



TOKA C.R. · PLATAFORMA CIUDADANA · COMODORO RIVADAVIA

Protocolo TOKA de Seguridad

Documento técnico e institucional que describe el funcionamiento, la arquitectura, el flujo de respuesta, la seguridad, la privacidad y las integraciones del Protocolo TOKA de Seguridad, con el estado real de implementación de cada componente.

Versión 1.0 · Agosto de 2026 · Documento público

Auditoría técnica realizada sobre el código fuente y la base de datos.

**TOKA NO REEMPLAZA A LOS SERVICIOS OFICIALES DE EMERGENCIA.
Es una herramienta tecnológica complementaria.**

ÍNDICE

Contenido del documento

1. Presentación y alcance institucional
2. Qué es el Protocolo TOKA de Seguridad
3. Antes de la alerta: preparación y consentimiento
4. Durante la activación: secuencia real
5. Durante el incidente: seguimiento y evidencias
6. Después de la alerta: cierre, expediente y trazabilidad
7. Arquitectura del Protocolo TOKA de Seguridad
8. Integración con WhatsApp Cloud API
9. Seguridad, privacidad y protección de datos
10. Estado actual y limitaciones
11. Conclusión institucional

Criterio de honestidad técnica

Cada capacidad descrita en este documento fue verificada contra el código fuente y el esquema de base de datos de TOKA. Se utilizan tres estados: IMPLEMENTADO (operativo y verificado), PARCIAL (desarrollado, con dependencias externas o configuración pendiente) y PENDIENTE (diseñado o proyectado, no operativo). No se describe como funcional ninguna capacidad que no lo sea.

Este documento no contiene credenciales, claves de acceso, tokens, contraseñas, direcciones internas ni datos personales de usuarios. Sólo se nombran los tipos de credenciales que requiere cada integración.

SECCIÓN 1

Presentación y alcance institucional

TOKA C.R. es una plataforma ciudadana desarrollada en Comodoro Rivadavia, provincia del Chubut. Dentro de esa plataforma, el Protocolo TOKA de Seguridad es un sistema que permite a una persona activar, desde su teléfono y con un único gesto, una alerta personal que registra el incidente, obtiene su ubicación, captura evidencia y comunica la situación a los contactos de confianza que esa misma persona configuró previamente.

Alcance y límite del servicio

El Protocolo TOKA no reemplaza a los servicios oficiales de emergencia. No sustituye al 911, a la policía, a los bomberos, al sistema de salud ni a ningún organismo público de respuesta. No garantiza intervención de fuerzas de seguridad ni tiempos de respuesta.

El Protocolo TOKA es una herramienta tecnológica complementaria orientada a facilitar la activación de una alerta, la comunicación, la localización, el seguimiento y la coordinación con los contactos definidos por la propia persona usuaria, según las capacidades efectivamente implementadas que se detallan en este documento.

Destinatarios del documento

Este documento está redactado para ser leído por la Secretaría de Seguridad, organismos públicos, municipios, instituciones educativas y sociales, potenciales aliados tecnológicos e inversores. Describe la arquitectura real del sistema y su estado de implementación, sin proyecciones comerciales ni funcionalidades hipotéticas.

SECCIÓN 2

Qué es el Protocolo TOKA de Seguridad

El Protocolo es un ciclo completo y continuo que se ejecuta aunque el equipo pierda conexión. Su secuencia operativa es la siguiente:



Principios de diseño verificados en el código

- Continuidad ante fallas: si no hay servidor, red o GPS, el protocolo no se detiene; la información queda en una cola local del dispositivo y se sincroniza al recuperar conexión.
- Integridad de la evidencia: cada archivo capturado se sella con una huella SHA-256 calculada en el dispositivo, antes de ser transmitido.
- Consentimiento explícito: ubicación, cámara, micrófono, evidencias, comunicaciones, seguimiento, almacenamiento, transmisión y datos de salud se habilitan por categorías independientes.
- Aislamiento por persona: toda la información del incidente pertenece exclusivamente a quien lo generó, con reglas de acceso aplicadas en la propia base de datos.
- Modo prueba: el sistema permite recorrer el circuito completo marcándolo como ensayo, sin que sea tratado como una emergencia real.

SECCIÓN 3 · ANTES DE LA ALERTA

Preparación y consentimiento

Antes de que exista una alerta, la persona usuaria configura su protocolo desde su cuenta. Nada de esto ocurre de forma automática ni silenciosa.

