldada por hardware

Nuestro estándar de puestos de ingeniería exige MFA resistente al phishing con FIDO2/WebAuthn, autenticación SSH criptográfica y cambios de código firmados. El acceso del cliente sigue los mecanismos compatibles y aprobados de su IdP y PAM.

Control GitOps de producción

Los cambios rutinarios siguen código firmado, revisión entre pares y validación de políticas. Las merge/pull requests identifican cambio y aprobaciones; GitLab CI valida y un controlador GitOps como Argo CD reconcilia la configuración declarativa aprobada. Los elementos de red usan la automatización y el control de cambios autorizados por el cliente.

Se prohíben los cambios improvisados en producción. Las emergencias siguen el procedimiento break-glass autorizado por el cliente, con evidencias de sesión, revisión posterior y reconciliación con la fuente de verdad.

3. Endurecimiento de infraestructura, Kubernetes y telecomunicaciones

La base técnica cubre aislamiento de cargas, segmentación de gestión, procedencia del software y suministro de secretos. El diseño documenta los controles de cada carga compatible y cualquier excepción aprobada.

Dominio	Estándar de ingeniería
Kubernetes y OpenShift	Perfiles restringidos, incluidos SCC restricted-v2 de OpenShift cuando proceda, ejecución no root, seccomp RuntimeDefault y eliminación de capacidades Linux (ALL). Los sistemas de archivos raíz de solo lectura se configuran por separado; se valida el SCC efectivo y los permisos del namespace en admisión.
Segmentación de red	NetworkPolicies con denegación por defecto de entrada y salida, flujos explícitos y mTLS donde los servicios seleccionados lo admitan. Separación mediante zonas de firewall entre gestión OSS/ENM, adaptadores CAMARA/NEF/SCEF, gateways y portales públicos.
Cadena de suministro y CI/CD	Verificación de procedencia de imágenes, generación de SBOM, análisis de vulnerabilidades y umbrales CVE acordados antes de promover imágenes. Políticas de admisión OPA Gatekeeper o Kyverno cuando se elijan para la plataforma de destino.
Gestión de secretos	Sin secretos en texto claro en Git. Credenciales, certificados y tokens se suministran mediante gestores aprobados como HashiCorp Vault, o flujos External Secrets o Sealed Secrets correctamente configurados.

La admisión SCC, la raíz de solo lectura, el cifrado de red y los controles de suministro son medidas distintas. Las CNF u otras cargas que requieran excepciones necesitan revisión de seguridad documentada y controles compensatorios.

4. Agentes de IA y controles Model Context Protocol

La entrega asistida por IA y las integraciones MCP operan dentro de límites explícitos de datos, herramientas y aprobación.

Ejecución privada y aprobada de modelos

Los flujos del cliente usan inferencia privada aprobada, como modelos OpenShift AI o vLLM alojados por el cliente dentro de su perímetro. Código, manifiestos y telemetría propietarios quedan fuera de servicios públicos de IA de consumo. Se aprueban previamente las condiciones de retención y exclusión de entrenamiento.

Herramientas delimitadas de forma determinista

Los servidores MCP exponen herramientas de solo lectura o restringidas por esquema con cuentas acotadas. Los agentes no ejecutan shells arbitrarios ni eluden RBAC. El servicio conectado autoriza cada acción.

Aprobación humana en producción

Los agentes preparan manifiestos, validaciones previas y evidencias de control. Las modificaciones en producción requieren aprobación humana autenticada y atribuible y validación CI/CD determinista; firma y aprobación quedan vinculadas al cambio.

Auditoría conservada por el cliente

Prompts, consultas de contexto e invocaciones MCP generan registros en su SIEM u observabilidad central. Contenido, ocultación, acceso y retención resistente a alteraciones se configuran dentro de su perímetro para proteger secretos y contexto sensible.

Una validación previa favorable no autoriza el despliegue ni acredita su salud. Siguen vigentes la autorización del sistema destino, la admisión y la aceptación operativa.

