KYNODE

Security Whitepaper

Versión: 2.1 · Abril 2026

Contacto: Disponible bajo solicitud

CLASIFICACIÓN: PÚBLICO — PARA STAKEHOLDERS

1. Resumen Ejecutivo

KYNODE opera una plataforma de gestión clínica y administrativa diseñada para entornos de conectividad limitada o nula. La arquitectura fue concebida desde su origen bajo el principio de **Security by Design**: la protección de datos de pacientes no es una capa añadida, sino el fundamento estructural del sistema.

KYNODE procesa la documentación clínica localmente y sincroniza a la nube únicamente indicadores epidemiológicos y operativos anonimizados. Este documento describe las medidas de seguridad implementadas sin revelar detalles propietarios de la arquitectura interna.

---

2. Modelo de Amenazas

KYNODE opera en entornos donde los vectores de ataque incluyen:

VECTOR	MITIGACIÓN
Interceptación de datos en tránsito	Cifrado asimétrico de extremo a extremo
Acceso físico no autorizado al dispositivo Edge	Los datos clínicos identificables permanecen en el equipo local
Suplantación de identidad de nodo	Autenticación por clave única + rotación periódica
Fuerza bruta en credenciales	Rate limiting + hashing adaptativo de contraseñas
Escalación de privilegios	Control de acceso basado en roles y módulos
Manipulación de registros clínicos	Hashes de integridad criptográfica por registro

---

3. Protección de Datos del Paciente

3.1 Principio de Data Minimization

La información que se transmite desde los puntos de atención hacia la nube es **exclusivamente epidemiológica y operativa**. Los datos de identificación personal (PHI) **nunca abandonan el dispositivo local**.

Datos que NUNCA se transmiten:

- Nombre del paciente
- Documento de identidad
- Historial médico narrativo
- Transcripciones de audio
- Notas médicas en texto libre
- `doctor_diagnosis`
- Dirección o localidad exacta
- Alergias y antecedentes

Datos transmitidos (anonimizados):

- Rango de edad
- Sexo
- Signos vitales numéricos
- Código CIE-10 validado
- Grupo EPI-11 validado
- País, estado y municipio
- Resultado operativo de la consulta
- Datos operativos de inventario y dispensación farmacéutica

3.2 Anonimización Irreversible

Cada paciente recibe un identificador aleatorio universal (UUID v4) que no tiene correlación matemática con su identidad real. La conversión de edad exacta a rangos demográficos (`0–5` , `6–17` , `18–35` , `36–60` , `60+`) reduce el riesgo de reidentificación estadística.

3.3 Validación Anti-Filtración

El sistema ejecuta una verificación automatizada en cada registro antes de la transmisión, confirmando que ningún campo de información protegida (PHI) se haya infiltrado en el payload de sincronización. La lista de PHI protegida incluye explícitamente `doctor_diagnosis` , `transcript` , `audio_path` , `name` , `identification` , `locality` , `medical_history` y `allergies` . Si se detecta una anomalía, **la transmisión se bloquea inmediatamente**.

---

4. Arquitectura de Sincronización

4.1 Arquitectura Híbrida Offline-First

KYNODE opera con dos rutas de sincronización:

- **Ruta A (preferida):** el nodo local procesa, almacena y sincroniza posteriormente al cloud.
- **Ruta B (fallback):** cuando el nodo no está disponible, el dispositivo autorizado de sincronización puede transmitir datos anonimizados directamente al cloud.

En ambas rutas, los datos clínicos identificables permanecen únicamente en el dispositivo local. Solo viajan indicadores epidemiológicos y operativos anonimizados.

4.2 Política de Transporte

- El payload de sincronización se valida contra esquema estricto antes de salir del nodo.
- Si el cifrado falla, la exportación se bloquea.
- No existe un fallback silencioso a texto plano en producción.

---

5. Cifrado

5.1 Cifrado en Tránsito

CAPA	PROTOCOLO
Red local (Edge ↔ dispositivos autorizados)	TLS 1.2+
Sincronización (Edge → Nube)	NaCl SealedBox
Plataforma Cloud	HTTPS / TLS 1.3

5.2 Cifrado del Payload de Sincronización

Los datos epidemiológicos que viajan desde el Edge hacia la nube están cifrados con **criptografía asimétrica de clave pública**. Solo el servidor central posee la clave privada de descifrado.

Política de cifrado obligatorio:

- El cifrado está activado por defecto.
- Si el proceso de cifrado falla, la exportación se bloquea completamente.
- No existe un fallback silencioso a texto plano en producción.

5.3 Cifrado en Reposo

- Las contraseñas de usuario se almacenan utilizando hashing adaptativo con salt único por usuario.
- La base de datos cloud está protegida por el cifrado nativo del proveedor de infraestructura.
- En Edge, la protección de datos en reposo depende de las capacidades del hardware desplegado; se aplican controles compensatorios cuando el hardware no soporta root of trust.