Configuración personal

- Contactos de confianza: lista propia de personas a avisar, con validación de formato internacional de teléfono en el momento de guardarlos.
- Método de activación: se define cómo se dispara el protocolo.
- Capacidades habilitadas: cámara, video, audio y ubicación se activan o desactivan por separado.
- Canales de aviso: se seleccionan los canales por los que se intentará comunicar la alerta.

Consentimiento granular

El sistema almacena un registro de consentimiento con nueve categorías independientes: ubicación, cámara, micrófono, evidencias, comunicaciones, seguimiento, almacenamiento, transmisión y salud. Sin consentimiento, la capacidad correspondiente no se ejecuta.

Permisos del dispositivo

Los permisos de ubicación, cámara y micrófono los otorga el sistema operativo del teléfono, no TOKA. Si la persona los deniega, el protocolo continúa con el resto de las capacidades y deja constancia del estado del sensor, por ejemplo GPS sin permiso o sin señal.

Condiciones necesarias para activar

Se requiere sesión iniciada en TOKA y una configuración de protocolo guardada. El sistema impide activaciones duplicadas: si ya hay un incidente en curso, se reutiliza el mismo.

Componente	Estado	Detalle verificado
Configuración del protocolo	IMPLEMENTADO	Tabla propia por persona usuaria, con acceso restringido a su titular.
Contactos de confianza	IMPLEMENTADO	Alta, edición y validación de formato internacional del número.
Consentimiento por categorías	IMPLEMENTADO	Nueve categorías registradas y consultadas antes de operar.
Permisos de sensores	IMPLEMENTADO	Solicitud al sistema operativo y registro del estado resultante.

SECCIÓN 4 · DURANTE LA ACTIVACIÓN

Secuencia real de activación

Existen dos formas de disparo verificadas en el código:

- Pulsación sostenida de 5 segundos sobre el identificador de TOKA en pantalla, con indicador de progreso y vibración al completarse.
- Botón de volumen hacia abajo sostenido 5 segundos, únicamente con la aplicación en primer plano y en los dispositivos que lo permiten.

Al cumplirse el umbral, la aplicación abre el Protocolo con orden de activación inmediata: no hay pantallas de confirmación intermedias.

Secuencia ejecutada

1. Validación: se verifica que no exista otro incidente activo y se bloquea la doble activación.
2. Creación del incidente: se genera un identificador único y se registra el alta con origen, nota, nivel de batería, estado de conectividad, método de activación y modo, real o de prueba. Si el servidor no responde, el incidente queda registrado en el equipo y se sincroniza después.
3. Obtención de contexto: se toma nivel de batería, tipo y calidad de conexión y condiciones meteorológicas del punto del incidente.
4. Ubicación: comienza el seguimiento continuo por GPS y se conserva localmente la última ubicación conocida, incluso si luego se pierde la señal.
5. Evidencia: según lo consentido: grabación de video, segmentos de audio y fotografías periódicas, cada archivo sellado con huella SHA-256.
6. Comunicación: se ejecuta una secuencia guiada de aviso a los contactos de confianza y, en paralelo, un aviso interno dentro de TOKA.
7. Despacho ampliado: transcurrido un minuto de recolección de evidencia se produce el envío consolidado del incidente con su expediente asociado.

Qué se genera, almacena y transmite

Se genera y almacena: registro del incidente, puntos de recorrido con precisión, altitud, velocidad y rumbo, señales periódicas de estado, archivos de evidencia con su huella digital y eventos de la línea de tiempo del incidente. Los archivos se guardan en un depósito privado, organizados por persona e incidente.

Se transmite: un mensaje de alerta con identificación de la persona, momento del hecho, enlace de ubicación y enlace al expediente, dirigido exclusivamente a los contactos de confianza cargados por la propia persona usuaria y a los avisos internos de la plataforma.

SECCIÓN 4 (continuación)

Canales de comunicación

Componente	Estado	Detalle verificado
WhatsApp Cloud API (servidor)	PARCIAL	Integración completa desarrollada, con envío por plantilla oficial y respaldo en texto libre. Requiere credenciales de Meta aún no cargadas. Ver sección 8.
WhatsApp por enlace nativo	IMPLEMENTADO	Respaldo operativo: abre la conversación con el mensaje precargado y la persona confirma el envío.
Aviso interno en TOKA	IMPLEMENTADO	Operativo. Notifica a los contactos que también son usuarios de TOKA y publica el aviso en el canal interno del incidente.
Correo electrónico	PARCIAL	Adaptador desarrollado y compatible con varios proveedores. Requiere alta del proveedor y del remitente institucional.
SMS	PENDIENTE	No existe envío automático. Sólo se abre el redactor de mensajes del teléfono, que la persona debe enviar.
Llamada telefónica	PENDIENTE	No existe llamada automatizada. Sólo se abre el marcador del teléfono.