5. Alineación regulatoria y de cumplimiento

Mapeamos controles y evidencias con las obligaciones y marcos seleccionados para el encargo. Su equipo de seguridad documenta aplicabilidad, evidencias y responsables de aceptación.

Marcos de seguridad empresarial

Mapeo con criterios SOC 2 Type II, ISO/IEC 27001 y NIST SP 800-53 Rev. 5.

Telecomunicaciones e infraestructura crítica

Especificaciones SCAS de 3GPP, obligaciones FCC CPNI y requisitos NIS2 pertinentes según servicios y jurisdicción.

Referencias cloud y contenedores

CIS Benchmarks aplicables a Kubernetes y Red Hat OpenShift, con excepciones y evidencias de corrección documentadas.

La alineación y las evidencias no acreditan certificación ni garantizan cumplimiento normativo. SynapseTel Cloud no se ha sometido a un examen SOC 2 Type I o Type II. Los informes de proveedores cubren sus propios servicios.

6. Seguridad de puestos y personal

Los requisitos de personal y dispositivos se aplican antes de conceder acceso a sistemas del cliente.

Dirección técnica desde Estados Unidos

Los encargos están dirigidos por arquitectos principales sénior evaluados que operan desde Estados Unidos. Se identifican responsabilidades y personal autorizado.

Puestos protegidos

Los dispositivos corporativos de ingeniería requieren cifrado completo FileVault o BitLocker, gestión automática de parches, EDR y políticas de firewall aplicadas.

Confidencialidad desde el inicio

Firmamos un acuerdo mutuo de confidencialidad antes de descubrir la arquitectura o revisar repositorios. El material del cliente sigue los límites de acceso y confidencialidad aprobados.

La incorporación aborda verificaciones, residencia, estado de dispositivos y evidencias de acceso específicos del cliente.

7. Contacto de seguridad y divulgación de vulnerabilidades

InfoSec y compras pueden solicitar cuestionarios y evidencias del encargo. Los investigadores pueden comunicar vulnerabilidades potenciales de synapsetel.com o activos públicos por el mismo contacto.

Correo de seguridad

security@synapsetel.com

Acuse de recibo

Acusamos recibo de consultas de seguridad e informes de vulnerabilidades en un plazo de 24 horas.

Incluya URL afectada, descripción breve, pasos de reproducción y contacto. Evite datos de abonados, credenciales o pruebas destructivas. Coordine previamente cualquier prueba que exceda el uso normal.

[Ver el contacto de divulgación en security.txt](#)

Portal administrativo y límites de garantía

El modelo sin custodia de producción no elimina el tratamiento administrativo. El portal usa Netlify para alojamiento, Supabase para autenticación, base de datos y archivos privados, Stripe para facturación y GitHub para código.

Registros administrativos permitidos

El portal trata identidades, contactos autorizados, solicitudes y estados, documentos aprobados, acuerdos y referencias de facturación. Configuración de producción, diagnósticos sin filtrar, secretos y datos de abonados permanecen bajo control del cliente.

Acceso y archivos de la aplicación

El acceso combina autenticación, pertenencia a la organización, roles y políticas de base de datos y almacenamiento. El personal requiere verificación en dos pasos. La entrega privada verifica el acceso antes de emitir una URL firmada temporal.

Evidencias y continuidad

Las comprobaciones de la aplicación y garantías de proveedores son distintas de una auditoría organizativa independiente. Validar adjuntos no acredita DLP automático ni análisis antimalware. La producción del cliente es independiente del portal; el encargo documenta canales alternativos y notificación de incidentes.

El contrato documenta tratamiento permitido, retención y eliminación, incidentes, accesos y responsabilidades. El acuse de consultas web es distinto de los objetivos operativos contratados de respuesta y resolución.

Referencias de garantías de proveedores

Revise directamente con cada proveedor el producto cubierto, período, plan y acceso al informe.

[GitHub](#)

[Netlify](#)

[Supabase](#)

[Stripe](#)