6. Autenticación y Control de Acceso

6.1 Autenticación de Usuarios

- Hashing adaptativo con factor de costo elevado.
- Protección anti-fuerza bruta mediante rate limiting y lockout persistente.
- Sesiones firmadas criptográficamente con expiración automática.

6.2 Autenticación de Nodos Edge

Cada nodo Edge recibe una clave API única:

- Se muestra una sola vez al administrador.
- Se almacena como hash criptográfico irreversible.
- Puede ser rotada en cualquier momento.
- Se valida en cada sincronización.

6.3 Control de Acceso Basado en Roles

ROL	PERMISOS
Administrador global	Gestión completa
Administrador	Gestión de su organización
Lectura	Acceso de solo lectura

La segregación multi-tenant impide acceso a datos de otra organización dentro del modelo de permisos implementado.

6.4 Sesiones de Soporte Remoto

KYNODE reserva las sesiones temporales de soporte remoto para laboratorio, staging o recuperación excepcional aprobada. En despliegues productivos no forman parte de la operación normal y permanecen deshabilitadas por defecto. El alcance técnico exacto de cualquier sesión SSH se trata como acceso privilegiado al nodo y no se usa para emitir claims de aislamiento de datos clínicos.

---

7. Integridad de Datos

7.1 Hashes de Integridad

Cada registro clínico generado en el dispositivo Edge incluye un **hash de integridad criptográfica** (HMAC-SHA256). Esto permite verificar que el registro no fue alterado durante el transporte o almacenamiento.

7.2 Deduplicación Determinística

El sistema utiliza hashes determinísticos para garantizar que un mismo registro no se ingeste múltiples veces, incluso cuando es transportado por diferentes vías de sincronización.

7.3 Validación de Esquemas

Cada registro recibido se valida contra un esquema estricto antes de ser almacenado. Registros con campos faltantes, tipos incorrectos o valores fuera de rango son rechazados automáticamente.

---

8. Seguridad de Red

8.1 Rate Limiting

CAPA	LÍMITE	VENTANA
Por dirección IP	10 solicitudes	60 segundos
Por organización	100 solicitudes	60 segundos
Por sesión de usuario	60 solicitudes	60 segundos
Por intento de login	5 intentos	60 segundos

8.2 CORS Estricto

Las políticas de Cross-Origin Resource Sharing están configuradas en modo **deny-by-default**. Solo los orígenes explícitamente autorizados pueden interactuar con las APIs del sistema.

8.3 Control de Payload

El tamaño máximo de cada solicitud de sincronización es de **5 MB**. Payloads que excedan este límite son rechazados antes de ser procesados.

---

9. Auditoría y Trazabilidad

9.1 Log de Auditoría

Las acciones administrativas críticas y los eventos explícitamente instrumentados se registran en un log de auditoría con los siguientes metadatos:

- Identidad del usuario
- Tipo de acción
- Marca temporal (UTC)
- Dirección IP de origen cuando aplica
- Detalles del recurso afectado

9.2 Acciones Auditadas

Creación y modificación de usuarios · Creación y suspensión de nodos · Rotación de claves API · Revocación de nodos · Ingestión de datos · Exportación de reportes · Intentos de acceso fallidos

---

10. Cumplimiento Normativo

KYNODE ha sido diseñado en alineación con los siguientes marcos regulatorios:

MARCO	APLICABILIDAD
GDPR (UE)	Data Minimization, Right to Erasure, Privacy by Design
Ley 1581 de 2012 (Colombia)	Protección de Datos Personales
Resolución 1995 de 1999 (Colombia)	Manejo de Historia Clínica
OWASP Top 10	Mitigación activa de vulnerabilidades web críticas

> **Nota:** Este documento refleja las medidas implementadas y operativas al momento de su publicación. KYNODE se posiciona como plataforma de gestión clínica y administrativa, no como sistema autónomo de diagnóstico o prescripción.

---

11. Gestión de Incidentes

11.1 Política de Respuesta

En caso de un incidente de seguridad confirmado:

1. **Contención inmediata**: Aislamiento del componente afectado

2. **Evaluación de impacto**: Determinación del alcance y datos potencialmente comprometidos
3. **Notificación**: Comunicación a las organizaciones afectadas según la normativa aplicable
4. **Remediación**: Corrección de la vulnerabilidad y actualización de controles
5. **Post-mortem**: Documentación del incidente y lecciones aprendidas

11.2 Contacto de Seguridad

Para reportar vulnerabilidades o incidentes de seguridad, contacte al equipo de KYNODE a través de los canales oficiales disponibles en **kynode.com**.

---

12. Actualizaciones y Mantenimiento

- Los dispositivos Edge soportan validación criptográfica de payloads.
- Las actualizaciones Cloud se despliegan mediante pipeline con verificación de tipos y tests automatizados.
- Las dependencias de seguridad se monitorean contra vulnerabilidades conocidas.

Este documento se actualiza periódicamente para reflejar mejoras en la postura de seguridad de KYNODE. La versión más reciente está disponible bajo solicitud.