Qué ocurre si un canal no está disponible

El sistema consulta las capacidades reales de cada canal antes de intentar el envío. Si el envío por servidor no está disponible, la interfaz lo informa con claridad y ofrece de inmediato la alternativa nativa del teléfono: conversación de WhatsApp, redactor de SMS o marcador. En ningún caso se muestra un aviso como enviado si no lo fue.

Qué ocurre sin conexión

El protocolo continúa. Ubicación, señales de estado, evidencias y el propio incidente quedan en una cola local del dispositivo y se envían automáticamente al recuperar la red, con reintentos periódicos y reintento inmediato cuando el equipo vuelve a estar en línea.

SECCIÓN 5 · DURANTE EL INCIDENTE

Seguimiento, evidencias y sincronización

Componente	Estado	Detalle verificado
Seguimiento de ubicación	IMPLEMENTADO	Recorrido continuo por GPS durante un mínimo de 15 minutos, con precisión, altitud, velocidad, rumbo, batería y estado del sensor en cada punto.
Última ubicación conocida	IMPLEMENTADO	Se conserva en el propio equipo, de modo que subsiste aunque se pierda la señal o se cierre la aplicación.
Señal periódica de estado	IMPLEMENTADO	Cada 60 segundos se registra batería, conectividad y última posición, aun sin movimiento.
Captura de evidencia	IMPLEMENTADO	Video inicial, segmentos de audio y fotografías periódicas, según el consentimiento otorgado.
Integridad de archivos	IMPLEMENTADO	Huella SHA-256 calculada en el dispositivo y conservada junto al archivo y en el expediente.
Almacenamiento privado	IMPLEMENTADO	Depósito no público, con rutas separadas por persona e incidente y enlaces temporales firmados.
Funcionamiento sin conexión	IMPLEMENTADO	Cola local en el dispositivo con reintentos automáticos; nada se descarta ante un fallo de red.
Reintentos de aviso	PARCIAL	La lógica de reintentos escalonados y el punto de entrada automático están desarrollados; la frecuencia programada de ejecución debe verificarse en el entorno de operación.
Estado del incidente	IMPLEMENTADO	Panel en vivo con puntos registrados, evidencias tomadas, elementos pendientes de envío, batería, red y estado del GPS.
Cancelación o finalización	IMPLEMENTADO	La persona puede cerrar el protocolo en cualquier momento; se detienen las capturas y se fuerza una sincronización final.

SECCIÓN 6 · DESPUÉS DE LA ALERTA

Cierre, expediente y trazabilidad

Al finalizar, el incidente se cierra registrando fecha y hora de cierre, última posición conocida con su precisión, batería, estado de conectividad y condiciones meteorológicas. Se detienen todos los temporizadores, observadores de ubicación y capturas activas.

Expediente compartible

El sistema genera un expediente consolidado del incidente, accesible mediante un enlace con identificador único. Ese identificador se emite con 256 bits de aleatoriedad y no se guarda en la base de datos: sólo se conserva su huella criptográfica, de modo que ni siquiera desde el sistema puede reconstruirse el enlace. El expediente caduca a las 72 horas, puede revocarse y los archivos se sirven mediante enlaces firmados de una hora de duración.

Qué permanece almacenado

- Registro del incidente con su estado final y sus datos de contexto.
- Recorrido completo de ubicación asociado al incidente.
- Archivos de evidencia con su huella de integridad, tamaño, orden y coordenadas de captura.
- Historial de envíos por canal, con sus estados e intentos.
- Eventos de la línea de tiempo del incidente.
- Acuses de entrega recibidos desde el proveedor de mensajería, con verificación de firma.

Acceso posterior

El acceso a toda esa información queda restringido a su titular por reglas aplicadas en la propia base de datos. El expediente público sólo es accesible por quien posea el enlace, dentro de su período de validez y mientras no haya sido revocado.

Componente	Estado	Detalle verificado
Cierre del incidente	IMPLEMENTADO	Estado final, última posición, contexto y sincronización forzada.
Conservación histórica	IMPLEMENTADO	Incidente, recorrido, evidencias, envíos y eventos quedan registrados.
Expediente por enlace	IMPLEMENTADO	Identificador conocido sólo por quien lo recibe, huella almacenada, vencimiento a 72 horas y revocación.
Auditoría de mensajería	IMPLEMENTADO	Cada acuse recibido se valida por firma y se archiva sin duplicados.
Auditoría de configuración y consentimiento	PARCIAL	Se guarda el estado vigente, pero no un historial de cambios.
Registro de visitas al expediente	PENDIENTE	No se registra quién consultó el enlace ni cuándo.
Política automática de retención y borrado	PENDIENTE	No existe purga programada; la información se conserva hasta su eliminación manual.

SECCIÓN 7

Arquitectura del Protocolo TOKA de Seguridad



Componentes que participan realmente

Componente	Estado	Detalle verificado
Aplicación TOKA (PWA)	IMPLEMENTADO	Aplicación web instalable en el teléfono; contiene el disparo, la captura y la cola local.
Interfaz del protocolo	IMPLEMENTADO	Pantalla dedicada con configuración, activación, panel en vivo y cierre.
Motor del protocolo	IMPLEMENTADO	Orquesta captura, ubicación, señales de estado, cola y cierre en el dispositivo.
Cola local de resiliencia	IMPLEMENTADO	Base de datos del navegador que retiene todo lo pendiente y lo reenvía.
Servidor de TOKA	IMPLEMENTADO	Funciones de servidor que consolidan el incidente y ejecutan el despacho de avisos.
Base de datos	IMPLEMENTADO	Trece tablas del protocolo con reglas de acceso por titular activadas.
Autenticación	IMPLEMENTADO	Sesión verificada; la identidad se resuelve en el servidor, no en el teléfono.
Almacenamiento de evidencias	IMPLEMENTADO	Depósito privado con enlaces firmados de vigencia limitada.
Ubicación	IMPLEMENTADO	Servicio de geolocalización del dispositivo, con estado del sensor registrado.
Notificaciones internas	IMPLEMENTADO	Avisos push a los contactos que son usuarios de TOKA.
WhatsApp Cloud API	PARCIAL	Integración desarrollada; PENDIENTE DE CONFIGURACIÓN de credenciales de Meta.
Webhook de estado de mensajes	IMPLEMENTADO	Punto de entrada público verificado y con validación de firma en cada evento.
Correo electrónico	PARCIAL	Adaptador multiproveedor listo; PENDIENTE DE CONFIGURACIÓN del proveedor y del remitente.
SMS y llamadas automatizadas	PENDIENTE	Sin proveedor integrado; sólo funciones nativas del teléfono.
Sistema de evidencias y expediente	IMPLEMENTADO	Consolidación, huellas de integridad y enlace temporal de consulta.
Controles de acceso (RLS)	IMPLEMENTADO	Reglas por titular activas en todas las tablas del protocolo; sin acceso anónimo.
Auditoría	PARCIAL	Completa para mensajería y eventos del incidente; sin historial de configuración ni de consultas.
Integración con organismos oficiales	PENDIENTE	No existe conexión con el 911 ni con sistemas públicos de despacho.

SECCIÓN 8

Integración con WhatsApp Cloud API

TOKA integra la API oficial de WhatsApp provista por Meta. La integración se resuelve íntegramente del lado del servidor: el teléfono nunca manipula credenciales.

Qué está implementado en TOKA

- Envío mediante plantilla oficial aprobada, con los datos del incidente como parámetros.
- Respaldo automático a mensaje de texto libre cuando la plantilla no está disponible o la conversación se encuentra abierta.
- Traducción de los errores devueltos por Meta a mensajes comprensibles para la persona usuaria.
- Webhook oficial publicado y operativo: responde la verificación de Meta y valida la firma criptográfica de cada notificación entrante.
- Archivo de cada acuse de entrega con control de duplicados.
- Reintentos escalonados ante fallos de envío.

Qué depende de Meta

- Aprobación de la cuenta de WhatsApp Business y verificación del negocio.
- Aprobación de la plantilla de mensaje de alerta de seguridad.
- Habilitación del número emisor y de sus límites de envío.

Credenciales necesarias (tipos, sin valores)

Credencial requerida	Estado actual
Token de acceso de la aplicación de Meta	PENDIENTE DE CONFIGURACIÓN
Identificador del número de teléfono emisor	PENDIENTE DE CONFIGURACIÓN
Identificador de la cuenta de WhatsApp Business	PENDIENTE DE CONFIGURACIÓN
Nombre e idioma de la plantilla de alerta	PENDIENTE DE CONFIGURACIÓN
Secreto de la aplicación (validación de firma)	CONFIGURADO
Identificador de verificación del webhook	CONFIGURADO
Dirección pública del webhook	PUBLICADA Y OPERATIVA

Efecto práctico hoy

Mientras el token de acceso y el identificador del número emisor no estén cargados, el envío automático de WhatsApp desde el servidor no se ejecuta y el sistema lo informa como no disponible. La alerta sigue funcionando por aviso interno de TOKA y por la apertura asistida de WhatsApp, SMS o llamada en el propio teléfono. Cargadas esas credenciales y aprobada la plantilla, el envío automático queda operativo sin cambios de arquitectura.

SECCIÓN 9

Seguridad, privacidad y protección de datos

Consentimiento

El protocolo opera sobre consentimiento expreso y granular. Cada categoría —ubicación, cámara, micrófono, evidencias, comunicaciones, seguimiento, almacenamiento, transmisión y salud— se habilita de forma independiente y puede desactivarse. La activación es siempre un acto deliberado de la persona.

Minimización de datos

Sólo se recolecta información asociada a un incidente activo. Fuera de una activación, el sistema no consulta sensores, no toma ubicación y no realiza comunicaciones. El mensaje enviado a los contactos contiene lo estrictamente necesario para asistir: identificación, momento, ubicación y acceso al expediente.

Controles de acceso y RLS

Todas las tablas del protocolo tienen activadas reglas de seguridad a nivel de fila: la información de un incidente sólo es legible y modificable por su titular. Los usuarios anónimos no tienen acceso a ninguna tabla del protocolo. El canal interno del incidente admite además la visibilidad del equipo de moderación asignado, y el registro de auditoría de mensajería queda reservado al personal habilitado.

Protección de evidencias

Los archivos se guardan en un depósito privado, nunca en una dirección pública permanente. Cada archivo lleva una huella SHA-256 calculada en el dispositivo de origen, lo que permite demostrar que no fue alterado posteriormente. El acceso se realiza mediante enlaces firmados de vigencia breve.

Protección de la ubicación

El recorrido se asocia al incidente y hereda sus reglas de acceso. La última ubicación conocida se conserva en el propio dispositivo para resistir la pérdida de señal y no se expone a terceros.

Trazabilidad y auditoría

El sistema conserva la línea de tiempo del incidente, el historial de envíos por canal con sus intentos y los acuses de entrega verificados por firma criptográfica. Los eventos entrantes se archivan sin duplicados.

Separación de datos y secretos

Las credenciales de integraciones externas residen exclusivamente en el entorno del servidor. La aplicación instalada en el teléfono no las contiene ni puede leerlas. Los identificadores de acceso al expediente se almacenan únicamente como huella criptográfica.

Principios rectores

Consentimiento previo, finalidad determinada, minimización, integridad verificable, acceso restringido al titular, transparencia sobre el estado real del sistema y no sustitución de los servicios públicos de emergencia.

SECCIÓN 10

Estado actual y limitaciones

IMPLEMENTADO

- Configuración personal del protocolo, contactos de confianza con validación de formato y consentimiento por nueve categorías.
- Activación por pulsación sostenida de 5 segundos y por volumen hacia abajo con la aplicación en primer plano, con bloqueo de activaciones duplicadas.
- Creación y registro del incidente con identificador único, contexto de batería, conectividad, método de activación y modo real o de prueba.
- Seguimiento de ubicación por un mínimo de 15 minutos, última ubicación conocida persistente y señal de estado cada 60 segundos.
- Captura de video, audio y fotografías con huella SHA-256 y almacenamiento privado.
- Funcionamiento sin conexión con cola local y reintentos automáticos.
- Expediente consolidado accesible por enlace único, con vencimiento a 72 horas y posibilidad de revocación.
- Aviso interno en TOKA mediante notificaciones push, operativo.
- Webhook oficial de estado de mensajes publicado, verificado y con validación de firma.
- Reglas de acceso por titular activas en las trece tablas del protocolo.
- Cierre seguro del incidente con sincronización final.

PARCIALMENTE IMPLEMENTADO

- WhatsApp Cloud API: integración completa desarrollada; falta la carga de credenciales de Meta y la aprobación de la plantilla de alerta.
- Correo electrónico: adaptador multiproveedor desarrollado; falta el alta del proveedor y del remitente institucional.
- Reintentos automáticos de aviso: lógica y punto de entrada desarrollados; la periodicidad programada debe verificarse en el entorno de operación.
- Auditoría: completa para mensajería y eventos del incidente; sin historial de cambios de configuración ni de consentimiento.

PENDIENTE

- SMS automático: no existe proveedor integrado; sólo se abre el redactor del teléfono, que la persona debe enviar.
- Llamada telefónica automatizada: no existe; sólo se abre el marcador.
- Activación con la pantalla apagada o la aplicación cerrada: no es posible en una aplicación web instalable; requiere un módulo nativo de Android.
- Integración con organismos oficiales de emergencia: no existe conexión con el 911 ni con sistemas públicos de despacho.
- Registro de consultas al expediente: no se audita quién accede al enlace.
- Política automática de retención y eliminación de datos: no está programada.

SECCIÓN 11

Auditoría de seguridad de la plataforma

Con fecha 26 de agosto de 2026 se ejecutó una revisión automatizada de seguridad sobre la base de datos y las reglas de acceso de la plataforma. El resultado no arrojó hallazgos críticos. Se registraron seis observaciones de nivel advertencia, ninguna de ellas referida a las tablas del Protocolo TOKA de Seguridad ni a la exposición de credenciales.

Resultado general

- Hallazgos críticos: ninguno.
- Hallazgos de nivel advertencia: seis, con plan de tratamiento definido.
- Datos del protocolo (incidentes, ubicaciones, evidencias, expedientes): sin observaciones.
- Credenciales y secretos: no se detectó exposición; permanecen en el entorno del servidor.

Observaciones y tratamiento

Componente	Estado	Detalle verificado
Contacto en perfiles	EN REVISIÓN	Los teléfonos y WhatsApp del perfil sólo se entregan mediante funciones controladas. Se verifica periódicamente que el acceso directo a esas columnas continúe revocado.
Funciones con privilegio	CONTROLADO	Se revocó la ejecución anónima de las funciones que no la requieren. Las que permanecen abiertas sólo sostienen lecturas públicas ya previstas.
Solicitudes de artista	PLANIFICADO	El correo de contacto se resguarda; se prevé reemplazar la validación de pertenencia por una columna de titularidad vinculada a la cuenta.
Métricas de contratación	PLANIFICADO	El alta de registros de métricas se restringirá a personas identificadas para evitar el ingreso de datos falsos en las estadísticas comerciales.
Registro de visitas	PLANIFICADO	Se agregará una comprobación para impedir que un registro de visita se atribuya a una cuenta distinta de la propia.

Alcance de esta sección

El detalle técnico de cada observación, los nombres internos de tablas y funciones y cualquier credencial quedan fuera de este documento público y se conservan en el registro interno de seguridad de la plataforma.

SECCIÓN 12

Conclusión institucional

El Protocolo TOKA de Seguridad es un sistema real y operativo en su núcleo: registra el incidente, sigue la ubicación, captura evidencia con integridad verificable, resiste la falta de conexión, consolida un expediente y protege la información con reglas de acceso aplicadas en la base de datos.

Sus limitaciones están claramente delimitadas y son, en su mayoría, de configuración y no de arquitectura: el envío automático por WhatsApp y por correo electrónico está desarrollado y queda operativo al completar el alta de credenciales y plantillas ante los proveedores. El SMS y la llamada automatizada requieren la incorporación de un proveedor, y la activación con la pantalla apagada exige un desarrollo nativo adicional.

TOKA declara de manera expresa que este protocolo no reemplaza a los servicios oficiales de emergencia y se presenta como una herramienta tecnológica complementaria, orientada a facilitar la activación de una alerta, la comunicación, la localización, el seguimiento y la coordinación con los contactos definidos por la propia persona usuaria.

Posibilidad de articulación institucional

La arquitectura permite incorporar destinatarios institucionales, canales adicionales y procedimientos de derivación acordados con organismos públicos. Cualquier articulación de ese tipo requiere convenio previo, definición de responsabilidades y protocolos operativos conjuntos, y no se encuentra implementada al día de la fecha.

Documento público · Versión 1.1 · Agosto de 2026 · TOKA C.R., Comodoro Rivadavia, Chubut, Argentina. Elaborado sobre auditoría del código fuente y del esquema de base de datos. No contiene credenciales, secretos ni datos personales.